aws

아마존 GuardDuty 사용 설명서

아마존 GuardDuty

아마존 GuardDuty: 아마존 GuardDuty 사용 설명서

Table of Contents

아마존이란 GuardDuty 무엇입니까?

GuardDuty Amazon은 AWS 환경을 지속적으로 모니터링하여 잠재적인 보안 위험을 찾아내는 위협 탐지 서비스입니다. GuardDuty AWS CloudTrail 관리 이벤트기본 데이터 소스, AWS CloudTrail 이벤트 로그, VPC 흐름 로그 (Amazon EC2 인스턴스), DNS 로그 등을 분석하고 처리합니다. GuardDuty 다른 AWS 서비스의 모니터링 로그 및 이벤트도 제공합니다. 이러한 소스에는 EKS 감사 로그, RDS 로그인 활동, S3 로그, EBS 볼륨, 런타임 모니터링 및 Lambda 네트워크 활동 로그가 포함됩니다. GuardDuty이러한 로그 및 이벤트 소스를 기능이라는 용어로 통합합니다.

GuardDuty 악성 IP 주소 및 도메인 목록, 기계 학습 (ML) 모델 등의 위협 인텔리전스 피드를 사용하여 환경 내에서 예상치 못한 무단 악의적인 활동을 식별합니다 AWS . 여기에는 권한 상승, 노출된 자격 증명의 사용, 악성 IP 주소, 도메인과의 통신, Amazon EC2 인스턴스 및 컨테이너 워크로드에서의 멀웨어 존재, 데이터베이스에서 비정상적인 패턴의 로그인 이벤트 발견 등과 같은 문제가 포함됩니다.

예를 들어, 잠재적으로 손상된 EC2 인스턴스 및 멀웨어를 제공하거나 비트코인을 채굴하는 컨테이너 워크로드를 GuardDuty 탐지할 수 있습니다. 또한 AWS 계정 액세스 행동을 모니터링하여 무단 인프라 배포 (지역에 배포된 적이 없는 인스턴스), 비정상적인 API 호출, 암호 강도를 낮추기 위해 암호 정책을 변경한 경우 등 잠재적 침해의 징후가 있는지 확인합니다.

활성화하면 GuardDuty 환경의 보안 상태를 파악할 수 있습니다. AWS 잠재적인 보안 위험을 식별하면 결과를 생성하고 추가 세부 정보를 제공합니다. 검색 결과 GuardDuty 생성 시 알림을 EventBridge 받도록 Amazon을 설정할 수도 있습니다. GuardDuty 또한 사용자 환경의 대표적인 보안 문제를 해결하기 위한 단계를 권장합니다.

생성된 결과를 Amazon Simple Storage 서비스 (Amazon S3) 버킷으로 내보낼 수 있습니다. GuardDuty 또한 AWS Security Hub Amazon Detective와 같은 다른 AWS 보안 관련 서비스와도 통합되므로 사용자 환경의 보안 동향을 분석하고 조사하는 데 도움이 됩니다.

사용 GuardDuty

다음과 같은 GuardDuty 방법으로 사용할 수 있습니다.

GuardDuty 콘솔

> https://console.aws.amazon.com/guardduty
>
> 콘솔은 액세스 및 사용을 위한 브라우저 기반 인터페이스입니다. GuardDuty GuardDuty 콘솔은 GuardDuty 계정, 데이터, 리소스에 대한 액세스를 제공합니다.

AWS 명령줄 도구

AWS 명령줄 도구를 사용하면 시스템 명령줄에서 명령을 실행하여 GuardDuty 작업과 AWS 작업을 수행할 수 있습니다. 작업을 수행하는 스크립트를 작성하는 경우 명령줄 도구가 유용합니다.

설치 및 사용에 대한 자세한 내용은 사용 AWS CLIAWS Command Line Interface 설명서를 참조하십시오. 사용 가능한 AWS CLI 명령을 보려면 CLI 명령 참조를 참조하십시오. GuardDuty

GuardDuty HTTPS API

서비스에 직접 HTTPS 요청을 발행할 수 있는 GuardDuty HTTPS API를 사용하여 AWS 프로그래밍 방식으로 액세스할 GuardDuty 수 있습니다. 자세한 내용은 API 참조를 참조하십시오. GuardDuty

AWS SDK

AWS 다양한 프로그래밍 언어 및 플랫폼 (Java, Python, Ruby, .NET, iOS, Android 등) 의 라이브러리와 샘플 코드로 구성된 소프트웨어 개발 키트 (SDK) 를 제공합니다. SDK는 프로그래밍 방식으로 액세스할 수 있는 편리한 방법을 제공합니다. GuardDuty 다운로드 및 설치 방법을 비롯하여 AWS SDK에 대한 자세한 내용은 Amazon Web Services용 도구 페이지를 참조하세요.

GuardDuty 요금

처음 사용하는 GuardDuty 경우 지역별 AWS 계정별로 30일 무료 평가판이 제공됩니다. AWS 자세한 내용은 요금을 참조하십시오.

지원되는 지역 AWS

활성화할 수 있는 AWS 지역에 대한 자세한 내용은 GuardDuty 을 참조하십시오리전 및 엔드포인트.

시작하기 GuardDuty

이 자습서에서는 에 대한 실무 소개를 제공합니다. GuardDuty 독립 실행형 계정 또는 GuardDuty GuardDuty 관리자로 활성화하기 위한 최소 요구 사항은 AWS Organizations 1단계에서 다룹니다. 2~5단계에서는 결과를 최대한 GuardDuty 활용하기 위해 에서 권장하는 추가 기능을 사용하는 방법을 다룹니다.

주제

시작하기 전 준비 사항

GuardDuty AWS CloudTrail 이벤트 로그, AWS CloudTrail 관리 이벤트, Amazon VPC 흐름 로그, DNS 로그 기본 데이터 소스 등을 모니터링하는 위협 탐지 서비스입니다. GuardDuty 또한 보호 유형과 관련된 기능을 별도로 활성화한 경우에만 해당 보호 유형과 관련된 기능을 분석합니다. 기능으로는 Kubernetes 감사 로그, RDS 로그인 활동, S3 로그, EBS 볼륨, 런타임 모니터링 및 Lambda 네트워크 활동 로그가 있습니다. 이러한 데이터 소스 및 기능 (활성화된 경우) 을 사용하면 계정에 대한 보안 탐지 결과가 GuardDuty 생성됩니다.

GuardDuty활성화하면 환경 모니터링이 시작됩니다. 언제든지 모든 지역의 모든 계정을 GuardDuty 비활성화할 수 있습니다. 이렇게 하면 기본 데이터 소스와 GuardDuty 별도로 활성화된 모든 기능을 처리할 수 없게 됩니다.

기본 데이터 소스의 명시적 활성화는 필요하지 않습니다. Amazon은 이러한 서비스에서 직접 독립적인 데이터 스트림을 GuardDuty 가져옵니다. 새 GuardDuty 계정의 경우, 에서 지원되는 사용 가능한 모든 보호 유형이 기본적으로 AWS 리전 활성화되고 30일 무료 평가 기간에 포함됩니다. 일부 또는 전부를 옵트아웃할 수 있습니다. 기존 GuardDuty 고객인 경우, 사용 가능한 보호 플랜 중 일부 또는 전체를 사용하도록 선택할 수 있습니다. AWS 리전자세한 내용은 의 각 보호 유형과 관련된 기능을 참조하십시오 GuardDuty.

GuardDuty활성화할 때는 다음 항목을 고려하십시오.

- GuardDuty 지역 서비스이므로 이 페이지에서 따르는 모든 구성 절차를 모니터링하려는 각 지역에서 반복해야 GuardDuty 합니다.

  지원되는 모든 GuardDuty AWS 지역에서 활성화하는 것이 좋습니다. 이렇게 하면 GuardDuty 활발히 사용하지 않는 지역에서도 무단 또는 비정상적 활동에 대한 결과를 얻을 수 있습니다. 또한 GuardDuty 이를 통해 IAM과 같은 글로벌 AWS 서비스의 AWS CloudTrail 이벤트를 모니터링할 수 있습니다. 지원되는 모든 지역에서 GuardDuty 활성화되지 않은 경우 글로벌 서비스와 관련된 활동을 탐지하는 기능이 저하됩니다. 사용 가능한 지역의 GuardDuty 전체 목록은 을 참조하십시오리전 및 엔드포인트.

- AWS 계정에서 관리자 권한이 있는 모든 사용자가 GuardDuty 활성화할 수 있지만 최소 권한이라는 보안 모범 사례에 따라 특별히 관리할 GuardDuty IAM 역할, 사용자 또는 그룹을 생성하는 것이 좋습니다. GuardDuty 활성화에 필요한 권한에 대한 자세한 내용은 을 참조하십시오. GuardDuty를 활성화하는 데 필요한 권한

- 어느 곳에서든 GuardDuty AWS 리전처음으로 활성화하면 기본적으로 멀웨어 보호를 포함하여 해당 지역에서 지원되는 사용 가능한 모든 보호 유형도 활성화됩니다. GuardDuty 라는 계정에 대한 서비스 연결 역할을 생성합니다. `AWSServiceRoleForAmazonGuardDuty` 이 역할에는 에서 직접 이벤트를 소비 및 GuardDuty 분석하여 보안 결과를 생성할 수 있는 권한 및 신뢰 정책이 포함됩니다. 기본 데이터 소스 맬웨어 보호는 계정에 대해 `AWSServiceRoleForAmazonGuardDutyMalwareProtection`이라는 또 다른 서비스 연결 역할을 생성합니다. 이 역할에는 Malware Protection이 에이전트 없는 검사를 수행하여 계정에서 멀웨어를 탐지할 수 있도록 하는 권한 및 신뢰 정책이 포함됩니다. GuardDuty GuardDuty 이를 통해 계정에서 EBS 볼륨 스냅샷을 생성하고 해당 스냅샷을 서비스 계정과 공유할 수 있습니다. GuardDuty 자세한 정보는 에 대한 서비스 연결 역할 권한 GuardDuty을 참조하세요. 서비스 연결 역할에 대한 자세한 내용은 서비스 연결 역할 사용을 참조하세요.

- 어느 지역에서든 GuardDuty 처음으로 활성화하면 AWS 계정이 해당 지역의 30일 GuardDuty 무료 평가판에 자동으로 등록됩니다.

1단계: 아마존 활성화 GuardDuty

사용의 GuardDuty 첫 번째 단계는 계정에서 활성화하는 것입니다. GuardDuty활성화되면 즉시 현재 지역의 보안 위협을 모니터링하기 시작합니다.

관리자로서 조직 내 다른 계정의 GuardDuty 검색 결과를 GuardDuty 관리자로 관리하려면 구성원 계정을 추가하고 해당 계정에 GuardDuty 대해서도 활성화해야 합니다. 옵션을 선택하여 해당 환경에서 GuardDuty 활성화하는 방법을 알아보십시오.

Standalone account environment

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 시작하기를 선택합니다.
3. 활성화를 선택합니다 GuardDuty.

Multi-account environment

> **Important**
>
> 이 프로세스의 사전 요구 사항으로, 관리하려는 모든 계정과 동일한 조직에 속해야 하며, 조직 GuardDuty 내 관리자를 위임하려면 AWS Organizations 관리 계정에 대한 액세스 권한이 있어야 합니다. 관리자를 위임하려면 추가 권한이 필요할 수 있습니다. 자세한 내용은 위임된 GuardDuty 관리자 계정을 지정하는 데 필요한 권한 섹션을 참조하세요.

위임된 관리자 계정을 지정하려면 GuardDuty

1. 관리 계정을 사용하여 https://console.aws.amazon.com/organizations/ 에서 AWS Organizations 콘솔을 엽니다.
2. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   계정에서 GuardDuty 이미 활성화되었나요?

   - 이 (GuardDuty 가) 아직 활성화되지 않은 경우 시작하기를 선택한 다음 시작 페이지에서 GuardDuty 위임된 관리자를 지정할 수 있습니다. GuardDuty
   - GuardDuty 가 활성화된 경우 설정 페이지에서 GuardDuty 위임된 관리자를 지정할 수 있습니다.
3. 조직의 위임 관리자로 지정하려는 계정의 12자리 AWS 계정 ID를 입력하고 GuardDuty 위임을 선택합니다.

   > **Note**
   >
   > 이 (GuardDuty 가) 아직 활성화되지 않은 경우 위임된 관리자를 지정하면 현재 지역에서 해당 계정을 GuardDuty 사용할 수 있습니다.

멤버 계정 추가

이 절차에서는 를 통해 GuardDuty 위임된 관리자 계정에 구성원 계정을 추가하는 방법을 설명합니다. AWS Organizations초대를 통해 멤버를 추가하는 옵션도 있습니다. 에서 GuardDuty 구성원을 연결하는 두 가지 방법에 대한 자세한 내용은 을 참조하십시오. Amazon에서 여러 계정 관리 GuardDuty

1. 위임된 관리자 계정에 로그인
2. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
3. 탐색 창에서 Settings(설정)를 선택한 다음 Accounts(계정)를 선택합니다.

   계정 테이블에는 조직의 모든 계정이 표시됩니다.
4. 계정 ID 옆의 확인란을 선택하여 멤버로 추가할 계정을 선택합니다. 그런 다음 작업 메뉴에서 멤버 추가를 선택합니다.

> **Tip**
>
> 자동 활성화 기능을 켜서 새 계정을 멤버로 자동 추가할 수 있습니다. 하지만 이 기능은 기능이 활성화된 후 조직에 가입하는 계정에만 적용됩니다.

2단계: 샘플 결과 생성 및 기본 작업 탐색

보안 문제를 GuardDuty 발견하면 검색 결과가 생성됩니다. GuardDuty 검색 결과는 해당 고유한 보안 문제와 관련된 세부 정보가 포함된 데이터 세트입니다. 결과의 세부 정보는 문제를 조사하는 데 도움이 될 수 있습니다.

GuardDuty 에서 발견한 실제 보안 문제에 대응하기 전에 GuardDuty 기능을 테스트하고 결과를 숙지하는 데 사용할 수 있는 자리 표시자 값이 포함된 샘플 결과 생성을 지원합니다. GuardDuty 에서 GuardDuty 사용할 수 있는 각 검색 결과 유형에 대한 샘플 결과를 생성하려면 아래 가이드를 따르십시오. 계정 내에서 시뮬레이션된 보안 이벤트를 생성하는 것을 포함하여 샘플 결과를 생성하는 추가 방법에 대한 자세한 내용은 을 참조하십시오. 샘플 결과

샘플 결과 생성 및 탐색

1. 탐색 창에서 설정을 선택합니다.
2. [Settings] 페이지의 [Sample findings] 아래에서 [Generate sample findings]를 선택합니다.

3. 탐색 창에서 요약을 선택하여 AWS 환경에서 생성된 결과에 대한 통찰력을 확인하십시오. 요약 대시보드의 구성 요소에 대한 자세한 내용은 요약 대시보드 섹션을 참조하세요.
4. 탐색 창에서 결과를 선택합니다. 샘플 결과는 현재 결과 페이지에 접두사 [SAMPLE]과 함께 표시됩니다.
5. 목록에서 결과를 선택하면 결과에 대한 세부 정보가 표시됩니다.
    - 결과 세부 정보 창에 제공되는 다양한 정보 필드를 검토할 수 있습니다. 결과 유형마다 필드가 다를 수 있습니다. 모든 결과 유형에 제공되는 필드에 대한 자세한 내용은 결과 세부 정보 섹션을 참조하세요. 세부 정보 창에서 다음 작업을 수행할 수 있습니다.
        - 창 상단에서 결과 ID를 선택하면 결과에 대한 전체 JSON 세부 정보가 열립니다. 이 패널에서 전체 JSON 파일을 다운로드할 수도 있습니다. JSON에는 콘솔 보기에 포함되지 않은 몇 가지 추가 정보가 포함되어 있으며, 다른 도구 및 서비스에서 수집할 수 있는 형식입니다.
        - 영향을 받는 리소스 섹션을 확인하세요. 실제 조사 결과에서 여기의 정보는 계정 내에서 조사해야 할 리소스를 식별하는 데 도움이 되며 AWS Management Console 적절하고 실행 가능한 리소스로 연결되는 링크를 포함합니다.
        - + 또는 - 아이콘을 선택하여 해당 세부 정보에 대한 포괄적 또는 배타적 필터를 만들 수 있습니다. 필터에 대한 자세한 내용은 조사 결과 필터링 섹션을 참조하세요.
6. 모든 샘플 결과 보관
    a. 목록 상단에 있는 확인란을 선택하여 모든 결과를 선택합니다.
    b. 보관하려는 결과를 모두 선택 취소합니다.
    c. 작업 메뉴를 선택하고 보관을 선택하여 샘플 결과를 숨깁니다.

> **Note**
>
> 보관된 결과를 보려면 현재를 선택한 다음 보관됨을 선택하여 결과 보기를 전환합니다.

3단계: GuardDuty 결과를 Amazon S3 버킷으로 내보내기 구성

GuardDuty 검색 결과를 내보내도록 설정을 구성하는 것이 좋습니다. 이렇게 하면 검색 결과를 S3 버킷으로 내보내 GuardDuty 90일 보존 기간이 지난 후 무기한 저장할 수 있기 때문입니다. 이를 통해 시간 경과에 따른 결과 기록을 보관하거나 환경 내 문제를 추적할 수 있습니다. AWS 여기에서 설명하는 프로세스는 새 S3 버킷을 설정하고 콘솔 내에서 결과를 암호화하도록 새 KMS 키를 생성하는 과정을 안

내합니다. 기존 버킷 또는 다른 계정의 버킷을 사용하는 방법을 포함하여 이에 대한 자세한 내용은 결과 내보내기 섹션을 참조하세요.

S3 결과 내보내기 옵션 구성

1. 결과를 암호화하려면 해당 키를 암호화에 사용할 수 GuardDuty 있는 정책이 포함된 KMS 키가 필요합니다. 다음 단계는 새 KMS 키를 생성하는 데 도움이 됩니다. 다른 계정의 KMS 키를 사용하는 경우 키를 AWS 계정 소유한 사람에게 로그인하여 키 정책을 적용해야 합니다. KMS 키와 S3 버킷의 리전이 동일해야 합니다. 하지만 결과를 내보내려는 각 리전에 동일한 버킷과 키 페어를 사용할 수 있습니다.

   a. https://console.aws.amazon.com/kms 에서 AWS KMS 콘솔을 엽니다.

   b. 를 변경하려면 AWS 리전페이지 오른쪽 상단에 있는 지역 선택기를 사용하십시오.

   c. 탐색 창에서 고객 관리형 키를 선택합니다.

   d. 키 생성을 선택합니다.

   e. 키 유형에서 대칭을 선택한 후 다음을 선택합니다.

      > **Note**
      >
      > KMS 키 생성에 대한 구체적 단계는AWS Key Management Service 개발자 안내서의 Creating keys를 참조하세요.

   f. 키의 별칭을 입력하고 다음을 선택합니다.

   g. 다음을 선택하고, 다시 다음을 선택하여 기본 관리 및 사용 권한을 수락합니다.

   h. 구성을 검토한 후에는 완료를 선택하여 키를 생성합니다.

   i. 고객 관리형 키 페이지에서 키 별칭을 선택합니다.

   j. 키 정책 탭에서 정책 보기로 전환을 선택합니다.

   k. 편집을 선택하고 KMS 키에 다음 키 정책을 추가하여 키에 대한 액세스 권한을 GuardDuty 부여합니다. 이 설명문에서는 GuardDuty 이 정책을 추가한 키만 사용할 수 있습니다. 키 정책을 편집할 때는 JSON 구문이 유효한지 확인해야 합니다. 마지막 문 앞에 문을 추가하면 닫는 대괄호 뒤에 쉼표를 추가해야 합니다.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
```

```
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
}
```

*Region1*을 KMS 키의 리전으로 바꿉니다. *444455556666#* KMS 키를 소유한 것으로 교체하십시오. AWS 계정 *KMS# #### ## ### KMS* 키의 키 KeyId ID로 바꾸십시오. 지역 AWS 계정, 키 ID 등 모든 값을 식별하려면 KMS 키의 ARN을 확인하세요. 키 ARN을 찾으려면 Finding the key ID and ARN을 참조하세요.

마찬가지로 *111122223333#* 해당 계정의 것으로 바꾸십시오. AWS 계정 GuardDuty *## 2 # ### ####* 바꾸십시오. GuardDuty *SourceDetectorID# ## 2 GuardDuty ### ### ID# #####.*

계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

I. 저장을 선택합니다.

2. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
3. 탐색 창에서 설정을 선택합니다.
4. 결과 내보내기 옵션에서 지금 구성을 선택합니다.
5. 새 버킷을 선택합니다. S3 버킷에 대해 고유한 이름을 입력합니다.
6. (선택 사항) 샘플 결과를 생성하여 새 내보내기 설정을 테스트할 수 있습니다. 탐색 창에서 설정을 선택합니다.
7. 샘플 결과 섹션에서 샘플 결과 생성을 선택합니다. 새 샘플 결과는 최대 5분 내에 생성된 S3 GuardDuty 버킷의 항목으로 표시됩니다.

4단계: SNS를 통한 알림 GuardDuty 검색 설정

GuardDuty Amazon과 통합되며 EventBridge, 이를 사용하여 결과 데이터를 다른 애플리케이션 및 서비스에 전송하여 처리할 수 있습니다. EventBridge 를 사용하면 GuardDuty 검색 결과를 사용하여

검색 결과 이벤트를 AWS Lambda 함수, Amazon EC2 Systems Manager 자동화, Amazon Simple Notification Service (SNS) 등과 같은 대상에 연결하여 결과에 대한 자동 응답을 시작할 수 있습니다.

이 예제에서는 EventBridge 규칙의 대상이 될 SNS 주제를 생성한 다음, 해당 주제를 사용하여 EventBridge 결과 데이터를 캡처하는 규칙을 생성합니다. GuardDuty 결과 규칙은 결과 세부 정보를 이메일 주소로 전달합니다. 결과를 Slack 또는 Amazon Chime으로 보내는 방법과 결과 알림 유형을 수정하는 방법을 알아보려면 Amazon SNS 주제 및 엔드포인트 설정 섹션을 참조하세요.

결과 알림에 대한 SNS 주제 생성

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 탐색 창에서 주제를 선택합니다.
3. 주제 생성을 선택합니다.
4. 유형에서 표준을 선택합니다.
5. 이름에 **GuardDuty**을 입력합니다.
6. 주제 생성을 선택합니다. 새로운 주제에 대한 주제 세부 정보가 열립니다.
7. 구독 섹션에서 구독 생성을 선택합니다.
8. 프로토콜에서 이메일을 선택합니다.
9. 엔드포인트에서 알림을 전송할 이메일 주소를 입력합니다.
10. 구독 생성을 선택합니다.

    구독을 생성한 후에는 이메일을 통해 구독을 확인해야 합니다.
11. 구독 메시지를 확인하려면 이메일 수신함으로 이동한 다음 구독 메시지에서 구독 확인을 선택합니다.

> **Note**
>
> 이메일 확인 상태를 확인하려면 SNS 콘솔로 이동하여 구독을 선택합니다.

GuardDuty 결과를 캡처하고 형식을 지정하는 EventBridge 규칙을 만들려면

1. https://console.aws.amazon.com/events/ 에서 EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.
4. 규칙에 대해 이름과 설명을 입력하십시오.

규칙은 동일한 지역과 동일한 이벤트 버스의 다른 규칙과 동일한 이름을 가질 수 없습니다.

5. 이벤트 버스에서 기본값을 선택합니다.
6. 규칙 유형에서 이벤트 패턴이 있는 규칙을 선택합니다.
7. 다음을 선택합니다.
8. 이벤트 소스(Event source)에서 AWS 이벤트(events)를 선택합니다.
9. 이벤트 패턴에서 이벤트 패턴 양식을 선택합니다.
10. 이벤트 소스에서 AWS 서비스를 선택합니다.
11. AWS 서비스에서 GuardDuty를 선택합니다.
12. 이벤트 유형에서 GuardDuty 찾기를 선택합니다.
13. 다음을 선택합니다.
14. 대상 유형에서 AWS 서비스를 선택합니다.
15. 대상 선택에서 SNS 주제를 선택하고, 주제에서 앞서 생성한 SNS 주제의 이름을 선택합니다.
16. 추가 설정 섹션의 대상 입력 구성에서 입력 변환기를 선택합니다.

    입력 변환기를 추가하면 보낸 JSON 검색 데이터가 사람이 읽을 수 있는 GuardDuty 메시지로 포맷됩니다.
17. Configure input transformer(입력 구성 변환기)를 선택합니다.
18. 대상 입력 변환기 섹션의 입력 경로에 다음 코드를 붙여넣습니다.

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. 이메일 형식을 지정하려면 템플릿에 다음 코드를 붙여넣고 빨간색 텍스트를 해당 지역에 적합한 값으로 바꿔야 합니다.

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
```

```
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. 확인을 선택합니다.
21. 다음을 선택합니다.
22. (선택 사항) 규칙에 대해 하나 이상의 태그를 입력하십시오. 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하십시오.
23. 다음을 선택합니다.
24. 규칙의 세부 정보를 검토하고 규칙 생성을 선택합니다.
25. (선택 사항) 2단계의 프로세스를 사용하여 샘플 결과를 생성하고 새 규칙을 테스트합니다. 생성된 각 샘플 결과에 대해 이메일을 받게 됩니다.

다음 단계

계속 GuardDuty 사용하다 보면 환경과 관련된 검색 결과의 유형을 이해하게 될 것입니다. 새로운 결과를 받을 때마다 결과 세부 정보 창의 결과 설명에서 자세히 알아보기를 선택하거나 결과 유형에서 결과 이름을 검색하여 해당 결과에 대한 해결 권장 사항을 비롯한 정보를 찾아볼 수 있습니다.

다음 기능은 AWS 환경에 가장 적합한 결과를 제공할 수 GuardDuty 있도록 튜닝하는 데 도움이 됩니다.

- 인스턴스 ID, 계정 ID, S3 버킷 이름 등과 같은 특정 기준에 따라 결과를 쉽게 정렬하려면 내에서 필터를 생성하고 저장할 수 있습니다 GuardDuty. 자세한 정보는 조사 결과 필터링을 참조하세요.
- 환경에서 예상되는 동작에 대한 결과를 받는 경우 억제 규칙으로 정의한 기준을 기반으로 결과를 자동으로 보관할 수 있습니다.
- 신뢰할 수 있는 IP의 하위 집합에서 검색 결과가 생성되지 않도록 하거나 IP가 GuardDuty 정상 모니터링 범위를 벗어나도록 하려면 신뢰할 수 있는 IP 및 위협 목록을 설정할 수 있습니다.

개념 및 용어

Amazon을 시작하면서 GuardDuty Amazon의 주요 개념에 대해 배우면 도움이 될 수 있습니다.

계정

AWS 리소스가 포함된 표준 Amazon Web Services (AWS) 계정입니다. AWS 계정으로 로그인하여 활성화할 수 GuardDuty 있습니다.

에서 다른 계정을 초대하여 계정을 GuardDuty 활성화하고 해당 AWS 계정과 연결되도록 할 수도 GuardDuty 있습니다. 초대를 수락하면 계정이 관리자 GuardDuty 계정 계정으로 지정되고 추가된 계정은 멤버 계정이 됩니다. 그러면 사용자를 대신하여 해당 계정의 GuardDuty 결과를 보고 관리할 수 있습니다.

관리자 계정의 사용자는 자신의 계정과 모든 구성원 계정에 대한 GuardDuty 결과를 구성하고 GuardDuty 보고 관리할 수 있습니다. 최대 10,000개의 회원 계정을 보유할 수 GuardDuty 있습니다.

구성원 계정 사용자는 GuardDuty 관리 콘솔 또는 GuardDuty API를 통해 자신의 계정에서 GuardDuty 결과를 구성하고 GuardDuty 보고 관리할 수 있습니다. 멤버 계정의 사용자는 다른 멤버 계정의 결과를 보거나 관리할 수 없습니다.

AWS 계정은 GuardDuty 관리자 계정과 구성원 계정을 동시에 사용할 수 없습니다. AWS 계정은 멤버십 초대 한 개만 수락할 수 있습니다. 멤버십 초대 수락은 선택 사항입니다.

자세한 정보는 Amazon에서 여러 계정 관리 GuardDuty을 참조하세요.

감지기

모든 GuardDuty 결과는 GuardDuty 서비스를 나타내는 객체인 탐지기와 연결됩니다. 탐지기는 지역적 독립체이므로 GuardDuty 작동하는 각 AWS 리전 기관마다 고유한 탐지기가 필요합니다. GuardDuty 지역에서 활성화하면 고유한 32자리 영숫자 DetectorID가 있는 새 탐지기가 해당 지역에 생성됩니다. detectorId의 형식은 `12abc34d567e8fa901bc2d34e56789f0`입니다.

계정 및 현재 지역의 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

> **Note**
>
> 다중 계정 환경에서 멤버 계정에 대한 모든 결과는 관리자 계정의 탐지기까지 적용됩니다.

CloudWatch 이벤트 알림 빈도 구성, 처리할 선택적 데이터 소스 활성화 또는 비활성화와 같은 일부 GuardDuty 기능은 탐지기를 통해 구성됩니다. GuardDuty

데이터 소스

한 세트의 데이터의 출처 또는 위치. 사용자 AWS 환경에서 무단 또는 예상치 못한 활동을 탐지하기 위함입니다. GuardDuty AWS CloudTrail 이벤트 로그, AWS CloudTrail 관리 이벤트, S3에 대한 AWS CloudTrail 데이터 이벤트, VPC 흐름 로그, DNS 로그, EKS 감사 로그, RDS 로그인 활동 모니터링 및 EBS 볼륨의 데이터를 분석하고 처리합니다. 자세한 정보는 기본 데이터 소스을 참조하세요.

기능

GuardDuty 보호 계획에 맞게 구성된 기능 객체는 사용자 환경에서 무단 또는 예상치 못한 활동을 탐지하는 데 도움이 됩니다. AWS 각 GuardDuty 보호 계획은 데이터를 분석하고 처리할 해당 기능 개체를 구성합니다. 일부 기능 객체에는 EKS 감사 로그, RDS 로그인 활동 모니터링 및 EBS 볼륨이 포함됩니다. 자세한 정보는 에서 기능 활성화 GuardDuty을 참조하세요.

결과

GuardDuty에서 발견된 잠재적인 보안 문제. 자세한 정보는 아마존 GuardDuty 조사 결과 이해을 참조하세요.

결과는 GuardDuty 콘솔에 표시되며 보안 문제에 대한 자세한 설명을 포함합니다. GetFindings및 ListFindingsAPI 작업을 호출하여 생성된 결과를 검색할 수도 있습니다.

Amazon CloudWatch 이벤트를 통해서도 GuardDuty 결과를 확인할 수 있습니다. GuardDuty HTTPS 프로토콜을 CloudWatch 통해 Amazon에 결과를 전송합니다. 자세한 정보는 Amazon CloudWatch Events를 사용하여 GuardDuty 결과에 대한 사용자 지정 응답 생성을 참조하세요.

스캔 옵션

GuardDuty 멀웨어 보호가 활성화되면 스캔하거나 건너뛸 Amazon EC2 인스턴스 및 Amazon Elastic Block Store (EBS) 볼륨을 지정할 수 있습니다. 이 기능을 사용하면 EC2 인스턴스 및 EBS 볼륨과 연결된 기존 태그를 포함 태그 목록 또는 제외 태그 목록에 추가할 수 있습니다. 포함 태그 목록에 추가한 태그와 관련된 리소스는 맬웨어 스캔의 대상이 되지만 제외 태그 목록에 추가된 리소스는 스캔되지 않습니다. 자세한 정보는 사용자 정의 태그를 사용하는 스캔 옵션을 참조하세요.

스냅샷 보존

GuardDuty 멀웨어 보호가 활성화되면 EBS 볼륨의 스냅샷을 계정에 보관할 수 있는 옵션이 제공됩니다. AWS GuardDuty EBS 볼륨의 스냅샷을 기반으로 복제 EBS 볼륨을 생성합니다. 맬웨어 보호 스캔에서 EBS 볼륨 복제본의 맬웨어를 탐지한 경우에만 EBS 볼륨의 스냅샷을 유지할 수 있습니

다. 복제 EBS 볼륨에서 멀웨어가 탐지되지 않으면 스냅샷 보존 설정에 관계없이 EBS 볼륨의 스냅샷을 GuardDuty 자동으로 삭제합니다. 자세한 정보는 스냅샷 보존을 참조하세요.

억제 규칙

억제 규칙은 몇 가지 속성을 고유하게 조합하여 결과 범위를 제한할 수 있습니다. 예를 들어 GuardDuty 필터를 통해 특정 VPC에 있거나, 특정 AMI를 실행하거나, 특정 EC2 태그를 사용하는 `Recon:EC2/Portscan` 인스턴스에서만 자동 보관하도록 규칙을 정의할 수 있습니다. 그러면 이 규칙에 따라 포트 스캔 결과가 기준을 만족하는 인스턴스에서 자동으로 아카이브됩니다. 하지만 암호화폐 채굴과 같은 다른 악의적인 활동을 수행하는 인스턴스를 GuardDuty 탐지할 경우 여전히 경고를 보낼 수 있습니다.

GuardDuty 관리자 계정에 정의된 금지 규칙은 구성원 계정에 적용됩니다. GuardDuty GuardDuty 멤버 계정은 금지 규칙을 수정할 수 없습니다.

금지 규칙을 GuardDuty 사용해도 여전히 모든 결과가 생성됩니다. 억제 규칙은 결과 범위를 제한하는 동시에 모든 활동에 대해 완전하면서 변경 불가능하도록 기록을 유지합니다.

일반적으로 억제 규칙은 광범위한 위협에 집중할 수 있도록 하기 위해 사용자 환경에서 오탐지로 판단된 결과를 숨기고 가치가 낮은 결과의 노이즈를 줄이는 데 사용됩니다. 자세한 정보는 억제 규칙을 참조하세요.

신뢰할 수 있는 IP 목록

AWS 환경과의 매우 안전한 통신을 위한 신뢰할 수 있는 IP 주소 목록. GuardDuty 신뢰할 수 있는 IP 목록을 기반으로 검색 결과를 생성하지 않습니다. 자세한 정보는 신뢰할 수 있는 IP 목록 및 위협 목록 사용을 참조하세요.

위협 IP 목록

알려진 악성 IP 주소 목록입니다. 잠재적으로 의심스러운 활동으로 인한 탐지 결과를 생성하는 것 외에도 이러한 위협 목록을 기반으로 조사 결과를 생성합니다. GuardDuty 자세한 내용은 신뢰할 수 있는 IP 목록 및 위협 목록 사용을(를) 참조하세요.

에서 기능 활성화 GuardDuty

Amazon을 GuardDuty 처음으로 활성화하거나 내에서 보호 유형을 활성화하면 AWS 환경 기본 데이터 소스 내에서 GuardDuty 해당 유형의 처리가 GuardDuty 시작됩니다. GuardDuty 는 이러한 데이터 소스를 사용하여 VPC 흐름 로그, DNS 로그, 이벤트 및 관리 로그와 같은 AWS CloudTrail 이벤트 스트림을 처리합니다. 그런 다음 이러한 이벤트를 분석하여 잠재적 보안 위협을 식별하고 계정에서 결과를 생성합니다.

로그 데이터 소스 외에도 AWS 환경 내 다른 AWS 서비스의 추가 데이터를 사용하여 잠재적인 보안 위협을 모니터링하고 분석할 GuardDuty 수 있습니다.

기능 활성화

추가 GuardDuty 보호 (예: S3 보호, 런타임 모니터링 또는 EKS 보호) 를 추가할 때 보호 유형에 해당하는 GuardDuty 기능을 구성할 수 있습니다. 과거에는 API에서 GuardDuty 보호가 `dataSources` 호출되었습니다. 그러나 2023년 3월 이후에는 이제 새로운 GuardDuty 보호 유형이 구성되거나 구성되지 않습니다. `features` `dataSources` GuardDuty 2023년 3월 이전에 출시된 보호 유형을 API와 같이 `dataSources` 구성할 수 있지만 새 보호 유형은 에서만 사용할 수 `features` 있습니다.

콘솔을 통해 GuardDuty 구성 및 보호 유형을 관리하는 경우 이 변경의 직접적인 영향을 받지 않으므로 별도의 조치를 취할 필요가 없습니다. 기능 활성화는 내에서 보호 유형을 GuardDuty 활성화하기 위해 호출되는 API의 동작에 영향을 줍니다. GuardDuty 자세한 정보는 GuardDuty API 변경을 참조하세요.

GuardDuty 2023년 3월 API 변경

GuardDuty API는 목록에 속하지 않는 보호 기능을 구성합니다. 기본 데이터 소스 기능 객체에는 기능 이름 및 상태와 같은 기능 세부 정보가 포함되며 일부 기능에 대한 추가 구성이 포함될 수 있습니다. 이 마이그레이션은 Amazon GuardDuty API 참조의 다음 API에 영향을 줍니다.

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration

- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

기능 활성화와 데이터 소스 비교

GuardDuty 과거에는 모든 기능이 API의 `dataSources` 객체를 통해 전달되었습니다. 2023년 3월부터 API의 `features` `dataSources` 객체 대신 객체를 GuardDuty 선호합니다. 이전의 모든 데이터 소스에는 해당 기능이 있지만 최신 기능에는 해당 데이터 소스가 없을 수 있습니다.

다음 목록은 API를 통해 전달된 `dataSources` 및 `features` 객체 간의 비교를 보여줍니다.

- `dataSources` 객체에는 각 보호 유형에 대한 객체와 상태가 포함되어 있습니다. `features`객체는 각 보호 유형에 해당하는 GuardDuty 사용 가능한 기능 목록입니다.

  2023년 3월부터 사용자 AWS 환경에서 새 기능을 구성할 수 있는 유일한 방법은 GuardDuty 기능 활성화뿐입니다.
- API 요청 또는 응답의 `dataSources` GuardDuty 스키마는 사용 가능한 각 AWS 리전 위치에서 동일합니다. 하지만 일부 리전에서는 모든 기능을 사용하지 못할 수 있습니다. 따라서 사용 가능한 기능 이름은 리전에 따라 다를 수 있습니다.

기능 활성화의 작동 방식 이해

GuardDuty API는 해당하는 경우 계속해서 `dataSources` 객체를 반환하고 동일한 정보가 포함된 `features` 객체도 다른 형식으로 반환합니다. GuardDuty 2023년 3월 이전에 출시된 기능은 `dataSources` 객체와 `features` 객체를 통해 사용할 수 있습니다. GuardDuty 2023년 3월 이후 출시된 기능은 `features` 객체를 통해서만 사용할 수 있습니다. 같은 API 요청에서 `dataSources` 및 `features` 객체 표기법을 모두 사용하여 탐지기를 생성 또는 업데이트하거나 AWS Organizations 를 설명할 수 없습니다. GuardDuty 보호 유형을 활성화하려면 이제 객체도 포함된 동일한 API를 사용하여 기존 데이터 원본을 `features` `features` 객체로 마이그레이션해야 합니다.

> **Note**
>
> GuardDuty 이번 수정 후에는 새 데이터 소스를 추가하지 않을 예정입니다.

GuardDuty 데이터 소스 사용을 중단했습니다. 하지만 기본 데이터 소스 지원은 계속됩니다. GuardDuty 모범 사례에서는 계정에 이미 활성화된 모든 보호 유형에 기능 활성화를 사용하는 것이 좋습니다. 또한 모범 사례에 따라 계정에 새 보호 유형을 활성화할 때 기능 활성화를 사용해야 합니다.

기능 활성화 통합 변경 사항

- API, SDK 또는 AWS CloudFormation 템플릿을 통해 GuardDuty 구성을 관리하고 잠재적인 새 GuardDuty 기능을 활성화하려면 코드와 템플릿을 각각 수정해야 합니다. 자세한 내용은 Amazon GuardDuty API 참조의 업데이트된 API를 참조하십시오.
- 업그레이드 이전에 구성된 GuardDuty 기능의 경우 API, SDK 또는 템플릿을 계속 사용할 수 있습니다. AWS CloudFormation 하지만 `feature` 객체 사용으로 전환하는 것이 좋습니다.

  모든 데이터 소스에는 동일한 기능 객체가 있습니다. 자세한 정보는 `dataSources`를 `features`로 매핑을 참조하세요.
- 현재 `features` 객체의 `additionalConfiguration`은 특정 보호 유형에서만 사용 가능합니다.
  - 이러한 보호 유형의 경우 기능은 로 `AdditionalConfiguration` `status` 설정되어 `ENABLED` 있지만 기능 구성이 로 `status` `ENABLED` 설정되어 있지 않으면 이 경우 아무 조치도 취하지 않습니다. GuardDuty
  - 이로 인해 영향을 받는 API는 다음과 같습니다.
    - UpdateDetector
    - UpdateMemberDetectors
    - UpdateOrganizationConfiguration

`dataSources`를 `features`로 매핑

다음 표는 보호 유형, `dataSources` 및 `features`의 매핑을 보여줍니다.

GuardDuty 보호 유형	데이터 소스 이름*	기능 이름
VPC 흐름 로그	`flowLogs`(읽기 전용, 수정 불가)	`FLOW_LOGS` (읽기 전용, 수정 불가)
DNS 로그	`dnsLogs`(읽기 전용, 수정 불가)	`DNS_LOGS`(읽기 전용, 수정 불가)

GuardDuty 보호 유형	데이터 소스 이름*	기능 이름
CloudTrail 이벤트	cloudLogs (읽기 전용, 수정 불가)	CLOUD_LOGS (읽기 전용, 수정 불가)
S3	s3Logs	S3_DATA_EVENTS
EKS 감사 로그 모니터링	kubernetes.auditlogs	EKS_AUDIT_LOGS
맬웨어 보호	malwareProtection.scanEc2InstanceWithFindings.ebsVolumes	EBS_MALWARE_PROTECTION
RDS 로그인 이벤트	GuardDuty 이러한 보호 유형에 대한 기능 활성화 지원만 제공합니다.	RDS_LOGIN_EVENTS
EKS 런타임 모니터링		EKS_RUNTIME_MONITORING
런타임 모니터링		RUNTIME_MONITORING

GuardDuty 보호 유형	데이터 소스 이름*	기능 이름
GuardDuty Amazon EKS 클러스터용 보안 에이전트		EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
GuardDuty Amazon ECS-Fargate 클러스터용 보안 에이전트		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT
GuardDuty Amazon EC2 인스턴스용 보안 에이전트		RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT
Lambda 보호	LAMBDA_NETWORK_LOGS	

*GetUsageStatistics는 고유한 `dataSource` 이름을 사용합니다. 자세한 내용은 비용 추정 GuardDuty 또는 GetUsageStatistics 단원을 참조하세요.

기본 데이터 소스

GuardDuty 기본 데이터 소스를 사용하여 알려진 악성 도메인 및 IP 주소와의 통신을 탐지하고 비정상적인 동작을 식별합니다. 이러한 소스에서 다른 소스로 전송되는 동안에는 모든 GuardDuty 로그 데이터가 암호화됩니다. GuardDuty프로파일링 및 이상 탐지를 위해 이러한 로그 소스에서 다양한 필드를 추출한 다음 이러한 로그를 삭제합니다.

다음 섹션에서는 지원되는 각 데이터 원본을 GuardDuty 사용하는 방법을 설명합니다. GuardDuty 에서 활성화하면 이 로그 소스를 GuardDuty 자동으로 모니터링하기 시작합니다. AWS 계정

주제

- AWS CloudTrail 이벤트 로그
- AWS CloudTrail 관리 이벤트
- VPC 흐름 로그
- DNS 로그

AWS CloudTrail 이벤트 로그

AWS CloudTrail , AWS SDK, 명령줄 도구 및 특정 AWS 서비스를 사용하여 이루어진 API 호출을 포함하여 계정에 대한 API 호출 기록을 제공합니다. AWS AWS Management Console CloudTrail 또한 지원하는 서비스의 AWS API를 호출한 사용자 및 계정 CloudTrail, 호출이 호출된 소스 IP 주소, 호출이 호출된 시간을 식별하는 데도 도움이 됩니다. 자세한 내용은AWS CloudTrail 사용 설명서에서 AWS CloudTrail란 무엇입니까? 섹션을 참조하세요.

GuardDuty 또한 관리 이벤트를 모니터링합니다. CloudTrail GuardDuty활성화하면 독립적이고 복제된 이벤트 스트림을 CloudTrail 통해 직접 CloudTrail 관리 이벤트를 소비하기 시작하고 CloudTrail 이벤트 로그를 분석합니다. 에 기록된 이벤트에 GuardDuty 액세스할 때는 추가 요금이 부과되지 않습니다. CloudTrail

GuardDuty CloudTrail 이벤트를 관리하거나 기존 CloudTrail 구성에 영향을 주지 않습니다. 마찬가지로, CloudTrail 구성은 이벤트 로그를 사용하고 GuardDuty 처리하는 방법에 영향을 주지 않습니다. CloudTrail 이벤트 액세스 및 보존을 관리하려면 CloudTrail 서비스 콘솔 또는 API를 사용하세요. 자세한 내용은 AWS CloudTrail 사용 설명서에서 이벤트 기록과 함께 CloudTrail 이벤트 보기를 참조하십시오.

AWS CloudTrail 글로벌 이벤트 GuardDuty 처리 방법

대부분의 AWS 서비스에서는 CloudTrail 이벤트가 생성된 AWS 리전 위치에 이벤트가 기록됩니다. AWS Identity and Access Management (IAM), (AWS STS), 아마존 심플 스토리지 서비스 AWS Security Token Service (Amazon S3), CloudFront Amazon 및 Amazon Route 53 (Route 53) 과 같은 글로벌 서비스의 경우 이벤트는 이벤트가 발생한 지역에서만 생성되지만 전 세계적으로 중요합니다.

네트워크 구성 또는 사용자 권한과 같은 보안 가치가 있는 CloudTrail 글로벌 서비스 이벤트를 사용하면 해당 이벤트를 복제하여 활성화한 각 지역에서 처리합니다. GuardDuty GuardDuty 이 동작은 각 지역의 사용자 및 역할 프로필을 GuardDuty 유지하는 데 도움이 되며, 이는 이상 이벤트를 탐지하는 데 필수적입니다.

사용할 수 GuardDuty 있는 모든 기능을 AWS 리전 활성화하는 것이 좋습니다. AWS 계정이렇게 하면 GuardDuty 활발하게 사용하지 않을 수도 있는 지역에서도 무단 또는 비정상적 활동에 대한 결과를 얻을 수 있습니다.

AWS CloudTrail 관리 이벤트

관리 이벤트는 컨트롤 플레인 이벤트라고도 합니다. 이러한 이벤트는 AWS 계정의 리소스에 대해 수행되는 관리 작업에 대한 통찰력을 제공합니다.

GuardDuty모니터링하는 CloudTrail 관리 이벤트의 예는 다음과 같습니다.

- 보안 구성(IAM `AttachRolePolicy` API 작업)
- 데이터 라우팅 규칙 구성(Amazon EC2 `CreateSubnet` API 작업)
- 로깅 설정 (AWS CloudTrail `CreateTrail`API 작업)

VPC 흐름 로그

Amazon VPC의 VPC 흐름 로그 기능은 사용자 환경 내의 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스에 연결된 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처합니다. AWS

활성화하면 GuardDuty 계정 내 Amazon EC2 인스턴스의 VPC 흐름 로그 분석이 즉시 시작됩니다. 이때 이 서비스는 독립적이고 중복된 흐름 로그 스트림을 통해 VPC 흐름 로그 기능에서 직접 VPC 흐름 로그 이벤트를 사용합니다. 이 프로세스는 기존 흐름 로그 구성에는 영향을 미치지 않습니다.

GuardDuty 람다 프로텍션

Lambda 보호는 Amazon의 선택적 개선 사항입니다. GuardDuty 현재 Lambda 네트워크 활동 모니터링에는 VPC 네트워킹을 사용하지 않는 로그를 포함하여 계정에 대한 모든 Lambda 함수의 Amazon VPC 흐름 로그가 포함되어 있습니다. Lambda 함수를 잠재적인 보안 위협으로부터 보호하려면 계정에서 Lambda 보호를 구성해야 합니다. GuardDuty 자세한 정보는 GuardDuty 람다 프로텍션을 참조하세요.

GuardDuty 런타임 모니터링

EC2 인스턴스용 EKS 런타임 모니터링 또는 런타임 모니터링에서 보안 에이전트를 관리 (수동 또는 통해 GuardDuty) 하고 GuardDuty 현재 Amazon EC2 인스턴스에 배포되어 있고 이 수집된 런타임 이벤트 유형 인스턴스로부터 수신한 경우, 이 Amazon EC2 인스턴스의 VPC 흐름 로그 분석에 GuardDuty 대해서는 요금이 부과되지 않습니다. AWS 계정 이렇게 하면 계정에서 이중 사용 비용이 발생하는 GuardDuty 것을 방지할 수 있습니다.

GuardDuty 흐름 로그를 관리하거나 계정에서 액세스할 수 있게 만들지 않습니다. 흐름 로그의 액세스 및 보존을 관리하려면 VPC 흐름 로그 기능을 구성해야 합니다.

DNS 로그

Amazon EC2 인스턴스에 AWS DNS 확인자를 사용하는 경우 (기본 설정), GuardDuty 내부 DNS 확인자를 통해 요청 및 응답 DNS 로그에 액세스하고 이를 처리할 수 있습니다. AWS OpenDNS 또는 GoogleDNS와 같은 다른 DNS 확인자를 사용하거나 자체 DNS 확인자를 설정하는 경우 이 데이터 원본의 데이터에 액세스하여 데이터를 처리할 수 없습니다. GuardDuty

활성화하면 독립된 GuardDuty 데이터 스트림에서 DNS 로그를 즉시 분석하기 시작합니다. 이 데이터 스트림은 Route 53 해석기 쿼리 로깅 기능을 통해 제공되는 데이터와는 별개입니다. 이 기능의 구성은 GuardDuty 분석에 영향을 주지 않습니다.

> **Note**
>
> GuardDuty 시작된 Amazon EC2 인스턴스의 DNS 로그 모니터링을 지원하지 않습니다. 해당 환경에서는 Amazon Route 53 Resolver 쿼리 로깅 기능을 사용할 수 AWS Outposts 없기 때문입니다.

아마존에서의 EKS 보호 GuardDuty

EKS 감사 로그 모니터링을 사용하면 Amazon Elastic Kubernetes Service(Amazon EKS)의 EKS 클러스터에서 잠재적으로 의심스러운 활동을 탐지할 수 있습니다. EKS 감사 로그 모니터링은 EKS 감사 로그를 사용하여 사용자, Kubernetes API를 사용하는 애플리케이션 및 컨트롤 플레인의 시간순 활동을 캡처합니다. 자세한 정보는 EKS 감사 로그 모니터링을 참조하세요.

> **Note**
>
> EKS 런타임 모니터링은 런타임 모니터링의 일부로 관리됩니다. 자세한 정보는 GuardDuty 런타임 모니터링을 참조하세요.

EKS 보호의 기능

EKS 감사 로그 모니터링

EKS 감사 로그는 사용자, Kubernetes API를 사용하는 애플리케이션, 컨트롤 플레인의 활동을 포함하여 Amazon EKS 클러스터 내에서 순차적인 작업을 캡처합니다. 감사 로깅은 모든 Kubernetes 클러스터의 구성 요소입니다.

자세한 내용은 Kubernetes 설명서의 Auditing을 참조하십시오.

Amazon EKS를 사용하면 EKS 컨트롤 플레인 로깅 기능을 통해 EKS 감사 CloudWatch 로그를 Amazon 로그로 수집할 수 있습니다. GuardDuty Amazon EKS 컨트롤 플레인 로깅을 관리하지 않으며, Amazon EKS에서 EKS 감사 로그를 활성화하지 않은 경우 계정에서 EKS 감사 로그에 액세스할 수 있도록 설정하지 않습니다. EKS 감사 로그에 대한 액세스 및 보존을 관리하려면 Amazon EKS 컨트롤 플레인 로깅 기능을 구성해야 합니다. 자세한 내용은 Amazon EKS 사용 설명서의 컨트롤 플레인 로그 활성화 및 비활성화를 참조하세요.

EKS 감사 로그 모니터링 구성에 대한 자세한 내용은 EKS 감사 로그 모니터링 섹션을 참조하세요.

EKS 감사 로그 모니터링

EKS 감사 로그 모니터링을 사용하면 Amazon Elastic Kubernetes Service의 EKS 클러스터에서 잠재적으로 의심스러운 활동을 탐지할 수 있습니다. EKS 감사 로그 모니터링을 활성화하면 GuardDuty 즉

시 Amazon EKS EKS 감사 로그 모니터링 클러스터에서 모니터링을 시작하여 잠재적으로 악의적이고 의심스러운 활동이 있는지 분석합니다. 독립적이고 중복된 감사 로그 스트림을 통해 Amazon EKS 컨트롤 플레인 로깅 기능에서 직접 Kubernetes 감사 로그 이벤트를 사용합니다. 이 프로세스는 추가 설정이 필요하지 않고 기존 Amazon EKS 컨트롤 플레인 로깅 구성에 영향을 미치지 않습니다.

EKS 감사 로그 모니터링을 비활성화하면 Amazon EKS 리소스에 대한 EKS 감사 로그의 모니터링 및 분석이 GuardDuty 즉시 중지됩니다.

EKS 감사 로그 모니터링은 가능한 모든 지역에서 사용 가능하지 않을 수도 있습니다. AWS 리전 GuardDuty 자세한 정보는 리전별 기능 가용성을 참조하세요.

30일 무료 평가판 기간이 계정에 미치는 영향 GuardDuty

- 처음 GuardDuty 활성화하면 EKS Protection의 EKS 감사 로그 모니터링이 30일 무료 평가 기간에 이미 포함되어 있습니다.
- 기존 GuardDuty 계정은 30일 무료 평가 기간을 통해 처음으로 EKS 감사 로그 모니터링을 활성화할 수 있습니다.

독립형 계정에 대한 EKS 감사 로그 모니터링 구성

선호하는 액세스 방법을 선택하여 독립형 계정에 대해 EKS 감사 로그 모니터링을 활성화 또는 비활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 EKS 보호를 선택합니다.
3. 구성 탭에서 EKS 감사 로그 모니터링의 현재 구성 상태를 볼 수 있습니다. EKS 감사 로그 모니터링 섹션에서 활성화 또는 비활성화를 선택하여 EKS 감사 로그 모니터링 기능을 활성화하거나 비활성화합니다.
4. 저장을 선택합니다.

API/CLI

- 위임된 GuardDuty 관리자 계정의 지역 탐지기 ID를 사용하여 updateDetectorAPI 작업을 실행하고 `features` 개체 이름은 OR로 `EKS_AUDIT_LOGS` 전달하고 상태는 `ENABLED` `DISABLED` OR로 전달합니다.

또는 a AWS CLI 명령을 실행하여 EKS 감사 로그 모니터링을 활성화하거나 비활성화할 수도 있습니다. 다음 예제 코드는 GuardDuty EKS 감사 로그 모니터링을 활성화합니다. 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

계정 및 현재 지역에 detectorId 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
```

다중 계정 환경에서 EKS 감사 로그 모니터링 구성

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만이 조직의 구성원 계정에 대해 EKS 감사 로그 모니터링 기능을 활성화하거나 비활성화할 수 있습니다. GuardDuty 구성원 계정은 자신의 계정에서 이 구성을 수정할 수 없습니다. 위임된 GuardDuty 관리자 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 이 위임된 GuardDuty 관리자 계정은 조직에 가입하는 모든 새 계정에 대해 EKS 감사 로그 모니터링을 자동으로 활성화하도록 선택할 수 있습니다. 다중 계정 환경에 대한 자세한 내용은 Amazon에서의 다중 계정 관리를 참조하십시오. GuardDuty

위임된 관리자 계정에 대한 EKS 감사 로그 모니터링 구성 GuardDuty

선호하는 액세스 방법을 선택하여 GuardDuty 위임된 관리자 계정에 대해 EKS 감사 로그 모니터링을 구성하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   관리 계정 보안 인증 정보를 사용해야 합니다.
2. 탐색 창에서 EKS 보호를 선택합니다.
3. 구성 탭에서 해당 섹션을 통해 EKS 감사 로그 모니터링 현재 구성 상태를 볼 수 있습니다. 위임된 GuardDuty 관리자 계정의 구성을 업데이트하려면 EKS 감사 로그 모니터링 창에서 편집을 선택합니다.
4. 다음 중 하나를 수행하십시오.

모든 계정에 대해 활성화 사용

- 모든 계정에 대해 활성화를 선택합니다. 그러면 조직에 가입하는 새 GuardDuty 계정을 포함하여 AWS 조직의 모든 활성 계정에 대한 보호 계획이 활성화됩니다.
- 저장을 선택합니다.

수동으로 계정 구성 사용

- 위임된 GuardDuty 관리자 계정 계정에만 보호 계획을 활성화하려면 계정 수동 구성을 선택합니다.
- 위임된 GuardDuty 관리자 계정 (이 계정) 섹션에서 활성화를 선택합니다.
- 저장을 선택합니다.

API/CLI

리전 탐지기 ID를 사용하고 `features` 객체 `name`을 `EKS_AUDIT_LOGS`으로, `status`를 `ENABLED` 또는 `DISABLED` 상태로 설정하여 전달해 updateDetector API를 실행합니다.

계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

다음 AWS CLI 명령을 실행하여 EKS 감사 로그 모니터링을 활성화하거나 비활성화할 수 있습니다. 위임된 GuardDuty 관리자 계정의 유효한 *###* ID를 사용해야 합니다.

> **Note**
>
> 다음 예시 코드는 EKS 감사 로그 모니터링을 활성화합니다.
> *12abc34d567e8fa901bc2d34e56789f0# ### ### ####, 555555555555# ### # ## #### #####. detector-id GuardDuty* AWS 계정 GuardDuty

`detectorId`계정과 현재 지역에 맞는 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

EKS 감사 로그 모니터링을 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

모든 멤버 계정에 대해 EKS 감사 로그 모니터링 자동 활성화

원하는 액세스 방법을 선택하여 조직의 기존 멤버 계정에 대해 EKS 감사 로그 모니터링을 활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 다음 중 하나를 수행하십시오.

   EKS 보호 페이지 사용

   1. 탐색 창에서 EKS 보호를 선택합니다.
   2. 구성 탭에서 조직의 활성 멤버 계정에 대한 EKS 감사 로그 모니터링의 현재 상태를 볼 수 있습니다.

      EKS 감사 로그 모니터링 구성을 업데이트하려면 편집을 선택합니다.
   3. 모든 계정에 대해 활성화를 선택합니다. 이 작업을 통해 조직의 기존 계정과 새 계정 모두에 대해 EKS 감사 로그 모니터링이 자동으로 활성화됩니다.
   4. 저장을 선택합니다.

      > **Note**
      >
      > 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

   계정 페이지 사용

   1. 탐색 창에서 Accounts(계정)를 선택합니다.
   2. 계정 페이지에서 초대 기준으로 계정 추가 전에 자동 활성화 기본 설정을 선택합니다.
   3. 자동 활성화 기본 설정 관리 창의 EKS 감사 로그 모니터링에서 모든 계정에 대해 활성화를 선택합니다.
   4. 저장을 선택합니다.

모든 계정에 대해 활성화 옵션을 사용할 수 없고 조직의 특정 계정에 대해 EKS 감사 로그 모니터링 구성을 사용자 지정하려면 멤버 계정에서 EKS 감사 로그 모니터링을 선택적으로 활성화 또는 비활성화 섹션을 참조하세요.

API/CLI

- 멤버 계정에 대해 EKS 감사 로그 모니터링을 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다.
- 다음 예시는 단일 멤버 계정에 EKS 감사 로그 모니터링을 활성화하는 방법을 보여줍니다. 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

  계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

  > **Note**
  >
  > 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

모든 기존 활성 멤버 계정에 대해 EKS 감사 로그 모니터링 활성화

원하는 액세스 방법을 선택하여 조직의 모든 기존 활성 멤버 계정에 대해 EKS 감사 로그 모니터링을 활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 EKS 보호를 선택합니다.

3. EKS Protection 페이지에서 GuardDuty시작된 맬웨어 검사 구성의 현재 상태를 볼 수 있습니다. 활성 멤버 계정 섹션에서 작업을 선택합니다.
4. 작업 드롭다운 메뉴에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다.
5. 저장을 선택합니다.

API/CLI

- 멤버 계정에 대해 EKS 감사 로그 모니터링을 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다.
- 다음 예시는 단일 멤버 계정에 EKS 감사 로그 모니터링을 활성화하는 방법을 보여줍니다. 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

  계정과 현재 지역에 `detectorId` 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

새 멤버 계정에 대해 EKS 감사 로그 모니터링 자동 활성화

구성 GuardDuty 시작 멀웨어 검사를 선택하기 GuardDuty 전에 새로 추가된 회원 계정을 활성화해야 합니다. 초대를 통해 관리되는 구성원 계정은 해당 계정에 대해 GuardDuty 시작 멀웨어 검사를 수동으로 구성할 수 있습니다. 자세한 정보는 Step 3 - Accept an invitation을 참조하세요.

원하는 액세스 방법을 선택하여 조직에 가입한 새 계정에 대해 EKS 감사 로그 모니터링을 활성화합니다.

Console

위임된 GuardDuty 관리자 계정은 EKS 감사 로그 모니터링 또는 계정 페이지를 사용하여 조직의 새 구성원 계정에 대해 EKS 감사 로그 모니터링을 활성화할 수 있습니다.

새 멤버 계정에 대해 EKS 감사 로그 모니터링 자동 활성화

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 다음 중 하나를 수행하십시오.
   - EKS 보호 페이지 사용:
     1. 탐색 창에서 EKS 보호를 선택합니다.
     2. EKS 보호 페이지의 EKS 감사 로그 모니터링에서 편집을 선택합니다.
     3. 수동으로 계정 구성을 선택합니다.
     4. 새 멤버 계정에 대해 자동으로 활성화를 선택합니다. 이 단계를 통해 새 계정이 조직에 가입할 때마다 해당 계정에 대해 EKS 감사 로그 모니터링이 자동으로 활성화됩니다. 조직이 위임한 GuardDuty 관리자 계정만 이 구성을 수정할 수 있습니다.
     5. 저장을 선택합니다.
   - 계정 페이지 사용:
     1. 탐색 창에서 Accounts(계정)를 선택합니다.
     2. 계정 페이지에서 자동 활성화 기본 설정을 선택합니다.
     3. 자동 활성화 기본 설정 관리 창의 EKS 감사 로그 모니터링에서 새 계정에 대해 활성화를 선택합니다.
     4. 저장을 선택합니다.

API/CLI

- 새 계정에 대해 EKS 감사 로그 모니터링을 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 실행합니다.
- 다음 예시는 조직에 가입한 새 멤버에 대해 EKS 감사 로그 모니터링을 활성화하는 방법을 보여 줍니다. 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

  계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

멤버 계정에서 EKS 감사 로그 모니터링을 선택적으로 활성화 또는 비활성화

원하는 액세스 방법을 선택하여 조직의 선택적 멤버 계정에 대해 EKS 감사 로그 모니터링을 활성화 또는 비활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.

   계정 페이지의 EKS 감사 로그 모니터링 열에서 멤버 계정 상태를 검토합니다.
3. EKS 감사 로그 모니터링 활성화 또는 비활성화

   EKS 감사 로그 모니터링을 구성할 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다. 보호 계획 편집 드롭다운에서 EKS 감사 로그 모니터링을 선택한 다음 적절한 옵션을 선택합니다.

API/CLI

멤버 계정에 대해 EKS 감사 로그 모니터링을 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.

다음 예시는 단일 멤버 계정에 EKS 감사 로그 모니터링을 활성화하는 방법을 보여줍니다. 비활성화하려면 ENABLED를 DISABLED로 바꿉니다. 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

아마존의 Lambda 보호 GuardDuty

Lambda 보호를 사용하면 AWS 환경에서 AWS Lambda 함수가 간접적으로 호출될 때 잠재적인 보안 위협을 식별할 수 있습니다. Lambda Protection을 활성화하면 VPC 네트워킹을 사용하지 않는 로그를 포함하여 계정에 대한 모든 Lambda VPC 흐름 로그 함수에서 시작하여 Lambda 함수가 호출될 때 생성되는 Lambda 네트워크 활동 로그의 모니터링을 GuardDuty 시작합니다. Lambda 함수에 잠재적으로 악의적인 코드가 있음을 나타내는 의심스러운 네트워크 트래픽을 GuardDuty 식별하면 탐지 결과가 생성됩니다. GuardDuty

> **Note**
>
> Lambda 네트워크 활동 모니터링에는 Lambda@Edge 함수에 대한 로그는 포함되지 않습니다.

언제든지 모든 계정 또는 AWS 리전사용 가능한 계정에 대해 Lambda 보호를 구성할 수 있습니다. 기본적으로 기존 GuardDuty 계정은 30일 평가 기간으로 Lambda Protection을 활성화할 수 있습니다. 새 GuardDuty 계정의 경우 Lambda Protection이 이미 활성화되어 있으며 30일 평가 기간에 포함되어 있습니다. 사용량 통계에 대한 자세한 내용은 비용 추정 섹션을 참조하세요.

GuardDuty Lambda 함수를 호출하여 생성된 네트워크 활동 로그를 모니터링합니다. 현재 Lambda 네트워크 활동 모니터링에는 VPC 네트워킹을 사용하지 않는 로그를 포함하여 계정에 대한 모든 Lambda 함수의 Amazon VPC 흐름 로그가 포함되고, Lambda 함수 호출을 통해 생성된 DNS 쿼리 데이터와 같은 다른 네트워크 활동으로의 확장을 포함하여 변경될 수 있습니다. 다른 형태의 네트워크 활동 모니터링으로 확장하면 Lambda Protection을 위해 처리할 데이터의 양이 증가할 GuardDuty 것입니다. 이는 Lambda 보호 사용에 따른 비용에 직접적인 영향을 미칩니다. 추가 네트워크 활동 로그의 모니터링을 GuardDuty 시작할 때마다 릴리스되기 최소 30일 전에 Lambda Protection을 활성화한 계정에 알림을 제공합니다.

Lambda 보호의 기능

Lambda 네트워크 활동 모니터링

Lambda Protection을 활성화하면 계정에 연결된 Lambda 함수가 호출될 때 생성되는 Lambda 네트워크 활동 로그를 GuardDuty 모니터링합니다. 이를 통해 Lambda 함수에 대한 잠재적 보안 위협을 탐지할 수 있습니다. GuardDuty VPC 네트워킹을 사용하지 않는 함수를 포함하여 모든 Lambda 함수의 VPC 흐름 로그를 모니터링합니다. VPC 네트워킹을 사용하도록 구성된 Lambda 함수의 경우, Lambda에서 생성한 ENI (엘라스틱 네트워크 인터페이스) 에 대한 VPC 흐름 로그를 활성화할 필요가 없습니

다. GuardDuty GuardDuty 검색 결과를 생성하기 위해 처리된 Lambda 네트워크 활동 로그 데이터 양(GB) 에 대한 요금만 청구합니다. GuardDuty 스마트 필터를 적용하고 위협 탐지와 관련된 Lambda 네트워크 활동 로그의 하위 집합을 분석하여 비용을 최적화합니다. 요금에 대한 자세한 내용은 Amazon GuardDuty 요금을 참조하십시오.

GuardDuty Lambda 네트워크 활동 로그 (VPC 및 비 VPC 흐름 로그 포함) 를 관리하거나 계정에서 액세스할 수 있게 만들지 않습니다.

Lambda 보호 구성

독립형 계정에 대한 Lambda 보호 구성

연결된 계정의 AWS Organizations경우 다음 섹션에 설명된 대로 GuardDuty 콘솔 또는 API 지침을 통해 이 프로세스를 자동화할 수 있습니다.

선호하는 액세스 방법을 선택하여 독립형 계정에 대해 Lambda 보호를 활성화 또는 비활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 Lambda 보호를 선택합니다.
3. Lambda 보호 페이지에는 계정의 현재 상태가 표시됩니다. 활성화 또는 비활성화를 선택하여 언제든 기능을 활성화 또는 비활성화할 수 있습니다.
4. 저장을 선택합니다.

API/CLI

리전 탐지기 ID를 사용하고 `features` 객체 `name`을 `LAMBDA_NETWORK_LOGS`으로, `status`를 `ENABLED` 또는 `DISABLED` 상태로 설정하여 전달해 updateDetector API를 실행합니다.

다음 명령을 실행하여 Lambda 네트워크 활동 모니터링을 활성화하거나 비활성화할 수도 있습니다. AWS CLI 유효한 *`### ID`*를 사용해야 합니다.

> **Note**
>
> 다음 예시 코드는 Lambda 네트워크 활동 모니터링을 활성화합니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

다중 계정 환경에서 Lambda 보호 구성

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만 조직의 구성원 계정에 대해 Lambda Protection을 활성화하거나 비활성화할 수 있습니다. GuardDuty 멤버 계정은 자신의 계정에서 이 구성을 수정할 수 없습니다. 위임된 GuardDuty 관리자 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 위임된 GuardDuty 관리자 계정은 조직에 가입할 때 모든 새 계정에 대해 Lambda 네트워크 활동 모니터링을 자동으로 활성화하도록 선택할 수 있습니다. 다중 계정 환경에 대한 자세한 내용은 GuardDutyAmazon에서의 다중 계정 관리를 참조하십시오.

위임된 관리자 계정을 위한 Lambda 보호 구성 GuardDuty

선호하는 액세스 방법을 선택하여 위임된 관리자 계정에 대한 GuardDuty Lambda 네트워크 활동 모니터링을 활성화하거나 비활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   관리 계정 보안 인증 정보를 사용해야 합니다.
2. 탐색 창의 설정 아래에서 Lambda 보호를 선택합니다.
3. Lambda 보호 페이지에서 편집을 선택합니다.
4. 다음 중 하나를 수행하십시오.

   모든 계정에 대해 활성화 사용

   - 모든 계정에 대해 활성화를 선택합니다. 그러면 조직에 가입한 새 GuardDuty 계정을 포함하여 AWS 조직의 모든 활성 계정에 대한 보호 계획이 활성화됩니다.
   - 저장을 선택합니다.

수동으로 계정 구성 사용

- 위임된 GuardDuty 관리자 계정 계정에만 보호 계획을 활성화하려면 계정 수동 구성을 선택합니다.
- 위임된 GuardDuty 관리자 계정 (이 계정) 섹션에서 활성화를 선택합니다.
- 저장을 선택합니다.

API/CLI

리전 탐지기 ID를 사용하고 `features` 객체 `name`을 `LAMBDA_NETWORK_LOGS`으로, `status`를 `ENABLED` 또는 `DISABLED` 상태로 설정하여 전달해 updateDetector API를 실행합니다.

다음 명령을 실행하여 Lambda 네트워크 활동 모니터링을 활성화하거나 비활성화할 수 있습니다. AWS CLI *### GuardDuty ### ### ### ### ID# #### ###.*

> **Note**
>
> 다음 예시 코드는 Lambda 네트워크 활동 모니터링을 활성화합니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

모든 멤버 계정에 대해 Lambda 네트워크 활동 모니터링 자동 활성화

원하는 액세스 방법을 선택하여 모든 멤버 계정에 대해 Lambda 네트워크 활동 모니터링 기능을 활성화합니다. 여기에는 기존 멤버 계정과 조직에 새로 가입한 계정이 포함됩니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.

2. 다음 중 하나를 수행하십시오.

   Lambda 보호 사용

   1. 탐색 창에서 Lambda 보호를 선택합니다.
   2. 모든 계정에 대해 활성화를 선택합니다. 이 작업을 통해 조직의 기존 계정과 새 계정 모두에 대해 Lambda 네트워크 활동 모니터링이 자동으로 활성화됩니다.
   3. 저장을 선택합니다.

   > **Note**
   >
   > 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

   계정 페이지 사용

   1. 탐색 창에서 Accounts(계정)를 선택합니다.
   2. 계정 페이지에서 초대 기준으로 계정 추가 전에 자동 활성화 기본 설정을 선택합니다.
   3. 자동 활성화 기본 설정 관리 창의 Lambda 네트워크 활동 모니터링에서 모든 계정에 대해 활성화를 선택합니다.

   > **Note**
   >
   > 기본적으로 이 작업을 수행하면 새 구성원 계정에 GuardDuty 대한 자동 활성화 옵션이 자동으로 설정됩니다.

   4. 저장을 선택합니다.

   모든 계정에 대해 활성화 옵션을 사용할 수 없는 경우 멤버 계정에 대해 선택적으로 Lambda 네트워크 활동 모니터링 활성화 또는 비활성화 섹션을 참조하세요.

API/CLI

- 멤버 계정에 대해 Lambda 네트워크 활동 모니터링을 선택적으로 활성화 또는 비활성화하려면 자체 `### ID`를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.

- 다음 예시는 단일 멤버 계정에 Lambda 네트워크 활동 모니터링을 활성화하는 방법을 보여줍니다. 멤버 계정을 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

  사용자 계정과 현재 지역에 detectorId 맞는 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

모든 기존 활성 멤버 계정에 대해 Lambda 네트워크 활동 모니터링 활성화

원하는 액세스 방법을 선택하여 조직의 모든 기존 활성 멤버 계정에 대해 Lambda 네트워크 활동 모니터링을 활성화합니다.

Console

모든 기존 활성 멤버 계정에 대해 Lambda 네트워크 활동 모니터링 구성

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 Lambda 보호를 선택합니다.
3. Lambda 보호 페이지에서 구성의 현재 상태를 볼 수 있습니다. 활성 멤버 계정 섹션에서 작업을 선택합니다.
4. 작업 드롭다운 메뉴에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다.
5. 확인을 선택합니다.

API/CLI

- 멤버 계정에 대해 Lambda 네트워크 활동 모니터링을 선택적으로 활성화 또는 비활성화하려면 자체 ### ID를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.

- 다음 예시는 단일 멤버 계정에 Lambda 네트워크 활동 모니터링을 활성화하는 방법을 보여줍니다. 멤버 계정을 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

  계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

새 멤버 계정에 대해 Lambda 네트워크 활동 모니터링 자동 활성화

원하는 액세스 방법을 선택하여 조직에 가입하는 새 계정에 대해 Lambda 네트워크 활동 모니터링을 활성화합니다.

Console

위임된 GuardDuty 관리자 계정은 Lambda 보호 또는 계정 페이지를 사용하여 조직의 새 구성원 계정에 대해 Lambda 네트워크 활동 모니터링을 활성화할 수 있습니다.

새 멤버 계정에 대해 Lambda 네트워크 활동 모니터링 자동 활성화

1. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.

2. 다음 중 하나를 수행하십시오.
   - Lambda 보호 사용:
     1. 탐색 창에서 Lambda 보호를 선택합니다.
     2. Lambda 보호 페이지에서 편집을 선택합니다.
     3. 수동으로 계정 구성을 선택합니다.
     4. 새 멤버 계정에 대해 자동으로 활성화를 선택합니다. 이 단계를 통해 새 계정이 조직에 가입할 때마다 해당 계정에 대해 Lambda 보호가 자동으로 활성화됩니다. 조직이 위임한 GuardDuty 관리자 계정만 이 구성을 수정할 수 있습니다.

5. 저장을 선택합니다.

- 계정 페이지 사용:

1. 탐색 창에서 Accounts(계정)를 선택합니다.
2. 계정 페이지에서 자동 활성화 기본 설정을 선택합니다.
3. 자동 활성화 기본 설정 관리 창의 Lambda 네트워크 활동 모니터링에서 새 계정에 대해 활성화를 선택합니다.
4. 저장을 선택합니다.

API/CLI

- 새 멤버 계정에 대해 Lambda 네트워크 활동 모니터링을 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 간접적으로 호출합니다.
- 다음 예시는 단일 멤버 계정에 Lambda 네트워크 활동 모니터링을 활성화하는 방법을 보여줍니다. 비활성화하려면 멤버 계정에 대해 선택적으로 Lambda 네트워크 활동 모니터링 활성화 또는 비활성화 섹션을 참조하세요. 조직에 가입하는 모든 새 계정에 대해 활성화하지 않으려면 `AutoEnable`을 `NONE`으로 설정합니다.

  계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

  공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.
- 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

멤버 계정에 대해 선택적으로 Lambda 네트워크 활동 모니터링 활성화 또는 비활성화

원하는 액세스 방법을 선택하여 멤버 계정에 대해 Lambda 네트워크 활동 모니터링을 선택적으로 활성화 또는 비활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.

2. 탐색 창의 설정 아래에서 계정을 선택합니다.

   계정 페이지에서 Lambda 네트워크 활동 모니터링 열을 검토합니다. Lambda 네트워크 활동 모니터링의 활성화 여부를 나타냅니다.-

3. Lambda 보호를 구성할 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다.
4. 보호 계획 편집 드롭다운 메뉴에서 Lambda 네트워크 활동 모니터링을 선택한 다음 해당되는 작업을 선택합니다.

API/CLI

자체 *### ID*를 사용하여 updateMemberDetectors API를 간접적으로 호출합니다.

다음 예시는 단일 멤버 계정에 Lambda 네트워크 활동 모니터링을 활성화하는 방법을 보여줍니다. 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

Amazon의 멀웨어 보호 GuardDuty

맬웨어 보호는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 컨테이너 워크로드에 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨을 스캔하여 맬웨어의 잠재적 존재를 탐지하는 데 도움이 됩니다. 맬웨어 보호는 스캔 시 특정 Amazon EC2 인스턴스 및 컨테이너 워크로드를 포함 또는 제외할지 결정할 수 있는 검사 옵션을 제공합니다. 또한 Amazon EC2 인스턴스 또는 컨테이너 워크로드에 연결된 Amazon EBS 볼륨의 스냅샷을 계정에 보관하는 옵션도 제공합니다. GuardDuty 스냅샷은 맬웨어가 발견되고 맬웨어 보호 결과가 생성되는 경우에만 보관됩니다.

멀웨어 보호는 Amazon EC2 인스턴스 및 컨테이너 워크로드에서 잠재적으로 악의적인 활동을 탐지하기 위한 두 가지 유형의 스캔, GuardDuty 즉 시작 멀웨어 스캔과 온디맨드 멀웨어 스캔을 제공합니다. 다음 표에서는 두 스캔 유형 사이의 비교를 보여줍니다.

Factor	GuardDuty-시작된 멀웨어 스캔	온디맨드 맬웨어 스캔
스캔 간접 호출 방법	GuardDuty시작된 멀웨어 스캔을 활성화하면 Amazon EC2 인스턴스 또는 컨테이너 GuardDuty 워크로드에 맬웨어가 존재할 가능성이 있음을 나타내는 검색 결과가 GuardDuty 생성될 때마다 잠재적으로 영향을 받을 수 있는 리소스에 연결된 Amazon EBS 볼륨에서 에이전트 없는 멀웨어 스캔이 자동으로 시작됩니다. 자세한 정보는 GuardDuty-멀웨어 검사 시작을 참조하세요.	Amazon EC2 인스턴스 또는 컨테이너 워크로드와 연결된 Amazon 리소스 이름(ARN)을 제공하여 온디맨드 맬웨어 스캔을 시작할 수 있습니다. 리소스에 대한 검색 결과가 생성되지 않은 경우에도 온디맨드 맬웨어 검사를 시작할 수 있습니다. GuardDuty 자세한 정보는 온디맨드 맬웨어 스캔을 참조하세요.
구성 필요	GuardDuty시작된 악성코드 검사를 사용하려면 계정에서 해당 검사를 활성화해야 합니다. 자세한 정보는 시작한 멀웨어 GuardDuty 검사 구성을 참조하세요.	계정이 활성화되어 있어야 GuardDuty 합니다. 온디맨드 멀웨어 검사를 사용하려면 기능 수준에서 구성할 필요가 없습니다.

Factor	GuardDuty-시작된 멀웨어 스캔	온디맨드 맬웨어 스캔
새 스캔 시작까지의 대기 시간	둘 중 하나를 GuardDuty 생성할 때마다 GuardDuty시작된 멀웨어 스캔을 호출하는 결과 24시간에 한 번만 맬웨어 검사가 자동으로 시작됩니다.	이전 검사 시작 시간으로부터 1시간 후 언제든지 동일한 리소스에서 온디맨드 맬웨어 검사를 시작할 수 있습니다.
30일 무료 평가판 사용 가능성	계정에서 GuardDuty '시작 멀웨어 스캔'을 처음으로 활성화하면 30일 무료 평가 기간*을 사용할 수 있습니다.	신규 또는 기존 계정에 대한 온디맨드 멀웨어 스캔에는 무료 평가 기간*이 없습니다. GuardDuty
스캔 옵션	멀웨어 검사를 GuardDuty 시작하도록 구성한 후에는 멀웨어 보호를 통해 검사하거나 건너뛸 리소스를 선택할 수도 있습니다. 맬웨어 보호는 스캔에서 제외하기로 선택한 리소스에 대해 자동 스캔을 시작하지 않습니다.	온디맨드 멀웨어 검사는 글로벌 태그 —를 지원합니다. `GuardDutyExcluded` 사용자 정의 태그를 사용하는 스캔 옵션리소스 ARN을 수동으로 제공하므로 온디맨드 멀웨어 스캔에는 적용되지 않습니다.

*EBS 볼륨 스냅샷을 생성하고 스냅샷을 유지하는 경우 사용 비용이 발생합니다. 스냅샷을 보존하도록 계정을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 스냅샷 보존

멀웨어 방지는 선택적 개선 GuardDuty 사항이며 리소스 성능에 영향을 미치지 않도록 설계되었습니다. 멀웨어 방지가 내에서 GuardDuty 작동하는 방식에 대한 자세한 내용은 을 참조하십시오맬웨어 보호의 기능. 다양한 멀웨어 보호 기능에 대한 자세한 내용은 AWS 리전을 참조하십시오리전 및 엔드포인트.

> **Note**
>
> GuardDuty 멀웨어 보호 기능은 Amazon EKS 또는 Amazon ECS와 함께 Fargate를 지원하지 않습니다.

맬웨어 보호의 기능

Elastic Block Storage(EBS) 볼륨

이 섹션에서는 GuardDuty 시작된 멀웨어 스캔과 온디맨드 멀웨어 스캔을 포함한 멀웨어 보호가 Amazon EC2 인스턴스 및 컨테이너 워크로드와 관련된 Amazon EBS 볼륨을 스캔하는 방법을 설명합니다. 계속하기 전에 다음 사용자 지정을 고려하세요.

- 스캔 옵션 - 맬웨어 보호는 스캔 프로세스에서 Amazon EC2 인스턴스 및 Amazon EBS 볼륨을 포함하거나 제외하도록 태그를 지정하는 기능을 제공합니다. GuardDuty시작된 멀웨어 스캔만 사용자 정의 태그가 있는 스캔 옵션을 지원합니다. GuardDuty시작 악성코드 검사와 온디맨드 악성코드 검사 모두 글로벌 태그를 지원합니다. `GuardDutyExcluded` 자세한 정보는 사용자 정의 태그를 사용하는 스캔 옵션을 참조하세요.
- 스냅샷 보존 — 멀웨어 보호는 Amazon EBS 볼륨의 스냅샷을 계정에 보관하는 옵션을 제공합니다. AWS 이 옵션은 기본적으로 꺼져 있습니다. GuardDuty 시작된 악성코드 검사와 온디맨드 악성코드 검사 모두에 대해 스냅샷 보존을 선택할 수 있습니다. 자세한 정보는 스냅샷 보존을 참조하세요.

Amazon EC2 인스턴스 또는 컨테이너 워크로드에 맬웨어가 존재할 가능성을 나타내는 검색 결과가 GuardDuty 생성되고 Malware Protection에서 시작 검사 유형을 GuardDuty 활성화한 경우 검사 옵션에 따라 -initiated 맬웨어 검사가 호출될 수 있습니다. GuardDuty

Amazon EC2 인스턴스와 연결된 Amazon EBS 볼륨에서 온디맨드 맬웨어 스캔을 시작하려면 Amazon EC2 인스턴스의 Amazon 리소스 이름(ARN)을 제공하세요.

온디맨드 멀웨어 스캔 또는 자동으로 GuardDuty 시작되는 멀웨어 스캔에 대한 응답으로, 잠재적으로 영향을 받을 수 있는 리소스에 연결된 관련 EBS 볼륨의 스냅샷을 GuardDuty 생성하여 해당 볼륨과 공유합니다GuardDuty 서비스 계정. 이 스냅샷에서 서비스 계정에 암호화된 복제 GuardDuty EBS 볼륨을 생성합니다.

스캔이 완료되면 암호화된 복제본 EBS 볼륨과 EBS 볼륨의 스냅샷을 GuardDuty 삭제합니다. 멀웨어가 발견되고 스냅샷 보존 설정을 켜도 EBS 볼륨의 스냅샷은 삭제되지 않고 계정에 자동으로 보존됩니다. AWS 맬웨어가 없는 경우 스냅샷 보존 설정과 무관하게 EBS 볼륨의 스냅샷이 유지되지 않습니다. 기본적으로 스냅샷 보존 설정은 해제되어 있습니다. 스냅샷 비용 및 보존에 대한 자세한 내용은 Amazon EBS 요금을 참조하세요.

GuardDuty 서비스 계정의 각 복제 EBS 볼륨을 최대 55시간 동안 보관합니다. 서비스가 중단되거나 복제 EBS 볼륨 및 해당 멀웨어 스캔에 장애가 발생하는 경우 해당 EBS 볼륨을 7일 이상 보존하지 않습니

다. GuardDuty 볼륨 보존 기간 연장은 중단이나 장애를 분류하고 해결하기 위한 것입니다. GuardDuty 멀웨어 보호 기능은 장애 또는 장애가 해결된 후 또는 연장된 보존 기간이 경과하면 서비스 계정에서 복제본 EBS 볼륨을 삭제합니다.

멀웨어 스캔을 지원하는 Amazon EBS 볼륨

멀웨어 보호 기능을 GuardDuty 지원하는 모든 AWS 리전 곳에서 암호화되지 않았거나 암호화된 Amazon EBS 볼륨을 스캔할 수 있습니다. Amazon EBS 볼륨은 둘 중 하나 AWS 관리형 키또는 고객 관리 키로 암호화될 수 있습니다. 현재 일부는 Amazon EBS 볼륨을 암호화하는 두 가지 방법을 모두 AWS 리전 지원하는 반면 다른 일부는 고객 관리 키만 지원합니다.

이 기능이 아직 지원되지 않는 자세한 내용은 을 참조하십시오. China Regions

다음 목록은 Amazon EBS 볼륨의 암호화 여부를 GuardDuty 사용하는 키를 설명합니다.

- 암호화되지 않았거나 암호화된 Amazon EBS GuardDuty 볼륨은 자체 키를 사용하여 Amazon EBS 복제 볼륨을 암호화합니다. AWS 관리형 키

  계정이 AWS 관리형 키 EBS용 기본값으로 암호화된 Amazon EBS 볼륨의 스캔을 지원하지 AWS 리전 않는 계정에 속하는 경우 를 참조하십시오. Amazon EBS 볼륨의 기본 AWS KMS 키 ID 수정
- 고객 관리 키로 암호화된 Amazon EBS 볼륨 — 동일한 키를 GuardDuty 사용하여 복제 EBS 볼륨을 암호화합니다.

멀웨어 보호는 as를 사용한 `productCode` Amazon EC2 인스턴스 스캔을 지원하지 않습니다. `marketplace` 이러한 Amazon EC2 인스턴스에 대해 맬웨어 스캔이 시작되면 스캔을 건너뛰게 됩니다. 자세한 설명은 맬웨어 스캔 중에 리소스를 건너뛴 이유에서 `UNSUPPORTED_PRODUCT_CODE_TYPE` 섹션을 참조하십시오.

Amazon EBS 볼륨의 기본 AWS KMS 키 ID 수정

기본적으로 암호화를 로 설정하고 KMS 키 ID를 지정하지 않고 CreateVolumeAPI를 호출하면 EBS 암호화를 위한 기본 AWS KMS 키로 암호화되는 Amazon EBS 볼륨이 생성됩니다. `true` 하지만 암호화 키가 명시적으로 제공되지 않은 경우 ModifyEbsDefaultKmsKeyIdAPI를 호출하거나 해당 명령을 사용하여 기본 키를 수정할 수 있습니다. AWS CLI

EBS 기본 키 ID를 수정하려면 IAM 정책 `ec2:modifyEbsDefaultKmsKeyId`에 다음 필수 권한을 추가합니다. 암호화하도록 선택하지만 관련 KMS 키 ID를 지정하지 않은 새로 생성된 모든 Amazon EBS 볼륨은 기본 키 ID를 사용합니다. 다음 방법 중 하나를 사용하여 EBS 기본 키 ID를 업데이트하십시오.

Amazon EBS 볼륨의 기본 KMS 키 ID 수정

다음 중 하나를 수행하십시오.

- API 사용 — API를 사용할 수 있습니다. ModifyEbsDefaultKmsKeyId 볼륨의 암호화 상태를 확인하는 방법에 대한 자세한 내용은 Amazon EBS 볼륨 생성을 참조하십시오.
- AWS CLI 명령 사용 — 다음 예에서는 KMS 키 ID를 제공하지 않는 경우 Amazon EBS 볼륨을 암호화하는 기본 KMS 키 ID를 수정합니다. 지역을 KM 키 ID의 지역으로 바꿔야 합니다 AWS 리전 .

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

위의 명령은 다음 출력과 유사한 출력을 생성합니다.

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

자세한 내용은 modify-ebs-default-kms-key-id를 참조하십시오.

맬웨어 보호의 사용자 지정

이 단원에서는 맬웨어 스캔이 호출될 때 온디맨드로 시작되거나 온디맨드를 통해 시작될 때 Amazon EC2 인스턴스 또는 컨테이너 워크로드에 대한 검사 옵션을 사용자 지정하는 방법을 설명합니다. GuardDuty

일반 설정

스냅샷 보존

GuardDuty EBS 볼륨의 스냅샷을 계정에 보관할 수 있는 옵션을 제공합니다. AWS 기본적으로 스냅샷 보존 설정은 해제되어 있습니다. 스캔이 시작되기 전에 이를 설정한 경우에만 스냅샷이 유지됩니다.

스캔이 시작되면 EBS 볼륨의 스냅샷을 기반으로 복제 EBS 볼륨을 GuardDuty 생성합니다. 스캔이 완료되고 계정의 스냅샷 보존이 이미 설정되어 있으면 맬웨어가 발견되어 맬웨어 보호 결과 유형이 생성된 경우에만 EBS 볼륨의 스냅샷이 유지됩니다. 스냅샷 보존 설정을 켰는지 여부에 관계없이 멀웨어가 탐지되지 않으면 EBS 볼륨의 스냅샷이 GuardDuty 자동으로 삭제됩니다.

스냅샷 사용 비용

맬웨어 스캔 중에 Amazon EBS 볼륨의 스냅샷이 GuardDuty 생성되므로 이 단계와 관련된 사용 비용이 발생합니다. 계정에서 스냅샷 보존을 설정한 경우 맬웨어가 발견되고 스냅샷이 유지되면 이에 따른 사용 비용이 발생합니다. 스냅샷 비용 및 보존에 대한 내용은 Amazon EBS 요금을 참조하세요.

선호하는 액세스 방법을 선택하여 스냅샷 보존을 설정합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창의 보호 플랜에서 맬웨어 보호를 선택합니다.
3. 콘솔 하단 섹션에서 일반 설정을 선택합니다. 스냅샷을 유지하려면 스냅샷 보존을 설정합니다.

API/CLI

1. UpdateMalwareScanSettings를 실행하여 스냅샷 보존 설정의 현재 구성을 업데이트하십시오.
2. 또는 GuardDuty 멀웨어 보호에서 탐지 결과를 생성할 때 다음 AWS CLI 명령을 실행하여 스냅샷을 자동으로 보존할 수 있습니다.

   *detector-id*를 유효한 자체 detectorId로 바꿔야 합니다.
3. 사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId

   ```
   aws guardduty update-malware-scan-settings --detector-
   id 60b87779336485625554d637e0e4bb3b2 --ebs-snapshot-preservation
    "RETENTION_WITH_FINDING"
   ```
4. 스냅샷 보존을 해제하려면 RETENTION_WITH_FINDING을 NO_RETENTION으로 바꿉니다.

사용자 정의 태그를 사용하는 스캔 옵션

또한 GuardDuty 시작된 멀웨어 스캔을 사용하면 Amazon EC2 인스턴스 및 Amazon EBS 볼륨을 검사 및 위협 탐지 프로세스에서 포함하거나 제외하도록 태그를 지정할 수도 있습니다. 포함 또는 제외 태그 목록에서 태그를 편집하여 GuardDuty 시작된 각 맬웨어 검사를 사용자 지정할 수 있습니다. 각 목록에는 최대 50개의 태그가 포함될 수 있습니다.

EC2 리소스에 연결된 사용자 정의 태그가 아직 없는 경우 Linux 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅 또는 Windows 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅을 참조하세요.

> **Note**
>
> 온디맨드 맬웨어 스캔은 사용자 정의 태그를 사용하는 스캔 옵션을 지원하지 않습니다. 글로벌 `GuardDutyExcluded` 태그를 지원합니다.

맬웨어 스캔에서 EC2 인스턴스 제외

스캔 프로세스 중에 Amazon EC2 인스턴스 또는 Amazon EBS 볼륨을 제외하려는 경우, 모든 Amazon EC2 인스턴스 또는 Amazon EBS `true` 볼륨에 대해 `GuardDutyExcluded` 태그를 로 설정하고 스캔하지 않을 수 있습니다. GuardDuty `GuardDutyExcluded` 태그에 대한 자세한 내용은 맬웨어 보호에 대한 서비스 연결 역할 권한 섹션을 참조하세요. 또한 Amazon EC2 인스턴스 태그를 제외 목록에 추가할 수 있습니다. 제외 태그 목록에 여러 태그를 추가하면 이러한 태그 중 하나 이상을 포함하는 모든 Amazon EC2 인스턴스가 맬웨어 스캔 프로세스에서 제외됩니다.

선호하는 액세스 방법을 선택하여 Amazon EC2 인스턴스와 연결된 태그를 제외 목록에 추가합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty
2. 탐색 창의 보호 플랜에서 맬웨어 보호를 선택합니다.
3. 포함/제외 태그 섹션을 확장합니다. 태그 추가를 선택합니다.
4. 제외 태그를 선택한 다음 확인을 선택합니다.
5. 제외하려는 태그의 **`Key`** 및 **`Value`** 쌍을 지정합니다. **`Value`** 입력은 선택 사항입니다. 태그를 모두 추가한 후 저장을 선택합니다.

> **Important**
>
> 태그 키와 값은 대/소문자를 구분합니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 태그 제한 또는 Windows 인스턴스용 Amazon EC2 사용 설명서의 태그 제한을 참조하세요.

키 값이 제공되지 않고 EC2 인스턴스에 지정된 키 태그가 지정된 경우, 이 EC2 인스턴스는 태그에 할당된 값에 관계없이 GuardDuty -initiated 멀웨어 스캔 프로세스에서 제외됩니다.

API/CLI

- EC2 인스턴스 또는 컨테이너 워크로드를 스캔 프로세스에서 제외하여 맬웨어 스캔 설정을 업데이트합니다.

  다음 AWS CLI 예제 명령은 제외 태그 목록에 새 태그를 추가합니다. 예시 *detector-id*를 유효한 자체 `detectorId`로 바꿔야 합니다.

  `MapEquals`는 `Key/Value` 쌍의 목록입니다.

  계정과 현재 지역의 태그를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> 태그 키와 값은 대/소문자를 구분합니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 태그 제한 또는 Windows 인스턴스용 Amazon EC2 사용 설명서의 태그 제한을 참조하세요.

맬웨어 스캔에 EC2 인스턴스 포함

EC2 인스턴스를 스캔하려면 포함 목록에 해당 태그를 추가합니다. 포함 태그 목록에 태그를 추가하면 추가된 태그가 하나도 포함되지 않은 EC2 인스턴스는 맬웨어 스캔에서 제외됩니다. 포함 태그 목록에 여러 태그를 추가한 경우 해당 태그 중 하나 이상이 포함된 EC2 인스턴스가 맬웨어 스캔에 포함됩니다. 스캔 프로세스 도중 EC2 인스턴스를 건너뛰는 경우가 있습니다. 자세한 정보는 맬웨어 스캔 중에 리소스를 건너뛴 이유을 참조하세요.

선호하는 액세스 방법을 선택하여 EC2 인스턴스와 연결된 태그를 포함 목록에 추가합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창의 보호 플랜에서 맬웨어 보호를 선택합니다.
3. 포함/제외 태그 섹션을 확장합니다. 태그 추가를 선택합니다.
4. 포함 태그를 선택한 다음 확인을 선택합니다.
5. 새 포함 태그 추가를 선택하고 포함하려는 태그의 **Key** 및 **Value** 쌍을 지정합니다. **Value** 입력은 선택 사항입니다.

   포함 태그를 모두 추가한 후 저장을 선택합니다.

   키 값이 제공되지 않고 EC2 인스턴스에 지정된 키 태그가 지정된 경우 EC2 인스턴스는 태그의 할당된 값과 관계없이 맬웨어 보호 스캔 프로세스에 포함됩니다.

API/CLI

- 맬웨어 스캔 설정을 업데이트하여 EC2 인스턴스 또는 컨테이너 워크로드를 스캔 프로세스에 포함합니다.

  다음 AWS CLI 예제 명령은 포함 태그 목록에 새 태그를 추가합니다. 예시 *detector-id*를 유효한 자체 `detectorId`로 바꿔야 합니다. *TestKey*예제와 를 EC2 리소스에 연결된 태그의 `Key` 및 `Value` 쌍으로 바꾸십시오. *TestValue*

  `MapEquals`는 `Key/Value` 쌍의 목록입니다.

  계정과 현재 지역의 태그를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> 태그 키와 값은 대/소문자를 구분합니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 태그 제한 또는 Windows 인스턴스용 Amazon EC2 사용 설명서의 태그 제한을 참조하세요.

> **Note**
>
> 새 태그를 감지하는 데 최대 5분이 걸릴 수 있습니다. GuardDuty

언제든지 포함 태그 또는 제외 태그 중 하나를 선택할 수 있지만 둘 다 선택할 수는 없습니다. 태그를 전환하려면 새 태그를 추가할 때 드롭다운 메뉴에서 해당 태그를 선택하고 선택을 확인합니다. 이 작업을 수행하면 현재 태그가 모두 지워집니다.

글로벌 `GuardDutyExcluded` 태그

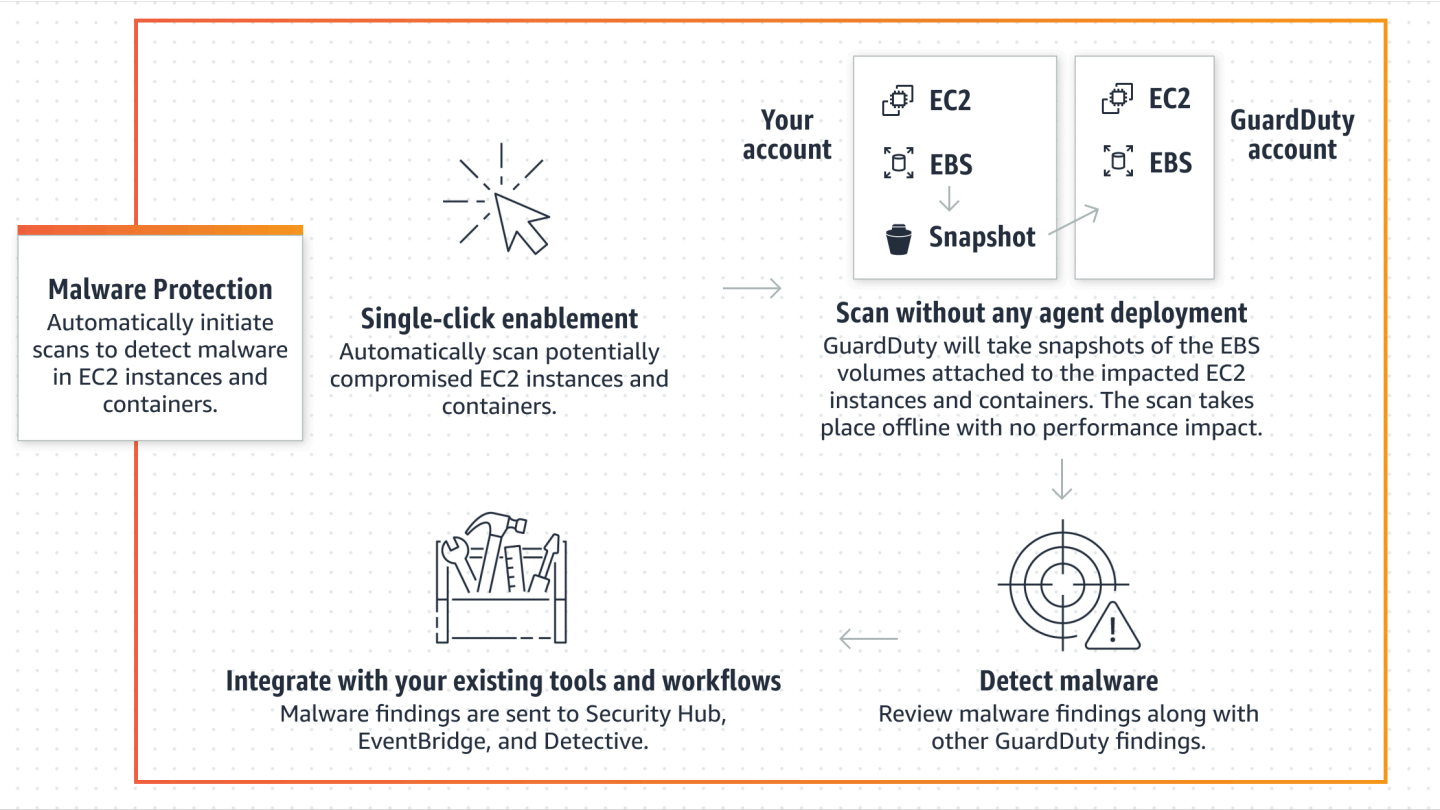
기본적으로 EBS 볼륨의 스냅샷은 `GuardDutyScanId` 태그로 생성됩니다. 이 태그를 제거하면 스냅샷에 액세스할 수 GuardDuty 없으므로 제거하지 마십시오. 맬웨어 보호의 두 스캔 유형 모두 `GuardDutyExcluded` 태그가 `true`로 설정된 Amazon EC2 인스턴스 또는 Amazon EBS 볼륨을 스캔하지 않습니다. 맬웨어 보호에서 이러한 리소스를 스캔하는 경우 스캔 ID가 생성되지만 `EXCLUDED_BY_SCAN_SETTINGS` 이유에 따라 건너뛰게 됩니다. 자세한 정보는 맬웨어 스캔 중에 리소스를 건너뛴 이유을 참조하세요.

GuardDuty-멀웨어 검사 시작

GuardDuty-initiated 맬웨어 스캔을 활성화하면 Amazon EC2 인스턴스 또는 컨테이너 워크로드에 맬웨어가 존재할 가능성을 나타내는 악성 활동을 GuardDuty 탐지하고 GuardDuty 잠재적으로 영향을 받는 Amazon EC2 인스턴스 또는 컨테이너 워크로드에 연결된 Amazon Elastic Block Store (Amazon EBS) 볼륨에서 에이전트 없는 스캔을 GuardDuty 자동으로 시작하여 맬웨어의 존재를 탐지합니다. GuardDuty시작된 멀웨어 스캔을 호출하는 결과 스캔 옵션을 사용하는 경우 스캔하려는 리소스와 연결된 포함 태그를 추가하거나 스캔 프로세스에서 건너뛰려는 리소스와 연결된 제외 태그를 추가할 수 있습니다. 자동 스캔 시작 시에는 항상 스캔 옵션을 고려합니다. 맬웨어 보호에서 맬웨어의 존재를 탐지한 경우에만 EBS 볼륨의 스냅샷을 유지하도록 스냅샷 보존을 설정할 수도 있습니다. 자세한 정보는 맬웨어 보호의 사용자 지정을 참조하세요.

탐지 결과를 GuardDuty 생성하는 각 Amazon EC2 인스턴스 및 컨테이너 워크로드에 대해 자동으로 GuardDuty 시작되는 멀웨어 스캔이 24시간마다 한 번씩 호출됩니다. Amazon EC2 인스턴스 또는 컨테이너 워크로드에 연결된 Amazon EBS 볼륨을 스캔하는 방법에 대한 내용은 맬웨어 보호의 기능 섹션을 참조하세요.

다음 이미지는 시작된 멀웨어 스캔의 작동 방식을 GuardDuty 설명합니다.



멀웨어가 발견되면 생성됩니다. GuardDuty 맬웨어 보호 결과 유형 동일한 리소스에서 멀웨어를 나타내는 검색 결과가 생성되지 GuardDuty 않으면 GuardDuty 시작된 멀웨어 스캔이 실행되지 않습니다. 동일한 리소스에서 온디맨드 맬웨어 스캔을 시작할 수도 있습니다. 자세한 정보는 온디맨드 맬웨어 스캔을 참조하세요.

30일 무료 평가판 기간이 계정에 미치는 영향 GuardDuty

언제든지 모든 계정에 대해 또는 사용 가능한 AWS 리전멀웨어 검사 기능을 켜거나 끌 수 있습니다. GuardDuty

- 처음 (새 GuardDuty 계정) 을 GuardDuty 활성화할 때, GuardDuty 시작된 멀웨어 스캔은 이미 켜져 있으며 30일 무료 평가 기간에 포함됩니다.
- 30일 무료 평가판 기간을 통해 기존 GuardDuty 계정에서 처음으로 GuardDuty 악성코드 검사를 활성화할 수 있습니다.

- 온디맨드 멀웨어 스캔이 일반화되기 전에 멀웨어 보호를 사용하던 기존 GuardDuty 계정이 있고 이 GuardDuty 계정에 대한 가격 책정 모델을 이미 사용하고 있는 경우 AWS 리전, 시작 멀웨어 스캔을 계속 사용하기 GuardDuty 위해 별도의 조치를 취할 필요가 없습니다.

> **Note**
>
> 30일 무료 평가판 기간 중인 경우 Amazon EBS 볼륨 스냅샷 생성과 보존에 따른 사용 비용은 계속 적용됩니다. 자세한 내용은 Amazon EBS 요금을 참조하세요.

GuardDuty시작된 맬웨어 검사를 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오. 시작한 멀웨어 GuardDuty 검사 구성

시작한 멀웨어 GuardDuty 검사 구성

독립 GuardDuty 실행형 계정에 대해 시작된 멀웨어 검사 구성

연결된 계정의 AWS Organizations경우 다음 섹션에 설명된 대로 콘솔 설정을 통해 이 프로세스를 자동화할 수 있습니다.

GuardDuty시작된 멀웨어 검사를 활성화 또는 비활성화하려면

선호하는 액세스 방법을 선택하여 독립 GuardDuty 실행형 계정에 대해 시작 멀웨어 검사를 구성하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창의 보호 플랜에서 맬웨어 보호를 선택합니다.
3. 멀웨어 보호 패널에는 계정에 대해 GuardDuty 시작된 멀웨어 검사의 현재 상태가 나열됩니다. 활성화 또는 비활성화를 선택하여 언제든지 활성화 또는 비활성화할 수 있습니다.
4. 저장을 선택합니다.

API/CLI

- 리전 탐지기 ID를 사용하고 `EbsVolumes`가 `true` 또는 `false`로 설정된 `dataSources` 객체를 전달하여 updateDetector API를 실행합니다.

다음 AWS 명령을 실행하여 명령줄 도구를 사용하여 GuardDuty -initiated 맬웨어 검사를 활성화하거나 비활성화할 수도 있습니다. AWS CLI 유효한 *### ID*를 사용해야 합니다.

> **Note**
>
> 다음 예제 코드는 GuardDuty -initiated 맬웨어 검사를 활성화합니다. 비활성화하려면 `true`를 `false`로 바꿉니다.

사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

다중 GuardDuty 계정 환경에서 시작한 멀웨어 검사 구성

다중 계정 환경에서는 GuardDuty 관리자 계정 계정만 -시작 맬웨어 검사를 구성할 수 있습니다. GuardDuty GuardDuty 관리자 계정 계정은 구성원 계정에 대해 GuardDuty -initiated 맬웨어 검사 사용을 활성화하거나 비활성화할 수 있습니다. 관리자 계정으로 구성원 계정에 대한 악성 코드 검사를 GuardDuty 구성하면 구성원 계정은 관리자 계정 설정을 따르며 콘솔을 통해 이러한 설정을 수정할 수 없습니다. GuardDuty AWS Organizations 지원을 통해 구성원 계정을 관리하는 관리자 계정 계정은 조직의 모든 기존 계정과 새 계정에서 자동으로 GuardDuty 시작된 맬웨어 스캔을 활성화하도록 선택할 수 있습니다. 자세한 정보는 를 통한 GuardDuty 계정 관리 AWS Organizations을 참조하세요.

신뢰할 수 있는 액세스를 설정하여 악성코드 검사를 시작할 수 있도록 합니다 GuardDuty.

GuardDuty 위임된 관리자 계정이 조직의 관리 계정과 동일하지 않은 경우, 관리 계정은 해당 조직에 대해 GuardDuty 시작 멀웨어 검사를 활성화해야 합니다. 이렇게 하면 위임된 관리자 계정을 통해 관리되는 내부 구성원 계정을 만들 수 있습니다. 맬웨어 보호에 대한 서비스 연결 역할 권한 AWS Organizations

> **Note**
>
> 위임된 GuardDuty 관리자 계정을 지정하기 전에 을 참조하십시오. 사용 고려 사항 및 권장 사항

원하는 액세스 방법을 선택하여 위임된 GuardDuty 관리자 계정으로 조직의 구성원 계정에 대해 악성 코드 검사를 GuardDuty 시작한 후 실행하도록 허용하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   로그인하려면 AWS Organizations 조직의 관리 계정을 사용하세요.

2. a. 위임된 GuardDuty 관리자 계정을 지정하지 않은 경우:

      설정 페이지의 위임된 GuardDuty 관리자 계정 아래에 조직의 정책을 관리하도록 지정하려는 12자리 숫자를 **`account ID`** 입력합니다. GuardDuty 위임을 선택합니다.

   b. i. 관리 계정과 다른 위임된 GuardDuty 관리자 계정을 이미 지정한 경우:

      설정 페이지의 위임된 관리자에서 권한 설정을 켭니다. 이 작업을 수행하면 위임된 GuardDuty 관리자 계정이 구성원 계정에 관련 권한을 부여하고 해당 구성원 계정에서 악성코드 스캔을 GuardDuty 시작할 수 있습니다.

      ii. 관리 계정과 동일한 위임된 GuardDuty 관리자 계정을 이미 지정한 경우 해당 구성원 계정에 대해 직접 GuardDuty 시작된 멀웨어 검사를 활성화할 수 있습니다. 자세한 정보는 자동 GuardDuty 활성화된 멀웨어 스캔을 모든 회원 계정에 대해 자동으로 활성화합니다.을 참조하세요.

      > **Tip**
      >
      > 위임된 GuardDuty 관리자 계정이 관리 계정과 다른 경우, 위임된 GuardDuty 관리자 계정에 권한을 제공하여 구성원 계정에 대해 악성 코드 검사를 GuardDuty 시작할 수 있도록 허용해야 합니다.

3. 다른 지역의 구성원 계정에 대해 위임된 GuardDuty 관리자 계정으로 GuardDuty 시작 멀웨어 검사를 활성화하도록 허용하려면 계정을 변경하고 위 단계를 반복하세요 AWS 리전.

API/CLI

1. 관리 계정 보안 인증 정보를 사용하여 다음 명령을 실행합니다.

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (선택 사항) GuardDuty 위임된 관리자 계정이 아닌 관리 계정에 대해 시작 맬웨어 검사를 활성화하려면 관리 계정이 먼저 자신의 계정에 맬웨어 보호에 대한 서비스 연결 역할 권한 명시적으로 맬웨어 검사를 만든 다음 다른 구성원 계정과 마찬가지로 위임된 관리자 계정에서 GuardDuty 시작된 맬웨어 검사를 활성화합니다.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. 현재 선택한 계정에서 위임된 관리자 계정을 지정했습니다. GuardDuty AWS 리전한 지역에서 계정을 위임된 GuardDuty 관리자 계정으로 지정한 경우, 다른 모든 지역에서는 해당 계정이 위임된 GuardDuty 관리자 계정이어야 합니다. 다른 모든 리전에 대해서도 위 단계를 반복합니다.

GuardDuty위임된 관리자 계정에 대한 악성코드 검사 시작 구성 GuardDuty

선호하는 액세스 방법을 선택하여 위임된 관리자 계정에 대해 GuardDuty -시작된 멀웨어 검사를 활성화하거나 비활성화합니다. GuardDuty

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   관리 계정 보안 인증 정보를 사용해야 합니다.
2. 탐색 창에서 맬웨어 보호를 선택합니다.
3. 멀웨어 보호 페이지에서 실행 멀웨어 검사 GuardDuty 옆의 편집을 선택합니다.
4. 다음 중 하나를 수행하십시오.

   모든 계정에 대해 활성화 사용

   - 모든 계정에 대해 활성화를 선택합니다. 그러면 조직에 가입한 새 GuardDuty 계정을 포함하여 AWS 조직의 모든 활성 계정에 대한 보호 계획이 활성화됩니다.
   - 저장을 선택합니다.

   수동으로 계정 구성 사용

   - 위임된 GuardDuty 관리자 계정 계정에만 보호 계획을 활성화하려면 계정 수동 구성을 선택합니다.
   - 위임된 GuardDuty 관리자 계정 (이 계정) 섹션에서 활성화를 선택합니다.
   - 저장을 선택합니다.

API/CLI

리전 탐지기 ID를 사용하고 `features` 객체 `name`을 `EBS_MALWARE_PROTECTION`으로, `status`를 `ENABLED` 또는 `DISABLED` 상태로 설정하여 전달해 updateDetector API를 실행합니다.

다음 명령을 실행하여 GuardDuty -initiated 맬웨어 검사를 활성화하거나 비활성화할 수 있습니다. AWS CLI *### GuardDuty ### ### ### ### ID# #### ###.*

> **Note**
>
> 다음 예제 코드는 GuardDuty 시작된 멀웨어 검사를 활성화합니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

자동 GuardDuty 활성화된 멀웨어 스캔을 모든 회원 계정에 대해 자동으로 활성화합니다.

원하는 액세스 방법을 선택하여 모든 회원 계정에 대해 GuardDuty -initiated 맬웨어 검사 기능을 활성화하십시오. 여기에는 기존 멤버 계정과 조직에 새로 가입한 계정이 포함됩니다.

Console

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 다음 중 하나를 수행하십시오.

   맬웨어 보호 페이지 사용

   1. 탐색 창에서 맬웨어 보호를 선택합니다.
   2. 멀웨어 보호 페이지의 GuardDuty시작 멀웨어 검사 섹션에서 편집을 선택합니다.

3. 모든 계정에 대해 활성화를 선택합니다. 이 작업을 수행하면 조직의 기존 계정과 새 계정 모두에 대해 자동으로 GuardDuty 시작된 맬웨어 검사가 활성화됩니다.
4. 저장을 선택합니다.

> **Note**
>
> 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

계정 페이지 사용

1. 탐색 창에서 Accounts(계정)를 선택합니다.
2. 계정 페이지에서 초대 기준으로 계정 추가 전에 자동 활성화 기본 설정을 선택합니다.
3. 자동 활성화 환경설정 관리 창에서 악성코드 스캔이 GuardDuty시작된 모든 계정에 대해 활성화를 선택합니다.
4. 맬웨어 보호 페이지의 GuardDuty시작 맬웨어 검사 섹션에서 편집을 선택합니다.
5. 모든 계정에 대해 활성화를 선택합니다. 이 작업을 수행하면 조직의 기존 계정과 새 계정 모두에 대해 자동으로 GuardDuty 시작된 맬웨어 검사가 활성화됩니다.
6. 저장을 선택합니다.

> **Note**
>
> 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

계정 페이지 사용

1. 탐색 창에서 Accounts(계정)를 선택합니다.
2. 계정 페이지에서 초대 기준으로 계정 추가 전에 자동 활성화 기본 설정을 선택합니다.
3. 자동 활성화 환경설정 관리 창에서 악성코드 스캔이 GuardDuty시작된 모든 계정에 대해 활성화를 선택합니다.
4. 저장을 선택합니다.

모든 계정에 대해 활성화 옵션을 사용할 수 없는 경우 회원 계정에 대한 악성 코드 검사를 선택적으로 활성화 또는 GuardDuty 비활성화합니다. 섹션을 참조하세요.

API/CLI

- *### ### ## ## ### ### ##### ###### ####### GuardDuty ## ### ID# updateMemberDetectors#### API ### ######.*
- 다음 예는 단일 회원 계정에 대해 GuardDuty 시작된 멀웨어 스캔을 활성화하는 방법을 보여줍니다. 멤버 계정을 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

  사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.
- 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

기존의 모든 활성 회원 계정에 대해 GuardDuty 시작된 멀웨어 스캔을 활성화합니다.

원하는 액세스 방법을 선택하여 조직의 모든 기존 활성 구성원 계정에 대해 GuardDuty -initiated 맬웨어 검사를 활성화하십시오.

기존의 모든 활성 구성원 계정에 대해 GuardDuty -시작된 맬웨어 검사를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 맬웨어 보호를 선택합니다.
3. 멀웨어 방지에서는 GuardDuty 시작된 멀웨어 스캔 구성의 현재 상태를 볼 수 있습니다. 활성 멤버 계정 섹션에서 작업을 선택합니다.
4. 작업 드롭다운 메뉴에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다.
5. 저장을 선택합니다.

새 회원 계정에 대해 자동으로 GuardDuty 시작된 멀웨어 검사를 활성화합니다.

구성 GuardDuty 시작 멀웨어 검사를 선택하기 GuardDuty 전에 새로 추가된 구성원 계정을 활성화해야 합니다. 초대를 통해 관리되는 구성원 계정은 해당 계정에 대해 GuardDuty 시작 멀웨어 검사를 수동으로 구성할 수 있습니다. 자세한 정보는 Step 3 - Accept an invitation을 참조하세요.

원하는 액세스 방법을 선택하여 조직에 가입한 새 계정에 대해 GuardDuty -initiated 멀웨어 스캔을 활성화하세요.

Console

위임된 GuardDuty 관리자 계정은 멀웨어 GuardDuty 보호 또는 계정 페이지를 사용하여 조직의 새 구성원 계정에 대해 시작 멀웨어 검사를 활성화할 수 있습니다.

새 회원 계정에 대해 자동으로 GuardDuty 시작된 멀웨어 스캔을 활성화하려면

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 다음 중 하나를 수행하십시오.
   - 맬웨어 보호 페이지 사용:
     1. 탐색 창에서 맬웨어 보호를 선택합니다.
     2. 멀웨어 보호 페이지의 GuardDuty시작 멀웨어 검사에서 편집을 선택합니다.
     3. 수동으로 계정 구성을 선택합니다.
     4. 새 멤버 계정에 대해 자동으로 활성화를 선택합니다. 이 단계를 수행하면 새 계정이 조직에 가입할 때마다 해당 계정에 대해 사용자가 GuardDuty 시작한 맬웨어 검사가 자동으로 활성화됩니다. 조직 위임 GuardDuty 관리자 계정만 이 구성을 수정할 수 있습니다.
     5. 저장을 선택합니다.
   - 계정 페이지 사용:
     1. 탐색 창에서 Accounts(계정)를 선택합니다.
     2. 계정 페이지에서 자동 활성화 기본 설정을 선택합니다.
     3. 자동 활성화 기본 설정 관리 창에서 GuardDuty시작 멀웨어 검사 중인 새 계정에 대해 활성화를 선택합니다.
     4. 저장을 선택합니다.

API/CLI

- *# ### ### ## GuardDuty -initiated ### ### ###### ####### ## ### ID# UpdateOrganizationConfiguration#### API ### ######.*
- 다음 예는 단일 회원 계정에 대해 GuardDuty 시작된 멀웨어 스캔을 활성화하는 방법을 보여줍니다. 비활성화하려면 회원 계정에 대한 악성 코드 검사를 선택적으로 활성화 또는 GuardDuty 비활성화합니다. 섹션을 참조하세요. 조직에 가입하는 모든 새 계정에 대해 활성화하지 않으려면 `AutoEnable`을 `NONE`으로 설정합니다.

  사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
   "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
  ```

  공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.
- 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

회원 계정에 대한 악성 코드 검사를 선택적으로 활성화 또는 GuardDuty 비활성화합니다.

선호하는 액세스 방법을 선택하여 구성원 계정에 대해 실행 멀웨어 GuardDuty 검사를 선택적으로 구성하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.
3. 계정 페이지에서 GuardDuty-initiated 멀웨어 스캔 열에서 회원 계정 상태를 검토하십시오.
4. GuardDuty시작 멀웨어 검사를 구성하려는 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다.
5. 보호 계획 편집 메뉴에서 GuardDuty-시작된 맬웨어 검사에 적합한 옵션을 선택합니다.

API/CLI

GuardDuty ## ### ID# updateMemberDetectors#### API ### ######.

다음 예는 단일 회원 계정에 대해 GuardDuty 시작된 멀웨어 스캔을 활성화하는 방법을 보여줍니다. 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty ## ### ID# #### updateMemberDetectorsAPI ### ######. 다음 예는 단일 회원 계정에 대해 GuardDuty 시작된 멀웨어 스캔을 활성화하는 방법을 보여줍니다. 비활성화하려면 true를 false로 바꿉니다.

사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty초대를 통해 관리하는 조직의 기존 계정에 대해 자동 악성코드 스캔을 활성화합니다.

구성원 계정에서 GuardDuty 멀웨어 보호 서비스 연결 역할 (SLR) 을 생성해야 합니다. 관리자 계정은 에서 관리하지 않는 구성원 계정에서 GuardDuty -initiated 멀웨어 검사 기능을 활성화할 수 없습니다. AWS Organizations

현재 https://console.aws.amazon.com/guardduty/ GuardDuty 콘솔에서 다음 단계를 수행하여 기존 회원 계정에 대해 GuardDuty 시작 멀웨어 검사를 활성화할 수 있습니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   관리자 계정 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.
3. GuardDuty시작된 멀웨어 스캔을 활성화하려는 회원 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다.
4. 작업을 선택합니다.
5. 멤버 연결 해제를 선택합니다.
6. 멤버 계정의 탐색 창에 있는 보호 플랜에서 맬웨어 보호를 선택합니다.
7. GuardDuty'시작 멀웨어 검사 활성화'를 선택합니다. GuardDuty 회원 계정에 대한 SLR을 생성합니다. SLR에 대한 내용은 맬웨어 보호에 대한 서비스 연결 역할 권한 섹션을 참조하세요.
8. 관리자 계정 계정의 탐색 창에서 계정을 선택합니다.
9. 조직에 다시 추가해야 하는 멤버 계정을 선택합니다.
10. 작업을 선택하고 멤버 추가를 선택합니다.

API/CLI

1. 관리자 계정 계정을 사용하여 악성 코드 검사를 GuardDuty 시작하려는 구성원 계정에서 DisassociateMembersAPI를 실행하십시오.
2. 회원 계정을 사용하여 실행된 멀웨어 검사를 UpdateDetector GuardDuty활성화하도록 호출하십시오.

사용자 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. 관리자 계정 계정을 사용하여 CreateMembersAPI를 실행하여 구성원을 조직에 다시 추가합니다.

GuardDuty시작된 멀웨어 스캔을 호출하는 결과

Amazon EC2 인스턴스 또는 컨테이너 워크로드에서 멀웨어를 나타내는 의심스러운 동작이 GuardDuty 감지되면 GuardDuty 시작된 멀웨어 스캔이 호출됩니다.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce(아웃바운드만 해당)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic

- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce(아웃바운드만 해당)
- UnauthorizedAccess:EC2/SSHBruteForce(아웃바운드만 해당)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic

- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

온디맨드 맬웨어 스캔

온디맨드 맬웨어 스캔은 Amazon EC2 인스턴스에 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨에 맬웨어가 있는지 탐지하는 데 도움이 됩니다. 구성이 필요하지 않고 스캔하려는 Amazon EC2 인스턴스의 Amazon 리소스 이름(ARN)을 제공하여 온디맨드 맬웨어 스캔을 시작할 수 있습니다. 콘솔이나 API를 통해 온디맨드 멀웨어 검사를 시작할 수 있습니다. GuardDuty 온디맨드 맬웨어 스캔을 시작하기 전에 원하는 스냅샷 보존 설정을 지정할 수 있습니다. 다음 시나리오는 온디맨드 맬웨어 검사 유형을 사용할 시기를 식별하는 데 도움이 될 수 있습니다. GuardDuty

- GuardDuty시작된 멀웨어 스캔을 활성화하지 않고도 Amazon EC2 인스턴스에서 멀웨어의 존재를 탐지하고자 합니다.
- GuardDuty시작 멀웨어 스캔을 활성화했는데 스캔이 자동으로 호출되었습니다. 생성된 맬웨어 보호 결과 유형에 대한 권장 해결 방법을 따른 후 동일한 리소스에서 스캔을 시작하려는 경우 이전 스캔 시작 시간으로부터 1시간이 경과한 후에 온디맨드 맬웨어 스캔을 시작할 수 있습니다.

  온디맨드 맬웨어 스캔의 경우 이전 맬웨어 스캔이 시작된 시점으로부터 24시간이 경과하지 않아도 됩니다. 동일한 리소스에서 온디맨드 맬웨어 스캔을 시작하려면 1시간이 지나야 합니다. 동일한 EC2 인스턴스에서의 맬웨어 스캔 중복을 방지하려면 동일한 Amazon EC2 인스턴스 다시 스캔 섹션을 참조하세요.

> **Note**
>
> 온디맨드 멀웨어 스캔은 30일 무료 평가 기간에 포함되지 않습니다. GuardDuty 사용 비용은 각 맬웨어 스캔에 대해 스캔한 총 Amazon EBS 볼륨에 적용됩니다. 자세한 내용은 Amazon GuardDuty 요금을 참조하십시오. Amazon EBS 볼륨 스냅샷 비용 및 보존에 대한 자세한 내용은 Amazon EBS 요금을 참조하세요.

온디맨드 맬웨어 스캔 작동 방식

온디맨드 맬웨어 스캔을 사용하면 Amazon EC2 인스턴스를 현재 사용 중인 경우에도 해당 인스턴스의 맬웨어 스캔 요청을 시작할 수 있습니다. 온디맨드 멀웨어 스캔을 시작한 후, 스캔을 위해 Amazon 리소스 이름 (ARN) 이 제공된 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨의 스냅샷을 GuardDuty 생성합니다. 다음으로 GuardDuty 이 스냅샷을 와 공유합니다. GuardDuty 서비스 계정 GuardDuty 서비스 계정의 해당 스냅샷에서 암호화된 복제 EBS 볼륨을 생성합니다. GuardDuty Amazon EBS 볼륨 스캔 방식에 대한 자세한 내용은 Elastic Block Storage(EBS) 볼륨 섹션을 참조하세요.

> **Note**
>
> GuardDuty 온디맨드 멀웨어 스캔을 시작할 point-in-time 때 Amazon EBS 볼륨에 이미 기록된 데이터의 스냅샷을 생성합니다.

맬웨어가 발견되고 스냅샷 보존 설정을 활성화한 경우 EBS 볼륨의 스냅샷은 AWS 계정에 자동으로 보관됩니다. 온디맨드 맬웨어 스캔은 맬웨어 보호 결과 유형을 생성합니다. 맬웨어가 없는 경우 스냅샷 보존 설정과 무관하게 EBS 볼륨의 스냅샷이 삭제됩니다.

기본적으로 EBS 볼륨의 스냅샷은 `GuardDutyScanId` 태그로 생성됩니다. 이 태그를 제거하면 스냅샷에 액세스할 수 없게 GuardDuty 되므로 제거하지 마십시오. 맬웨어 보호의 두 스캔 유형 모두 `GuardDutyExcluded` 태그가 `true`로 설정된 Amazon EC2 인스턴스 또는 Amazon EBS 볼륨을 스캔하지 않습니다. 맬웨어 보호에서 이러한 리소스를 스캔하는 경우 스캔 ID가 생성되지만 `EXCLUDED_BY_SCAN_SETTINGS` 이유에 따라 건너뛰게 됩니다. 자세한 정보는 맬웨어 스캔 중에 리소스를 건너뛴 이유을 참조하세요.

AWS Organizations 서비스 제어 정책 — 액세스 거부

의 서비스 제어 정책 (SCP) 을 사용하여 위임된 GuardDuty 관리자 계정은 권한을 제한하고 계정 소유의 Amazon EC2 인스턴스에 대한 온디맨드 멀웨어 스캔 시작과 같은 작업을 거부할 수 있습니다. AWS Organizations

GuardDuty 멤버 계정으로서 Amazon EC2 인스턴스에 대한 온디맨드 멀웨어 스캔을 시작하면 오류가 발생할 수 있습니다. 관리 계정에 연결하여 멤버 계정에 SCP가 설정된 이유를 이해할 수 있습니다. 자세한 내용은 권한에 대한 SCP 효과를 참조하세요.

온디맨드 맬웨어 스캔 시작하기

GuardDuty 관리자 계정은 계정에 다음과 같은 사전 요구 사항이 설정된 활성 구성원 계정을 대신하여 온디맨드 맬웨어 검사를 시작할 수 있습니다. 독립 실행형 계정 및 활성 멤버 계정은 자체 Amazon EC2 인스턴스에 대한 온디맨드 멀웨어 스캔을 시작할 GuardDuty 수도 있습니다.

필수 조건

- GuardDuty 온디맨드 멀웨어 스캔을 시작하려는 AWS 리전 위치에서 활성화되어 있어야 합니다.
- AWS 관리형 정책: AmazonGuardDutyFullAccess가 IAM 사용자 또는 IAM 역할에 연결되어 있어야 합니다. IAM 사용자 또는 IAM 역할과 연결된 액세스 키와 보안 암호 키가 필요합니다.
- 위임된 GuardDuty 관리자 계정은 활성 구성원 계정을 대신하여 온디맨드 맬웨어 검사를 시작할 수 있습니다.
- 맬웨어 보호에 대한 서비스 연결 역할 권한이 없는 멤버 계정인 경우 계정에 속한 Amazon EC2 인스턴스에서 온디맨드 맬웨어 스캔을 시작하면 맬웨어 보호에 대한 SLR이 자동으로 생성됩니다.

> **Important**
>
> GuardDuty시작이든 온디맨드든 상관없이 멀웨어 검사가 아직 진행 중일 때는 아무도 멀웨어 방지에 대한 SLR 권한을 삭제하지 않도록 하십시오. 권한을 삭제하면 스캔이 성공적으로 완료되지 않고 확실한 스캔 결과를 얻을 수 없습니다.

온디맨드 맬웨어 스캔을 시작하기 전에 지난 1시간 동안 동일한 리소스에서 스캔이 시작되지 않았는지 확인합니다. 시작된 경우 중복으로 제외됩니다. 자세한 정보는 동일한 리소스 다시 스캔을 참조하세요.

온디맨드 맬웨어 스캔 시작

원하는 액세스 방법을 선택하여 온디맨드 맬웨어 스캔을 시작하세요.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 여십시오. GuardDuty
2. 다음 옵션 중 하나를 사용하여 스캔을 시작합니다.
   a. 맬웨어 보호 페이지 사용:
      i. 탐색 창의 보호 플랜에서 맬웨어 보호를 선택합니다.

ii. 맬웨어 보호 페이지에서 스캔을 시작하려는 Amazon EC2 인스턴스 ARN[1]을 입력합니다.

b. 맬웨어 스캔 페이지 사용:

i. 탐색 창에서 맬웨어 스캔을 선택합니다.

ii. 온디맨드 스캔 시작을 선택하고 스캔을 시작하려는 Amazon EC2 인스턴스 ARN[1]을 입력합니다.

iii. 다시 스캔하는 경우 맬웨어 스캔 페이지에서 Amazon EC2 인스턴스 ID를 선택합니다.

온디맨드 스캔 시작 드롭다운을 확장하고 선택한 인스턴스 다시 스캔을 선택합니다.

3. 한 가지 방법을 사용하여 스캔을 성공적으로 시작하면 스캔 ID가 생성됩니다. 이 스캔 ID를 사용하여 스캔 진행 상황을 추적할 수 있습니다. 자세한 정보는 맬웨어 스캔 상태 및 결과 모니터링을 참조하세요.

API/CLI

온디맨드 `resourceArn` 멀웨어 스캔을 시작하려는 Amazon EC2 인스턴스 1을 StartMalwareScan수락하는 호출입니다.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

스캔을 성공적으로 시작하면 `StartMalwareScan`에서 `scanId`를 반환합니다. Ivoke DescribeMalwareScansMonitor는 시작된 검사의 진행 상황을 모니터링합니다.

[1]Amazon EC2 인스턴스 ARN의 형식에 대한 자세한 내용은 Amazon 리소스 이름(ARN)을 참조하세요. Amazon EC2 인스턴스의 경우 파티션, 리전, AWS 계정 ID 및 Amazon EC2 인스턴스 ID의 값을 바꿔 다음 예시 ARN 형식을 사용할 수 있습니다. 인스턴스 ID의 길이에 대한 자세한 내용은 리소스 ID를 참조하세요.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

동일한 Amazon EC2 인스턴스 다시 스캔

스캔이 시작되었든 온디맨드로 GuardDuty 시작되었든 관계없이 이전 멀웨어 스캔 시작 시간으로부터 1시간 후에 동일한 EC2 인스턴스에서 새로운 온디맨드 멀웨어 스캔을 시작할 수 있습니다. 이전 맬웨

어 스캔을 시작한 지 1시간 이내에 새 맬웨어 스캔이 시작되면 요청에서 다음 오류가 발생하고, 이 요청에 대한 스캔 ID가 생성되지 않습니다.

```
A scan was initiated on this resource recently. You can request a scan on
the same resource one hour after the previous scan start time.
```

동일한 리소스에서 새 스캔을 시작하는 방법에 대한 자세한 내용은 온디맨드 맬웨어 스캔 시작 섹션을 참조하세요.

맬웨어 스캔 상태를 추적하려면 검사 상태를 모니터링하여 멀웨어를 차단할 수 있습니다. GuardDuty 섹션을 참조하세요.

검사 상태를 모니터링하여 멀웨어를 차단할 수 있습니다. GuardDuty

각 GuardDuty 멀웨어 보호 검사의 검사 상태를 모니터링할 수 있습니다. 스캔 상태의 가능한 값은 `Completed`, `Running`, `Skipped`, `Failed`입니다.

스캔이 완료되면 상태가 `Completed`인 스캔에 스캔 결과가 입력됩니다. 스캔 결과의 가능한 값은 `Clean` 및 `Infected`입니다. 스캔 유형을 사용하여 맬웨어 스캔이 `GuardDuty initiated` 또는 `On demand`였는지 여부를 식별할 수 있습니다.

각 맬웨어 스캔에 대한 스캔 결과의 보존 기간은 90일입니다. 선호하는 액세스 방법을 선택하여 맬웨어 스캔 상태를 추적합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 맬웨어 스캔을 선택합니다.
3. 필터 기준에서 사용할 수 있는 다음 속성을 기준으로 맬웨어 스캔을 필터링할 수 있습니다.

   - 스캔 ID
   - 계정 ID
   - EC2 인스턴스 ARN
   - 스캔 유형
   - 스캔 상태

   필터 기준에 사용되는 속성에 대한 자세한 내용은 결과 세부 정보 섹션을 참조하세요.

API/CLI

- 맬웨어 스캔에서 결과가 나오면 EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE, GUARDDUTY_FINDING_ID, SCAN_STATUS 및 SCAN_START_TIME을 기준으로 맬웨어 스캔을 필터링할 수 있습니다.

  GUARDDUTY_FINDING_ID필터 기준은 를 GuardDuty 시작할 때 사용할 수 있습니다. SCAN_TYPE 모든 필터 기준에 대한 내용은 결과 세부 정보 섹션을 참조하세요.
- 아래 명령에서 예시 *filter-criteria*를 변경할 수 있습니다. 현재는 한 번에 하나의 CriterionKey에 따라 필터링할 수 있습니다. CriterionKey에 대한 옵션은 EC2_INSTANCE_ARN, SCAN_ID, ACCOUNT_ID, SCAN_TYPE, GUARDDUTY_FINDING_ID, SCAN_STATUS 및 SCAN_START_TIME입니다.

  아래와 같이 CriterionKey를 사용하는 경우 예시 EqualsValue를 유효한 자체 AWS *scan-id*로 바꿔야 합니다.

  예시 detector-id를 유효한 자체 *detector-id*로 바꿉니다. *max-results*(최대 50) 및 *sort-criteria*를 변경할 수 있습니다. AttributeName은 필수이며 scanStartTime이어야 합니다.

```
aws guardduty describe-malware-scans --detector-
id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
{"EqualsValue":"123456789012"}}] }'
```

- 이 명령의 응답에는 영향을 받는 리소스 및 맬웨어 결과(Infected인 경우)에 대한 세부 정보가 포함된 최대 1개의 결과가 표시됩니다.

GuardDuty 서비스 계정 기준 AWS 리전

스냅샷이 생성되어 GuardDuty 서비스 계정과 공유되면 CloudTrail 로그에 새 이벤트가 생성됩니다. 이 이벤트는 해당하는 AND snapshotId userId (해당 GuardDuty 서비스 계정 AWS 리전) 를 지정합니다. 자세한 정보는 맬웨어 보호의 기능을 참조하세요.

다음 예제는 요청의 요청 본문을 보여주는 CloudTrail 이벤트의 스니펫입니다. ModifySnapshotAttribute

```
"requestParameters": {
```

```
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

다음 표에는 각 지역의 GuardDuty 서비스 계정이 나와 있습니다. `userId`는 GuardDuty 서비스 계정이며 선택한 지역에 따라 달라집니다.

AWS 리전	리전 코드	GuardDuty 서비스 계정 ID (**`userId`**)
미국 동부(버지니아 북부)	us-east-1	652050842985
미국 동부(오하이오)	us-east-2	178123968615
미국 서부(캘리포니아 북부)	us-west-1	669213148797
미국 서부(오레곤)	us-west-2	447226417196
아시아 태평양(뭄바이)	ap-south-1	913179291432
아시아 태평양(오사카)	ap-northeast-3	089661699081
아시아 태평양(서울)	ap-northeast-2	039163547507
아시아 태평양(도쿄)	ap-northeast-1	874749492622
아시아 태평양(싱가포르)	ap-southeast-1	247460962669
아시아 태평양(시드니)	ap-southeast-2	124839743349
캐나다(중부)	ca-central-1	175877067165
캐나다 서부(캘거리)	ca-west-1	894794104037

AWS 리전	리전 코드	GuardDuty 서비스 계정 ID (**`userId`**)
유럽(프랑크푸르트)	eu-central-1	002294850712
유럽(아일랜드)	eu-west-1	283769539786
유럽(런던)	eu-west-2	310125036783
유럽(파리)	eu-west-3	866607715269
유럽(스톡홀름)	eu-north-1	693780578038
중국(베이징)	cn-north-1	448721096076
중국(닝샤)	cn-northwest-1	480864352451
남아메리카(상파울루)	sa-east-1	546914126324
아시아 태평양(하이데라바드) (옵트인)	ap-south-2	682251015962
아시아 태평양(멜버른) (옵트인)	ap-southeast-4	353488359550
유럽(스페인) (옵트인)	eu-south-2	936182149045
유럽(취리히) (옵트인)	eu-central-2	867642063380
이스라엘(텔아비브) (옵트인)	il-central-1	619233833001
유럽(밀라노) (옵트인)	eu-south-1	977238331021
아시아 태평양(홍콩) (옵트인)	ap-east-1	249472122084
중동(바레인) (옵트인)	me-south-1	404001805210
아프리카(케이프타운) (옵트인)	af-south-1	957664736811

AWS 리전	리전 코드	GuardDuty 서비스 계정 ID (**`userId`**)
아시아 태평양(자카르타) (옵트인)	ap-southeast-3	452118225523
중동(UAE) (옵트인)	me-central-1	828603743433

맬웨어 보호 할당량

맬웨어 보호에는 이 기능에서 사용하는 다양한 리소스의 기본 가용성이 있습니다.

범위	기본값	설명
압축 또는 보관된 파일의 데이터 추출 및 분석	5	보관된 파일에 허용되는 최대 중첩 레벨 수.
보관 파일 내 파일 수	1000	아카이브 내에서 스캔할 수 있는 최대 파일 수. 이 수는 아카이브에서 추출된 파일 수와 모든 중첩된 아카이브에서 추출된 파일 수의 합계입니다.
위협 수	32	검색 결과 패널에서 확인할 수 있는 최대 위협 수입니다. GuardDuty 멀웨어 보호에서 더 많은 위협 이름을 탐지했을 수 있습니다. 탐지된 위협 이름 수가 기본값보다 많으면 GuardDuty 콘솔의 세부 정보 패널에서 검색 결과 이름 아래에 있는 찾기 ID를 선택하여 JSON 세부 정보를 볼 수 있습니다.
탐지된 위협당 파일 수	5	탐지된 위협당 식별된 최대 파일 수. 예를 들어 단일 위협과 관련된 파일 10개를

범위	기본값	설명
		GuardDuty 탐지하면 위협에는 최대 5개의 파일이 표시됩니다.
인스턴스별 스캔당 EBS 볼륨	11	EC2 인스턴스당 GuardDuty 스캔할 수 있는 최대 EBS 볼륨 수입니다. 스캔해야 하는 EBS 볼륨이 11개를 초과하는 경우 GuardDuty 멀웨어 보호는 `deviceName` 알파벳순으로 정렬하여 처음 11개의 EBS 볼륨을 선택합니다.
EBS 볼륨 크기	2048기가바이트	Amazon EC2 인스턴스 및 컨테이너 워크로드와 관련된 GuardDuty 멀웨어 보호 기능은 최대 2048GB 크기의 각 Amazon EBS 볼륨을 스캔할 수 있습니다. 이 할당량은 멀웨어 방지가 지원되는 각 AWS 리전 지역에 적용됩니다.

범위	기본값	설명
지원되는 파일 시스템 유형	GuardDuty 멀웨어 보호는 다음과 같은 파일 시스템 유형을 검사할 수 있습니다. • New Technology File System(NTFS) • X File System(XFS) • Second extended(ext2) File System • Fourth extended(ext4) File System • File Allocation Table(FAT) File System • Virtual File Allocation Table(VFAT) File System	해당 사항 없음
스캔 옵션 태그	50	맬웨어 스캔 옵션 설정을 사용자 지정하기 위해 추가할 수 있는 리소스 태그의 최대 수. 자세한 정보는 사용자 정의 태그를 사용하는 스캔 옵션을 참조하세요.
결과 보존 기간	90	검색 결과를 보관하는 최대 GuardDuty 일수. 최신 정보는 아마존 할당량 GuardDuty 섹션을 참조하세요.

범위	기본값	설명
맬웨어 스캔 보존 기간	90	GuardDuty 멀웨어 보호에서 검사 기록을 보관하는 최대 일수입니다. 최근 맬웨어 스캔 조회에 대한 자세한 내용은 검사 상태를 모니터링하여 멀웨어를 차단할 수 있습니다. GuardDuty 섹션을 참조하세요.
온디맨드 맬웨어 스캔의 초당 트랜잭션(TPS)	1	각 리전에서 초당 시작할 수 있는 온디맨드 맬웨어 스캔 요청 수.
온디맨드 맬웨어 스캔의 버스트 한도	1	각 리전에서 초당 동시에 시작할 수 있는 온디맨드 맬웨어 스캔 요청 수.

GuardDuty RDS 보호

Amazon의 RDS Protection은 Amazon Aurora 데이터베이스 (Amazon Aurora MySQL 호환 에디션 및 Aurora PostgreSQL 호환 에디션) 에 대한 잠재적 액세스 위협에 대해 RDS 로그인 활동을 GuardDuty 분석하고 프로파일링합니다. 이 기능을 사용하면 잠재적으로 의심스러운 로그인 동작을 식별할 수 있습니다. RDS 보호는 데이터베이스 인스턴스의 성능에 영향을 주지 않도록 설계되어 추가 인프라가 필요하지 않습니다.

RDS Protection이 데이터베이스 위협을 나타내는 잠재적으로 의심스럽거나 비정상적인 로그인 시도를 탐지하면 잠재적으로 손상된 데이터베이스에 대한 세부 정보가 포함된 새로운 결과를 생성합니다. GuardDuty

Amazon GuardDuty 내에서 이 기능을 사용할 수 AWS 리전 있는 모든 계정의 RDS 보호 기능을 언제든지 활성화하거나 비활성화할 수 있습니다. 기존 GuardDuty 계정은 30일 평가 기간으로 RDS 보호를 활성화할 수 있습니다. 새 GuardDuty 계정의 경우 RDS 보호가 이미 활성화되어 있으며 30일 무료 평가 기간에 포함되어 있습니다. 자세한 정보는 비용 추정을 참조하세요.

> **Note**
>
> RDS 보호 기능이 활성화되지 않은 경우 RDS 로그인 활동을 수집하거나 GuardDuty 비정상적이거나 의심스러운 로그인 동작을 탐지하지 못합니다.

RDS 보호를 아직 GuardDuty 지원하지 않는 AWS 리전 위치에 대한 자세한 내용은 을 참조하십시오. 리전별 기능 가용성

지원되는 Amazon Aurora 데이터베이스

다음 표는 지원되는 Aurora 데이터베이스 버전을 보여줍니다.

Amazon Aurora DB 엔진	지원되는 엔진 버전
Aurora MySQL	• 2.10.2 이상 • 3.02.1 이상
Aurora PostgreSQL	• 10.17 이상 • 11.12 이상

Amazon Aurora DB 엔진	지원되는 엔진 버전
	• 12.7 이상 • 13.3 이상 • 14.3 이상 • 15.2 이상 • 16.1 이상

RDS 보호가 RDS 로그인 활동 모니터링을 사용하는 방법

Amazon의 RDS 보호를 GuardDuty 사용하면 계정에서 지원되는 Amazon Aurora (Aurora) 데이터베이스를 보호할 수 있습니다. RDS 보호 기능을 활성화하면 계정의 Aurora 데이터베이스에서 RDS 로그인 활동을 GuardDuty 즉시 모니터링하기 시작합니다. GuardDuty RDS 로그인 활동을 지속적으로 모니터링하고 프로파일링하여 이전에 확인되지 않은 외부 행위자가 사용자 계정의 Aurora 데이터베이스에 무단으로 액세스하는 등의 의심스러운 활동이 있는지 확인합니다. RDS 보호를 처음 활성화하거나 새로 생성한 데이터베이스 인스턴스가 있는 경우 정상 동작의 기준을 정하기 위한 학습 기간이 필요합니다. 이러한 이유로 새로 활성화 또는 생성된 데이터베이스 인스턴스에는 최대 2주 동안 관련 변칙적인 로그인 결과가 나타나지 않을 수 있습니다. 자세한 정보는 RDS 로그인 활동 모니터링을 참조하세요.

RDS Protection은 일련의 성공, 실패 또는 불완전한 로그인 시도에서 비정상적인 패턴과 같은 잠재적 위협을 탐지하면 잠재적으로 손상된 데이터베이스 인스턴스에 대한 세부 정보가 포함된 새로운 탐지 결과를 GuardDuty 생성합니다. 자세한 정보는 RDS 보호 결과 유형을 참조하세요. RDS 보호를 비활성화하면 RDS 로그인 활동 모니터링이 GuardDuty 즉시 중지되며 지원되는 데이터베이스 인스턴스에 대한 잠재적 위협을 탐지할 수 없습니다.

> **Note**
>
> GuardDuty 사용자 지원되는 데이터베이스 또는 RDS 로그인 활동을 관리하거나 RDS 로그인 활동을 사용자에게 제공하지 않습니다.

독립형 계정에 대한 RDS 보호 구성

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

2. 탐색 창에서 RDS 보호를 선택합니다.
3. RDS 보호 페이지에는 계정의 현재 상태가 표시됩니다. 활성화 또는 비활성화를 선택하여 언제든 기능을 활성화 또는 비활성화할 수 있습니다. 선택 항목을 확인합니다.

API/CLI

리전 탐지기 ID를 사용하고 `features` 객체 `name`을 `RDS_LOGIN_EVENTS`로, `status`를 `ENABLED` 또는 `DISABLED` 상태로 설정하여 전달해 updateDetector API를 실행합니다.

다음 AWS CLI 명령을 실행하여 RDS 보호를 활성화하거나 비활성화할 수도 있습니다. 유효한 *###ID*를 사용해야 합니다.

> **Note**
>
> 다음 예시 코드는 RDS 보호를 활성화합니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

계정 및 현재 지역에 `detectorId` 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

다중 계정 환경에서 RDS 보호 구성

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만이 조직의 구성원 계정에 대해 RDS 보호 기능을 활성화하거나 비활성화할 수 있습니다. GuardDuty구성원 계정은 자신의 계정에서 이 구성을 수정할 수 없습니다. 위임된 GuardDuty 관리자 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 이 위임된 GuardDuty 관리자 계정은 조직에 가입하는 모든 새 계정에 대해 RDS 로그인 활동 모니터링을 자동으로 활성화하도록 선택할 수 있습니다. 다중 계정 환경에 대한 자세한 내용은 Amazon에서의 다중 계정 관리를 참조하십시오. GuardDuty

위임된 관리자 계정을 위한 RDS 보호 구성 GuardDuty

선호하는 액세스 방법을 선택하여 GuardDuty 위임된 관리자 계정에 대해 RDS 로그인 활동 모니터링을 구성하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   관리 계정 보안 인증 정보를 사용해야 합니다.
2. 탐색 창에서 RDS 보호를 선택합니다.
3. RDS 보호 페이지에서 편집을 선택합니다.
4. 다음 중 하나를 수행하십시오.

   모든 계정에 대해 활성화 사용

   - 모든 계정에 대해 활성화를 선택합니다. 그러면 조직에 가입한 새 GuardDuty 계정을 포함하여 AWS 조직의 모든 활성 계정에 대한 보호 계획이 활성화됩니다.
   - 저장을 선택합니다.

   수동으로 계정 구성 사용

   - 위임된 GuardDuty 관리자 계정 계정에만 보호 계획을 활성화하려면 계정 수동 구성을 선택합니다.
   - 위임된 GuardDuty 관리자 계정 (이 계정) 섹션에서 활성화를 선택합니다.
   - 저장을 선택합니다.

API/CLI

리전 탐지기 ID를 사용하고 `features` 객체 `name`을 `RDS_LOGIN_EVENTS`으로, `status`를 `ENABLED` 또는 `DISABLED` 상태로 설정하여 전달해 updateDetector API를 실행합니다.

다음 AWS CLI 명령을 실행하여 RDS 보호를 활성화 또는 비활성화할 수 있습니다. 위임된 GuardDuty 관리자 계정의 유효한 `###` ID를 사용해야 합니다.

> **Note**
>
> 다음 예시 코드는 RDS 보호를 활성화합니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

모든 멤버 계정에서 RDS 보호 자동 활성화

원하는 액세스 방법을 선택하여 모든 멤버 계정에서 RDS 보호 기능을 활성화합니다. 여기에는 기존 멤버 계정과 조직에 새로 가입한 계정이 포함됩니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.

2. 다음 중 하나를 수행하십시오.

   RDS 보호 페이지 사용

   1. 탐색 창에서 RDS 보호를 선택합니다.
   2. 모든 계정에 대해 활성화를 선택합니다. 이 작업을 통해 조직의 기존 계정과 새 계정 모두에 대해 RDS 보호가 자동으로 활성화됩니다.
   3. 저장을 선택합니다.

      > **Note**
      >
      > 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

   계정 페이지 사용

   1. 탐색 창에서 Accounts(계정)를 선택합니다.
   2. 계정 페이지에서 초대 기준으로 계정 추가 전에 자동 활성화 기본 설정을 선택합니다.
   3. 자동 활성화 기본 설정 관리 창의 RDS 로그인 활동 모니터링에서 모든 계정에 대해 활성화를 선택합니다.
   4. 저장을 선택합니다.

모든 계정에 대해 활성화 옵션을 사용할 수 없는 경우 멤버 계정에서 RDS 보호를 선택적으로 활성화 또는 비활성화 섹션을 참조하세요.

API/CLI

- 멤버 계정에 대해 RDS 보호를 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.
- 다음 예시에서는 단일 멤버 계정에 RDS 보호를 활성화하는 방법을 보여줍니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

  계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

모든 기존 활성 멤버 계정에서 RDS 보호 활성화

원하는 액세스 방법을 선택하여 조직의 모든 기존 활성 멤버 계정에 대해 RDS 보호를 활성화합니다.

Console

모든 기존 활성 멤버 계정에서 RDS 보호 구성

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 RDS 보호를 선택합니다.

3. RDS 보호 페이지에서 구성의 현재 상태를 볼 수 있습니다. 활성 멤버 계정 섹션에서 작업을 선택합니다.
4. 작업 드롭다운 메뉴에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다.
5. 확인을 선택합니다.

API/CLI

- 멤버 계정에 대해 RDS 보호를 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.
- 다음 예시에서는 단일 멤버 계정에 RDS 보호를 활성화하는 방법을 보여줍니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

  계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

새 멤버 계정에서 RDS 보호 자동 활성화

원하는 액세스 방법을 선택하여 조직에 가입하는 새 계정에 대해 RDS 로그인 활동을 활성화합니다.

Console

위임된 GuardDuty 관리자 계정은 콘솔을 통해 RDS 보호 또는 계정 페이지를 사용하여 조직의 새 구성원 계정을 활성화할 수 있습니다.

새 멤버 계정에서 RDS 보호 자동 활성화

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.

2. 다음 중 하나를 수행하십시오.
   - RDS 보호 페이지 사용:
     1. 탐색 창에서 RDS 보호를 선택합니다.
     2. RDS 보호 페이지에서 편집을 선택합니다.
     3. 수동으로 계정 구성을 선택합니다.
     4. 새 멤버 계정에 대해 자동으로 활성화를 선택합니다. 이 단계를 통해 새 계정이 조직에 가입할 때마다 해당 계정에 대해 RDS 보호가 자동으로 활성화됩니다. 조직이 위임한 GuardDuty 관리자 계정만 이 구성을 수정할 수 있습니다.
     5. 저장을 선택합니다.
   - 계정 페이지 사용:
     1. 탐색 창에서 Accounts(계정)를 선택합니다.
     2. 계정 페이지에서 자동 활성화 기본 설정을 선택합니다.
     3. 자동 활성화 기본 설정 관리 창의 RDS 로그인 활동 모니터링에서 새 계정에 대해 활성화를 선택합니다.
     4. 저장을 선택합니다.

API/CLI

- 멤버 계정에 대해 RDS 보호를 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 간접적으로 호출합니다.
- 다음 예시에서는 단일 멤버 계정에 RDS 보호를 활성화하는 방법을 보여줍니다. 비활성화하려면 멤버 계정에서 RDS 보호를 선택적으로 활성화 또는 비활성화 섹션을 참조하세요. 조직에 가입하는 모든 새 계정에 대해 활성화하지 않으려면 `autoEnable`을 `NONE`으로 설정합니다.

  계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

멤버 계정에서 RDS 보호를 선택적으로 활성화 또는 비활성화

원하는 액세스 방법을 선택하여 멤버 계정에 대해 RDS 로그인 활동 모니터링을 선택적으로 활성화 또는 비활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.

   계정 페이지의 RDS 로그인 활동 열에서 멤버 계정 상태를 검토합니다.
3. RDS 로그인 활동을 선택적으로 활성화 또는 비활성화

   RDS 보호를 구성할 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다. 보호 계획 편집 드롭다운 메뉴에서 RDS 로그인 활동을 선택한 다음 적절한 옵션을 선택합니다.

API/CLI

멤버 계정에 대해 RDS 보호를 선택적으로 활성화 또는 비활성화하려면 자체 *`### ID`*를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.

다음 예시에서는 단일 멤버 계정에 RDS 보호를 활성화하는 방법을 보여줍니다. 비활성화하려면 `ENABLED`를 `DISABLED`로 바꿉니다.

계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

RDS 보호의 기능

RDS 로그인 활동 모니터링

RDS 로그인 활동은 AWS 환경의 지원되는 Amazon Aurora 데이터베이스에 대해 성공 및 실패한 로그인 시도를 모두 캡처합니다. 데이터베이스를 보호할 수 있도록 GuardDuty RDS Protection은 로그인 활동을 지속적으로 모니터링하여 의심스러운 로그인 시도가 있는지 확인합니다. 예를 들어 공격자는 데이터베이스의 암호를 추측하여 Amazon Aurora 데이터베이스에 대한 무차별 암호 대입 액세스를 시도할 수 있습니다.

RDS 보호 기능을 활성화하면 Aurora 서비스에서 직접 데이터베이스의 RDS 로그인 활동을 GuardDuty 자동으로 모니터링하기 시작합니다. 비정상적인 로그인 동작이 나타나는 경우 잠재적으로 손상된 데이터베이스에 대한 세부 정보가 포함된 검색 결과를 GuardDuty 생성합니다. RDS 보호를 처음 활성화하거나 새로 생성한 데이터베이스 인스턴스가 있는 경우 정상 동작의 기준을 정하기 위한 학습 기간이 필요합니다. 이러한 이유로 새로 활성화 또는 생성된 데이터베이스 인스턴스에는 최대 2주 동안 관련 변칙적인 로그인 결과가 나타나지 않을 수 있습니다.

RDS 보호 기능은 추가 설정이 필요하지 않으므로 기존 Amazon Aurora 데이터베이스 구성에는 영향을 주지 않습니다. GuardDuty 지원되는 데이터베이스 또는 RDS 로그인 활동을 관리하거나 RDS 로그인 활동을 사용할 수 있게 만들지 않습니다.

새 구성원 계정이 조직에 가입할 때 해당 계정에 대해 RDS 보호 기능을 자동으로 활성화하도록 선택한 경우 이 작업을 수행하면 새 구성원 계정이 자동으로 GuardDuty 활성화됩니다. RDS 로그인 활동 모니터링을 기능으로 구성하는 방법에 대한 자세한 내용은 GuardDuty RDS 보호 섹션을 참조하세요.

GuardDuty 런타임 모니터링

런타임 모니터링은 운영 체제 수준, 네트워킹 및 파일 이벤트를 관찰하고 분석하여 환경의 특정 AWS 워크로드에서 잠재적 위협을 탐지하는 데 도움이 됩니다.

GuardDuty 처음에는 Amazon Elastic Kubernetes Service (Amazon EKS) 리소스만 지원하는 런타임 모니터링을 출시했습니다. 하지만 이제 런타임 모니터링 기능을 사용하여 Amazon Elastic Container Service (Amazon ECS) 및 AWS Fargate Amazon Elastic Compute Cloud (Amazon EC2) 리소스에 대한 위협 탐지 기능을 제공할 수도 있습니다.

이 문서 및 런타임 모니터링과 관련된 기타 섹션에서는 리소스 유형이라는 용어를 GuardDuty 사용하여 Amazon EKS, Fargate Amazon ECS 및 Amazon EC2 리소스를 지칭합니다.

런타임 모니터링은 파일 액세스, 프로세스 실행, 명령줄 인수 및 네트워크 연결과 같은 런타임 동작에 대한 가시성을 추가하는 GuardDuty 보안 에이전트를 사용합니다. 잠재적 위협을 모니터링하려는 각 리소스 유형에 대해 해당 특정 리소스 유형의 보안 에이전트를 자동 또는 수동으로 관리할 수 있습니다 (Fargate (Amazon ECS만 해당) 제외). 보안 에이전트를 자동으로 관리한다는 것은 사용자를 대신하여 보안 에이전트를 설치하고 GuardDuty 업데이트하도록 허용한다는 의미입니다. 반면, 리소스의 보안 에이전트를 수동으로 관리하는 경우 필요에 따라 보안 에이전트를 설치하고 업데이트해야 합니다.

이 확장된 기능을 통해 개별 워크로드 및 인스턴스에서 실행되는 애플리케이션과 데이터를 대상으로 GuardDuty 할 수 있는 잠재적 위협을 식별하고 이에 대응할 수 있습니다. 예를 들어, 취약한 웹 애플리케이션을 실행하는 단일 컨테이너를 손상시키는 것으로 위협이 시작될 수 있습니다. 이 웹 애플리케이션에 기본 컨테이너와 워크로드에 대한 액세스 권한이 있을 수 있습니다. 이 시나리오에서 자격 증명을 잘못 구성하면 계정과 그 안에 저장된 데이터에 대한 액세스 권한이 더 광범위해질 수 있습니다.

개별 컨테이너 및 워크로드의 런타임 이벤트를 분석하여 초기 단계에서 컨테이너 및 관련 AWS 자격 증명의 손상을 잠재적으로 식별하고 환경 내 데이터에 대한 권한 상승 시도, 의심스러운 API 요청, 악의적인 액세스 등을 탐지할 GuardDuty 수 있습니다.

내용

- EKS 런타임 모니터링에서 런타임 모니터링으로 마이그레이션
- 리소스의 런타임 커버리지 평가
- CPU 및 메모리 모니터링 설정
- 를 사용하는 수집된 런타임 이벤트 유형 GuardDuty
- Amazon ECR 리포지토리 호스팅 에이전트 GuardDuty
- GuardDuty 에이전트 릴리스 기록
- 리소스 비활성화 및 정리가 미치는 영향

작동 방식

런타임 모니터링을 사용하려면 런타임 모니터링을 활성화한 다음 보안 에이전트를 관리해야 합니다. GuardDuty 다음 목록은 이 2단계 프로세스를 설명합니다.

1. Amazon EC2 인스턴스, Amazon ECS 클러스터 및 Amazon EKS 워크로드에서 수신하는 런타임 이벤트를 GuardDuty 수락할 수 있도록 계정에 대한 런타임 모니터링을 활성화하십시오.
2. 런타임 동작을 모니터링하려는 개별 리소스의 GuardDuty 에이전트를 관리합니다. 리소스 유형에 따라 GuardDuty 보안 에이전트를 수동으로 배포하거나 사용자 대신 관리하도록 허용하여 GuardDuty 배포하도록 선택할 수 있습니다. 이를 자동 에이전트 구성이라고 합니다.

   GuardDuty 는 각 리소스 유형에 대해 보안 에이전트를 인증하는 인스턴스 ID 역할을 사용하여 관련 런타임 이벤트를 VPC 엔드포인트로 보냅니다.

> **Note**
>
> GuardDuty 런타임 이벤트에 액세스할 수 있게 해주지는 않습니다.

EKS 런타임 모니터링 또는 EC2 인스턴스용 런타임 모니터링에서 보안 에이전트를 관리 (수동 또는 통해 GuardDuty) 하고 GuardDuty 현재 Amazon EC2 인스턴스에 배포되어 있고 이 수집된 런타임 이벤트 유형 인스턴스로부터 수신한 경우, 이 Amazon EC2 인스턴스의 VPC 흐름 로그 분석에 GuardDuty 대해서는 요금이 부과되지 않습니다. AWS 계정 이렇게 하면 계정에서 이중 사용 비용이 발생하는 GuardDuty 것을 방지할 수 있습니다.

다음 항목에서는 런타임 모니터링을 활성화하고 GuardDuty 보안 에이전트를 관리하는 방법이 리소스 유형별로 어떻게 다른지 설명합니다.

내용

Amazon EC2 인스턴스에서 런타임 모니터링이 작동하는 방식

Amazon EC2 인스턴스는 사용자 환경에서 여러 유형의 애플리케이션과 워크로드를 실행할 수 있습니다. AWS 런타임 모니터링을 활성화하고 GuardDuty 보안 에이전트를 관리하면 기존 Amazon EC2 인스턴스와 잠재적으로 새로운 인스턴스에서 위협을 탐지하는 GuardDuty 데 도움이 됩니다. 이 기능은 Amazon ECS에서 관리되는 Amazon EC2 인스턴스도 지원합니다.

런타임 모니터링을 활성화하면 Amazon EC2 인스턴스 내에서 현재 실행 중인 프로세스와 새 프로세스의 런타임 이벤트를 GuardDuty 사용할 준비가 됩니다. GuardDuty EC2 인스턴스에서 로 런타임 이벤트를 보내려면 보안 에이전트가 필요합니다. GuardDuty

Amazon EC2 인스턴스의 경우 GuardDuty 보안 에이전트는 인스턴스 수준에서 작동합니다. 계정의 Amazon EC2 인스턴스를 모두 모니터링할지 아니면 일부만 모니터링할지 결정할 수 있습니다. 선택적 인스턴스를 관리하려는 경우 이러한 인스턴스에만 보안 에이전트가 필요합니다.

GuardDuty 또한 Amazon ECS 클러스터 내 Amazon EC2 인스턴스에서 실행 중인 새 작업 및 기존 작업의 런타임 이벤트를 사용할 수 있습니다.

GuardDuty 보안 에이전트를 설치하기 위해 런타임 모니터링은 다음 두 가지 옵션을 제공합니다.

- 자동 에이전트 구성 사용 (권장), 또는
- 보안 에이전트를 수동으로 관리합니다.

다음을 통한 자동 에이전트 구성 사용 GuardDuty (권장)

사용자를 GuardDuty 대신하여 Amazon EC2 인스턴스에 보안 에이전트를 설치할 수 있는 자동 에이전트 구성을 사용하십시오. GuardDuty 또한 보안 에이전트에 대한 업데이트도 관리합니다.

기본적으로 계정의 모든 인스턴스에 보안 에이전트를 GuardDuty 설치합니다. 일부 EC2 인스턴스에만 보안 에이전트를 설치하고 관리하려면 필요에 따라 EC2 인스턴스에 포함 또는 제외 태그를 추가하십시오. GuardDuty

계정에 속한 모든 Amazon EC2 인스턴스의 런타임 이벤트를 모니터링하고 싶지 않은 경우도 있습니다. 제한된 수의 인스턴스에 대한 런타임 이벤트를 모니터링하려는 경우 선택한 인스턴스에 `GuardDutyManaged` 다음과 `true` 같은 포함 태그를 추가하십시오. Amazon EC2용 자동 에이전트 구성을 사용할 수 있게 되면서, EC2 인스턴스에 포함 태그 (`GuardDutyManaged:true`) 가 있으면 자동 에이전트 구성을 명시적으로 활성화하지 않아도 해당 태그를 적용하고 선택한 인스턴스의 보안 에이전트를 관리합니다. GuardDuty

반면, 런타임 이벤트를 모니터링하고 싶지 않은 EC2 인스턴스의 수가 제한되어 있는 경우에는 선택한 인스턴스에 제외 태그 (:) `GuardDutyManaged` 를 추가하십시오. `false` GuardDuty 이러한 EC2 리소스에 대한 보안 에이전트를 설치하거나 관리하지 않음으로써 제외 태그를 준수합니다.

영향

한 조직 AWS 계정 또는 조직에서 자동 에이전트 구성을 사용하는 경우 사용자를 GuardDuty 대신하여 다음 단계를 수행할 수 있습니다.

- GuardDuty SSM으로 관리되고 https://console.aws.amazon.com/systems-manager/ 콘솔의 플릿 관리자 아래에 나타나는 모든 Amazon EC2 인스턴스에 대해 하나의 SSM 연결을 생성합니다.
- 자동 에이전트 구성이 비활성화된 상태에서 포함 태그 사용 — 런타임 모니터링을 활성화한 후 자동 에이전트 구성을 활성화하지 않고 Amazon EC2 인스턴스에 포함 태그를 추가하면 사용자를 대신하여 보안 에이전트를 관리할 수 있게 됩니다 GuardDuty . 그러면 SSM 연결이 포함 태그 (:) 가 있는 각 인스턴스에 보안 에이전트를 설치합니다. `GuardDutyManaged true`
- 자동 에이전트 구성을 활성화하면 SSM 연결이 계정에 속한 모든 EC2 인스턴스에 보안 에이전트를 설치합니다.
- 자동 에이전트 구성과 함께 제외 태그 사용 — 자동 에이전트 구성을 활성화하기 전에 Amazon EC2 인스턴스에 제외 태그를 추가하면 선택한 이 인스턴스에 대한 보안 에이전트의 설치 및 관리를 금지할 수 있음을 의미합니다. GuardDuty

  이제 자동 에이전트 구성을 활성화하면 SSM 협회는 제외 태그가 지정된 인스턴스를 제외한 모든 EC2 인스턴스에 보안 에이전트를 설치하고 관리합니다.
- GuardDuty 공유 VPC를 포함한 모든 VPC에 VPC 엔드포인트를 생성합니다. 단, 해당 VPC에 종료되거나 종료된 인스턴스 상태에 있지 않은 Linux EC2 인스턴스가 하나 이상 있어야 합니다. 다양한 인스턴스 상태에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 인스턴스 수명 주기를 참조하십시오.

  GuardDuty 또한 지원합니다자동화된 보안 에이전트와 공유 VPC 사용. 조직의 모든 사전 요구 사항을 고려한 경우 공유 VPC를 사용하여 런타임 이벤트를 수신합니다. AWS 계정 GuardDuty

> **Note**
>
> 생성한 VPC 엔드포인트 사용에 대한 추가 비용은 없습니다. GuardDuty

보안 에이전트를 수동으로 관리합니다.

Amazon EC2의 보안 에이전트를 수동으로 관리하는 두 가지 방법이 있습니다.

- 에서 GuardDuty 관리 문서를 사용하여 이미 AWS Systems Manager SSM으로 관리되는 Amazon EC2 인스턴스에 보안 에이전트를 설치할 수 있습니다.

  새 Amazon EC2 인스턴스를 시작할 때마다 SSM이 활성화되어 있는지 확인하십시오.
- RPM 패키지 관리자 (RPM) 스크립트를 사용하여 Amazon EC2 인스턴스가 SSM으로 관리되는지 여부에 관계없이 Amazon EC2 인스턴스에 보안 에이전트를 설치할 수 있습니다.

다음 단계

Amazon EC2 인스턴스 모니터링을 위한 런타임 모니터링 구성을 시작하려면 을 참조하십시오.
Amazon EC2 인스턴스 지원을 위한 사전 요구 사항

Fargate와 런타임 모니터링이 작동하는 방식 (Amazon ECS만 해당)

런타임 모니터링을 활성화하면 작업의 런타임 이벤트를 사용할 준비가 GuardDuty 됩니다. 이러한 작업은 Amazon ECS 클러스터 내에서 실행되며, Amazon ECS 클러스터는 다시 AWS Fargate (Fargate) 인스턴스에서 실행됩니다. 이러한 런타임 이벤트를 GuardDuty 수신하려면 완전 관리형 전용 보안 에이전트를 사용해야 합니다.

현재 런타임 모니터링은 에서 시작한 작업을 지원하지 않습니다. AWS CodePipeline

현재 런타임 모니터링은 Amazon ECS 클러스터 (AWS Fargate) 의 보안 에이전트 관리를 통해서만 지원합니다. GuardDuty Amazon ECS 클러스터에서 보안 에이전트를 수동으로 관리하는 기능은 지원되지 않습니다.

AWS 계정 또는 조직의 자동 에이전트 구성을 사용하여 사용자 대신 GuardDuty 보안 에이전트를 GuardDuty 관리하도록 허용할 수 있습니다. GuardDuty Amazon ECS 클러스터에서 시작되는 새 Fargate 작업에 보안 에이전트를 배포하기 시작합니다. 다음 목록은 보안 에이전트를 활성화할 때 예상되는 사항을 지정합니다. GuardDuty

GuardDuty 보안 에이전트 활성화가 미치는 영향

GuardDuty 가상 사설 클라우드 (VPC) 엔드포인트 생성

보안 에이전트를 배포할 때 GuardDuty 보안 에이전트가 런타임 이벤트를 전달하는 데 사용하는 VPC 엔드포인트를 생성합니다. GuardDuty GuardDuty

> **Note**
>
> 생성한 VPC 엔드포인트 사용에 대한 추가 비용은 없습니다. GuardDuty

GuardDuty 사이드카 컨테이너를 추가합니다.

실행을 시작하는 새 Fargate 작업 또는 서비스의 경우 GuardDuty 컨테이너 (사이드카) 가 Amazon ECS Fargate 작업 내의 각 컨테이너에 연결됩니다. GuardDuty 보안 에이전트는 연결된 컨테이너 내에서 실행됩니다. GuardDuty 이렇게 하면 이러한 작업 내에서 실행되는 각 컨테이너의 런타임 이벤트를 수집하는 GuardDuty 데 도움이 됩니다.

Fargate 작업을 시작할 때 GuardDuty 컨테이너 (사이드카) 를 정상 상태로 시작할 수 없는 경우 런타임 모니터링은 작업 실행을 방해하지 않도록 설계되었습니다.

기본적으로 Fargate 태스크는 변경할 수 없습니다. GuardDuty 작업이 이미 실행 상태일 때는 사이드카를 배포하지 않습니다. 이미 실행 중인 작업의 컨테이너를 모니터링하려는 경우 작업을 중지했다가 다시 시작하면 됩니다.

Amazon EKS 클러스터에서 런타임 모니터링이 작동하는 방식

런타임 모니터링은 보안 에이전트라고도 GuardDuty 하는 EKS `aws-guardduty-agent` 애드온을 사용합니다. GuardDuty보안 에이전트가 EKS 클러스터에 배포되면 이러한 EKS 클러스터에 대한 런타임 이벤트를 수신할 수 있습니다. GuardDuty

계정 또는 클러스터 수준에서 Amazon EKS 클러스터의 런타임 이벤트를 모니터링할 수 있습니다. 위협 탐지를 위해 모니터링하려는 Amazon EKS 클러스터의 GuardDuty 보안 에이전트만 관리할 수 있습니다. GuardDuty 보안 에이전트를 수동으로 관리하거나 자동 에이전트 구성을 사용하여 사용자 대신 GuardDuty 관리하도록 허용하여 보안 에이전트를 관리할 수 있습니다.

자동 에이전트 구성 접근 방식을 사용하여 사용자 대신 보안 에이전트 배포를 관리할 수 GuardDuty 있는 경우 Amazon VPC (Virtual Private Cloud) 엔드포인트가 자동으로 생성됩니다. 보안 에이전트는 이 Amazon VPC 엔드포인트를 GuardDuty 사용하여 런타임 이벤트를 에 전달합니다.

> **Note**
>
> 생성한 VPC 엔드포인트 사용에 대한 추가 비용은 없습니다. GuardDuty

현재는 Amazon EC2 인스턴스에서 실행되는 Amazon EKS 클러스터를 GuardDuty 지원합니다. GuardDuty 에서 실행되는 AWS Fargate Amazon EKS 클러스터를 지원하지 않습니다.

런타임 모니터링 구성 이후

런타임 커버리지 평가

런타임 모니터링을 활성화하고 GuardDuty 보안 에이전트를 배포한 후에는 보안 에이전트를 배포한 리소스의 적용 범위 상태를 지속적으로 [1] 평가하는 것이 좋습니다. 적용 범위는 정상 또는 비정상일 수 있습니다. 정상 커버리지 상태는 운영 체제 수준의 활동이 있을 때 해당 리소스로부터 런타임 이벤트를 수신하고 있음을 GuardDuty 나타냅니다.

리소스의 커버리지 상태가 정상이 되면 런타임 이벤트를 수신하고 이를 분석하여 위협을 탐지할 수 있습니다. GuardDuty 컨테이너 워크로드 및 인스턴스에서 실행되는 작업 또는 애플리케이션에서 잠재적 보안 위협이 GuardDuty 탐지되면 하나 이상의 Runtime Monitoring 검색 유형을 GuardDuty 생성합니다.

[1] 보장 상태가 비정상에서 정상으로 변경되거나 다른 방식으로 변경될 때 알림을 받도록 Amazon EventBridge (EventBridge) 을 구성할 수도 있습니다.

자세한 정보는 리소스의 런타임 커버리지 평가을 참조하세요.

GuardDuty 잠재적 위협을 탐지합니다.

리소스의 런타임 이벤트를 수신하기 GuardDuty 시작하면 해당 이벤트를 분석하기 시작합니다. Amazon EC2 인스턴스, Amazon ECS 클러스터 또는 Amazon EKS 클러스터에서 잠재적 보안 위협을 GuardDuty 탐지하면 하나 이상의 보안 위협이 생성됩니다. 런타임 모니터링 검색 유형 검색 결과 세부 정보에 액세스하여 영향을 받는 리소스 세부 정보를 볼 수 있습니다.

런타임 모니터링에서 30일 무료 평가판은 어떻게 작동하나요?

30일 무료 평가 기간은 런타임 모니터링 기능이 Amazon EC2 인스턴스 및 AWS Fargate (Amazon ECS만 해당) 로 확장되기 전에 이미 EKS 런타임 모니터링을 활성화한 새 GuardDuty 계정과 기존 계정에 대해 다르게 적용됩니다.

GuardDuty 평가 기간을 사용하고 있거나 EKS 런타임 모니터링을 활성화한 적이 없습니다.

다음 목록은 30일 평가 기간을 사용 중이거나 EKS 런타임 모니터링을 활성화한 적이 없는 경우 GuardDuty 30일 무료 평가 기간이 어떻게 작동하는지 설명합니다.

- 처음 GuardDuty 활성화하면 런타임 모니터링 및 EKS 런타임 모니터링이 기본적으로 활성화되지 않습니다.

  계정 또는 조직에 대해 런타임 모니터링을 활성화하는 경우 위협 탐지를 위해 모니터링하려는 리소스의 GuardDuty 보안 에이전트도 구성해야 합니다. 예를 들어 Amazon EC2 인스턴스에 런타임 모니터링을 사용하려면 런타임 모니터링을 활성화한 후 Amazon EC2용 보안 에이전트도 구성해야 합니다. 이 작업을 수동으로 수행할지 아니면 자동으로 수행할지 선택할 수 있습니다. GuardDuty
- 런타임 모니터링 보호 계획은 계정 수준에서 활성화됩니다. 30일 무료 평가판 기간은 리소스 수준에서 작동합니다. GuardDuty 보안 에이전트가 특정 리소스 유형에 배포된 후 이 리소스 유형과 관련된 첫 번째 런타임 이벤트를 GuardDuty 수신하면 30일 무료 평가판이 시작됩니다. 예를 들어, 리소스 수준 (Amazon EC2 인스턴스, Amazon ECS 클러스터 및 Amazon EKS 클러스터의 경우)에 GuardDuty 에이전트를 배포했습니다. Amazon EC2 인스턴스에 대한 첫 번째 런타임 이벤트를 GuardDuty 수신하면 Amazon EC2에 한해 30일 무료 평가판이 시작됩니다.
- EKS 런타임 모니터링만 활성화하려는 경우 — 처음 GuardDuty 활성화하면 EKS 런타임 모니터링이 기본적으로 활성화되지 않습니다 (런타임 모니터링 릴리스 이후). EKS 런타임 모니터링을 활성화해야 합니다. 최적의 상태로 사용하려면 GuardDuty 보안 에이전트를 수동으로 관리하거나 에이전트를 대신 GuardDuty 관리하도록 자동 에이전트 구성을 활성화해야 합니다. EKS 런타임 모니터링의 30일 무료 평가 기간은 Amazon EKS 리소스에 대한 첫 번째 런타임 이벤트를 GuardDuty 수신할 때 시작됩니다.

런타임 모니터링을 시작하기 전에 EKS 런타임 모니터링을 활성화했습니다.

- EKS 런타임 모니터링 보호 계획이 활성화되어 있고 GuardDuty 콘솔 환경을 사용하여 이 보호 계획을 사용하는 기존 GuardDuty 계정의 경우 — 런타임 모니터링이 발표됨에 따라 EKS 런타임 모니터링 콘솔 환경이 이제 런타임 모니터링으로 통합되었습니다. EKS 런타임 모니터링의 기존 구성은 동일하게 유지됩니다. 계속해서 API/CLI 지원을 사용하여 EKS 런타임 모니터링과 관련된 작업을 수행할 수 있습니다.
- EKS 런타임 모니터링을 런타임 모니터링의 일부로 사용하려면 계정 또는 조직에 대해 런타임 모니터링을 구성해야 합니다. 런타임 모니터링과 동일한 구성을 유지하려면 을 참조하십시오EKS 런타

임 모니터링에서 런타임 모니터링으로 마이그레이션. 하지만 Amazon EKS 리소스의 30일 무료 평가판에는 영향을 주지 않습니다.

- 런타임 모니터링 보호 플랜은 지역별 계정 수준에서 활성화됩니다. GuardDuty 보안 에이전트가 지정된 리소스 유형 (Amazon EC2 인스턴스 및 Amazon ECS 클러스터) 중 하나에 배포된 후, 리소스와 관련된 첫 번째 런타임 이벤트를 GuardDuty 수신하면 30일 무료 평가판이 시작됩니다. 각 리소스 유형과 관련된 30일 무료 평가판이 제공됩니다.

  예를 들어 런타임 모니터링을 활성화한 후 Amazon EC2 인스턴스에만 GuardDuty 에이전트를 배포하도록 선택하면 Amazon EC2 인스턴스에 대한 첫 번째 런타임 이벤트를 GuardDuty 수신할 때만 이 리소스에 대한 30일 무료 평가판이 시작됩니다. 나중에 Fargate용 GuardDuty 에이전트 (Amazon ECS만 해당) 를 배포하면 Amazon ECS 클러스터에 대한 첫 번째 런타임 이벤트를 GuardDuty 수신한 경우에만 이 리소스에 대한 30일 무료 평가판이 시작됩니다. 계정에 EKS 런타임 모니터링이 이미 활성화되어 있다는 점을 고려하면 Amazon EKS 리소스의 30일 무료 평가판을 재설정하지 GuardDuty 않습니다.

주요 개념 - 보안 에이전트 관리 접근 방식 GuardDuty

Amazon EKS 클러스터 및 Amazon ECS 클러스터에서 보안 에이전트를 관리하는 데 도움이 되는 주요 개념을 생각해 보십시오.

내용

- Fargate (Amazon ECS 전용) 리소스 - 보안 에이전트를 관리하는 접근 방식 GuardDuty
- Amazon EKS 클러스터 - GuardDuty 보안 에이전트를 관리하는 접근 방식

Fargate (Amazon ECS 전용) 리소스 - 보안 에이전트를 관리하는 접근 방식 GuardDuty

런타임 모니터링은 계정의 모든 Amazon ECS 클러스터 (계정 수준) 또는 선택적 클러스터 (클러스터 수준) 에서 잠재적인 보안 위협을 탐지하는 옵션을 제공합니다. 실행할 GuardDuty 각 Amazon ECS Fargate 작업에 대해 자동 에이전트 구성을 활성화하면 해당 작업 내의 각 컨테이너 워크로드에 대한 사이드카 컨테이너가 추가됩니다. GuardDuty 보안 에이전트는 이 사이드카 컨테이너에 배포됩니다. 이를 통해 Amazon ECS 작업 내 컨테이너의 런타임 동작을 파악할 수 있습니다. GuardDuty

현재 런타임 모니터링은 Amazon ECS 클러스터 (AWS Fargate) 의 보안 에이전트 관리를 통해서만 지원합니다. GuardDuty Amazon ECS 클러스터에서 보안 에이전트를 수동으로 관리하는 기능은 지원되지 않습니다.

계정을 구성하기 전에 GuardDuty 보안 에이전트를 어떻게 관리할 것인지 평가하고 Amazon ECS 작업에 속하는 컨테이너의 런타임 동작을 잠재적으로 모니터링하십시오. 다음 접근 방식을 고려해 보십시오.

주제

- 모든 Amazon ECS 클러스터의 GuardDuty 보안 에이전트를 관리합니다.
- 대부분의 Amazon ECS 클러스터에 대한 GuardDuty 보안 에이전트를 관리하지만 일부 Amazon ECS 클러스터는 제외합니다.
- 선택적 Amazon ECS 클러스터를 위한 GuardDuty 보안 에이전트 관리

모든 Amazon ECS 클러스터의 GuardDuty 보안 에이전트를 관리합니다.

이 접근 방식은 계정 수준에서 잠재적 보안 위협을 탐지하는 데 도움이 됩니다. 계정에 속한 모든 Amazon ECS 클러스터의 잠재적 보안 위협을 GuardDuty 탐지하려는 경우 이 접근 방식을 사용하십시오.

대부분의 Amazon ECS 클러스터에 대한 GuardDuty 보안 에이전트를 관리하지만 일부 Amazon ECS 클러스터는 제외합니다.

AWS 환경에 있는 대부분의 Amazon ECS 클러스터에 대한 잠재적 보안 위협을 탐지하고 일부 클러스터는 GuardDuty 제외하려는 경우 이 접근 방식을 사용하십시오. 이 접근 방식은 클러스터 수준에서 Amazon ECS 작업 내 컨테이너의 런타임 동작을 모니터링하는 데 도움이 됩니다. 예를 들어, 계정에 속하는 Amazon ECS 클러스터의 수는 1000개입니다. 하지만 930개의 Amazon ECS 클러스터만 모니터링하려고 합니다.

이 방법을 사용하려면 모니터링하지 않으려는 Amazon ECS 클러스터에 미리 정의된 GuardDuty 태그를 추가해야 합니다. 자세한 정보는 Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)을 참조하세요.

선택적 Amazon ECS 클러스터를 위한 GuardDuty 보안 에이전트 관리

일부 Amazon ECS 클러스터의 잠재적 보안 위협을 GuardDuty 탐지하려는 경우 이 접근 방식을 사용하십시오. 이 접근 방식은 클러스터 수준에서 Amazon ECS 작업 내 컨테이너의 런타임 동작을 모니터링하는 데 도움이 됩니다. 예를 들어, 계정에 속하는 Amazon ECS 클러스터의 수는 1000개입니다. 하지만 230개 클러스터만 모니터링하려고 합니다.

이 방법을 사용하려면 모니터링하려는 Amazon ECS 클러스터에 사전 정의된 GuardDuty 태그를 추가해야 합니다. 자세한 정보는 Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)을 참조하세요.

Amazon EKS 클러스터 - GuardDuty 보안 에이전트를 관리하는 접근 방식

계정 수준 또는 클러스터 수준에서 EKS 클러스터의 런타임 이벤트를 GuardDuty 사용하려면 해당 클러스터의 GuardDuty 보안 에이전트를 관리해야 합니다.

GuardDuty보안 에이전트를 관리하는 접근 방식

2023년 9월 13일 이전에는 계정 수준에서 보안 에이전트를 GuardDuty 관리하도록 구성할 수 있었습니다. 이 동작은 기본적으로 에 속하는 모든 EKS 클러스터의 보안 에이전트를 관리한다는 것을 나타냅니다. GuardDuty AWS 계정이제 보안 GuardDuty 에이전트를 관리할 EKS 클러스터를 선택하는 데 도움이 되는 세분화된 기능을 제공합니다. GuardDuty

GuardDuty 보안 에이전트를 수동으로 관리합니다. 방법을 선택한 경우에도 모니터링하려는 EKS 클러스터를 선택할 수 있습니다. 하지만 에이전트를 수동으로 관리하려면 AWS 계정 에 대한 Amazon VPC 엔드포인트를 생성해야 합니다.

> **Note**
>
> GuardDuty 보안 에이전트를 관리하는 데 사용하는 접근 방식에 관계없이 EKS 런타임 모니터링은 계정 수준에서 항상 활성화됩니다.

주제

- 다음을 통해 보안 에이전트를 관리합니다. GuardDuty
- GuardDuty 보안 에이전트를 수동으로 관리합니다.

다음을 통해 보안 에이전트를 관리합니다. GuardDuty

GuardDuty 사용자를 대신하여 보안 에이전트를 배포하고 관리합니다. 언제든 다음 접근 방식 중 하나를 사용하여 계정의 EKS 클러스터를 모니터링할 수 있습니다.

주제

- 모든 EKS 클러스터 모니터링
- 모든 EKS 클러스터를 모니터링하고 선택적 EKS 클러스터 제외
- 선택적 EKS 클러스터 모니터링

모든 EKS 클러스터 모니터링

- 이 접근 방식을 사용하는 경우 - 계정의 모든 EKS 클러스터에 대해 보안 에이전트를 배포하고 GuardDuty 관리하려는 경우 이 접근 방식을 사용합니다. 기본적으로 계정에서 새로 만든 EKS 클러스터에도 보안 에이전트를 배포합니다. GuardDuty
- 이 접근 방식을 사용할 때의 영향:
  - GuardDuty GuardDuty 보안 에이전트가 런타임 이벤트를 전송하는 Amazon VPC (가상 사설 클라우드) 엔드포인트를 생성합니다. GuardDuty 보안 에이전트를 관리하는 경우 Amazon VPC 엔드포인트를 생성하는 데 드는 추가 비용은 없습니다. GuardDuty
  - 작업자 노드에 활성 `guardduty-data` VPC 엔드포인트에 대한 유효한 네트워크 경로가 있어야 합니다. GuardDuty EKS 클러스터에 보안 에이전트를 배포합니다. Amazon Elastic Kubernetes Service(Amazon EKS)는 EKS 클러스터 내의 노드에 보안 에이전트 배포를 조정합니다.
  - IP 가용성에 따라 VPC 엔드포인트를 생성할 서브넷을 GuardDuty 선택합니다. 고급 네트워크 토폴로지를 사용하는 경우 연결이 가능한지 검증해야 합니다.
- 고려 사항 - 현재 이 옵션을 사용하면 EKS 런타임 모니터링에서 공유 VPC를 생성하지 않습니다.

모든 EKS 클러스터를 모니터링하고 선택적 EKS 클러스터 제외

- 이 접근 방식을 사용하는 경우 - 계정의 모든 EKS 클러스터에 대한 보안 에이전트를 관리하되 선택적 EKS 클러스터는 GuardDuty 제외하려는 경우 이 방법을 사용합니다. 이 방법은 런타임 이벤트를 수신하지 않으려는 EKS 클러스터에 태그를 지정할 수 있는 태그 기반[1] 접근 방식을 사용합니다. 사전 정의된 태그에는 키-값 쌍으로 `GuardDutyManaged-false`가 있어야 합니다.
- 이 접근 방식을 사용할 때의 영향:
  - 이 방법을 사용하려면 모니터링에서 제외하려는 EKS 클러스터에 태그를 추가한 후에만 GuardDuty 에이전트 자동 관리를 활성화해야 합니다.

    따라서 다음을 통해 보안 에이전트를 관리합니다. GuardDuty 의 영향이 이 접근 방식에도 적용됩니다. GuardDuty 에이전트 자동 관리를 활성화하기 전에 태그를 추가하면 모니터링에서 제외되는 EKS 클러스터의 보안 에이전트를 배포하거나 관리하지 않습니다. GuardDuty
- 고려 사항:
  - 자동 에이전트 구성을 활성화하기 전에 선택적 EKS 클러스터의 `false` 경우 태그 키-값 쌍을 `GuardDutyManaged` 다음과 같이 추가해야 합니다. 그렇지 않으면 태그를 사용할 때까지 GuardDuty 보안 에이전트가 모든 EKS 클러스터에 배포됩니다.
  - 신뢰할 수 있는 ID를 제외하고는 태그가 수정되지 않도록 해야 합니다.

> **Important**
>
> 서비스 제어 정책 또는 IAM 정책을 사용하여 EKS 클러스터의 GuardDutyManaged 태그 값을 수정하는 권한을 관리합니다. 자세한 내용은 사용 설명서의 서비스 제어 정책 (SCP) 또는 IAM AWS Organizations 사용 설명서의 AWS 리소스 액세스 제어를 참조하십시오.

- 모니터링하지 않으려는 잠재적으로 새로운 EKS 클러스터의 경우 이 EKS 클러스터를 생성할 때 GuardDutyManaged-false 키-값 쌍을 추가해야 합니다.
- 이 접근 방식에도 모든 EKS 클러스터 모니터링에 대해 지정된 것과 동일한 고려 사항이 적용됩니다.

선택적 EKS 클러스터 모니터링

- 이 방법을 사용하는 경우 — 계정의 선택적 EKS 클러스터에 대한 업데이트만 보안 에이전트에 배포하고 GuardDuty 관리하려는 경우 이 방법을 사용하십시오. 이 방법은 런타임 이벤트를 수신하려는 EKS 클러스터에 태그를 지정할 수 있는 태그 기반[1] 접근 방식을 사용합니다.
- 이 접근 방식을 사용할 때의 영향:
  - 는 포함 태그를 사용하여 키-값 true 쌍으로 GuardDutyManaged -로 태그가 지정된 선택적 EKS 클러스터에 대해서만 보안 에이전트를 GuardDuty 자동으로 배포하고 관리합니다.
  - 이 접근 방식을 사용해도 모든 EKS 클러스터 모니터링에 대해 지정된 것과 동일한 영향을 미칩니다.
- 고려 사항:
  - GuardDutyManaged 태그의 값이 true로 설정되지 않으면 포함 태그가 예상대로 작동하지 않고 EKS 클러스터 모니터링에 영향을 미칠 수 있습니다.
  - 선택적 EKS 클러스터가 모니터링되도록 신뢰할 수 있는 ID를 제외하고는 태그가 수정되지 않도록 해야 합니다.

> **Important**
>
> 서비스 제어 정책 또는 IAM 정책을 사용하여 EKS 클러스터의 GuardDutyManaged 태그 값을 수정하는 권한을 관리합니다. 자세한 내용은 사용 설명서의 서비스 제어 정책 (SCP) 또는 IAM AWS Organizations 사용 설명서의 AWS 리소스 액세스 제어를 참조하십시오.

- 모니터링하지 않으려는 잠재적으로 새로운 EKS 클러스터의 경우 이 EKS 클러스터를 생성할 때 GuardDutyManaged-false 키-값 쌍을 추가해야 합니다.

- 이 접근 방식에도 모든 EKS 클러스터 모니터링에 대해 지정된 것과 동일한 고려 사항이 적용됩니다.

[1] 선택적 EKS 클러스터의 태그 지정에 대한 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS 리소스 태깅을 참조하세요.

GuardDuty 보안 에이전트를 수동으로 관리합니다.

- 이 접근 방식을 사용하는 경우 - 모든 EKS 클러스터에서 GuardDuty 보안 에이전트를 수동으로 배포하고 관리하려는 경우 이 접근 방식을 사용합니다. 계정에 EKS 런타임 모니터링이 활성화되어 있어야 합니다. EKS 런타임 모니터링을 활성화하지 않으면 GuardDuty 보안 에이전트가 예상대로 작동하지 않을 수 있습니다.
- 이 접근 방식 사용의 영향 — 모든 계정과 이 기능을 사용할 수 AWS 리전 있는 곳에서 EKS 클러스터 내 GuardDuty 보안 에이전트 소프트웨어 배포를 조정해야 합니다.
- 고려 사항 - 새 클러스터와 워크로드가 지속적으로 배포되는 상황에서 적용 범위 격차를 모니터링하고 해결하면서 안전한 데이터 흐름을 지원해야 합니다.

GuardDuty 런타임 모니터링 활성화

계정에서 런타임 모니터링을 활성화하기 전에 런타임 이벤트를 모니터링하려는 리소스 유형이 플랫폼 요구 사항을 지원하는지 확인하십시오. 자세한 정보는 필수 조건을 참조하세요.

런타임 모니터링을 시작하기 전에 EKS 런타임 모니터링을 사용한 경우 API를 사용하여 EKS 런타임 모니터링의 기존 구성을 확인하고 업데이트할 수 있습니다. 기존 구성을 EKS 런타임 모니터링에서 런타임 모니터링으로 마이그레이션할 수도 있습니다. 자세한 정보는 EKS 런타임 모니터링에서 런타임 모니터링으로 마이그레이션을 참조하세요.

> **Note**
>
> 현재 이 설명서에서는 콘솔로만 계정 및 조직에 대해 런타임 모니터링을 활성화하는 단계를 제공합니다. API Actions 또는 for를 사용하여 런타임 AWS CLI 모니터링을 GuardDuty 활성화할 수도 있습니다.

다음 항목의 단계를 사용하여 런타임 모니터링을 구성할 수 있습니다.

내용

런타임 모니터링을 활성화하기 위한 사전 요구 사항

런타임 모니터링을 활성화하고 GuardDuty 보안 에이전트를 관리하려면 위협 탐지를 위해 모니터링하려는 각 리소스 유형의 사전 요구 사항을 충족해야 합니다.

내용

Amazon EC2 인스턴스 지원을 위한 사전 요구 사항

EC2 인스턴스를 SSM 관리형으로 설정

런타임 이벤트를 GuardDuty 모니터링하려는 Amazon EC2 인스턴스는 AWS Systems Manager (SSM) 관리 대상이어야 합니다. 이는 보안 에이전트를 자동으로 관리하는 GuardDuty 데 사용하든 수동으로 관리하는 데 사용하든 상관 없습니다 (제외방법 2 - RPM 설치 스크립트 사용).

를 사용하여 Amazon EC2 인스턴스를 관리하려면 사용 AWS Systems Manager설명서의 Amazon EC2 인스턴스용 Systems Manager 설정을 참조하십시오.AWS Systems Manager

아키텍처 요구 사항 검증

OS 배포의 아키텍처는 GuardDuty 보안 에이전트의 작동 방식에 영향을 미칠 수 있습니다. Amazon EC2 인스턴스에 대한 런타임 모니터링을 사용하기 전에 다음 요구 사항을 충족해야 합니다.

- 현재 Amazon EC2에 대한 런타임 모니터링 지원은 Linux 버전에서만 사용할 수 있습니다. 우분투에 대한 지원은 현재 제공되지 않지만 가까운 장래에 지원될 예정입니다. 이 페이지의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

  다음 표는 Amazon EC2 인스턴스용 GuardDuty 보안 에이전트를 지원하는 것으로 확인된 OS 배포를 보여줍니다.

OS 배포판	커널 버전	커널 지원	CPU 아키텍처	
			x64(AMD64)	Graviton(ARM64)
AL2 및 AL2023	5.4, 5.10, 5.15, 6.1 * -	eBPF, Tracepoints, Kprobe	지원	지원

- 추가 요구 사항 - Amazon ECS/Amazon EC2가 있는 경우에만

  Amazon ECS/Amazon EC2의 경우, Amazon ECS에 최적화된 최신 AMI (2023년 9월 29일 또는 이후 날짜) 를 사용하거나 Amazon ECS 에이전트 버전 v1.77.0을 사용하는 것이 좋습니다.

- *현재 커널 버전에서는 다음과 관련된 항목을 생성할 수 없습니다. `6.1` GuardDuty 런타임 모니터링 검색 유형 DNS 이벤트

조직 서비스 제어 정책 검증

조직의 권한을 관리하기 위해 SCP (서비스 제어 정책) 를 설정한 경우 정책이 권한을 거부하지 않는지 확인하세요. `guardduty:SendSecurityTelemetry` 다양한 리소스 유형에서 런타임 GuardDuty 모니터링을 지원하는 데 필요합니다.

멤버 계정인 경우 연결된 위임 관리자와 연결하세요. 조직의 SCP 관리에 대한 자세한 내용은 서비스 제어 정책 (SCP) 을 참조하십시오.

자동 에이전트 구성을 사용하는 경우

자동 에이전트 구성 사용 (권장)하려면 다음 사전 요구 사항을 AWS 계정 충족해야 합니다.

- 자동 에이전트 구성과 함께 포함 태그를 사용하는 경우 새 인스턴스에 대한 SSM 연결을 GuardDuty 생성하려면 새 인스턴스가 SSM으로 관리되고 https://console.aws.amazon.com/systems-manager/ 콘솔의 Fleet Manager에 표시되는지 확인하십시오.
- 자동 에이전트 구성과 함께 제외 태그를 사용하는 경우:
  - 계정의 GuardDuty 자동 에이전트를 구성하기 전에`GuardDutyManaged: false` 태그를 추가하세요.

Amazon EC2 인스턴스를 시작하기 전에 해당 인스턴스에 제외 태그를 추가해야 합니다. Amazon EC2용 자동 에이전트 구성을 활성화하면 제외 태그 없이 시작되는 모든 EC2 인스턴스가 자동 에이전트 구성의 적용을 받게 GuardDuty 됩니다.

- 제외 태그가 작동하도록 하려면 인스턴스 구성을 업데이트하여 인스턴스 ID 문서를 인스턴스 메타데이터 서비스 (IMDS) 에서 사용할 수 있도록 하십시오. 이 단계를 수행하는 절차는 이미 계정에 포함되어 있습니다Runtime Monitoring 활성화.

GuardDuty 상담원의 CPU 및 메모리 제한

CPU 제한

Amazon EC2 인스턴스와 연결된 GuardDuty 보안 에이전트의 최대 CPU 한도는 총 vCPU 코어의 10% 입니다. 예를 들어 EC2 인스턴스에 vCPU 코어 4개가 있는 경우 보안 에이전트는 사용 가능한 총 400퍼센트 중 최대 40% 를 사용할 수 있습니다.

메모리 제한

Amazon EC2 인스턴스와 연결된 메모리에는 GuardDuty 보안 에이전트가 사용할 수 있는 제한된 메모리가 있습니다.

다음 표는 메모리 제한을 보여줍니다.

Amazon EC2 인스턴스의 메모리	에이전트의 GuardDuty 최대 메모리
8GB 미만	128MB
32기가바이트 미만	256MB
32GB 이상 또는 이와 같음	1GB

다음 단계

다음 단계는 런타임 모니터링을 구성하고 보안 에이전트를 관리하는 것입니다 (자동 또는 수동).

지원을 위한 사전 요구 사항 (AWS Fargate Amazon ECS만 해당)

아키텍처 요구 사항 검증

사용하는 플랫폼은 GuardDuty 보안 에이전트가 Amazon ECS 클러스터로부터 런타임 이벤트를 수신하도록 지원하는 GuardDuty 방식에 영향을 미칠 수 있습니다. 확인된 플랫폼 중 하나를 사용하고 있는지 검증해야 합니다.

초기 고려 사항:

- Amazon ECS 클러스터용 AWS Fargate (Fargate) 플랫폼은 Linux여야 합니다. 해당 플랫폼 버전은 최소 `1.4.0` 또는 `LATEST` 이상이어야 합니다. 플랫폼 버전에 대한 자세한 내용은 Amazon Elastic 컨테이너 서비스 개발자 안내서의 Linux 플랫폼 버전을 참조하십시오.

- Windows 플랫폼 버전은 아직 지원되지 않습니다.

검증된 플랫폼

OS 배포 및 CPU 아키텍처는 GuardDuty 보안 에이전트가 제공하는 지원에 영향을 줍니다. 다음 표는 GuardDuty 보안 에이전트를 배포하고 런타임 모니터링을 구성하기 위한 검증된 구성을 보여줍니다.

OS 배포판	커널 지원	CPU 아키텍처	
		x64(AMD64)	Graviton(ARM64)
Linux	eBPF, Tracepoints, Kprobe	지원	지원

ECR 권한 및 서브넷 세부 정보를 제공하십시오.

런타임 모니터링을 활성화하기 전에 다음 세부 정보를 제공해야 합니다.

권한이 있는 작업 실행 역할을 제공하십시오.

- 작업 실행 역할을 수행하려면 특정 Amazon Elastic Container 레지스트리 (Amazon ECR) 권한이 있어야 합니다. TaskExecutionRolePolicyAmazonECS 관리형 정책을 사용하거나 정책에 다음 권한을 추가할 수 있습니다. `TaskExecutionRole`

```
...
```

```
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Amazon ECR 권한을 더 제한하려면 GuardDuty 보안 에이전트를 호스팅하는 Amazon ECR 리포지토리 URI를 추가할 수 있습니다 (AWS Fargate Amazon ECS만 해당). 자세한 정보는 GuardDuty 에이전트용 리포지토리 AWS Fargate (Amazon ECS만 해당)을 참조하세요.

작업 정의에 서브넷 세부 정보를 제공하십시오.

퍼블릭 서브넷을 작업 정의의 입력으로 제공하거나 Amazon ECR VPC 엔드포인트를 생성할 수 있습니다.

- 작업 정의 옵션 사용 — Amazon Elastic Container Service API 참조에서 CreateService및 UpdateServiceAPI를 실행하려면 서브넷 정보를 전달해야 합니다. 자세한 내용은 Amazon Elastic 컨테이너 서비스 개발자 안내서의 Amazon ECS 작업 정의를 참조하십시오.
- Amazon ECR VPC 엔드포인트 옵션 사용 — Amazon ECR에 네트워크 경로 제공 - 보안 에이전트를 GuardDuty 호스팅하는 Amazon ECR 리포지토리 URI가 네트워크에서 액세스할 수 있는지 확인합니다. Fargate 작업이 프라이빗 서브넷에서 실행되는 경우 Fargate는 컨테이너를 다운로드하기 위한 네트워크 경로가 필요합니다. GuardDuty

  Fargate에서 컨테이너를 다운로드할 수 있도록 설정하는 방법에 대한 자세한 내용은 Amazon Elastic GuardDuty 컨테이너 서비스 개발자 안내서의 Amazon ECS와 Amazon ECR 사용을 참조하십시오.

조직 서비스 제어 정책 검증

조직의 권한을 관리하기 위해 SCP (서비스 제어 정책) 를 설정한 경우 정책이 권한을 거부하지 않는지 확인하세요. `guardduty:SendSecurityTelemetry` 다양한 리소스 유형에서 런타임 GuardDuty 모니터링을 지원하는 데 필요합니다.

멤버 계정인 경우 연결된 위임 관리자와 연결하세요. 조직의 SCP 관리에 대한 자세한 내용은 서비스 제어 정책 (SCP) 을 참조하십시오.

CPU 및 메모리 제한

Fargate 작업 정의에서는 작업 수준에서 CPU 및 메모리 값을 지정해야 합니다. 다음 표에는 작업 수준 CPU와 메모리 값의 유효한 조합과 해당 GuardDuty Security Agent의 컨테이너의 최대 메모리 제한이 나와 있습니다. GuardDuty

CPU 값	메모리 값	GuardDuty 에이전트 최대 메모리 제한
256(.25 vCPU)	512메가바이트, 1기가바이트, 2기가바이트	128MB
512(.5 vCPU)	1GB, 2GB, 3GB, 4GB	
1024(1 vCPU)	2기가바이트, 3기가바이트, 4기가바이트	
	5기가바이트, 6기가바이트, 7기가바이트, 8기가바이트	
2048(2 vCPU)	4~16GB(1GB 증분)	
4096(4 vCPU)	8GB에서 20GB 사이 (1GB 단위로 증가)	
8192 (8 vCPU)	16GB에서 28GB 사이 (4GB 단위로 증가)	256MB
	32GB에서 60GB 사이 (4GB 단위로 증가)	512MB
16384 (16 vCPU)	32~120GB(8GB 증분)	1GB

런타임 모니터링을 활성화하고 클러스터의 커버리지 상태가 정상인지 평가한 후 컨테이너 인사이트 메트릭을 설정하고 볼 수 있습니다. 자세한 설명은 Amazon ECS 클러스터에서 모니터링 설정 섹션을 참조하십시오.

다음 단계는 런타임 모니터링을 구성하고 보안 에이전트도 구성하는 것입니다.

Amazon EKS 클러스터 지원을 위한 사전 요구 사항

아키텍처 요구 사항 검증

사용하는 플랫폼은 GuardDuty 보안 에이전트가 EKS GuardDuty 클러스터의 런타임 이벤트 수신을 지원하는 방식에 영향을 미칠 수 있습니다. 확인된 플랫폼 중 하나를 사용하고 있는지 검증해야 합니다.

GuardDuty 에이전트를 수동으로 관리하는 경우 Kubernetes 버전이 현재 사용 중인 GuardDuty 에이전트 버전을 지원하는지 확인하십시오.

검증된 플랫폼

OS 배포판, 커널 버전 및 CPU 아키텍처는 보안 에이전트가 제공하는 지원에 영향을 줍니다. GuardDuty 다음 표에는 GuardDuty 보안 에이전트 배포 및 EKS 런타임 모니터링 구성을 위한 검증된 구성이 나와 있습니다.

OS 배포판	커널 버전	커널 지원	CPU 아키텍처		지원되는 Kubernetes 버전
			x64(AMD64)	Graviton(ARM64) (Graviton2 이상) [1]	
Ubuntu AL2 AL2023 [3]	5.4, 5.10, 5.15, 6.1 [2]	eBPF 트레이스포인트, 케이프로브	지원	지원	v1.21 - v1.29
Bottlerocket					v1.23 - v1.29

1. Amazon EKS 클러스터의 런타임 모니터링은 A1 인스턴스 유형과 같은 1세대 Graviton 인스턴스를 지원하지 않습니다.
2. 현재 커널 `6.1` 버전에서는 GuardDuty 다음과 관련된 항목을 생성할 런타임 모니터링 검색 유형 수 없습니다. DNS 이벤트
3. 런타임 모니터링은 GuardDuty 보안 에이전트 v1.6.0 이상이 릴리스된 AL2023 버전부터 지원합니다. 자세한 정보는 GuardDuty Amazon EKS 클러스터용 보안 에이전트을 참조하세요.

보안 에이전트가 지원하는 쿠버네티스 버전 GuardDuty

다음 표는 보안 에이전트가 지원하는 EKS 클러스터의 Kubernetes 버전을 보여줍니다. GuardDuty

Kubernetes 버전	Amazon EKS 애드온 GuardDuty 보안 에이전트 버전									
	v1.6.1	v1.6.0	v1.5.0	v1.4.1	v1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1.29	지원	지원	지원	지원	지원	지원 되지 않음	지원 되지 않음	지원 되지 않음	지원 되지 않음	지원 되지 않음
1.28						지원	지원			
1.27								지원		
1.26									지원	
1.25										지원
1.24										
1.23										
1.22										
1.21										

일부 GuardDuty 보안 에이전트 버전은 표준 지원이 종료됩니다. 에이전트 릴리스 버전에 대한 자세한 내용은 을 참조하십시오GuardDuty Amazon EKS 클러스터용 보안 에이전트.

CPU 및 메모리 제한

다음 표는 GuardDuty () `aws-guardduty-agent` 에 대한 Amazon EKS 추가 기능의 CPU 및 메모리 제한을 보여줍니다.

파라미터	최소 제한	최대 제한
CPU	200m	1,000m
메모리	256Mi	1024Mi

Amazon EKS 추가 기능 버전 1.5.0 이상을 사용하는 경우 CPU 및 메모리 값에 대한 추가 스키마를 구성할 수 있는 기능이 GuardDuty 제공됩니다. 구성 가능 범위에 대한 자세한 내용은 을 참조하십시오. 구성 가능한 파라미터 및 값

EKS 런타임 모니터링을 활성화하고 EKS 클러스터의 적용 범위 상태를 평가한 후 컨테이너 인사이트 지표를 설정하고 볼 수 있습니다. 자세한 정보는 CPU 및 메모리 모니터링 설정을 참조하세요.

다음 단계

다음 단계는 런타임 모니터링을 구성하고 보안 에이전트를 수동 또는 자동으로 관리하는 것입니다. GuardDuty

독립형 계정에 대해 런타임 모니터링을 활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 구성 탭에서 활성화를 선택하여 계정에 대한 런타임 모니터링을 활성화합니다.
4. Amazon EC2 인스턴스, Amazon ECS 클러스터 또는 Amazon EKS 클러스터 등 하나 이상의 리소스 유형에서 런타임 이벤트를 GuardDuty 수신하려면 다음 옵션을 사용하여 해당 리소스의 보안 에이전트를 관리하십시오.

   보안 에이전트를 활성화하려면 GuardDuty

   - Amazon EC2 인스턴스용 자동 보안 에이전트 관리
   - Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리
   - Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)
   - Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리
   - Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

다중 계정 환경에 대한 런타임 모니터링 활성화

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만이 구성원 계정에 대한 런타임 모니터링을 활성화 또는 비활성화하고 조직의 구성원 계정에 속하는 리소스 유형에 대한 자동 에이전트 구성을 관리할 수 있습니다. GuardDuty 구성원 계정은 자신의 계정에서 이 구성을 수정할 수 없습니다. 위임된

GuardDuty 관리자 계정 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 다중 계정 환경에 대한 자세한 내용은 Managing multiple accounts를 참조하세요.

위임된 관리자 계정의 GuardDuty 경우

위임된 GuardDuty 관리자 계정에 대해 런타임 모니터링을 활성화하려면

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 구성 탭 아래의 런타임 모니터링 구성 섹션에서 편집을 선택합니다.
4. 모든 계정에 대해 활성화 사용

   위임된 GuardDuty 관리자 계정을 포함하여 조직에 속한 모든 계정에 대해 런타임 모니터링을 활성화하려면 모든 계정에 대해 활성화를 선택합니다.
5. 수동으로 계정 구성 사용

   각 구성원 계정에 대해 개별적으로 런타임 모니터링을 활성화하려면 계정 수동 구성을 선택합니다.

   - 위임된 관리자(이 계정) 섹션에서 활성화를 선택합니다.
6. Amazon EC2 인스턴스, Amazon ECS 클러스터 또는 Amazon EKS 클러스터 등 하나 이상의 리소스 유형에서 런타임 이벤트를 GuardDuty 수신하려면 다음 옵션을 사용하여 해당 리소스의 보안 에이전트를 관리하십시오.

   보안 에이전트를 활성화하려면 GuardDuty

   - Amazon EC2 인스턴스용 자동 보안 에이전트 관리
   - Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리
   - Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)
   - Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리
   - Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

모든 회원 계정용

조직의 모든 구성원 계정에 대해 런타임 모니터링을 활성화하려면

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정을 사용하여 로그인합니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 런타임 모니터링 페이지의 구성 탭 아래에 있는 런타임 모니터링 구성 섹션에서 편집을 선택합니다.
4. 모든 계정에 대해 활성화를 선택합니다.
5. Amazon EC2 인스턴스, Amazon ECS 클러스터 또는 Amazon EKS 클러스터 등 하나 이상의 리소스 유형에서 런타임 이벤트를 GuardDuty 수신하려면 다음 옵션을 사용하여 해당 리소스의 보안 에이전트를 관리하십시오.

   보안 에이전트를 활성화하려면 GuardDuty

   - Amazon EC2 인스턴스용 자동 보안 에이전트 관리
   - Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리
   - Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)
   - Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리
   - Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

모든 기존 활성 회원 계정의 경우

조직의 기존 구성원 계정에 대해 런타임 모니터링을 활성화하려면

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   조직의 위임된 GuardDuty 관리자 계정을 사용하여 로그인합니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 런타임 모니터링 페이지의 구성 탭에서 런타임 모니터링 구성의 현재 상태를 볼 수 있습니다.
4. 런타임 모니터링 창의 활성 구성원 계정 섹션 아래에서 작업을 선택합니다.
5. 작업 드롭다운 메뉴에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다.

6. 확인을 선택합니다.
7. Amazon EC2 인스턴스, Amazon ECS 클러스터 또는 Amazon EKS 클러스터 등 하나 이상의 리소스 유형에서 런타임 이벤트를 GuardDuty 수신하려면 다음 옵션을 사용하여 해당 리소스의 보안 에이전트를 관리하십시오.

   보안 에이전트를 활성화하려면 GuardDuty

   - Amazon EC2 인스턴스용 자동 보안 에이전트 관리
   - Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리
   - Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)
   - Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리
   - Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

> **Note**
>
> 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

신규 회원 계정에만 런타임 모니터링을 자동 활성화합니다.

조직의 새 구성원 계정에 대해 런타임 모니터링을 활성화하려면

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   조직의 지정된 위임 GuardDuty 관리자 계정을 사용하여 로그인합니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 구성 탭의 런타임 모니터링 구성 섹션에서 편집을 선택합니다.
4. 수동으로 계정 구성을 선택합니다.
5. 새 멤버 계정에 대해 자동으로 활성화를 선택합니다.
6. Amazon EC2 인스턴스, Amazon ECS 클러스터 또는 Amazon EKS 클러스터 등 하나 이상의 리소스 유형에서 런타임 이벤트를 GuardDuty 수신하려면 다음 옵션을 사용하여 해당 리소스의 보안 에이전트를 관리하십시오.

   보안 에이전트를 활성화하려면 GuardDuty

   - Amazon EC2 인스턴스용 자동 보안 에이전트 관리

- Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리
- Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)
- Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리
- Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

선택적 활성 멤버 계정에만 해당됩니다.

개별 활성 멤버 계정에 대해 런타임 모니터링을 활성화하려면

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.
3. 계정 페이지에서 런타임 모니터링 및 에이전트 자동 관리 열의 값을 검토하십시오. 이 값은 해당 계정에 대해 런타임 모니터링 및 GuardDuty 에이전트 관리가 활성화되었는지 아니면 활성화되지 않았는지를 나타냅니다.
4. 계정 테이블에서 런타임 모니터링을 활성화하려는 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다.
5. 확인을 선택합니다.
6. 보호 계획 편집을 선택합니다. 적절한 작업을 선택합니다.
7. 확인을 선택합니다.
8. Amazon EC2 인스턴스, Amazon ECS 클러스터 또는 Amazon EKS 클러스터 등 하나 이상의 리소스 유형에서 런타임 이벤트를 GuardDuty 수신하려면 다음 옵션을 사용하여 해당 리소스의 보안 에이전트를 관리하십시오.

   보안 에이전트를 활성화하려면 GuardDuty

   - Amazon EC2 인스턴스용 자동 보안 에이전트 관리
   - Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리
   - Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)
   - Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리
   - Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

GuardDuty 보안 에이전트 관리

모니터링하려는 리소스의 GuardDuty 보안 에이전트를 관리할 수 있습니다. 둘 이상의 리소스 유형을 모니터링하려면 해당 리소스의 GuardDuty 에이전트를 관리해야 합니다.

> **Important**
>
> Amazon EC2 인스턴스용 GuardDuty 보안 에이전트를 사용하는 경우 Amazon EKS 클러스터 내의 기본 호스트에 에이전트를 설치하여 사용할 수 있습니다. 해당 EKS 클러스터에 보안 에이전트를 이미 배포한 경우 동일한 호스트에서 동시에 두 개의 보안 에이전트를 실행할 수 있습니다. 이 시나리오의 GuardDuty 작동 방식에 대한 자세한 내용은 을 참조하십시오이중 보안 에이전트 처리.

다음 항목은 보안 에이전트를 관리하기 위한 다음 단계를 안내합니다.

내용

- 자동화된 보안 에이전트와 공유 VPC 사용
- 호스트에 설치된 이중 보안 에이전트 처리
- Amazon EC2 인스턴스용 자동 보안 에이전트 관리
- Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리
- Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)
- Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리
- Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

자동화된 보안 에이전트와 공유 VPC 사용

보안 에이전트를 자동으로 GuardDuty 관리하도록 선택하면 Runtime Monitoring은 에서 동일한 조직에 속하는 공유 VPC를 사용할 수 AWS 계정 있도록 지원합니다. AWS Organizations사용자를 대신하여 조직의 공유 VPC와 관련된 세부 정보를 기반으로 Amazon VPC 엔드포인트 정책을 설정할 GuardDuty 수 있습니다.

이번 릴리스 이전에는 GuardDuty 보안 에이전트를 수동으로 관리하도록 선택한 경우에만 공유 VPC 사용이 GuardDuty 지원되었습니다.

내용

작동 방식

공유 VPC의 소유자 계정으로 모든 리소스 (Amazon EKS 또는 (AWS Fargate Amazon ECS만 해당)에 대한 런타임 모니터링 및 자동 에이전트 구성을 활성화하면 모든 공유 VPC가 공유 Amazon VPC 엔드포인트 및 공유 VPC 소유자 계정의 관련 보안 그룹을 자동으로 설치할 수 있습니다. GuardDuty 공유된 Amazon VPC와 연결된 조직 ID를 검색합니다.

이제 공유 Amazon VPC 소유자 계정과 동일한 조직에 속한 사용자도 동일한 Amazon VPC 엔드포인트를 공유할 수 있습니다. AWS 계정 GuardDuty 공유 VPC 소유자 계정 또는 참여 계정에 Amazon VPC 엔드포인트가 필요할 때 공유 VPC를 생성합니다. Amazon VPC 엔드포인트가 필요한 예로는 GuardDuty 활성화, 런타임 모니터링, EKS 런타임 모니터링 또는 새 Amazon ECS-Fargate 작업 시작 등이 있습니다. 이러한 계정이 모든 리소스 유형에 대해 Runtime Monitoring 및 자동 에이전트 구성을 활성화하면 Amazon VPC 엔드포인트를 GuardDuty 생성하고 공유 VPC 소유자 계정과 동일한 조직 ID를 사용하여 엔드포인트 정책을 설정합니다. GuardDuty `GuardDutyManaged`태그를 추가하고 생성한 Amazon VPC 엔드포인트에 `true` 대해 이 태그를 로 설정합니다. GuardDuty 공유된 Amazon VPC 소유자 계정이 리소스에 대해 런타임 모니터링 또는 자동 에이전트 구성을 활성화하지 않은 경우 Amazon VPC 엔드포인트 정책을 설정하지 않습니다. GuardDuty 공유 VPC 소유자 계정에서 런타임 모니터링을 구성하고 보안 에이전트를 자동으로 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. GuardDuty 런타임 모니터링 활성화

동일한 Amazon VPC 엔드포인트 정책을 사용하는 각 계정을 연결된 공유 Amazon VPC의 참가자 AWS 계정이라고 합니다.

다음 예는 공유 VPC 소유자 계정과 참가자 계정의 기본 VPC 엔드포인트 정책을 보여줍니다. 에는 공유 VPC 리소스와 연결된 조직 ID가 `aws:PrincipalOrgID` 표시됩니다. 이 정책의 사용은 소유자 계정의 조직에 있는 참가자 계정으로만 제한됩니다.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
```

```
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

공유 VPC 사용을 위한 사전 요구 사항

초기 설정을 위한 사전 요구 사항

공유 VPC의 소유자가 되려면 다음 단계를 수행하십시오. AWS 계정

1. 조직 생성 — AWS Organizations 사용 설명서의 조직 생성 및 관리에 나와 있는 단계에 따라 조직을 생성합니다.

   구성원 계정 추가 또는 제거에 대한 자세한 내용은 조직 AWS 계정 내 관리를 참조하십시오.
2. 공유 VPC 리소스 생성 - 소유자 계정에서 공유 VPC 리소스를 만들 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유하기를 참조하세요.

런타임 모니터링과 관련된 사전 요구 사항 GuardDuty

다음 목록은 다음과 관련된 사전 요구 사항을 제공합니다. GuardDuty

- 공유 VPC의 소유자 계정과 참여 계정은 내 다른 조직의 소유일 수 있습니다. GuardDuty 하지만 해당 사용자는 에서 AWS Organizations같은 조직에 속해야 합니다. 이는 Amazon VPC 엔드포인트와 공유 VPC의 보안 그룹을 생성하는 GuardDuty 데 필요합니다. 공유 VPC의 작동 방식에 대한 자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유를 참조하십시오.
- 공유 VPC 소유자 계정 및 참가자 계정의 모든 리소스에 대해 런타임 모니터링 또는 EKS 런타임 모니터링과 GuardDuty 자동화된 에이전트 구성을 활성화합니다. 자세한 정보는 Runtime Monitoring 활성화을 참조하세요.

이러한 구성을 이미 완료한 경우 다음 단계를 계속 진행하십시오.

- Amazon EKS 또는 Amazon ECS (AWS Fargate 전용) 작업을 사용할 때는 소유자 계정과 연결된 공유 VPC 리소스를 선택하고 해당 서브넷을 선택해야 합니다.

FAQ

다음 목록은 런타임 모니터링에서 GuardDuty 자동 에이전트 구성을 활성화한 상태에서 공유 VPC 리소스를 사용할 때 자주 묻는 질문에 대한 문제 해결 단계를 제공합니다.

저는 이미 런타임 모니터링 (또는 EKS 런타임 모니터링) 을 사용하고 있습니다. 공유 VPC를 활성화하려면 어떻게 해야 하나요?

공유 VPC를 만들기 위한 사전 요구 사항에 대한 자세한 내용은 을 참조하십시오. 필수 조건

공유 VPC 소유자 계정과 참가자 계정이 모두 사전 요구 사항을 GuardDuty 충족하면 Amazon VPC 엔드포인트 정책을 자동으로 설정하려고 시도합니다.

이번 릴리스 이전에 공유 VPC가 지원되지 않는 것에 대한 적용 범위 문제가 발생한 경우 사전 요구 사항을 따르십시오. AWS 계정 리소스 유형 (Amazon EKS 또는 Amazon ECS (AWS Fargate 전용) 작업) 이 공유 VPC 엔드포인트의 요구 사항을 GuardDuty 호출하면 새 VPC 엔드포인트 정책 설정을 시도합니다.

공유 VPC 소유자 계정으로서 공유 VPC 엔드포인트 정책을 조직 내 참가자 계정의 하위 집합으로 제한하고 싶습니다. 어떻게 해야 하나요?

엔드포인트와 연결된`GuardDutyManaged: true` 태그가 있는 경우 제거하세요. 이렇게 하면 공유 VPC의 VPC 엔드포인트 정책을 수정하거나 GuardDuty 재정의하려는 시도가 방지됩니다.

자세한 정보는 엔드포인트 정책을 사용하여 VPC 엔드포인트에 대한 액세스 제어를 참조하세요.

공유 VPC 엔드포인트가 에서 로 수정되는 **`aws:PrincipalAccount`** 이유는 무엇입니까? **`aws:PrincipalOrgId`** 이를 방지하려면 어떻게 해야 하나요?

에서 동일한 조직의 여러 AWS Organizations계정에서 GuardDuty VPC를 공유하는 것이 GuardDuty 감지되면 조직 ID를 지정하도록 정책을 수정하려고 시도합니다.

이를 방지하려면 공유 VPC `GuardDutyManaged` `true` 엔드포인트에서: 태그를 제거하세요. 이렇게 하면 공유 VPC의 VPC 엔드포인트 정책을 수정하거나 GuardDuty 재정의하려는 시도가 방지됩니다.

공유 VPC 소유자 계정 또는 참가자 계정 중 하나가 런타임 모니터링 (또는 EKS 런타임 모니터링) 을 GuardDuty 비활성화하면 어떻게 되나요?

공유 VPC 소유자 계정이 Runtime Monitoring (GuardDuty 또는 EKS Runtime Monitoring) 을 비활성화하면 참가자 계정에 속한 리소스 유형이 공유 VPC 엔드포인트를 사용했는지 또는 참가자 계정에서 특정 리소스 유형에 대해 GuardDuty 에이전트 관리를 활성화한 적이 있는지 GuardDuty 확인합니다. 그렇다면 VPC 엔드포인트와 보안 그룹을 삭제하지 GuardDuty 않습니다.

공유 VPC 참가자 계정이 런타임 모니터링 (GuardDuty 또는 EKS Runtime Monitoring) 을 비활성화해도 공유 VPC 소유자 계정에는 영향이 없으며 소유자 계정은 공유 VPC 리소스나 보안 그룹을 삭제하지 않습니다.

공유 VPC 리소스를 삭제하려면 어떻게 해야 하나요? 그 영향은 어떻게 되나요?

공유 VPC 소유자 계정은 사용자 계정 또는 Runtime Monitoring의 참여 계정에서 사용 중인 경우에도 공유 VPC 리소스를 삭제할 수 있습니다. 공유 VPC 삭제 및 그 영향에 대한 자세한 내용은 을 참조하십시오. To delete a VPC endpoint

호스트에 설치된 이중 보안 에이전트 처리

Amazon EC2 인스턴스는 여러 유형의 워크로드를 지원할 수 있습니다. Amazon EC2 인스턴스에 자동 보안 에이전트를 구성하는 경우 동일한 EC2 인스턴스에 EKS를 통해 다른 보안 에이전트가 있을 수 있습니다.

개요

런타임 모니터링을 활성화한 시나리오를 생각해 보십시오. 이제 Amazon EKS용 자동 에이전트를 활성화합니다. GuardDuty Amazon EC2용 자동 에이전트도 활성화했습니다. 동일한 기본 호스트에 두 개의 보안 에이전트 (하나는 Amazon EKS용이고 다른 하나는 Amazon EC2용) 와 함께 설치될 수 있습니다. 이로 인해 두 개의 보안 에이전트가 동일한 호스트 내에서 실행되어 런타임 이벤트를 수집하여 GuardDuty 전송하고 중복 결과가 생성될 수 있습니다.

영향

- 동일한 호스트에서 실행 중인 보안 에이전트가 둘 이상인 경우 계정에 필요한 CPU 및 메모리 처리 요구량이 두 배로 증가할 수 있습니다. 각 리소스 유형의 CPU 및 메모리 제한에 대한 자세한 내용은 해당 리소스의 항목을 참조하십시오필수 조건.
- GuardDuty 는 동일한 기본 호스트에서 런타임 이벤트를 수집하는 두 보안 에이전트가 겹치는 경우에도 사용자 계정에 런타임 이벤트 스트림 하나에 대해서만 요금이 부과되는 방식으로 런타임 모니터링 기능을 설계했습니다.

여러 GuardDuty 에이전트를 처리하는 방법

GuardDuty 두 보안 에이전트가 동일한 호스트에서 실행 중일 때를 탐지하고 그 중 하나만 런타임 이벤트를 적극적으로 수집하는 보안 에이전트로 지정합니다. 두 번째 에이전트는 응용 프로그램 성능에 미치는 영향을 방지하기 위해 최소한의 시스템 리소스를 사용합니다.

GuardDuty 다음 시나리오를 고려해 보십시오.

- EC2 인스턴스가 Amazon EKS 및 Amazon EC2 보안 에이전트의 범위에 모두 속하는 경우 EKS 보안 에이전트가 우선 순위를 갖습니다. 이는 Amazon EC2용 보안 에이전트 v1.1.0 이상을 사용하는 경우에만 적용됩니다. 이전 에이전트 버전은 우선 순위의 영향을 받지 않으므로 이전 에이전트 버전은 계속 실행되고 런타임 이벤트를 수집합니다.
- Amazon EKS와 Amazon GuardDuty EC2에 모두 관리형 보안 에이전트가 있고 Amazon EC2 인스턴스도 SSM으로 관리되는 경우 두 보안 에이전트 모두 호스트 수준에서 설치됩니다. 에이전트가 설치되면 어떤 보안 에이전트를 GuardDuty 계속 실행할지 결정합니다. 두 보안 에이전트가 모두 실행되면 결국에는 둘 중 하나만 런타임 이벤트를 수집하게 됩니다.
- EC2와 EKS에 연결된 보안 에이전트가 동시에 실행되는 경우 중복 기간에만 중복 결과가 GuardDuty 생성될 수 있습니다.

  이는 다음과 같은 경우에 발생할 수 있습니다.

  - EC2와 EKS의 보안 에이전트는 GuardDuty (자동으로) 또는
  - Amazon EKS 리소스에는 자동화된 보안 에이전트가 있습니다.
- EKS 보안 에이전트가 이미 실행 중인 경우 동일한 기본 호스트에 EC2 보안 에이전트를 수동으로 배포하고 모든 사전 요구 사항을 충족하는 경우 두 번째 보안 에이전트를 설치하지 GuardDuty 않을 수 있습니다.

Amazon EC2 인스턴스용 자동 보안 에이전트 관리

> **Note**
>
> 계속하기 전에 반드시 모든 사항을 Amazon EC2 인스턴스 지원을 위한 사전 요구 사항 따르십시오.

Amazon EC2 수동 에이전트에서 자동 에이전트로 마이그레이션

이 섹션은 이전에 보안 에이전트를 수동으로 관리하다가 이제는 GuardDuty 자동 에이전트 구성을 사용하려는 AWS 계정 경우에 적용됩니다. 이에 해당되지 않는 경우 계정에 대한 보안 에이전트 구성을 계속하십시오.

GuardDuty 자동 에이전트를 활성화하면 사용자 대신 보안 에이전트를 GuardDuty 관리합니다. 어떤 GuardDuty 단계를 거쳐야 하는지에 대한 자세한 내용은 을 참조하십시오자동 에이전트 구성 사용 (권장).

리소스 정리

SSM 연결 삭제

- Amazon EC2용 보안 에이전트를 수동으로 관리할 때 생성했을 수 있는 SSM 연결을 모두 삭제하십시오. 자세한 내용은 연결 삭제를 참조하십시오.
- 이렇게 하면 자동 에이전트를 계정 수준에서 사용하든 인스턴스 수준에서 사용하든 (포함 또는 제외 태그를 사용하여) SSM 작업 관리를 인수할 GuardDuty 수 있습니다. 수행할 수 GuardDuty 있는 SSM 작업에 대한 자세한 내용은 을 참조하십시오. 에 대한 서비스 연결 역할 권한 GuardDuty
- 이전에 보안 에이전트를 수동으로 관리하기 위해 만든 SSM 연결을 삭제하면 보안 에이전트를 자동으로 관리하기 위한 SSM 연결을 GuardDuty 생성할 때 잠시 겹칠 수 있습니다. 이 기간 동안에는 SSM 스케줄링에 따른 충돌이 발생할 수 있습니다. 자세한 내용은 Amazon EC2 SSM 일정을 참조하십시오.

Amazon EC2 인스턴스의 포함 및 제외 태그를 관리합니다.

- 포함 태그 — GuardDuty 자동 에이전트 구성을 활성화하지 않고 Amazon EC2 인스턴스에 포함 태그 `GuardDutyManaged` (`true`:) GuardDuty 를 붙이면 선택한 EC2 인스턴스에 보안 에이전트를 설치하고 관리하는 SSM 연결이 생성됩니다. 이는 일부 EC2 인스턴스에서만 보안 에이전트를 관리하는 데 도움이 되는 예상 동작입니다. 자세한 정보는 Amazon EC2 인스턴스에서 런타임 모니터링이 작동하는 방식을 참조하세요.

  보안 에이전트의 설치 및 관리를 GuardDuty 방지하려면 이러한 EC2 인스턴스에서 포함 태그를 제거하십시오. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 태그 추가 및 삭제를 참조하십시오.
- 제외 태그 - 계정의 모든 EC2 인스턴스에 대해 GuardDuty 자동 에이전트 구성을 활성화하려면 제외 태그 (:) 가 지정된 EC2 인스턴스가 없는지 확인하십시오. `GuardDutyManaged` `false`

독립형 계정을 위한 에이전트 구성 GuardDuty

Configure for all instances

독립형 계정의 모든 인스턴스에 대해 런타임 모니터링을 구성하려면

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 구성 탭에서 편집을 선택합니다.
4. EC2 섹션에서 활성화를 선택합니다.
5. 저장을 선택합니다.
6. GuardDuty 생성한 SSM 연결이 계정에 속한 모든 EC2 리소스에 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

   a. https://console.aws.amazon.com/systems-manager/ 에서 AWS Systems Manager 콘솔을 엽니다.

   b. SSM 연결의 대상 탭을 엽니다 (`GuardDutyRuntimeMonitoring-do-not-delete`). 태그 키가 다음과 같이 나타나는지 확인하십시오. InstanceIds

Using inclusion tag in selected instances

선택한 Amazon EC2 인스턴스에 대한 GuardDuty 보안 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하고 잠재적 위협을 GuardDuty 탐지하려는 인스턴스에`GuardDutyManaged: true` 태그를 추가합니다. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.
3. GuardDuty 생성한 SSM 연결이 포함 태그가 지정된 EC2 리소스에만 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

   https://console.aws.amazon.com/systems-manager/ 에서 콘솔을 엽니다. AWS Systems Manager

   - 생성되는 SSM 연결의 타겟 탭을 엽니다 (`GuardDutyRuntimeMonitoring-do-not-delete`). 태그 키는 GuardDutyManaged태그:로 표시됩니다.

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 인스턴스를 시작하기 전에 해당 인스턴스에 제외 태그를 추가해야 합니다. Amazon EC2용 자동 에이전트 구성을 활성화하면 제외 태그 없이 시작되는 모든 EC2 인스턴스가 자동 에이전트 구성의 적용을 받게 GuardDuty 됩니다.

선택한 Amazon EC2 인스턴스에 대한 GuardDuty 보안 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하지 GuardDuty 않으려는 인스턴스에`GuardDutyManaged: false` 태그를 추가하고 잠재적 위협을 탐지하십시오. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.
3. 인스턴스 메타데이터에서 제외 태그를 사용할 수 있게 하려면 다음 단계를 수행하십시오.
   a. 인스턴스의 세부 정보 탭에서 인스턴스 메타데이터의 Allow tags 상태를 확인합니다.

      현재 비활성화된 경우 다음 단계를 사용하여 상태를 활성화됨으로 변경합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   b. 태그를 허용하려는 인스턴스를 선택합니다.
   c. 작업 메뉴에서 인스턴스 설정을 선택합니다.
   d. 인스턴스 메타데이터에 태그 허용을 선택합니다.
   e. 인스턴스 메타데이터의 태그 액세스에서 허용을 선택합니다.
   f. 저장을 선택합니다.
4. 제외 태그를 추가한 후 모든 인스턴스에 대해 구성 탭에 지정된 것과 동일한 단계를 수행하십시오.

이제 런타임을 평가할 수 있습니다. Amazon EC2 인스턴스 적용 범위

다중 GuardDuty 계정 환경에서 에이전트 구성

위임된 관리자 계정의 경우 GuardDuty

Configure for all instances

런타임 모니터링에서 모든 계정에 대해 활성화를 선택한 경우 위임된 GuardDuty 관리자 계정에 대해 다음 옵션 중 하나를 선택하십시오.

- 옵션 1

  자동 에이전트 구성의 EC2 섹션에서 모든 계정에 대해 활성화를 선택합니다.

- 옵션 2
  - 자동 에이전트 구성의 EC2 섹션에서 계정 수동 구성을 선택합니다.
  - 위임된 관리자 (이 계정) 에서 활성화를 선택합니다.
- 저장을 선택합니다.

런타임 모니터링을 위해 수동으로 계정 구성을 선택한 경우 다음 단계를 수행하십시오.

- 자동 에이전트 구성의 EC2 섹션에서 수동 계정 구성을 선택합니다.
- 위임된 관리자 (이 계정) 에서 활성화를 선택합니다.
- 저장을 선택합니다.

위임된 GuardDuty 관리자 계정의 자동 에이전트 구성을 활성화하기 위해 어떤 옵션을 선택하든, GuardDuty 생성한 SSM 연결이 이 계정에 속한 모든 EC2 리소스에 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

1. https://console.aws.amazon.com/systems-manager/ 에서 AWS Systems Manager 콘솔을 엽니다.
2. SSM 연결의 대상 탭을 엽니다 (`GuardDutyRuntimeMonitoring-do-not-delete`). 태그 키가 다음과 같이 나타나는지 확인하십시오. InstanceIds

Using inclusion tag in selected instances

선택한 Amazon EC2 인스턴스에 대한 GuardDuty 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하고 잠재적 위협을 GuardDuty 탐지하려는 인스턴스에`GuardDutyManaged: true` 태그를 추가합니다. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.

   이 태그를 추가하면 선택한 EC2 인스턴스의 보안 GuardDuty 에이전트를 설치하고 관리할 수 있습니다. 자동 에이전트 구성을 명시적으로 활성화할 필요는 없습니다.
3. GuardDuty 생성한 SSM 연결이 포함 태그가 지정된 EC2 리소스에만 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

   https://console.aws.amazon.com/systems-manager/ 에서 콘솔을 엽니다. AWS Systems Manager

   - 생성되는 SSM 연결의 타겟 탭을 엽니다 (`GuardDutyRuntimeMonitoring-do-not-delete`). 태그 키는 GuardDutyManaged태그:로 표시됩니다.

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 인스턴스를 시작하기 전에 해당 인스턴스에 제외 태그를 추가해야 합니다. Amazon EC2용 자동 에이전트 구성을 활성화하면 제외 태그 없이 시작되는 모든 EC2 인스턴스가 자동 에이전트 구성의 적용을 받게 GuardDuty 됩니다.

선택한 Amazon EC2 인스턴스에 대한 GuardDuty 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하지 GuardDuty 않으려는 인스턴스에`GuardDutyManaged: false` 태그를 추가하고 잠재적 위협을 탐지하십시오. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.

3. 인스턴스 메타데이터에서 제외 태그를 사용할 수 있게 하려면 다음 단계를 수행하십시오.

   a. 인스턴스의 세부 정보 탭에서 인스턴스 메타데이터의 Allow tags 상태를 확인합니다.

      현재 비활성화된 경우 다음 단계를 사용하여 상태를 활성화됨으로 변경합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

   b. 작업 메뉴에서 인스턴스 설정을 선택합니다.

   c. 인스턴스 메타데이터에 태그 허용을 선택합니다.

4. 제외 태그를 추가한 후 모든 인스턴스에 대한 구성 탭에 지정된 것과 동일한 단계를 수행합니다.

이제 런타임을 Amazon EC2 인스턴스 적용 범위 평가할 수 있습니다.

모든 멤버 계정에 대해 자동 활성화됩니다.

> **Note**
> 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

Configure for all instances

다음 단계에서는 런타임 모니터링 섹션에서 모든 계정에 대해 활성화를 선택했다고 가정합니다.

1. Amazon EC2의 자동 에이전트 구성 섹션에서 모든 계정에 대해 활성화를 선택합니다.
2. GuardDuty create (`GuardDutyRuntimeMonitoring-do-not-delete`) 를 수행한 SSM 연결이 이 계정에 속한 모든 EC2 리소스에 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

   a. https://console.aws.amazon.com/systems-manager/ 에서 AWS Systems Manager 콘솔을 엽니다.

   b. SSM 연결의 대상 탭을 엽니다. 태그 키가 다음과 같이 나타나는지 확인하십시오. InstanceIds

Using inclusion tag in selected instances

선택한 Amazon EC2 인스턴스에 대한 GuardDuty 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하고 잠재적 위협을 GuardDuty 탐지하려는 EC2 인스턴스에`GuardDutyManaged: true` 태그를 추가합니다. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.

   이 태그를 추가하면 선택한 EC2 인스턴스의 보안 GuardDuty 에이전트를 설치하고 관리할 수 있습니다. 자동 에이전트 구성을 명시적으로 활성화할 필요는 없습니다.
3. GuardDuty 생성한 SSM 연결이 계정에 속한 모든 EC2 리소스에 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

   a. https://console.aws.amazon.com/systems-manager/ 에서 AWS Systems Manager 콘솔을 엽니다.

   b. SSM 연결의 대상 탭을 엽니다 (`GuardDutyRuntimeMonitoring-do-not-delete`). 태그 키가 다음과 같이 나타나는지 확인하십시오. InstanceIds

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 인스턴스를 시작하기 전에 해당 인스턴스에 제외 태그를 추가해야 합니다. Amazon EC2용 자동 에이전트 구성을 활성화하면 제외 태그 없이 시작되는 모든 EC2 인스턴스가 자동 에이전트 구성의 적용을 받게 GuardDuty 됩니다.

선택한 Amazon EC2 인스턴스에 대한 GuardDuty 보안 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하지 GuardDuty 않으려는 인스턴스에`GuardDutyManaged: false` 태그를 추가하고 잠재적 위협을 탐지하십시오. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.

3. 인스턴스 메타데이터에서 제외 태그를 사용할 수 있게 하려면 다음 단계를 수행하십시오.

   a. 인스턴스의 세부 정보 탭에서 인스턴스 메타데이터의 Allow tags 상태를 확인합니다.

      현재 비활성화된 경우 다음 단계를 사용하여 상태를 활성화됨으로 변경합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

   b. 작업 메뉴에서 인스턴스 설정을 선택합니다.

   c. 인스턴스 메타데이터에 태그 허용을 선택합니다.

4. 제외 태그를 추가한 후 모든 인스턴스에 대한 구성 탭에 지정된 것과 동일한 단계를 수행합니다.

이제 런타임을 Amazon EC2 인스턴스 적용 범위 평가할 수 있습니다.

새 회원 계정에만 자동 활성화됩니다.

위임된 GuardDuty 관리자 계정은 Amazon EC2 리소스에 대한 자동 에이전트 구성을 설정하여 새 구성원 계정이 조직에 가입할 때 자동으로 활성화되도록 할 수 있습니다.

Configure for all instances

다음 단계에서는 런타임 모니터링 섹션에서 새 멤버 계정에 대해 자동 활성화를 선택했다고 가정합니다.

1. 탐색 창에서 [런타임 모니터링] 을 선택합니다.
2. 런타임 모니터링 페이지에서 편집을 선택합니다.
3. 새 멤버 계정에 대해 자동으로 활성화를 선택합니다. 이 단계를 통해 새 계정이 조직에 가입할 때마다 Amazon EC2용 자동 에이전트 구성이 해당 계정에 자동으로 활성화됩니다. 조직의 위임된 GuardDuty 관리자 계정만 이 선택을 수정할 수 있습니다.
4. 저장을 선택합니다.

새 멤버 계정이 기관에 가입하면 해당 멤버에 대해 이 구성이 자동으로 활성화됩니다. 이 새 멤버 계정에 속하는 Amazon EC2 인스턴스의 보안 에이전트를 GuardDuty 관리하려면 모든 사전 요구 사항을 EC2 인스턴스의 경우 충족해야 합니다.

SSM 연결이 생성되면 (`GuardDutyRuntimeMonitoring-do-not-delete`) SSM 연결이 새 멤버 계정에 속한 모든 EC2 인스턴스에 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

- https://console.aws.amazon.com/systems-manager/ 에서 AWS Systems Manager 콘솔을 엽니다.
- SSM 연결의 대상 탭을 엽니다. 태그 키가 다음과 같이 나타나는지 확인하십시오. InstanceIds

Using inclusion tag in selected instances

계정에서 선택한 인스턴스에 대해 GuardDuty 보안 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하고 잠재적 위협을 GuardDuty 탐지하려는 인스턴스에`GuardDutyManaged: true` 태그를 추가합니다. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.

   이 태그를 추가하면 선택한 인스턴스에 대한 보안 GuardDuty 에이전트를 설치하고 관리할 수 있습니다. 자동 에이전트 구성을 명시적으로 활성화할 필요는 없습니다.
3. GuardDuty 생성한 SSM 연결이 포함 태그가 지정된 EC2 리소스에만 보안 에이전트를 설치하고 관리하는지 확인할 수 있습니다.

   a. https://console.aws.amazon.com/systems-manager/ 에서 콘솔을 엽니다. AWS Systems Manager

   b. 생성된 SSM 연결의 타겟 탭을 엽니다. 태그 키는 GuardDutyManaged태그:로 표시됩니다.

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 인스턴스를 시작하기 전에 해당 인스턴스에 제외 태그를 추가해야 합니다. Amazon EC2용 자동 에이전트 구성을 활성화하면 제외 태그 없이 시작되는 모든 EC2 인스턴스가 자동 에이전트 구성의 적용을 받게 GuardDuty 됩니다.

독립형 계정의 특정 인스턴스에 대한 GuardDuty 보안 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.

2. 모니터링하지 GuardDuty 않으려는 인스턴스에`GuardDutyManaged: false` 태그를 추가하고 잠재적 위협을 탐지하십시오. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.
3. 인스턴스 메타데이터에서 제외 태그를 사용할 수 있게 하려면 다음 단계를 수행하십시오.

   a. 인스턴스의 세부 정보 탭에서 인스턴스 메타데이터의 Allow tags 상태를 확인합니다.

      현재 비활성화된 경우 다음 단계를 사용하여 상태를 활성화됨으로 변경합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

   b. 작업 메뉴에서 인스턴스 설정을 선택합니다.

   c. 인스턴스 메타데이터에 태그 허용을 선택합니다.
4. 제외 태그를 추가한 후 모든 인스턴스에 대한 구성 탭에 지정된 것과 동일한 단계를 수행합니다.

이제 런타임을 Amazon EC2 인스턴스 적용 범위 평가할 수 있습니다.

선택적 멤버 계정만 해당

Configure for all instances

1. 계정 페이지에서 런타임 모니터링-자동 에이전트 구성 (Amazon EC2) 을 활성화하려는 계정을 하나 이상 선택합니다. 이 단계에서 선택한 계정에 런타임 모니터링이 이미 활성화되어 있는지 확인하십시오.
2. 보호 계획 편집에서 적절한 옵션을 선택하여 런타임 모니터링-자동 에이전트 구성 (Amazon EC2) 을 활성화합니다.
3. 확인을 선택합니다.

Using inclusion tag in selected instances

선택한 인스턴스에 대한 GuardDuty 보안 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 모니터링하고 잠재적 위협을 GuardDuty 탐지하려는 인스턴스에`GuardDutyManaged: true` 태그를 추가합니다. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.

이 태그를 추가하면 태그가 지정된 Amazon EC2 인스턴스의 보안 에이전트를 관리할 수 있습니다. GuardDuty 자동 에이전트 구성 (런타임 모니터링 - 자동 에이전트 구성 (EC2)) 을 명시적으로 활성화할 필요는 없습니다.

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 인스턴스를 시작하기 전에 해당 인스턴스에 제외 태그를 추가해야 합니다. Amazon EC2용 자동 에이전트 구성을 활성화하면 제외 태그 없이 시작되는 모든 EC2 인스턴스가 자동 에이전트 구성의 적용을 받게 GuardDuty 됩니다.

선택한 인스턴스에 대한 GuardDuty 보안 에이전트를 구성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.
2. 잠재적 위협을 모니터링하거나 탐지하지 GuardDuty 않으려는 EC2 인스턴스에`GuardDutyManaged: false` 태그를 추가하십시오. 이 태그를 추가하는 방법에 대한 자세한 내용은 개별 리소스에 태그 추가하기를 참조하십시오.
3. 인스턴스 메타데이터에서 제외 태그를 사용할 수 있게 하려면 다음 단계를 수행하십시오.
   a. 인스턴스의 세부 정보 탭에서 인스턴스 메타데이터의 Allow tags 상태를 확인합니다.

      현재 비활성화된 경우 다음 단계를 사용하여 상태를 활성화됨으로 변경합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   b. 작업 메뉴에서 인스턴스 설정을 선택합니다.
   c. 인스턴스 메타데이터에 태그 허용을 선택합니다.
4. 제외 태그를 추가한 후 모든 인스턴스에 대한 구성 탭에 지정된 것과 동일한 단계를 수행합니다.

이제 평가할 Amazon EC2 인스턴스 적용 범위 수 있습니다.

Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리

런타임 모니터링을 활성화한 후에는 GuardDuty 보안 에이전트를 수동으로 설치해야 합니다. 에이전트를 GuardDuty 설치하면 Amazon EC2 인스턴스로부터 런타임 이벤트를 수신합니다.

GuardDuty 보안 에이전트를 관리하려면 Amazon VPC 엔드포인트를 생성한 다음 단계에 따라 보안 에이전트를 수동으로 설치해야 합니다.

Amazon VPC 엔드포인트를 수동으로 생성

GuardDuty 보안 에이전트를 설치하려면 먼저 Amazon VPC (가상 사설 클라우드) 엔드포인트를 생성해야 합니다. 이렇게 하면 Amazon EC2 인스턴스의 런타임 이벤트를 GuardDuty 수신하는 데 도움이 됩니다.

> **Note**
>
> VPC 엔드포인트 사용에 대한 추가 비용은 없습니다.

Amazon VPC 엔드포인트를 만들려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/vpc/ 에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 VPC 프라이빗 클라우드에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.
4. 엔드포인트 생성 페이지에서 서비스 범주에 대해 기타 엔드포인트 서비스를 선택합니다.
5. 서비스 이름에 **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**를 입력합니다.

   `us-east-1#` 귀하의 것으로 교체하십시오. AWS 리전 AWS 계정 ID에 속하는 Amazon EC2 인스턴스와 동일한 지역이어야 합니다.
6. 서비스 확인을 선택합니다.
7. 서비스 이름이 성공적으로 확인되면 인스턴스가 있는 VPC를 선택합니다. 다음 정책을 추가하여 Amazon VPC 엔드포인트 사용을 지정된 계정으로만 제한합니다. 이 정책 아래에 제공된 조직 `Condition`을 사용하여 다음 정책을 업데이트하고 엔드포인트에 대한 액세스를 제한할 수 있습니다. 조직의 특정 계정 ID에 Amazon VPC 엔드포인트 지원을 제공하려면 을 참조하십시오. Organization condition to restrict access to your endpoint

   ```
   {
    "Version": "2012-10-17",
   ```

```
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

aws:PrincipalAccount 계정 ID는 VPC 및 VPC 엔드포인트를 포함하는 계정과 일치해야 합니다. 다음 목록은 VPC 엔드포인트를 다른 AWS 계정 ID와 공유하는 방법을 보여줍니다.

- VPC 엔드포인트에 액세스할 계정을 여러 개 지정하려면 다음 "aws:PrincipalAccount: "111122223333" 블록으로 대체하십시오.

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
       ]
  ```

  AWS 계정 ID를 VPC 엔드포인트에 액세스해야 하는 계정의 계정 ID로 바꿔야 합니다.

- 조직의 모든 구성원이 VPC 엔드포인트에 액세스할 수 있도록 허용하려면 다음 "aws:PrincipalAccount: "111122223333" 줄로 바꾸십시오.

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

  조직 o-abcdef0123# 조직 ID로 바꿔야 합니다.

- 조직 ID로 리소스에 액세스하는 것을 제한하려면 정책에 조직 ID를 추가하세요. `ResourceOrgID` 자세한 내용은 IAM 사용 설명서에서 `aws:ResourceOrgID` 섹션을 참조하십시오.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. 추가 설정에서 DNS 이름 활성화를 선택합니다.
9. Subnets에서 인스턴스가 있는 서브넷을 선택합니다.
10. 보안 그룹에서 VPC (또는 Amazon EC2 인스턴스) 에서 인바운드 포트 443이 활성화된 보안 그룹을 선택합니다. 인바운드 포트 443이 활성화된 보안 그룹이 아직 없는 경우 Linux 인스턴스용 Amazon EC2 사용 설명서의 보안 그룹 생성을 참조하십시오.

    VPC (또는 인스턴스) 에 대한 인바운드 권한을 제한하는 중에 문제가 발생하는 경우 모든 IP 주소에서 인바운드 443 포트에 대한 지원을 제공하십시오. (`0.0.0.0/0`)

보안 에이전트를 수동으로 설치

GuardDuty Amazon EC2 인스턴스에 GuardDuty 보안 에이전트를 설치하는 다음 두 가지 방법을 제공합니다.

- 방법 1 - 사용 AWS Systems Manager - 이 방법을 사용하려면 Amazon EC2 인스턴스를 관리해야 AWS Systems Manager 합니다.
- 방법 2 - RPM 설치 스크립트 사용 — Amazon EC2 인스턴스의 AWS Systems Manager 관리 여부에 관계없이 이 방법을 사용할 수 있습니다.

방법 1 - 사용 AWS Systems Manager

이 방법을 사용하려면 Amazon EC2 인스턴스가 AWS Systems Manager 관리되고 있는지 확인한 다음 에이전트를 설치하십시오.

AWS Systems Manager 관리형 아마존 EC2 인스턴스

Amazon EC2 인스턴스를 AWS Systems Manager 관리하려면 다음 단계를 사용하십시오.

- AWS Systems Manager AWS end-to-end 애플리케이션과 리소스를 관리하고 규모에 맞게 안전하게 운영할 수 있도록 지원합니다.

  를 사용하여 Amazon EC2 인스턴스를 관리하려면 사용 AWS Systems Manager설명서의 Amazon EC2 인스턴스용 Systems Manager 설정을 참조하십시오.AWS Systems Manager

- 다음 표는 새로운 GuardDuty 관리 AWS Systems Manager 문서를 보여줍니다.

문서 이름	문서 유형	용도
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	GuardDuty 보안 에이전트를 패키징하기.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Command	설치/제거 스크립트를 실행하여 보안 에이전트를 설치합니다. GuardDuty

에 대한 AWS Systems Manager자세한 내용은 사용AWS Systems Manager 설명서의 Amazon EC2 Systems Manager 문서를 참조하십시오.

를 사용하여 Amazon EC2 인스턴스용 GuardDuty 에이전트를 설치하려면 AWS Systems Manager

1. https://console.aws.amazon.com/systems-manager/ 에서 AWS Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 [문서] 를 선택합니다.
3. 아마존 소유에서 선택하십시오`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. [명령 실행]을 선택합니다.
5. 다음 실행 명령 파라미터를 입력합니다.
   - 조치: 설치를 선택합니다.
   - 설치 유형: 설치 또는 제거를 선택합니다.
   - 이름: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - 버전: 비어 있는 경우 최신 버전의 GuardDuty 보안 에이전트를 받게 됩니다. 릴리스 버전에 대한 자세한 내용은 을 참조하십시오GuardDuty Amazon EC2 인스턴스용 보안 에이전트.
6. 대상 Amazon EC2 인스턴스를 선택합니다. Amazon EC2 인스턴스를 하나 이상 선택할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 콘솔에서 명령AWS Systems Manager 실행을 참조하십시오.
7. GuardDuty 에이전트 설치가 정상인지 확인하십시오. 자세한 정보는 GuardDuty 보안 에이전트 설치 상태 검증을 참조하세요.

방법 2 - RPM 설치 스크립트 사용

> **Important**
>
> 시스템에 보안 에이전트 RPM 서명을 설치하기 전에 먼저 GuardDuty 보안 에이전트 RPM 서명을 확인하는 것이 좋습니다.

1. GuardDuty 보안 에이전트 RPM 서명을 확인하십시오.

   a. 적절한 공개 키, x86_64 RPM의 서명, arm64 RPM의 서명 및 Amazon S3 버킷에서 호스팅되는 RPM 스크립트에 대한 해당 액세스 링크를 다운로드하십시오.

   다음 템플릿을 사용하여 공개 키, x86_64 RPM의 서명, arm64 RPM의 서명 및 RPM 스크립트에 대한 해당 액세스 링크를 구성할 수 있습니다. RPM 스크립트에 액세스하려면 의 값 AWS 리전, AWS 계정 ID 및 GuardDuty 에이전트 버전을 바꾸십시오.

   - 공개 키:

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
     ```

   - GuardDuty 보안 에이전트 RPM 서명:

     x86_64 RPM의 시그니처

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
     amazon-guardduty-agent-1.1.0.x86_64.sig
     ```

     arm64 RPM의 시그니처

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
     amazon-guardduty-agent-1.1.0.arm64.sig
     ```

   - Amazon S3 버킷의 RPM 스크립트로 연결되는 링크에 액세스하십시오.

     x86_64 RPM용 액세스 링크

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
     amazon-guardduty-agent-1.1.0.x86_64.rpm
     ```

arm64 RPM을 위한 액세스 링크

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
amazon-guardduty-agent-1.1.0.arm64.rpm
```

다음 명령에서 적절한 공개 키, x86_64 RPM 서명, arm64 RPM 서명 및 Amazon S3 버킷에 호스팅된 RPM 스크립트에 대한 해당 액세스 링크를 다운로드하려면 계정 ID를 AWS 계정 적절한 ID로, 지역을 현재 지역으로 교체해야 합니다.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm ./amazon-guardduty-
agent-1.1.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig ./amazon-guardduty-
agent-1.1.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
publickey.pem ./publickey.pem
```

AWS 리전	지역명	AWS 계정 ID
eu-west-1	유럽(아일랜드)	694911143906
us-east-1	미국 동부(버지니아 북부)	593207742271
us-west-2	미국 서부(오레곤)	733349766148
eu-west-3	유럽(파리)	665651866788
us-east-2	미국 동부(오하이오)	307168627858
eu-central-1	유럽(프랑크푸르트)	323658145986
ap-northeast-2	아시아 태평양(서울)	914738172881
eu-north-1	유럽(스톡홀름)	591436053604
ap-east-1	아시아 태평양(홍콩)	258348409381
me-south-1	중동(바레인)	536382113932

eu-west-2	유럽(런던)	892757235363
ap-northeast-1	아시아 태평양(도쿄)	533107202818
ap-southeast-1	아시아 태평양(싱가포르)	174946120834
ap-south-1	아시아 태평양(뭄바이)	251508486986
ap-southeast-3	아시아 태평양(자카르타)	510637619217
sa-east-1	남아메리카(상파울루)	758426053663
ap-northeast-3	아시아 태평양(오사카)	273192626886
eu-south-1	유럽(밀라노)	266869475730
af-south-1	아프리카(케이프타운)	197869348890
ap-southeast-2	아시아 태평양(시드니)	005257825471
me-central-1	중동(UAE)	000014521398
us-west-1	미국 서부(캘리포니아 북부)	684579721401
ca-central-1	캐나다(중부)	354763396469
ap-south-2	아시아 태평양(하이데라바드)	950823858135
eu-south-2	유럽(스페인)	919611009337
eu-central-2	유럽(취리히)	529164026651
ap-southeast-4	아시아 태평양(멜버른)	251357961535
il-central-1	이스라엘(텔아비브)	870907303882

b. 공개 키를 데이터베이스로 가져오기

```
gpg --import publickey.pem
```

gpg는 가져오기를 성공적으로 보여줍니다.

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

c. 서명 확인

```
gpg --verify amazon-guardduty-agent-1.1.0.x86_64.sig amazon-guardduty-
agent-1.1.0.x86_64.rpm
```

확인에 통과하면 아래 결과와 비슷한 메시지가 표시됩니다. 이제 RPM을 사용하여 GuardDuty 보안 에이전트를 설치할 수 있습니다.

출력 예제:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

확인에 실패하면 RPM의 서명이 변조되었을 가능성이 있다는 의미입니다. 데이터베이스에서 퍼블릭 키를 제거하고 확인 프로세스를 다시 시도해야 합니다.

예제

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

d. 데이터베이스에서 퍼블릭 키를 제거합니다.

```
gpg --delete-keys AwsGuardDuty
```

2. 리눅스 또는 macOS에서 SSH로 연결하세요.
3. 다음 명령을 사용하여 GuardDuty 보안 에이전트를 설치합니다.

```
sudo rpm -ivh amazon-guardduty-agent-1.1.0.x86_64.rpm
```

4. GuardDuty 에이전트 설치가 정상인지 확인합니다. 단계에 대한 자세한 내용은 을 참조하십시오 GuardDuty 보안 에이전트 설치 상태 검증.

5. (선택 사항) 다음 명령을 사용하여 GuardDuty 보안 에이전트를 제거합니다.

```
sudo rpm -ev amazon-guardduty-agent
```

메모리 부족 오류

Amazon EC2용 GuardDuty 보안 에이전트를 수동으로 설치 또는 업데이트하는 동안 `out-of-memory` 오류가 발생하는 경우 을 참조하십시오. 메모리 부족 오류 문제 해결

GuardDuty 보안 에이전트 설치 상태 검증

GuardDuty 보안 에이전트가 정상인지 확인하려면

1. 리눅스 또는 macOS에서 SSH로 연결하세요.
2. 다음 명령을 실행하여 GuardDuty 보안 에이전트의 상태를 확인합니다.

```
sudo systemctl status amazon-guardduty-agent
```

보안 에이전트 설치 로그를 보려면 에서 확인할 수 있습니다`/var/log/amzn-guardduty-agent/`.

로그를 보려면 그렇게 `sudo journalctl -u amazon-guardduty-agent` 하십시오.

GuardDuty 보안 에이전트 수동 업데이트

Run 명령을 사용하여 GuardDuty 보안 에이전트를 업데이트할 수 있습니다. GuardDuty 보안 에이전트를 설치하는 데 사용한 것과 동일한 단계를 따를 수 있습니다.

보안 에이전트를 수동으로 제거

이 섹션에서는 Amazon EC2 리소스에서 GuardDuty 보안 에이전트를 제거하는 방법을 제공합니다. 런타임 모니터링을 추가로 비활성화하려는 경우 을 참조하십시오. 비활성화가 미치는 영향

방법 1 - 실행 명령 사용

Run 명령을 사용하여 GuardDuty 보안 에이전트를 제거하려면

1. AWS Systems Manager 사용 설명서의AWS Systems Manager Run Command에 지정된 단계에 따라 GuardDuty 보안 에이전트를 제거할 수 있습니다. 매개 변수의 제거 작업을 사용하여 보안 에이전트를 제거합니다. GuardDuty

Targets 섹션에서 보안 에이전트를 제거하려는 Amazon EC2 인스턴스에만 영향을 미치는지 확인하십시오.

다음 GuardDuty 문서 및 배포자를 사용하십시오.

- 문서 이름: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
- 유통사: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. 모든 세부 정보를 제공한 후 [Run] 을 선택하면 대상 Amazon EC2 인스턴스에 배포한 보안 에이전트가 제거됩니다.

   Amazon VPC 엔드포인트 구성을 제거하려면 런타임 모니터링과 Amazon EKS 런타임 모니터링을 모두 비활성화해야 합니다.

방법 2 - RPM 스크립트 사용

rpm을 사용하여 GuardDuty 보안 에이전트를 제거하려면

1. 리눅스 또는 macOS에서 SSH로 연결하세요.
2. 다음 명령은 연결하는 Amazon EC2 인스턴스에서 GuardDuty 보안 에이전트를 제거합니다.

   ```
   sudo rpm -e amazon-guardduty-agent
   ```

   이 명령과 관련된 로그를 확인할 수도 있습니다.

Amazon VPC 엔드포인트 삭제

런타임 모니터링을 비활성화하거나 계정의 GuardDuty 보안 에이전트를 제거하려는 경우 수동으로 Amazon VPC 엔드포인트를 수동으로 생성 생성한 Amazon VPC 엔드포인트를 삭제하도록 선택할 수도 있습니다 ().

콘솔을 사용하여 Amazon VPC 엔드포인트를 삭제하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. 런타임 모니터링을 활성화할 때 수동으로 생성한 엔드포인트를 선택합니다.
4. 작업(Actions), VPC 엔드포인트 삭제(Delete VPC endpoints)를 차례로 선택합니다.
5. 확인 메시지가 표시되면 **`delete`**를 입력합니다.

6. 삭제를 선택합니다.

를 사용하여 Amazon VPC 엔드포인트를 삭제하려면 AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- Remove-EC2VpcEndpointCmdlet (윈도우용 도구) PowerShell

Fargate용 자동 보안 에이전트 관리 (Amazon ECS만 해당)

독립형 GuardDuty 계정을 위한 에이전트 구성

현재 런타임 모니터링은 Amazon ECS 클러스터 (AWS Fargate) 의 보안 에이전트 관리를 통해서만 지원합니다. GuardDuty Amazon ECS 클러스터에서 보안 에이전트를 수동으로 관리하는 기능은 지원되지 않습니다.

Console

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 구성 탭에서:

   a. 모든 Amazon ECS 클러스터의 자동 에이전트 구성을 관리하려면 (계정 수준)

      자동 에이전트 구성 섹션에서 활성화를 선택합니다 AWS Fargate (ECS만 해당). 새 Fargate Amazon ECS 작업이 GuardDuty 시작되면 보안 에이전트의 배포를 관리합니다.

      - 저장을 선택합니다.

   b. 일부 Amazon ECS 클러스터를 제외하여 자동 에이전트 구성을 관리하려면 (클러스터 수준)

      i. 모든 작업을 제외하려는 Amazon ECS 클러스터에 태그를 추가합니다. 키-값 쌍은 -이어야 합니다. `GuardDutyManaged false`

      ii. 신뢰할 수 있는 엔티티를 제외하고 이러한 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙에 따른 경우를 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. 구성 탭의 자동 에이전트 구성 섹션에서 활성화를 선택합니다.

> **Note**
>
> 계정에 대한 GuardDuty 에이전트 자동 관리를 활성화하기 전에 항상 Amazon ECS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 해당 Amazon ECS 클러스터 내에서 시작되는 모든 작업에 보안 에이전트가 배포됩니다.

제외되지 않은 Amazon ECS 클러스터의 경우 GuardDuty 사이드카 컨테이너의 보안 에이전트 배포를 관리합니다.

iv. 저장을 선택합니다.

c. 일부 Amazon ECS 클러스터를 포함하여 자동 에이전트 구성을 관리하려면 (클러스터 수준)

i. 모든 작업을 포함하려는 Amazon ECS 클러스터에 태그를 추가합니다. 키-값 쌍은 -이어야 합니다. `GuardDutyManaged` `true`

ii. 신뢰할 수 있는 엔티티를 제외하고 이러한 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙에 따른 경우를 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

다중 계정 GuardDuty 환경을 위한 에이전트 구성

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만이 구성원 계정의 자동 에이전트 구성을 활성화 또는 비활성화하고 조직의 구성원 계정에 속하는 Amazon ECS 클러스터의 자동 에이전트 구성을 관리할 수 있습니다. GuardDuty멤버 계정은 이 구성을 수정할 수 없습니다. 위임된 GuardDuty 관리자 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 다중 계정 환경에 대한 자세한 내용은 에서 여러 계정 관리를 참조하십시오. GuardDuty

GuardDuty 위임된 관리자 계정에 대한 자동 에이전트 구성 활성화

Manage for all Amazon ECS clusters (account level)

런타임 모니터링에서 모든 계정에 대해 활성화를 선택한 경우 다음 옵션을 사용할 수 있습니다.

- 자동 에이전트 구성 섹션에서 모든 계정에 대해 활성화를 선택합니다. GuardDuty 시작되는 모든 Amazon ECS 작업을 위해 보안 에이전트를 배포하고 관리합니다.
- 수동으로 계정 구성을 선택합니다.

런타임 모니터링 섹션에서 수동으로 계정 구성을 선택한 경우 다음을 수행하십시오.

1. 자동 에이전트 구성 섹션에서 수동 계정 구성을 선택합니다.
2. 위임된 GuardDuty 관리자 계정 (이 계정) 섹션에서 활성화를 선택합니다.

저장을 선택합니다.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 키-값 쌍을 -로 사용하여 Amazon ECS 클러스터에 태그를 추가합니다. `GuardDutyManaged` `false`
2. 신뢰할 수 있는 주체에 의한 경우를 제외하고 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙을 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
4. 탐색 창에서 런타임 모니터링을 선택합니다.
5.

> **Note**
>
> 계정에 대해 자동 에이전트 구성을 활성화하기 전에 항상 Amazon ECS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 사이드카 컨테이너가 시작되는 Amazon ECS 작업의 모든 컨테이너에 연결됩니다.

   구성 탭 아래의 자동 에이전트 구성에서 활성화를 선택합니다.

   제외되지 않은 Amazon ECS 클러스터의 경우 GuardDuty 사이드카 컨테이너의 보안 에이전트 배포를 관리합니다.
6. 저장을 선택합니다.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 모든 작업을 포함하려는 Amazon ECS 클러스터에 태그를 추가합니다. 키-값 쌍은 -이어야 합니다. `GuardDutyManaged` `true`

2. 신뢰할 수 있는 엔티티를 제외하고 이러한 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙에 따른 경우를 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS 클러스터에 포함 태그를 사용하는 경우 자동 GuardDuty 에이전트 구성을 통해 에이전트를 명시적으로 활성화할 필요가 없습니다.

모든 멤버 계정에 대해 자동 활성화

Manage for all Amazon ECS clusters (account level)

다음 단계에서는 런타임 모니터링 섹션에서 모든 계정에 대해 활성화를 선택했다고 가정합니다.

1. 자동 에이전트 구성 섹션에서 모든 계정에 대해 활성화를 선택합니다. GuardDuty 시작되는 모든 Amazon ECS 작업을 위해 보안 에이전트를 배포하고 관리합니다.
2. 저장을 선택합니다.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 키-값 쌍을 -로 사용하여 Amazon ECS 클러스터에 태그를 추가합니다. `GuardDutyManaged` `false`
2. 신뢰할 수 있는 주체에 의한 경우를 제외하고 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙을 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
```

```
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
```

```
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
4. 탐색 창에서 런타임 모니터링을 선택합니다.
5.

> **Note**
>
> 계정에 대해 자동 에이전트 구성을 활성화하기 전에 항상 Amazon ECS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 사이드카 컨테이너가 시작되는 Amazon ECS 작업의 모든 컨테이너에 연결됩니다.

   구성 탭에서 편집을 선택합니다.
6. 자동 에이전트 구성 섹션에서 모든 계정에 대해 활성화를 선택합니다.

   제외되지 않은 Amazon ECS 클러스터의 경우 GuardDuty 사이드카 컨테이너의 보안 에이전트 배포를 관리합니다.
7. 저장을 선택합니다.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

런타임 모니터링을 활성화하는 방법에 관계없이 다음 단계는 조직의 모든 구성원 계정에 대한 선택적 Amazon ECS Fargate 작업을 모니터링하는 데 도움이 됩니다.

1. 자동 에이전트 구성 섹션에서 어떤 구성도 활성화하지 마십시오. 런타임 모니터링 구성을 이전 단계에서 선택한 것과 동일하게 유지하십시오.
2. 저장을 선택합니다.
3. 신뢰할 수 있는 엔티티를 제외하고 이러한 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙에 따른 경우를 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS 클러스터에 포함 태그를 사용하는 경우 GuardDuty 에이전트 자동 관리를 명시적으로 활성화할 필요가 없습니다.

기존 활성 멤버 계정에 대한 자동 에이전트 구성 활성화

Manage for all Amazon ECS clusters (account level)

1. 런타임 모니터링 페이지의 구성 탭에서 자동 에이전트 구성의 현재 상태를 볼 수 있습니다.
2. 자동 에이전트 구성 창의 활성 구성원 계정 섹션에서 작업을 선택합니다.
3. 작업에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다.
4. 확인을 선택합니다.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 키-값 쌍을 -로 사용하여 Amazon ECS 클러스터에 태그를 추가합니다. `GuardDutyManaged` `false`
2. 신뢰할 수 있는 주체에 의한 경우를 제외하고 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙을 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
4. 탐색 창에서 런타임 모니터링을 선택합니다.

5.

> **Note**
>
> 계정에 대해 자동 에이전트 구성을 활성화하기 전에 항상 Amazon ECS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 사이드카 컨테이너가 시작되는 Amazon ECS 작업의 모든 컨테이너에 연결됩니다.

   구성 탭의 자동 에이전트 구성 섹션의 활성 멤버 계정에서 작업을 선택합니다.

6. 작업에서 모든 활성 멤버 계정에 대해 활성화를 선택합니다.

   제외되지 않은 Amazon ECS 클러스터의 경우 GuardDuty 사이드카 컨테이너의 보안 에이전트 배포를 관리합니다.

7. 확인을 선택합니다.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 모든 작업을 포함하려는 Amazon ECS 클러스터에 태그를 추가합니다. 키-값 쌍은 -이어야 합니다. `GuardDutyManaged` `true`
2. 신뢰할 수 있는 엔티티를 제외하고 이러한 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙에 따른 경우를 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS 클러스터에 포함 태그를 사용하는 경우 자동 에이전트 구성을 명시적으로 활성화할 필요가 없습니다.

새 구성원을 위한 자동 에이전트 구성을 자동으로 활성화합니다.

Manage for all Amazon ECS clusters (account level)

1. 런타임 모니터링 페이지에서 편집을 선택하여 기존 구성을 업데이트합니다.
2. 자동 에이전트 구성 섹션에서 새 구성원 계정에 대해 자동으로 활성화를 선택합니다.
3. 저장을 선택합니다.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 키-값 쌍을 -로 사용하여 Amazon ECS 클러스터에 태그를 추가합니다. `GuardDutyManaged` `false`
2. 신뢰할 수 있는 주체에 의한 경우를 제외하고 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙을 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
```

```
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
4. 탐색 창에서 런타임 모니터링을 선택합니다.
5.

> **Note**
>
> 계정에 대해 자동 에이전트 구성을 활성화하기 전에 항상 Amazon ECS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 사이드카 컨테이너가 시작되는 Amazon ECS 작업의 모든 컨테이너에 연결됩니다.

   구성 탭 아래의 자동 에이전트 구성 섹션에서 새 구성원 계정 자동 활성화를 선택합니다.

   제외되지 않은 Amazon ECS 클러스터의 경우 GuardDuty 사이드카 컨테이너의 보안 에이전트 배포를 관리합니다.
6. 저장을 선택합니다.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 모든 작업을 포함하려는 Amazon ECS 클러스터에 태그를 추가합니다. 키-값 쌍은 -이어야 합니다. `GuardDutyManaged` `true`
2. 신뢰할 수 있는 엔티티를 제외하고 이러한 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙에 따른 경우를 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS 클러스터에 포함 태그를 사용하는 경우 자동 에이전트 구성을 명시적으로 활성화할 필요가 없습니다.

활성 멤버 계정에 대한 자동 에이전트 구성을 선택적으로 활성화합니다.

Manage for all Amazon ECS (account level)

1. 계정 페이지에서 런타임 모니터링-자동 에이전트 구성 (ECS-Fargate) 을 활성화하려는 계정을 선택합니다. 계정을 여러 개 선택할 수 있습니다. 이 단계에서 선택한 계정이 런타임 모니터링을 통해 이미 활성화되어 있는지 확인하십시오.
2. 보호 계획 편집에서 적절한 옵션을 선택하여 런타임 모니터링-자동 에이전트 구성 (ECS-Fargate) 을 활성화합니다.
3. 확인을 선택합니다.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 키-값 쌍을 -로 사용하여 Amazon ECS 클러스터에 태그를 추가합니다. `GuardDutyManaged` `false`
2. 신뢰할 수 있는 주체에 의한 경우를 제외하고 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙을 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
4. 탐색 창에서 런타임 모니터링을 선택합니다.
5.

> **Note**
>
> 계정에 대한 GuardDuty 에이전트 자동 관리를 활성화하기 전에 항상 Amazon ECS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 사이드카 컨테이너가 시작되는 Amazon ECS 작업의 모든 컨테이너에 연결됩니다.

   계정 페이지에서 런타임 모니터링-자동 에이전트 구성 (ECS-Fargate) 을 활성화하려는 계정을 선택합니다. 계정을 여러 개 선택할 수 있습니다. 이 단계에서 선택한 계정이 런타임 모니터링을 통해 이미 활성화되어 있는지 확인하십시오.

   제외되지 않은 Amazon ECS 클러스터의 경우 GuardDuty 사이드카 컨테이너의 보안 에이전트 배포를 관리합니다.
6. 보호 계획 편집에서 적절한 옵션을 선택하여 런타임 모니터링-자동 에이전트 구성 (ECS-Fargate) 을 활성화합니다.
7. 저장을 선택합니다.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 모니터링하려는 Amazon ECS 클러스터가 있는 선택된 계정에 대해 자동 에이전트 구성 (또는 런타임 모니터링-자동 에이전트 구성 (ECS-Fargate)) 을 활성화하지 않도록 하십시오.
2. 모든 작업을 포함하려는 Amazon ECS 클러스터에 태그를 추가합니다. 키-값 쌍은 -이어야 합니다. `GuardDutyManaged` `true`
3. 신뢰할 수 있는 엔티티를 제외하고 이러한 태그의 수정을 방지하십시오. AWS Organizations 사용 설명서의 승인된 원칙에 따른 경우를 제외하고 태그 수정 방지에 제공된 정책이 여기에 적용되도록 수정되었습니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS 클러스터에 포함 태그를 사용하는 경우 자동 에이전트 구성을 명시적으로 활성화할 필요가 없습니다.

Amazon EKS 클러스터의 보안 에이전트를 자동으로 관리

독립형 계정을 위한 자동 에이전트 구성

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 런타임 모니터링을 선택합니다.
3. 구성 탭에서 활성화를 선택하여 계정에 대한 자동 에이전트 구성을 활성화합니다.

GuardDuty 보안 에이전트를 배포하기 위한 기본 접근 방식	단계
다음을 통해 보안 에이전트를 관리합니다. GuardDuty (모든 EKS 클러스터 모니터링)	1. 자동 에이전트 구성 섹션에서 활성화를 선택합니다. GuardDuty 계정의 기존 EKS 클러스터 및 잠재적으로 새로 추가될 수 있는 모든 EKS 클러스터에 대한 보안 에이전트의 배포 및 업데이트를 관리합니다. 2. 저장을 선택합니다.

GuardDuty 보안 에이전트를 배포하기 위한 기본 접근 방식	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	다음 절차에서 해당하는 시나리오 중 하나를 선택합니다. 이 클러스터에 GuardDuty 보안 에이전트가 배포되지 않은 경우 EKS 클러스터를 모니터링에서 제외하려면 1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *CreateTagsec2:# #* 대체하십시오. `eks:TagResource` • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

GuardDuty 보안 에이전트를 배포하기 위한 기본 접근 방식	단계
	iam::123456789012:role/org-admins/iam-admin"]
	3. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty
	4. 탐색 창에서 런타임 모니터링을 선택합니다.
	Note 계정에 대한 GuardDuty 에이전트 자동 관리를 활성화하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다.
	5. 구성 탭 아래의 에이전트 관리 섹션에서 GuardDuty 활성화를 선택합니다. 모니터링에서 제외되지 않은 EKS 클러스터의 경우 GuardDuty GuardDuty 보안 에이전트의 배포 및 업데이트를 관리합니다.
	6. 저장을 선택합니다.
	이 클러스터에 GuardDuty 보안 에이전트가 이미 배포된 후 EKS 클러스터를 모니터링에서 제외하려면
	1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 이 단계 이후에는 이 클러스터의 보안 에이전트를 업데이트하지 않습니다. GuardDuty 하지만 보안 에이전

GuardDuty 보안 에이전트를 배포하기 위한 기본 접근 방식	단계
	트는 배포된 상태로 GuardDuty 유지되며 이 EKS 클러스터로부터 런타임 이벤트를 계속 수신합니다. 이는 사용량 통계에 영향을 미칠 수 있습니다. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *CreateTagsec2:# #* 대체하십시오. `eks:TagResource` • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 이 클러스터로부터의 런타임 이벤트 수신을 중지하려면 이 EKS 클러스터에서 배포된 보안 에이전트를 제거해야 합니다. 배포된 보안 에이전트 제거에 대한 자세한 내용은 리소스 비활성화 및 정리가 미치는 영향 섹션을 참조하세요.

GuardDuty 보안 에이전트를 배포하기 위한 기본 접근 방식	단계
포함 태그를 사용하여 선택적 EKS 클러스터 모니터링	1. 자동 에이전트 구성 섹션에서 비활성화를 선택해야 합니다. 런타임 모니터링을 활성화된 상태로 유지하십시오. 2. 저장을 선택합니다. 3. 키는 `GuardDutyManaged` 이고 값은 `true`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. GuardDuty 모니터링하려는 선택적 EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 4. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:UntagResource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-`

GuardDuty 보안 에이전트를 배포하기 위한 기본 접근 방식	단계
	admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
수동 에이전트 관리	1. 자동 에이전트 구성 섹션에서 비활성화를 선택해야 합니다. 런타임 모니터링을 활성화된 상태로 유지하십시오. 2. 저장을 선택합니다. 3. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

다중 계정 환경을 위한 자동 에이전트 구성

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만이 구성원 계정에 대한 자동 에이전트 구성을 활성화 또는 비활성화하고 조직의 구성원 계정에 속하는 EKS 클러스터용 자동 에이전트를 관리할 수 있습니다. GuardDuty 구성원 계정은 자신의 계정에서 이 구성을 수정할 수 없습니다. 위임된 GuardDuty 관리자 계정 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 다중 계정 환경에 대한 자세한 내용은 Managing multiple accounts를 참조하세요.

GuardDuty 위임된 관리자 계정을 위한 자동 에이전트 구성 구성

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
다음을 통해 보안 에이전트를 관리합니다. GuardDuty (모든 EKS 클러스터 모니터링)	런타임 모니터링 섹션에서 모든 계정에 대해 활성화를 선택한 경우 다음 옵션을 사용할 수 있습니다. • 자동 에이전트 구성 섹션에서 모든 계정에 대해 활성화를 선택합니다. GuardDuty 위임된 GuardDuty 관리자 계정 계정에 속하는 모든 EKS 클러스터와 조직의 기존 및 잠재적 신규 구성원 계정에 속하는 모든 EKS 클러스터에 대한 보안 에이전트를 배포하고 관리합니다. • 수동으로 계정 구성을 선택합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	런타임 모니터링 섹션에서 수동으로 계정 구성을 선택한 경우 다음을 수행하십시오. 1. 자동 에이전트 구성 섹션에서 수동 계정 구성을 선택합니다. 2. 위임된 GuardDuty 관리자 계정 (이 계정) 섹션에서 활성화를 선택합니다. 저장을 선택합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	다음 절차에서 해당하는 시나리오 중 하나를 선택합니다. 이 클러스터에 GuardDuty 보안 에이전트가 배포되지 않은 경우 EKS 클러스터를 모니터링에서 제외하려면 1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:Untag Resource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty 4. 탐색 창에서 런타임 모니터링을 선택합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계

> **Note**
>
> 계정에 대한 GuardDuty 에이전트 자동 관리를 활성화하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다.

5. 구성 탭 아래의 에이전트 관리 섹션에서 GuardDuty 활성화를 선택합니다.

   모니터링에서 제외되지 않은 EKS 클러스터의 경우 GuardDuty GuardDuty 보안 에이전트의 배포 및 업데이트를 관리합니다.
6. 저장을 선택합니다.

이 클러스터에 GuardDuty 보안 에이전트가 배포되었을 때 EKS 클러스터를 모니터링에서 제외하려면

1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다.

   Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요.
2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다.

   - *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource`
   - *`DeleteTagsec2:# #`* 대체하십시오. `eks:Untag Resource`
   - *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계

- *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정

  신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다.

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. 이 EKS 클러스터에 자동 에이전트를 사용하도록 설정한 경우 이 단계를 수행한 후에는 이 클러스터의 보안 GuardDuty 에이전트가 업데이트되지 않습니다. 하지만 보안 에이전트는 배포된 상태로 GuardDuty 유지되며 이 EKS 클러스터로부터 런타임 이벤트를 계속 수신합니다. 이는 사용량 통계에 영향을 미칠 수 있습니다.

   이 클러스터로부터의 런타임 이벤트 수신을 중지하려면 이 EKS 클러스터에서 배포된 보안 에이전트를 제거해야 합니다. 배포된 보안 에이전트 제거에 대한 자세한 내용은 리소스 비활성화 및 정리가 미치는 영향 섹션을 참조하세요.
4. 이 EKS 클러스터의 GuardDuty 보안 에이전트를 수동으로 관리한 경우에는 을 참조하십시오. 리소스 비활성화 및 정리가 미치는 영향

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
포함 태그를 사용하여 선택적 EKS 클러스터 모니터링	런타임 모니터링을 활성화하기로 선택한 방법에 관계없이 다음 단계는 계정의 선택적 EKS 클러스터를 모니터링하는 데 도움이 됩니다. 1. 자동 에이전트 구성 섹션에서 위임된 GuardDuty 관리자 계정 (이 계정) 에 대해 비활성화를 선택해야 합니다. 런타임 모니터링 구성을 이전 단계에서 구성한 것과 동일하게 유지하십시오. 2. 저장을 선택합니다. 3. 키는 `GuardDutyManaged` 이고 값은 `true`로 하여 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. GuardDuty 모니터링하려는 선택적 EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 4. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:Untag Resource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::12345678901 2:role/org-admins/iam-admin", "arn:aws:iam::1234`

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	56789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
보안 에이전트를 GuardDuty 수동으로 관리하십시오.	런타임 모니터링을 활성화하도록 선택한 방법에 관계없이 EKS 클러스터의 보안 에이전트를 수동으로 관리할 수 있습니다. 1. 자동 에이전트 구성 섹션에서 위임된 GuardDuty 관리자 계정 (이 계정) 에 대해 비활성화를 선택해야 합니다. 런타임 모니터링 구성을 이전 단계에서 구성한 것과 동일하게 유지하십시오. 2. 저장을 선택합니다. 3. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

모든 구성원 계정에 대해 자동 에이전트를 자동 활성화합니다.

> **Note**
>
> 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
다음을 통해 보안 에이전트를 관리합니다. GuardDuty (모든 EKS 클러스터 모니터링)	이 항목은 모든 구성원 계정에 대해 런타임 모니터링을 활성화하기 위한 것이므로 다음 단계에서는 런타임 모니터링 섹션에서 모든 계정에 대해 활성화를 선택했어야 한다고 가정합니다. 1. 자동 에이전트 구성 섹션에서 모든 계정에 대해 활성화를 선택합니다. GuardDuty 위임된 GuardDuty 관리자 계정 계정에 속하는 모든 EKS 클러스터와 조직의 기존 및 잠재적 신규 구성원 계정에 속하는 모든 EKS 클러스터에 대한 보안 에이전트를 배포하고 관리합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	2. 저장을 선택합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	다음 절차에서 해당하는 시나리오 중 하나를 선택합니다. 이 클러스터에 GuardDuty 보안 에이전트가 배포되지 않은 경우 EKS 클러스터를 모니터링에서 제외하려면 1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:Untag Resource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty 4. 탐색 창에서 런타임 모니터링을 선택합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계

> **Note**
>
> 계정에 대해 자동 에이전트를 활성화하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다.

5. 구성 탭의 런타임 모니터링 구성 섹션에서 편집을 선택합니다.
6. 자동 에이전트 구성 섹션에서 모든 계정에 대해 활성화를 선택합니다. 모니터링에서 제외되지 않은 EKS 클러스터의 경우 GuardDuty GuardDuty 보안 에이전트의 배포 및 업데이트를 관리합니다.
7. 저장을 선택합니다.

이 클러스터에 GuardDuty 보안 에이전트가 배포되었을 때 EKS 클러스터를 모니터링에서 제외하려면

1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다.

   Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요.
2. 이 EKS 클러스터에 자동 에이전트 구성을 사용하도록 설정한 경우 이 단계를 수행한 후에는 이 클러스터의 보안 에이전트가 업데이트되지 않습니다. GuardDuty 하지만 보안 에이전트는 배포된 상태로 GuardDuty 유지되며 이 EKS 클러스터로부터 런타임 이벤트를 계속 수신합니다. 이는 사용량 통계에 영향을 미칠 수 있습니다.

   이 클러스터로부터의 런타임 이벤트 수신을 중지하려면 이 EKS 클러스터에서 배포된 보안 에이전트를 제거해야 합니다. 배포된

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계

보안 에이전트 제거에 대한 자세한 내용은 리소스 비활성화 및 정리가 미치는 영향 섹션을 참조하세요.

3. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다.

   - *CreateTagsec2:# #* 대체하십시오. `eks:TagResource`
   - *DeleteTagsec2:# #* 대체하십시오. `eks:Untag Resource`
   - *access-project* 를 `GuardDutyManaged` 로 바꿉니다.
   - *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정

     신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다.

     ```
     "aws:PrincipalArn":["arn:aws:iam::12345678901
     2:role/org-admins/iam-admin", "arn:aws:iam::1234
     56789012:role/org-admins/iam-admin", "arn:aws:
     iam::123456789012:role/org-admins/iam-admin"]
     ```

4. 이 EKS 클러스터의 GuardDuty 보안 에이전트를 수동으로 관리하는 경우에는 을 참조하십시오. 리소스 비활성화 및 정리가 미치는 영향

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
포함 태그를 사용하여 선택적 EKS 클러스터 모니터링	런타임 모니터링을 활성화하기로 선택한 방법에 관계없이 다음 단계를 수행하면 조직 내 모든 구성원 계정의 선택적 EKS 클러스터를 모니터링할 수 있습니다. 1. 자동 에이전트 구성 섹션에서 어떤 구성도 활성화하지 마십시오. 런타임 모니터링 구성을 이전 단계에서 구성한 것과 동일하게 유지하십시오. 2. 저장을 선택합니다. 3. 키는 `GuardDutyManaged` 이고 값은 `true`로 하여 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. GuardDuty 모니터링하려는 선택적 EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 4. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:Untag Resource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
보안 에이전트를 GuardDuty 수동으로 관리하십시오.	런타임 모니터링을 활성화하도록 선택한 방법에 관계없이 EKS 클러스터의 보안 에이전트를 수동으로 관리할 수 있습니다. 1. 자동 에이전트 구성 섹션에서 어떤 구성도 활성화하지 마십시오. 런타임 모니터링 구성을 이전 단계에서 구성한 것과 동일하게 유지하십시오. 2. 저장을 선택합니다. 3. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

기존의 모든 활성 회원 계정에 대해 자동 에이전트를 활성화합니다.

> **Note**
>
> 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

조직의 기존 활성 구성원 계정에 대한 GuardDuty 보안 에이전트를 관리하려면

- 조직의 기존 활성 구성원 계정에 속하는 EKS 클러스터에서 런타임 이벤트를 GuardDuty 수신하려면 이러한 EKS 클러스터의 GuardDuty 보안 에이전트를 관리하는 기본 방법을 선택해야 합니다. 각각의 접근 방식에 대한 자세한 내용은 GuardDuty보안 에이전트를 관리하는 접근 방식 섹션을 참조하세요.

보안 에이전트를 관리하기 GuardDuty 위한 기본 접근 방식	단계
다음을 통해 보안 에이전트를 관리합니다. GuardDuty (모든 EKS 클러스터 모니터링)	모든 기존 활성 멤버 계정의 모든 EKS 클러스터 모니터링 1. 런타임 모니터링 페이지의 구성 탭에서 자동 에이전트 구성의 현재 상태를 볼 수 있습니다. 2. 자동 에이전트 구성 창의 활성 구성원 계정 섹션에서 작업을 선택합니다. 3. 작업에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다. 4. 확인을 선택합니다.

보안 에이전트를 관리하기 GuardDuty 위한 기본 접근 방식	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	다음 절차에서 해당하는 시나리오 중 하나를 선택합니다. 이 클러스터에 GuardDuty 보안 에이전트가 배포되지 않은 경우 EKS 클러스터를 모니터링에서 제외하려면 1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *CreateTagsec2:# #* 대체하십시오. `eks:TagResource` • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

보안 에이전트를 관리하기 GuardDuty 위한 기본 접근 방식	단계
	iam::123456789012:role/org-admins/iam-admin"]
	3. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty
	4. 탐색 창에서 런타임 모니터링을 선택합니다.
	Note 계정에 대해 자동 에이전트 구성을 활성화하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다.
	5. 구성 탭의 자동 에이전트 구성 창의 활성 멤버 계정에서 작업을 선택합니다.
	6. 작업에서 모든 활성 멤버 계정에 대해 활성화를 선택합니다.
	7. 확인을 선택합니다.
	이 클러스터에 GuardDuty 보안 에이전트가 이미 배포된 후 EKS 클러스터를 모니터링에서 제외하려면
	1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 이 단계 이후에는 이 클러스터의 보안 에이전트를 업데이트하지 않습니다. GuardDuty 하지만 보안 에이전트는 배포된 상태로 GuardDuty 유지되며 이 EKS 클

보안 에이전트를 관리하기 GuardDuty 위한 기본 접근 방식	단계
	러스터로부터 런타임 이벤트를 계속 수신합니다. 이는 사용량 통계에 영향을 미칠 수 있습니다. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *CreateTagsec2:# #* 대체하십시오. `eks:TagResource` • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 보안 에이전트를 관리하는 방법 (통해 GuardDuty 또는 수동으로) 에 관계없이 이 클러스터에서 런타임 이벤트 수신을 중지하려면 배포된 보안 에이전트를 이 EKS 클러스터에서 제거해야 합니다. 배포된 보안 에이전트 제거에 대한 자세한 내용은 리소스 비활성화 및 정리가 미치는 영향 섹션을 참조하세요.

보안 에이전트를 관리하기 GuardDuty 위한 기본 접근 방식	단계
포함 태그를 사용하여 선택적 EKS 클러스터 모니터링	1. 계정 페이지에서 런타임 모니터링을 활성화한 후에는 런타임 모니터링 - 자동 에이전트 구성을 활성화하지 마십시오. 2. 모니터링하고자 하는 선택한 계정에 속하는 EKS 클러스터에 태그를 추가합니다. 태그의 키-값 쌍은 `GuardDutyManaged -true`여야 합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. GuardDuty 모니터링하려는 선택적 EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 3. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:UntagResource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-`

보안 에이전트를 관리하기 GuardDuty 위한 기본 접근 방식	단계
	admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
보안 에이전트를 GuardDuty 수동으로 관리하십시오.	1. 자동 에이전트 구성 섹션에서 활성화를 선택하지 않도록 하십시오. 런타임 모니터링을 활성화된 상태로 유지하십시오. 2. 저장을 선택합니다. 3. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

새 구성원을 위한 자동 에이전트 구성을 자동으로 활성화합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
다음을 통해 보안 에이전트를 관리합니다. GuardDuty (모든 EKS 클러스터 모니터링)	1. 런타임 모니터링 페이지에서 편집을 선택하여 기존 구성을 업데이트합니다. 2. 자동 에이전트 구성 섹션에서 새 구성원 계정에 대해 자동으로 활성화를 선택합니다. 3. 저장을 선택합니다.
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	다음 절차에서 해당하는 시나리오 중 하나를 선택합니다. 이 클러스터에 GuardDuty 보안 에이전트가 배포되지 않은 경우 EKS 클러스터를 모니터링에서 제외하려면 1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *CreateTagsec2:# #* 대체하십시오. `eks:TagResource` • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty 4. 탐색 창에서 런타임 모니터링을 선택합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	> **Note** > 계정에 대해 자동 에이전트 구성을 활성화하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다. 5. 구성 탭의 GuardDuty 에이전트 관리 섹션에서 새 구성원 계정 자동 활성화를 선택합니다. 모니터링에서 제외되지 않은 EKS 클러스터의 경우 GuardDuty GuardDuty 보안 에이전트의 배포 및 업데이트를 관리합니다. 6. 저장을 선택합니다. 이 클러스터에 GuardDuty 보안 에이전트가 배포되었을 때 EKS 클러스터를 모니터링에서 제외하려면 1. GuardDuty 보안 에이전트를 통해 GuardDuty 관리하든 수동으로 관리하든 관계없이 키는 `GuardDuty Managed` A이고 값은 0으로 하여 이 EKS 클러스터에 태그를 추가하십시오. `false` Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 이 EKS 클러스터에 자동 에이전트를 활성화한 경우 이 단계를 수행한 후에는 이 클러스터의 보안 에이전트를 업데이트하지 않습니다. GuardDuty 하지만 보안 에이전트는 배포된 상태로 GuardDuty 유지되며 이 EKS 클러스터로부터 런타임 이벤트를 계속 수신합니다. 이는 사용량 통계에 영향을 미칠 수 있습니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	이 클러스터로부터의 런타임 이벤트 수신을 중지하려면 이 EKS 클러스터에서 배포된 보안 에이전트를 제거해야 합니다. 배포된 보안 에이전트 제거에 대한 자세한 내용은 리소스 비활성화 및 정리가 미치는 영향 섹션을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *CreateTagsec2:# #* 대체하십시오. `eks:TagResource` • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 이 EKS 클러스터의 GuardDuty 보안 에이전트를 수동으로 관리하는 경우에는 을 참조하십시오. 리소스 비활성화 및 정리가 미치는 영향

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
포함 태그를 사용하여 선택적 EKS 클러스터 모니터링	런타임 모니터링을 활성화하기로 선택한 방법에 관계없이 다음 단계는 조직의 새 구성원 계정에 대한 선택적 EKS 클러스터를 모니터링하는 데 도움이 됩니다. 1. 자동 에이전트 구성 섹션에서 새 구성원 계정에 대해 자동 활성화를 선택 해제해야 합니다. 런타임 모니터링 구성을 이전 단계에서 구성한 것과 동일하게 유지하십시오. 2. 저장을 선택합니다. 3. 키는 `GuardDutyManaged` 이고 값은 `true`로 하여 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. GuardDuty 모니터링하려는 선택적 EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 4. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *CreateTagsec2:# #* 대체하십시오. `eks:TagResource` • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
보안 에이전트를 GuardDuty 수동으로 관리하십시오.	런타임 모니터링을 활성화하도록 선택한 방법에 관계없이 EKS 클러스터의 보안 에이전트를 수동으로 관리할 수 있습니다. 1. 자동 에이전트 구성 섹션에서 새 구성원 계정 자동 활성화 확인란의 선택을 취소해야 합니다. 런타임 모니터링 구성을 이전 단계에서 구성한 것과 동일하게 유지하십시오. 2. 저장을 선택합니다. 3. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

활성 멤버 계정을 위한 자동 에이전트 구성 (선택적)

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
다음을 통해 보안 에이전트를 관리합니다. GuardDuty	1. 계정 페이지에서 자동 에이전트 구성을 활성화하려는 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다. 이 단계에서 선택한 계정에 EKS 런타임 모니터링이 이미 활성화되어 있는지 확인하세요.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
(모든 EKS 클러스터 모니터링)	2. 보호 계획 편집에서 적절한 옵션을 선택하여 런타임 모니터링 - 자동 에이전트 구성을 활성화합니다. 3. 확인을 선택합니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	다음 절차에서 해당하는 시나리오 중 하나를 선택합니다. 이 클러스터에 GuardDuty 보안 에이전트가 배포되지 않은 경우 EKS 클러스터를 모니터링에서 제외하려면 1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:Untag Resource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계

> **Note**
>
> 계정에 대해 자동 에이전트 구성을 활성화하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다.

4. 계정 페이지에서 에이전트 자동 관리를 활성화할 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다.
5. 보호 계획 편집에서 적절한 옵션을 선택하여 선택한 계정에 대해 Runtime Monitoring-자동 에이전트 구성을 활성화합니다.

   모니터링에서 제외되지 않은 EKS 클러스터의 경우 보안 GuardDuty 에이전트의 배포 및 업데이트를 관리합니다. GuardDuty
6. 저장을 선택합니다.

이 클러스터에 GuardDuty 보안 에이전트가 배포되었을 때 EKS 클러스터를 모니터링에서 제외하려면

1. 키는 `GuardDutyManaged` 이고 값은 `false`로 하여 이 EKS 클러스터에 태그를 추가합니다.

   Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요.

   이전에 이 EKS 클러스터에 대해 자동 에이전트 구성을 활성화한 경우 이 단계를 수행한 후에는 이 클러스터의 보안 에이전트가 업데이트되지 않습니다. GuardDuty 하지만 보안 에이전트는 배포된 상태로 GuardDuty 유지되며 이 EKS 클러스터로부터 런타임 이벤트를 계속 수신합니다. 이는 사용량 통계에 영향을 미칠 수 있습니다.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계

이 클러스터로부터의 런타임 이벤트 수신을 중지하려면 이 EKS 클러스터에서 배포된 보안 에이전트를 제거해야 합니다. 배포된 보안 에이전트 제거에 대한 자세한 내용은 리소스 비활성화 및 정리가 미치는 영향 섹션을 참조하세요.

2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다.

   - *CreateTagsec2:# #* 대체하십시오. `eks:TagResource`
   - *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource`
   - *access-project* 를 `GuardDutyManaged` 로 바꿉니다.
   - *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정

   신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다.

   ```
   "aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
   ```

3. 이 EKS 클러스터의 GuardDuty 보안 에이전트를 수동으로 관리하는 경우에는 제거해야 합니다. 자세한 정보는 리소스 비활성화 및 정리가 미치는 영향을 참조하세요.

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
포함 태그를 사용하여 선택적 EKS 클러스터 모니터링	런타임 모니터링을 활성화하기로 선택한 방법에 관계없이 다음 단계를 수행하면 선택한 계정에 속하는 선택적 EKS 클러스터를 모니터링할 수 있습니다. 1. 모니터링하려는 EKS 클러스터가 있는 선택된 계정에 대해 런타임 모니터링-자동 에이전트 구성을 활성화하지 않도록 하십시오. 2. 키는 `GuardDutyManaged` 이고 값은 `true`로 하여 EKS 클러스터에 태그를 추가합니다. Amazon EKS 클러스터에 태그를 지정하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 콘솔을 사용한 태그 작업을 참조하세요. 태그를 추가한 후에는 GuardDuty 모니터링하려는 선택적 EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 3. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *`CreateTagsec2:# #`* 대체하십시오. `eks:TagResource` • *`DeleteTagsec2:# #`* 대체하십시오. `eks:Untag Resource` • *`access-project`* 를 `GuardDutyManaged` 로 바꿉니다. • *`123456789012#`* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::12345678901 2:role/org-admins/iam-admin", "arn:aws:iam::1234`

GuardDuty보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	`56789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
보안 에이전트를 GuardDuty 수동으로 관리하십시오.	1. 런타임 모니터링 구성을 이전 단계에서 구성한 것과 동일하게 유지하십시오. 선택한 계정에 대해 런타임 모니터링 - 자동 에이전트 구성을 활성화하지 않았는지 확인하십시오. 2. 확인을 선택합니다. 3. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리

이 섹션에서는 런타임 모니터링을 활성화한 후 Amazon EKS 애드온 에이전트 (GuardDuty 에이전트) 를 관리하는 방법을 설명합니다. 런타임 모니터링을 사용하려면 런타임 모니터링을 활성화하고 Amazon EKS 애드온 () 을 구성해야 합니다. `aws-guardduty-agent` 이 두 단계 중 하나만 수행해도 잠재적 위협을 GuardDuty 탐지하거나 탐지 결과를 생성하는 데 도움이 되지 않습니다.

보안 에이전트를 GuardDuty 배포하기 위한 사전 요구 사항

이 섹션에서는 EKS 클러스터용 GuardDuty 보안 에이전트를 수동으로 배포하기 위한 사전 요구 사항을 설명합니다. 계속하기 전에 계정에 대해 런타임 모니터링을 이미 구성했는지 확인하십시오. 런타임 모니터링을 구성하지 않으면 GuardDuty 보안 에이전트 (EKS 애드온) 가 작동하지 않습니다. 자세한 정보는 GuardDuty 런타임 모니터링 활성화을 참조하세요. 이 단계들을 완료한 후 보안 에이전트 배포 GuardDuty 섹션을 참조하세요.

선호하는 액세스 방법을 선택하여 Amazon VPC 엔드포인트를 생성합니다.

Console

VPC 엔드포인트 생성

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창의 Virtual Private Cloud에서 엔드포인트를 선택합니다.
3. 엔드포인트 생성을 선택합니다.

4. 엔드포인트 생성 페이지에서 서비스 범주에 대해 기타 엔드포인트 서비스를 선택합니다.
5. 서비스 이름에 **com.amazonaws.*us-east-1*.guardduty-data**를 입력합니다.

   *us-east-1*을 올바른 리전으로 바꿉니다. ID에 속하는 EKS 클러스터와 동일한 지역이어야 합니다. AWS 계정
6. 서비스 확인을 선택합니다.
7. 서비스 이름이 성공적으로 확인되면 클러스터가 상주하는 VPC를 선택합니다. 다음 정책을 추가하여 VPC 엔드포인트 사용을 지정된 계정으로만 제한합니다. 이 정책 아래에 제공된 조직 `Condition`을 사용하여 다음 정책을 업데이트하고 엔드포인트에 대한 액세스를 제한할 수 있습니다. 조직의 특정 계정 ID에 VPC 엔드포인트 지원을 제공하려면 Organization condition to restrict access to your endpoint 섹션을 참조하세요.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

`aws:PrincipalAccount` 계정 ID는 VPC 및 VPC 엔드포인트를 포함하는 계정과 일치해야 합니다. 다음 목록은 VPC 엔드포인트를 다른 AWS 계정 ID와 공유하는 방법을 보여줍니다.

엔드포인트 액세스를 제한하는 조직 조건

- VPC 엔드포인트에 액세스할 계정을 여러 개 지정하려면 `"aws:PrincipalAccount": "111122223333"`을 다음과 같이 바꿉니다.

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- 조직의 모든 멤버가 VPC 엔드포인트에 액세스할 수 있도록 허용하려면 `"aws:PrincipalAccount": "111122223333"`을 다음과 같이 바꿉니다.

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- 리소스 액세스를 조직 ID로 제한하려면 정책에 `ResourceOrgID`를 추가합니다.

  자세한 내용은 ResourceOrgID를 참조하십시오.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. 추가 설정에서 DNS 이름 활성화를 선택합니다.
9. 서브넷에서 클러스터가 상주하는 서브넷을 선택합니다.
10. 보안 그룹에서 VPC(또는 EKS 클러스터)로부터 인바운드 포트 443이 활성화된 보안 그룹을 선택합니다. 인바운드 포트 443이 활성화된 보안 그룹이 아직 없는 경우 보안 그룹을 생성합니다.

    VPC(또는 클러스터)에 대한 인바운드 권한을 제한하는 도중 문제가 발생하는 경우 모든 IP 주소(`0.0.0.0/0`)로부터의 인바운드 443 포트에 대한 지원을 제공하세요.

API/CLI

- 호출 CreateVpcEndpoint.
- 파라미터에 대해 다음 값을 사용합니다.
  - 서비스 이름에 **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**를 입력합니다.

    *`us-east-1`*을 올바른 리전으로 바꿉니다. ID에 속한 EKS 클러스터와 동일한 지역이어야 합니다. AWS 계정

- DNSOptions에서 `true`로 설정하여 프라이빗 DNS 옵션을 활성화합니다.
- 에 대해서는 AWS Command Line Interface을 참조하십시오 create-vpc-endpoint.

Amazon EKS용 GuardDuty 보안 에이전트 (애드온) 파라미터를 구성합니다.

Amazon EKS용 GuardDuty 보안 에이전트의 특정 파라미터를 구성할 수 있습니다. 이 지원은 GuardDuty 보안 에이전트 버전 1.5.0 이상에서 사용할 수 있습니다. 최신 애드온 버전에 대한 자세한 내용은 을 참조하십시오. GuardDuty Amazon EKS 클러스터용 보안 에이전트

보안 에이전트 구성 스키마를 업데이트해야 하는 이유는 무엇입니까?

> GuardDuty 보안 에이전트의 구성 스키마는 Amazon EKS 클러스터 내의 모든 컨테이너에서 동일합니다. 기본값이 관련 워크로드 및 인스턴스 크기와 일치하지 않는 경우 CPU 설정, 메모리 설정 및 설정을 구성하는 것을 고려해 보십시오. `PriorityClass` `dnsPolicy` Amazon EKS 클러스터의 GuardDuty 에이전트를 관리하는 방법에 관계없이 이러한 파라미터의 기존 구성을 구성하거나 업데이트할 수 있습니다.

구성된 파라미터를 사용한 자동화된 에이전트 구성 동작

사용자를 대신하여 보안 에이전트 (EKS 애드온) 를 GuardDuty 관리하는 경우 필요에 따라 애드온을 업데이트합니다. GuardDuty 구성 가능한 매개 변수의 값을 기본값으로 설정합니다. 하지만 여전히 매개변수를 원하는 값으로 업데이트할 수 있습니다. 이로 인해 충돌이 발생하는 경우 충돌 해결의 기본 옵션은 입니다. `None`

구성 가능한 파라미터 및 값

애드온 파라미터를 구성하는 단계에 대한 자세한 내용은 다음을 참조하십시오.

- 보안 에이전트 배포 GuardDuty 또는
- 보안 에이전트를 수동으로 업데이트

다음 표는 Amazon EKS 추가 기능을 수동으로 배포하거나 기존 추가 기능 설정을 업데이트하는 데 사용할 수 있는 범위와 값을 제공합니다.

CPU 설정

파라미터	기본값	구성 가능한 범위
요청	200m	200미터에서 1만 미터 사이 (둘 다 포함)
Limits	1,000m	

메모리 설정

파라미터	기본값	구성 가능한 범위
요청	256Mi	256만~20000마일 사이, 둘 다 포함
Limits	1024Mi	

`PriorityClass` 설정

Amazon EKS 애드온을 GuardDuty 생성할 때 `PriorityClass` 할당되는 애드온은 다음과 같습니다. `aws-guardduty-agent.priorityclass` 즉, 에이전트 포드의 우선순위에 따라 어떤 조치도 취해지지 않습니다. 다음 `PriorityClass` 옵션 중 하나를 선택하여 이 애드온 매개 변수를 구성할 수 있습니다.

구성 가능 **`PriorityClass`**	**`preemptionPolicy`** 값	**`preemptionPolicy`** 설명	파드 값
`aws-guardduty-agent.priorityclass`	`Never`	액션 없음	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	이 값을 할당하면 에이전트 포드 값보다 낮은 우선순위 값으로 실행 중인 파드를 선점하게 됩니다.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000

구성 가능 **PriorityClass**	**preemptionPolicy** 값	**preemptionPolicy** 설명	파드 값
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] 쿠버네티스는 다음과 같은 두 가지 옵션을 제공합니다 — 및. `PriorityClass` `system-cluster-critical` `system-node-critical` 자세한 내용은 쿠버네티스 PriorityClass설명서를 참조하십시오.

dnsPolicy 설정

쿠버네티스가 지원하는 다음 DNS 정책 옵션 중 하나를 선택하십시오. 구성이 지정되지 않은 경우 `ClusterFirst` 이 기본값으로 사용됩니다.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

이러한 정책에 대한 자세한 내용은 쿠버네티스 설명서에서 파드의 DNS 정책을 참조하십시오.

보안 에이전트 배포 GuardDuty

이 섹션에서는 특정 EKS 클러스터에 처음으로 GuardDuty 보안 에이전트를 배포하는 방법을 설명합니다. 이 섹션을 진행하기 전에 사전 요구 사항을 이미 설정하고 계정에 대한 런타임 모니터링을 활성화했는지 확인하십시오. 런타임 모니터링을 활성화하지 않으면 GuardDuty 보안 에이전트 (EKS 애드온)가 작동하지 않습니다.

원하는 액세스 방법을 선택하여 처음으로 GuardDuty 보안 에이전트를 배포하십시오.

Console

1. https://console.aws.amazon.com/eks/home#/clusters에서 Amazon EKS 콘솔을 엽니다.
2. 클러스터 이름을 선택합니다.
3. 추가 기능(Add-ons) 탭을 선택합니다.

4. 추가 기능 더 가져오기를 선택합니다.
5. 애드온 선택 페이지에서 Amazon GuardDuty 런타임 모니터링을 선택합니다.
6. 선택한 추가 기능 설정 구성 페이지에서 기본 설정을 사용합니다. EKS 애드온 상태가 활성화 필요인 경우 활성화를 선택합니다. GuardDuty 이 작업을 수행하면 GuardDuty 콘솔이 열리고 계정에 대한 런타임 모니터링을 구성할 수 있습니다.
7. 계정에 대한 런타임 모니터링을 구성한 후 Amazon EKS 콘솔로 다시 전환하십시오. EKS 추가 기능의 상태가 설치 준비 완료로 변경되었을 것입니다.
8. (선택 사항) EKS 애드온 구성 스키마 제공

   애드온 버전의 경우 v1.5.0 이상을 선택하면 런타임 모니터링에서 에이전트의 특정 매개 변수 구성을 지원합니다. GuardDuty 매개변수 범위에 대한 자세한 내용은 을 참조하십시오. EKS 애드온 파라미터 구성

   a. 선택적 구성 설정을 확장하여 구성 가능한 매개변수와 예상 값 및 형식을 확인합니다.
   b. 매개변수를 설정합니다. 값은 에 제공된 범위 내에 있어야 EKS 애드온 파라미터 구성 합니다.
   c. 변경 내용 저장을 선택하여 고급 구성을 기반으로 애드온을 생성합니다.
   d. 충돌 해결 방법의 경우 매개 변수 값을 기본값이 아닌 값으로 업데이트할 때 선택한 옵션을 사용하여 충돌을 해결합니다. 나열된 옵션에 대한 자세한 내용은 Amazon EKS API 참조의 충돌 해결을 참조하십시오.
9. 다음을 선택합니다.
10. 검토 및 생성 페이지에서 세부 정보를 확인한 다음 생성을 선택합니다.
11. 클러스터 세부 정보로 돌아가서 리소스 탭을 선택합니다.
12. 접두사가 있는 새 포드를 볼 수 있습니다. aws-guardduty-agent

API/CLI

다음 옵션 중 하나를 사용하여 Amazon EKS 추가 기능 에이전트(`aws-guardduty-agent`)를 구성할 수 있습니다.

- 계정을 CreateAddon위해 실행하세요.

- > **Note**
  >
  > 애드온의 version 경우 v1.5.0 이상을 선택하면 런타임 모니터링이 에이전트의 특정 매개 변수 구성을 지원합니다. GuardDuty 자세한 정보는 EKS 애드온 파라미터 구성을 참조하세요.

  요청 파라미터에 대해 다음 값을 사용합니다.

  - addonName에 aws-guardduty-agent를 입력합니다.

    애드온 버전 v1.5.0 이상에서 지원되는 구성 가능한 값을 사용할 때 다음 AWS CLI 예제를 사용할 수 있습니다. 빨간색으로 강조 표시되고 구성된 값과 연결된 자리 표시자 값을 바꿔야 합니다. Example.json

    ```
    aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-values 'file://example.json'
    ```

    Example 예제.json

    ```
    {
     "priorityClassName": "aws-guardduty-agent.priorityclass-high",
     "dnsPolicy": "Default",
     "resources": {
      "requests": {
       "cpu": "237m",
       "memory": "512Mi"
      },
      "limits": {
       "cpu": "2000m",
       "memory": "2048Mi"
      }
     }
    }
    ```

  - 지원되는 addonVersion에 대한 내용은 보안 에이전트가 지원하는 쿠버네티스 버전 GuardDuty 섹션을 참조하세요.

- 또는 사용할 수도 있습니다. AWS CLI자세한 내용은 애드온 만들기를 참조하십시오.

보안 에이전트를 수동으로 업데이트

GuardDuty 보안 에이전트를 수동으로 관리하는 경우 계정에 맞게 업데이트해야 합니다. 새 에이전트 버전에 대한 알림을 받으려면 RSS 피드를 구독할 수 있습니다. GuardDuty 에이전트 릴리스 기록

보안 에이전트를 최신 버전으로 업데이트하여 추가된 지원 및 개선 사항의 혜택을 누릴 수 있습니다. 현재 에이전트 버전의 표준 지원이 종료되는 경우 런타임 모니터링 (또는 EKS 런타임 모니터링) 을 계속 사용하려면 현재 에이전트 버전을 업데이트해야 합니다. 릴리스 버전에 대한 자세한 내용은 을 참조하십시오GuardDuty Amazon EKS 클러스터용 보안 에이전트.

사전 조건

보안 에이전트 버전을 업데이트하기 전에 지금 사용하려는 에이전트 버전이 Kubernetes 버전과 호환되는지 확인하십시오. 자세한 정보는 보안 에이전트가 지원하는 쿠버네티스 버전 GuardDuty 을 참조하세요.

Console

1. https://console.aws.amazon.com/eks/home#/clusters에서 Amazon EKS 콘솔을 엽니다.
2. 클러스터 이름을 선택합니다.
3. 애드온을 선택하세요.
4. 추가 기능에서 GuardDuty런타임 모니터링을 선택합니다.
5. 편집을 선택하여 에이전트 세부 정보를 업데이트합니다.
6. GuardDuty 런타임 모니터링 구성 페이지에서 세부 정보를 업데이트합니다.
7. (선택 사항) 애드온 구성 매개변수 업데이트

   EKS 애드온 버전이 1.5.0 이상인 경우 애드온 구성 설정을 업데이트할 수도 있습니다.

   a. 구성 스키마를 보려면 선택적 구성 설정을 확장하십시오.
   b. 에 제공된 범위를 기반으로 매개변수 값을 EKS 애드온 파라미터 구성 업데이트합니다.
   c. 변경 사항 저장을 선택하여 업데이트를 시작합니다.
   d. 충돌 해결 방법의 경우 매개 변수 값을 기본값이 아닌 값으로 업데이트할 때 선택한 옵션을 사용하여 충돌을 해결합니다. 나열된 옵션에 대한 자세한 내용은 Amazon EKS API 참조의 충돌 해결을 참조하십시오.

API/CLI

Amazon EKS 클러스터의 GuardDuty 보안 에이전트를 업데이트하려면 추가 기능 업데이트를 참조하십시오.

> **Note**
>
> `version`애드온의 경우 v1.5.0 이상을 선택하면 런타임 모니터링이 에이전트의 특정 파라미터 구성을 지원합니다. GuardDuty 매개 변수 범위에 대한 자세한 내용은 을 참조하십시오. EKS 애드온 파라미터 구성

애드온 버전 v1.5.0 이상에서 지원되는 구성 가능한 값을 사용할 때 다음 AWS CLI 예제를 사용할 수 있습니다. 빨간색으로 강조 표시되고 구성된 값과 연결된 자리 표시자 값을 바꿔야 합니다.
`Example.json`

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example 예제.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Amazon EKS 추가 기능 버전이 1.5.0 이상이고 추가 스키마를 구성한 경우 클러스터에 값이 올바르게 나타나는지 여부를 확인할 수 있습니다. 자세한 정보는 구성 스키마 업데이트 확인을 참조하세요.

구성 스키마 업데이트 확인

매개변수를 구성한 후 다음 단계를 수행하여 구성 스키마가 업데이트되었는지 확인하십시오.

1. https://console.aws.amazon.com/eks/home#/clusters에서 Amazon EKS 콘솔을 엽니다.
2. 탐색 창에서 클러스터를 선택합니다.
3. 클러스터 페이지에서 업데이트를 확인하려는 클러스터 이름을 선택합니다.
4. 리소스 탭을 선택합니다.
5. 리소스 유형 창의 워크로드에서 선택합니다 DaemonSets.
6. 선택합니다 aws-guardduty-agent.
7. aws-guardduty-agent페이지에서 Raw view를 선택하여 형식이 지정되지 않은 JSON 응답을 확인합니다. 구성 가능한 매개변수에 제공된 값이 표시되는지 확인하십시오.

확인한 후 GuardDuty 콘솔로 전환하십시오. 해당하는 AWS 리전 항목을 선택하고 Amazon EKS 클러스터의 커버리지 상태를 확인하십시오. 자세한 정보는 Amazon EKS 클러스터 적용 범위을 참조하세요.

EKS 런타임 모니터링 구성 (API만 해당)

계정에서 EKS 런타임 모니터링을 구성하기 전에 현재 사용 중인 Kubernetes 버전을 지원하는 검증된 플랫폼 중 하나를 사용하고 있는지 확인하세요. 자세한 내용은 아키텍처 요구 사항 검증 섹션을 참조하세요.

독립형 계정에 대한 EKS 런타임 모니터링 구성

AWS Organizations에 연결된 계정의 경우 다중 계정 환경에서 EKS 런타임 모니터링 구성 섹션을 참조하세요.

원하는 액세스 방법을 선택하여 계정에 대해 EKS 런타임 모니터링을 활성화합니다.

API/CLI

GuardDuty보안 에이전트를 관리하는 접근 방식에 따라 원하는 접근 방식을 선택하고 다음 표에 언급된 단계를 따를 수 있습니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
GuardDuty (모든 EKS 클러스터 모니터링) 를 통해 보안 에이전트를 관리합니다.	1. 리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `ENABLED`로 설정합니다. GuardDuty 계정 내 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 2. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 및 `EKS_ADDON_MANAGEMENT` 를 모두 활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDuty Managed -false`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	• *ec2:# CreateTags* 로 eks:TagResource 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. eks:UntagResource • *access-project* 를 GuardDutyManaged 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 PrincipalArn 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** O를 로 설정하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오ENABLED. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다. STATUS EKS_RUNTIME_MONITORING 리전 탐지기 ID를 사용하고 features 객체 이름을 EKS_RUNTIME_MONITORING 으로, 상태를 ENABLED로 설정하여 전달해 updateDetector API를 실행합니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 모니터링에서 제외되지 않은 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
선택적 EKS 클러스터 모니터링 (포함 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDuty Managed -true`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	EKS_ADDON_MANAGEMENT 의 상태를 DISABLED로 설정합니다. GuardDuty GuardDutyManaged true-쌍 태그가 지정된 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 을 활성화하고 EKS_ADDON_MANAGEMENT 를 비활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
수동으로 보안 에이전트 관리	1. 리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `DISABLED`로 설정합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 을 활성화하고 `EKS_ADDON_MANAGEMENT` 를 비활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

다중 계정 환경에서 EKS 런타임 모니터링 구성

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만이 구성원 계정에 대한 EKS 런타임 모니터링을 활성화 또는 비활성화하고 조직의 멤버 계정에 속하는 EKS 클러스터의 GuardDuty 에이전트 관리를 관리할 수 있습니다. GuardDuty 구성원 계정은 자신의 계정에서 이 구성을 수정할 수 없습니다. 위임된 GuardDuty 관리자 계정 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 다중 계정 환경에 대한 자세한 내용은 Managing multiple accounts를 참조하세요.

GuardDuty 위임된 관리자 계정을 위한 EKS 런타임 모니터링 구성

선호하는 액세스 방법을 선택하여 EKS 런타임 모니터링을 활성화하고 위임된 관리자 계정에 속하는 EKS 클러스터의 GuardDuty 보안 에이전트를 관리하십시오. GuardDuty

API/CLI

GuardDuty보안 에이전트를 관리하는 접근 방식에 따라 원하는 접근 방식을 선택하고 다음 표에 언급된 단계를 따를 수 있습니다.

보안 에이전트를 관리하기 위한 기본 접근 방식 GuardDuty	단계
GuardDuty (모든 EKS 클러스터 모니터링) 를 통해 보안 에이전트를 관리합니다.	리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `ENABLED`로 설정합니다. GuardDuty 계정 내 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 및 `EKS_ADDON_MANAGEMENT` 를 모두 활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

보안 에이전트를 관리하기 위한 기본 접근 방식 GuardDuty	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDuty Managed -false`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** O를 로 설정하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오ENABLED. 그렇지

보안 에이전트를 관리하기 위한 기본 접근 방식 GuardDuty	단계
	않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다. STATUS EKS_RUNTIME_MONITORING 리전 탐지기 ID를 사용하고 features 객체 이름을 EKS_RUNTIME_MONITORING 으로, 상태를 ENABLED로 설정하여 전달해 updateDetector API를 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 모니터링에서 제외되지 않은 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

보안 에이전트를 관리하기 위한 기본 접근 방식 GuardDuty	단계
선택적 EKS 클러스터 모니터링 (포함 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDuty Managed -true`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다.

보안 에이전트를 관리하기 위한 기본 접근 방식 GuardDuty	단계
	EKS_ADDON_MANAGEMENT 의 상태를 DISABLED로 설정합니다. GuardDuty GuardDutyManaged true-쌍 태그가 지정된 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 을 활성화하고 EKS_ADDON_MANAGEMENT 를 비활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

보안 에이전트를 관리하기 위한 기본 접근 방식 GuardDuty	단계
수동으로 보안 에이전트 관리	1. 리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `DISABLED`로 설정합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 을 활성화하고 `EKS_ADDON_MANAGEMENT` 를 비활성화합니다. `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

모든 멤버 계정에 대해 EKS 런타임 모니터링 자동 활성화

원하는 액세스 방법을 선택하여 모든 멤버 계정에 대해 EKS 런타임 모니터링을 활성화합니다. 여기에는 위임된 GuardDuty 관리자 계정, 기존 구성원 계정, 조직에 가입하는 새 계정이 포함됩니다. 원하는 접근 방식을 선택하여 이러한 구성원 계정에 속하는 EKS 클러스터의 GuardDuty 보안 에이전트를 관리하십시오.

API/CLI

GuardDuty보안 에이전트를 관리하는 접근 방식에 따라 원하는 접근 방식을 선택하고 다음 표에 언급된 단계를 따를 수 있습니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
GuardDuty (모든 EKS 클러스터 모니터링) 를 통해 보안 에이전트를 관리합니다.	멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 계정 내 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
	코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDutyManaged -false`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:Untag Resource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** O를 로 설정하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오`ENABLED`. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다. `STATUS EKS_RUNTIME_MONITORING`

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
	리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `ENABLED`로 설정합니다. GuardDuty 모니터링에서 제외되지 않은 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 및 `EKS_ADDON_MANAGEMENT` 를 모두 활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
선택적 EKS 클러스터 모니터링(포함 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDutyManaged -true`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:Untag Resource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `DISABLED`로 설정합니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
	GuardDuty `GuardDutyManaged` `true`-쌍 태그가 지정된 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 을 활성화하고 `EKS_ADDON_MANAGEMENT` 를 비활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
수동으로 보안 에이전트 관리	1. 리전 탐지기 ID를 사용하고 `features` 객체 이름을 `EKS_RUNTIME_MONITORING` 으로, 상태를 `ENABLED`로 설정하여 전달해 updateDetector API를 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `DISABLED`로 설정합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 을 활성화하고 `EKS_ADDON_MANAGEMENT` 를 비활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

모든 기존 활성 멤버 계정에 대해 EKS 런타임 모니터링 구성

원하는 액세스 방법을 선택하여 EKS Runtime Monitoring을 활성화하고 조직의 기존 활성 회원 계정에 대한 GuardDuty 보안 에이전트를 관리하십시오.

API/CLI

GuardDuty보안 에이전트를 관리하는 접근 방식에 따라 원하는 접근 방식을 선택하고 다음 표에 언급된 단계를 따를 수 있습니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
GuardDuty (모든 EKS 클러스터 모니터링) 를 통해 보안 에이전트를 관리합니다.	멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 계정 내 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.
모든 EKS 클러스터를 모니터링하면서 일부 클러	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 GuardDutyManaged -false입니다. 태

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
스터 제외(제외 태그 사용)	그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 eks:TagResource 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. eks:Untag Resource • *access-project* 를 GuardDutyManaged 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 PrincipalArn 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** O를 로 설정하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오ENABLED. 그렇지 않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다. STATUS EKS_RUNTIME_MONITORING

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 모니터링에서 제외되지 않은 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
선택적 EKS 클러스터 모니터링(포함 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDutyManaged -true`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:Untag Resource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. `EKS_ADDON_MANAGEMENT` 의 상태를 `DISABLED`로 설정합니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
	GuardDuty `GuardDutyManaged` `true`-쌍 태그가 지정된 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 `EKS_RUNTIME_MONITORING` 을 활성화하고 `EKS_ADDON_MANAGEMENT` 를 비활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리하기 위한 기본 접근 방식	단계
수동으로 보안 에이전트 관리	1. 멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 DISABLED로 설정합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 을 활성화하고 EKS_ADDON_MANAGEMENT 를 비활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

새 멤버에 대해 EKS 런타임 모니터링 자동 활성화

위임된 GuardDuty 관리자 계정은 EKS Runtime Monitoring을 자동으로 활성화하고 조직에 가입하는 새 계정의 GuardDuty 보안 에이전트를 관리하는 방법에 대한 접근 방식을 선택할 수 있습니다.

API/CLI

GuardDuty보안 에이전트를 관리하는 접근 방식에 따라 원하는 접근 방식을 선택하고 다음 표에 언급된 단계를 따를 수 있습니다.

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
GuardDuty (모든 EKS 클러스터 모니터링) 를 통해 보안 에이전트를 관리합니다.	새 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 간접적으로 호출합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 계정 내 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 단일 계정에서 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 계정과 현재 지역을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
	문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDuty Managed -false`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** O를 로 설정하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오ENABLED. 그렇지

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
	않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다. STATUS EKS_RUNTIME_MONITORING 새 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 간접적으로 호출합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 모니터링에서 제외되지 않은 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 단일 계정에서 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 계정과 현재 지역을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu`

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
	ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]' 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
선택적 EKS 클러스터 모니터링 (포함 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDutyManaged -true`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 새 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 간접적으로 호출합니다.

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
	EKS_ADDON_MANAGEMENT 의 상태를 DISABLED로 설정합니다. GuardDuty GuardDutyManaged true-쌍 태그가 지정된 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 단일 계정에서 EKS_RUNTIME_MONITORING 을 활성화하고 EKS_ADDON_MANAGEMENT 를 비활성화합니다. 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 계정과 현재 지역을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
수동으로 보안 에이전트 관리	1. 새 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 간접적으로 호출합니다. EKS_ADDON_MANAGEMENT 의 상태를 DISABLED로 설정합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 단일 계정에서 EKS_RUNTIME_MONITORING 을 활성화하고 EKS_ADDON_MANAGEMENT 를 비활성화합니다. 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 계정과 현재 지역을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

보안 에이전트를 관리할 때 선호되는 접근 방식 GuardDuty	단계
	2. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

개별 활성 멤버 계정에 대해 EKS 런타임 모니터링 활성화

API/CLI

GuardDuty보안 에이전트를 관리하는 접근 방식에 따라 원하는 접근 방식을 선택하고 다음 표에 언급된 단계를 따를 수 있습니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
GuardDuty (모든 EKS 클러스터 모니터링) 를 통해 보안 에이전트를 관리합니다.	멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 계정 내 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",`

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계

```
 "Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] ]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
모든 EKS 클러스터를 모니터링하면서 일부 클러스터 제외(제외 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDuty Managed -false`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** O를 로 설정하기 전에 항상 EKS 클러스터에 제외 태그를 추가하십시오ENABLED. 그렇지

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
	않으면 GuardDuty 보안 에이전트가 계정의 모든 EKS 클러스터에 배포됩니다. STATUS EKS_RUNTIME_MONITORING 멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 ENABLED로 설정합니다. GuardDuty 모니터링에서 제외되지 않은 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 및 EKS_ADDON_MANAGEMENT 를 모두 활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
	> **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
선택적 EKS 클러스터 모니터링(포함 태그 사용)	1. 모니터링에서 제외하고자 하는 EKS 클러스터에 태그를 추가합니다. 키-값 쌍은 `GuardDutyManaged -true`입니다. 태그 추가에 대한 자세한 내용은 Amazon EKS 사용 설명서의 CLI API 또는 eksctl을 사용한 태그 작업을 참조하세요. 2. 신뢰할 수 있는 엔터티를 제외하고 태그를 수정하지 못하도록 하려면AWS Organizations 사용 설명서의 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지에 제공된 정책을 사용하세요. 이 정책에서 아래 세부 정보를 바꿉니다. • *ec2:# CreateTags* 로 `eks:TagResource` 대체하십시오. • *DeleteTagsec2:# #* 대체하십시오. `eks:UntagResource` • *access-project* 를 `GuardDutyManaged` 로 바꿉니다. • *123456789012#* 신뢰할 수 있는 주체의 ID로 바꾸십시오. AWS 계정 신뢰할 수 있는 엔터티가 두 개 이상 있는 경우 다음 예시를 사용하여 여러 개의 `PrincipalArn` 을 추가합니다. `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. 멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
	EKS_ADDON_MANAGEMENT 의 상태를 DISABLED로 설정합니다. GuardDuty GuardDutyManaged true-쌍 태그가 지정된 모든 Amazon EKS 클러스터의 보안 에이전트 배포 및 업데이트를 관리합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 을 활성화하고 EKS_ADDON_MANAGEMENT 를 비활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다. 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

GuardDuty 보안 에이전트를 관리할 때 선호되는 접근 방식	단계
수동으로 보안 에이전트 관리	1. 멤버 계정에 대해 EKS 런타임 모니터링을 선택적으로 활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 실행합니다. EKS_ADDON_MANAGEMENT 의 상태를 DISABLED로 설정합니다. 또는 자체 지역 탐지기 ID를 사용하여 AWS CLI 명령을 사용할 수도 있습니다. 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. 다음 예시에서는 EKS_RUNTIME_MONITORING 을 활성화하고 EKS_ADDON_MANAGEMENT 를 비활성화합니다. `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. 보안 에이전트를 관리하려면 Amazon EKS 클러스터의 보안 에이전트를 수동으로 관리 섹션을 참조하세요.

EKS 런타임 모니터링에서 런타임 모니터링으로 마이그레이션

GuardDuty 런타임 모니터링이 출시되면서 위협 탐지 범위가 Amazon ECS 컨테이너 및 Amazon EC2 인스턴스로 확대되었습니다. EKS 런타임 모니터링은 이제 런타임 모니터링으로 통합되었습니다. 런타임 모니터링을 활성화하고 런타임 동작을 모니터링하려는 각 리소스 유형 (Amazon EC2 인스턴스, Amazon ECS 클러스터, Amazon EKS 클러스터) 에 대한 개별 GuardDuty 보안 에이전트를 관리할 수 있습니다.

EKS 런타임 모니터링을 위한 별도의 GuardDuty 콘솔 환경은 없습니다. EKS 런타임 모니터링을 계속 사용하려면 API 또는 를 사용하여 구성해야 합니다. AWS Command Line Interface

EKS 런타임 모니터링에서 런타임 모니터링으로 마이그레이션하려면

1. GuardDuty 콘솔은 런타임 모니터링의 일부로 EKS 런타임 모니터링을 지원합니다.

   조직 및 계정별로 EKS 런타임 모니터링 구성 상태 확인 런타임 모니터링을 사용할 수 있습니다.

   런타임 모니터링을 활성화하기 전에 EKS 런타임 모니터링을 비활성화하지 마십시오. EKS 런타임 모니터링을 비활성화하면 Amazon EKS 추가 기능 관리도 비활성화됩니다. 나열된 순서대로 다음 단계를 계속 진행하십시오.
2. 모든 조건을 충족하는지 확인하세요런타임 모니터링을 활성화하기 위한 사전 요구 사항.
3. EKS 런타임 모니터링과 동일한 런타임 모니터링 조직 구성 설정을 복제하여 런타임 모니터링을 활성화하십시오. 자세한 정보는 Runtime Monitoring 활성화을 참조하세요.
   - 독립 실행형 계정이 있는 경우 런타임 모니터링을 활성화해야 합니다.

     GuardDuty 보안 에이전트가 이미 배포된 경우 해당 설정이 자동으로 복제되므로 설정을 다시 구성할 필요가 없습니다.
   - 자동 활성화 설정이 있는 조직이 있는 경우 런타임 모니터링에 대해 동일한 자동 활성화 설정을 복제해야 합니다.
   - 기존 활성 구성원 계정에 대한 설정을 개별적으로 구성한 조직의 경우 런타임 모니터링을 활성화하고 해당 구성원에 대한 GuardDuty 보안 에이전트를 개별적으로 구성해야 합니다.
4. 런타임 모니터링 및 GuardDuty 보안 에이전트 설정이 올바른지 확인한 후 API 또는 명령을 사용하여 EKS 런타임 모니터링을 비활성화하십시오 AWS CLI .
5. (선택 사항) GuardDuty 보안 에이전트와 관련된 리소스를 정리하려면 을 참조하십시오. 리소스 비활성화 및 정리가 미치는 영향

런타임 모니터링을 활성화하지 않고 EKS 런타임 모니터링을 계속 사용하려면 을 참조하십시오EKS 런타임 모니터링 구성 (API만 해당).

EKS 런타임 모니터링 구성 상태 확인

다음 API 또는 AWS CLI 명령을 사용하여 EKS 런타임 모니터링의 기존 구성 상태를 확인합니다.

계정의 기존 EKS 런타임 모니터링 구성 상태를 확인하려면

- GetDetector를 실행하여 사용자 계정의 구성 상태를 확인하십시오.

- 또는 AWS CLI다음을 사용하여 다음 명령을 실행할 수도 있습니다.

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

사용자 AWS 계정 및 현재 지역의 탐지기 ID를 교체해야 합니다. 계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId

조직의 기존 EKS 런타임 모니터링 구성 상태를 확인하려면 (위임된 GuardDuty 관리자 계정만 해당)

- DescribeOrganizationConfiguration를 실행하여 조직의 구성 상태를 확인합니다.

  또는 AWS CLI다음을 사용하여 다음 명령을 실행할 수도 있습니다.

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

탐지기 ID를 위임된 GuardDuty 관리자 계정의 탐지기 ID로, 지역은 현재 지역으로 대체해야 합니다. 계정과 현재 지역의 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. detectorId

런타임 모니터링으로 마이그레이션한 후 EKS 런타임 모니터링 비활성화

계정 또는 조직의 기존 설정이 런타임 모니터링에 복제되었는지 확인한 후 EKS 런타임 모니터링을 비활성화할 수 있습니다.

EKS 런타임 모니터링을 비활성화하려면

- 자신의 계정에서 EKS 런타임 모니터링을 비활성화하려면

  자체 지역 ### ID로 UpdateDetectorAPI를 실행하세요.

  또는 다음 명령어를 사용할 수도 있습니다. AWS CLI 12abc34d567e8fa901bc2d34e56789f0# ### ## ### ID# ######.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- 조직의 구성원 계정에 대한 EKS 런타임 모니터링을 비활성화하려면

조직의 위임된 GuardDuty 관리자 계정의 지역 *### ID# UpdateMemberDetectors*API를 실행합니다.

또는 다음 명령을 사용할 수 있습니다. AWS CLI *12abc34d567e8fa901bc2d34e56789f0# ### ### ### ### ## ### ID# ###, 111122223333# # ### #### ### ##### ### ### ID # #####. GuardDuty* AWS 계정

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- 조직의 EKS 런타임 모니터링 자동 활성화 설정을 업데이트하려면

EKS 런타임 모니터링 자동 활성화 설정을 조직의 새 (NEW) 또는 전체 (ALL) 구성원 계정으로 구성한 경우에만 다음 단계를 수행하십시오. 로 NONE 이미 구성한 경우에는 이 단계를 건너뛰어도 됩니다.

> **Note**
>
> EKS 런타임 모니터링 자동 활성화 구성을 설정하면 기존 구성원 계정이나 새 구성원 계정이 조직에 가입할 때 EKS 런타임 모니터링이 자동으로 활성화되지 않도록 설정할 수 있습니다. NONE

조직의 위임된 관리자 계정의 지역 *### ID# UpdateOrganizationConfiguration*API를 실행합니다. GuardDuty

또는 다음 명령을 사용할 수 있습니다. AWS CLI *12abc34d567e8fa901bc2d34e56789f0# ### ### ### ### ## ### ID# #####.* GuardDuty 자동 활성화를 위해 *EXISTING_VALUE#* 현재 구성으로 바꾸십시오. GuardDuty

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

리소스의 런타임 커버리지 평가

Runtime Monitoring을 활성화하고 GuardDuty 보안 에이전트가 리소스에 배포되면 해당 리소스 유형에 대한 커버리지 통계와 계정에 속한 리소스의 개별 커버리지 상태를 GuardDuty 제공합니다. 커버리

지 상태는 런타임 모니터링을 활성화하고, Amazon VPC 엔드포인트가 생성되었으며, 해당 리소스의 GuardDuty 보안 에이전트가 배포되었는지 확인하여 결정됩니다. 정상 커버리지 상태는 리소스와 관련된 런타임 이벤트가 있을 때 Amazon VPC 엔드포인트를 통해 해당 런타임 이벤트를 수신하고 동작을 모니터링할 수 있음을 나타냅니다. GuardDuty 런타임 모니터링을 구성하거나, Amazon VPC 엔드포인트를 생성하거나, GuardDuty 보안 에이전트를 배포할 때 문제가 발생한 경우, 적용 범위 상태가 비정상으로 표시됩니다. 커버리지 상태가 GuardDuty 비정상이면 해당 리소스의 런타임 동작을 수신 또는 모니터링할 수 없으며 런타임 모니터링 결과를 생성할 수 없습니다.

다음 항목은 커버리지 통계를 검토하고, EventBridge 알림을 구성하고, 특정 리소스 유형에 대한 커버리지 문제를 해결하는 데 도움이 됩니다.

내용

Amazon EC2 인스턴스 적용 범위

Amazon EC2 리소스의 경우 런타임 커버리지는 인스턴스 수준에서 평가됩니다. Amazon EC2 인스턴스는 사용자 환경에서 다양한 유형의 애플리케이션과 워크로드를 실행할 수 있습니다. AWS 이 기능은 Amazon ECS에서 관리되는 Amazon EC2 인스턴스도 지원하며, Amazon EC2 인스턴스에서 Amazon ECS 클러스터를 실행하는 경우 인스턴스 수준의 커버리지 문제는 Amazon EC2 런타임 커버리지에서 나타납니다.

주제

적용 범위 통계 검토

사용자 계정 또는 멤버 계정과 연결된 Amazon EC2 인스턴스의 적용 범위 통계는 선택한 EC2 인스턴스 중 정상 EC2 인스턴스가 차지하는 비율입니다. AWS 리전다음 등식은 이를 다음과 같이 나타냅니다.

(정상 인스턴스/모든 인스턴스) *100

Amazon ECS 클러스터용 GuardDuty 보안 에이전트도 배포한 경우, Amazon EC2 인스턴스에서 실행되는 Amazon ECS 클러스터와 관련된 모든 인스턴스 수준 커버리지 문제는 Amazon EC2 인스턴스 런타임 커버리지 문제로 나타납니다.

액세스 방법 중 하나를 선택하여 계정의 적용 범위 통계를 검토합니다.

Console

- AWS Management Console 로그인하고 https://console.aws.amazon.com/guardduty/ 에서 콘솔을 여십시오. GuardDuty
- 탐색 창에서 런타임 모니터링을 선택합니다.
- 런타임 커버리지 탭을 선택합니다.
- EC2 인스턴스 런타임 커버리지 탭에서는 인스턴스 목록 테이블에 있는 각 Amazon EC2 인스턴스의 커버리지 상태별로 집계된 커버리지 통계를 볼 수 있습니다.
  - 다음 열을 기준으로 인스턴스 목록 테이블을 필터링할 수 있습니다.
    - 계정 ID
    - 에이전트 관리 유형
    - 에이전트 버전
    - 적용 범위 상태
    - 인스턴스 ID
    - 클러스터 ARN
- 커버리지 상태가 비정상인 EC2 인스턴스가 있는 경우, Issue 열에는 비정상 상태의 이유에 대한 추가 정보가 포함됩니다.

API/CLI

- 고유한 유효한 탐지기 ID, 현재 지역 및 서비스 엔드포인트로 ListCoverageAPI를 실행하십시오. 이 API를 사용하여 인스턴스 목록을 필터링하고 정렬할 수 있습니다.
  - `CriterionKey`에 대한 다음 옵션 중 하나를 사용하여 예시 `filter-criteria`를 변경할 수 있습니다.
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`

- AGENT_VERSION
- MANAGEMENT_TYPE
- INSTANCE_ID
- CLUSTER_ARN

- EC2로 **filter-criteria** 포함된 RESOURCE_TYPE 경우 런타임 모니터링은 ISSUE를 다음으로 사용할 수 없습니다. AttributeName 이를 사용하면 API 응답 결과가 다음과 같이 나타납니다. InvalidInputException

  다음 옵션을 사용하여 sort-criteria에서 예시 AttributeName을 변경할 수 있습니다.

  - ACCOUNT_ID
  - COVERAGE_STATUS
  - INSTANCE_ID
  - UPDATED_AT
- *max-results*를 변경할 수 있습니다(최대 50개).
- 계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- GetCoverageStatistics API를 실행하여 를 기반으로 커버리지 집계 통계를 검색하십시오. statisticsType
  - 다음 옵션 중 하나를 사용하여 예시 statisticsType을 변경할 수 있습니다.
    - COUNT_BY_COVERAGE_STATUS - 적용 범위 상태별로 집계된 EKS 클러스터의 적용 범위 통계를 나타냅니다.
    - COUNT_BY_RESOURCE_TYPE— 목록에 있는 AWS 리소스 유형에 따라 집계된 커버리지 통계.
    - 명령에서 예시 filter-criteria를 변경할 수 있습니다. CriterionKey에 대해 다음 옵션을 사용할 수 있습니다.
      - ACCOUNT_ID
      - RESOURCE_TYPE

  - COVERAGE_STATUS
  - AGENT_VERSION
  - MANAGEMENT_TYPE
  - INSTANCE_ID
  - CLUSTER_ARN
- 계정과 현재 지역에 detectorId 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

EC2 인스턴스의 커버리지 상태가 비정상인 경우 을 참조하십시오. 적용 범위 문제 해결

적용 범위 상태 변경 알림 구성

Amazon EC2 인스턴스의 커버리지 상태가 비정상으로 표시될 수 있습니다. 커버리지 상태가 언제 변경되는지 확인하려면 주기적으로 커버리지 상태를 모니터링하고 상태가 비정상으로 바뀌면 문제를 해결하는 것이 좋습니다. 또는 보장 상태가 비정상에서 건강으로 또는 기타 상태로 변경될 때 알림을 받도록 Amazon EventBridge 규칙을 생성할 수 있습니다. 기본적으로 계정의 EventBridge 버스에 이 내용을 GuardDuty 게시합니다.

샘플 알림 스키마

EventBridge 규칙적으로 사전 정의된 샘플 이벤트와 이벤트 패턴을 사용하여 커버리지 상태 알림을 받을 수 있습니다. EventBridge 규칙 생성에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 규칙 생성을 참조하십시오.

또한 다음 예시 알림 스키마를 사용하여 사용자 지정 이벤트 패턴을 생성할 수 있습니다. 계정에 대한 값을 바꿔야 합니다. Amazon EC2 인스턴스의 커버리지 상태가 에서 Healthy 로 변경될 때 알림을 받으려면 *GuardDuty ### ## detail-type* 비정상이어야 합니다. Unhealthy 적용 범위 상태가 에서 Unhealthy 로 변경될 때 알림을 받으려면 의 값을 *GuardDuty ### ## detail-type* 정상으로 바꾸십시오. Healthy

```
{
  "version": "0",
```

```
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
  "time": "event timestamp (string)",
  "region": "AWS ##",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

적용 범위 문제 해결

Amazon EC2 인스턴스의 커버리지 상태가 비정상인 경우 Issue 열에서 이유를 확인할 수 있습니다.

EC2 인스턴스가 EKS 클러스터와 연결되어 있고 EKS용 보안 에이전트를 수동으로 설치하거나 자동 에이전트 구성을 통해 설치한 경우 적용 범위 문제를 해결하려면 을 참조하십시오. Amazon EKS 클러스터 적용 범위

다음 표에는 문제 유형과 해당 문제 해결 단계가 나열되어 있습니다.

문제 유형	이슈 메시지	문제 해결 단계
상담원 신고 없음	SSM 알림 대기 중	Amazon EC2 인스턴스가 이미 SSM으로 관리되고 있는지 확인하십시오. SSM 알림을 수신하는 데 몇 분 정도 걸릴 수 있습니다.
	(일부러 비워 두세요)	GuardDuty 보안 에이전트를 수동으로 관리하는 경우 아래 단계를 따랐는지 확인하십시오Amazon EC2 인스턴스의 보안 에이전트를 수동으로 관리.
		자동 에이전트 구성을 활성화한 경우: • EC2 인스턴스는 SSM으로 관리됩니다. • 보안 에이전트의 상태를 정기적으로 확인하십시오. 자세한 정보는 GuardDuty 보안 에이전트 설치 상태 검증을 참조하세요.
		조직에 SCP (서비스 제어 정책) 가 있는 경우 권한을 거부하지 않는지 확인하세요. `guardduty:SendSecurityTelemetry` 자세한 정보는 조직 서비스 제어 정책 검증을 참조하세요.
	상담원 연결이 끊겼습니다.	• 보안 에이전트의 상태를 확인하세요. 자세한 정보는 GuardDuty 보안 에이전트 설치 상태 검증을 참조하세요. • 보안 에이전트 로그를 보고 잠재적인 근본 원인을 식별하십시오. 로그는 문제를 직접 해결하는 데 사용할 수 있는 자세한 오류를 제공합니다. 로그 파일은 에서 `/var/log/amzn-guardduty-agent/` 확인할 수 있습니다. Do `sudo journalctl -u amazon-guardduty-agent` .
SSM 연결 생성 실패	GuardDuty 계정에 SSM 연결이 이미 있습니다.	1. 기존 연결을 수동으로 삭제합니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 연결 삭제를 참조하십시오.

문제 유형	이슈 메시지	문제 해결 단계
		2. 연결을 삭제한 후에는 Amazon EC2의 GuardDuty 자동 에이전트 구성을 비활성화했다가 다시 활성화합니다.
	계정에 SSM 연결이 너무 많습니다.	다음 두 옵션 중 하나를 선택하세요. • 사용하지 않는 SSM 연결을 모두 삭제합니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 연결 삭제를 참조하십시오. • 계정이 할당량 증가 대상이 되는지 확인하세요. 자세한 내용은 의 Systems Manager 서비스 할당량을 참조하십시오. AWS 일반 참조
SSM 연결 업데이트 실패	GuardDuty 계정에 SSM 연결이 존재하지 않습니다.	GuardDuty 계정에 SSM 연결이 없습니다. 런타임 모니터링을 비활성화한 다음 다시 활성화합니다.
SSM 연결 삭제 실패	GuardDuty 계정에 SSM 연결이 존재하지 않습니다.	계정에 SSM 연결이 없습니다. SSM 연결을 의도적으로 삭제한 경우에는 별도의 조치가 필요하지 않습니다.

문제 유형	이슈 메시지	문제 해결 단계
SSM 인스턴스 연결 실행 실패	아키텍처 요구 사항 또는 기타 사전 요구 사항이 충족되지 않았습니다.	검증된 운영 체제 배포에 대한 자세한 내용은 을 참조하십시오. Amazon EC2 인스턴스 지원을 위한 사전 요구 사항 이 문제가 계속 발생하는 경우 다음 단계를 통해 문제를 식별하고 잠재적으로 해결할 수 있습니다. 1. https://console.aws.amazon.com/systems-manager/에서 AWS Systems Manager 콘솔을 엽니다. 2. 탐색 창의 노드 관리에서 상태 관리자를 선택합니다. 3. 문서 이름 속성으로 필터링하고 를 입력합니다 AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. 해당 연결 ID를 선택하고 실행 기록을 확인합니다. 5. 실행 기록을 사용하여 실패를 확인하고 잠재적인 근본 원인을 식별하여 해결을 시도해 보십시오.
VPC 엔드포인트 생성 실패	공유 VPC *vpcId*에 대해 VPC 엔드포인트 생성이 지원되지 않음	런타임 모니터링은 조직 내에서 공유 VPC를 사용할 수 있도록 지원합니다. 자세한 정보는 자동화된 보안 에이전트와 공유 VPC 사용을 참조하세요.

문제 유형	이슈 메시지	문제 해결 단계
	자동 에이전트 구성과 함께 공유 VPC를 사용하는 경우에만 공유 VPC의 소유자 계정 ID *111122223333 vPCID##* 런타임 모니터링, 자동 에이전트 구성 또는 둘 다 활성화되어 있지 않습니다.	공유 VPC 소유자 계정은 하나 이상의 리소스 유형 (Amazon EKS 또는 Amazon ECS ()) 에 대해 런타임 모니터링 및 자동 에이전트 구성을 활성화해야 합니다.AWS Fargate자세한 정보는 런타임 모니터링과 관련된 사전 요구 사항 GuardDuty을 참조하세요.
	프라이빗 DNS를 활성화하려면 *vpcId*(서비스: Ec2, 상태 코드:400, 요청 ID: *a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*)에 대해 `enableDnsSupport` 및 `enableDnsHostnames` VPC 속성 모두 `true`로 설정되어야 합니다.	다음 `enableDnsSupport` 및 `enableDnsHostnames` VPC 속성이 `true`로 설정되어야 합니다. 자세한 내용을 알아보려면 VPC의 DNS 속성을 참조하세요. Amazon VPC 콘솔(https://console.aws.amazon.com/vpc/)을 사용하여 Amazon VPC를 생성하는 경우 DNS 호스트 이름 활성화와 DNS 확인 활성화를 모두 선택해야 합니다. 자세한 내용은 VPC 구성 옵션을 참조하세요.

문제 유형	이슈 메시지	문제 해결 단계
공유 VPC 엔드포인트 삭제 실패	*## ID 111122223333, ## VPC VPCID, ### ## ID 5555555555# #### ## VPC ##### ### ## ## ####.*	잠재적 단계는 다음과 같습니다. • 공유 VPC 참가자 계정의 런타임 모니터링 상태를 비활성화해도 공유 VPC 엔드포인트 정책 및 소유자 계정에 있는 보안 그룹에는 영향을 미치지 않습니다. 공유 VPC 엔드포인트 및 보안 그룹을 삭제하려면 공유 VPC 소유자 계정에서 런타임 모니터링 또는 자동 에이전트 구성 상태를 비활성화해야 합니다. • 공유 VPC 참가자 계정은 공유 VPC 소유자 계정에 호스팅된 공유 VPC 엔드포인트 및 보안 그룹을 삭제할 수 없습니다.
상담원이 신고하지 않음	(일부러 비워 놓음)	문제 유형이 지원 종료되었습니다. 이 문제가 계속 발생하지만 아직 발생하지 않은 경우 Amazon EC2용 GuardDuty 자동 에이전트를 활성화하십시오. 문제가 지속되면 런타임 모니터링을 몇 분 동안 비활성화했다가 다시 활성화하는 것을 고려해 보십시오.

Amazon ECS 클러스터 적용 범위

Amazon ECS 클러스터의 런타임 범위에는 Amazon ECS 컨테이너 인스턴스에서 실행되는 AWS Fargate (Fargate) 작업과 Amazon ECS 컨테이너 인스턴스가 포함됩니다. [1]

Fargate에서 실행되는 Amazon ECS 클러스터의 경우 런타임 커버리지는 작업 수준에서 평가됩니다. ECS 클러스터 런타임 범위에는 Fargate에 대한 런타임 모니터링 및 자동 에이전트 구성 (ECS만 해당)을 활성화한 후 실행되기 시작한 Fargate 작업이 포함됩니다. 기본적으로 Fargate 태스크는 변경할 수 없습니다. GuardDuty 이미 실행 중인 작업의 컨테이너를 모니터링하기 위한 보안 에이전트를 설치할 수 없습니다. 이러한 Fargate 작업을 포함하려면 작업을 중지했다가 다시 시작해야 합니다. 관련 서비스가 지원되는지 확인하십시오.

현재 런타임 모니터링은 에서 시작한 작업을 지원하지 않습니다. AWS CodePipeline

Amazon ECS 컨테이너에 대한 자세한 내용은 용량 생성을 참조하십시오.

내용

적용 범위 통계 검토

사용자 계정 또는 멤버 계정과 관련된 Amazon ECS 리소스의 커버리지 통계는 선택한 모든 Amazon ECS 클러스터에서 정상 Amazon ECS 클러스터가 차지하는 비율입니다. AWS 리전여기에는 Fargate 및 Amazon EC2 인스턴스 모두와 관련된 Amazon ECS 클러스터에 대한 적용 범위가 포함됩니다. 다음 등식은 이를 다음과 같이 나타냅니다.

(정상 클러스터/모든 클러스터)*100

고려 사항

- ECS 클러스터의 커버리지 통계에는 해당 ECS 클러스터와 관련된 Fargate 작업 또는 ECS 컨테이너 인스턴스의 커버리지 상태가 포함됩니다. Fargate 작업의 적용 범위 상태에는 실행 상태이거나 최근에 실행이 완료된 작업이 포함됩니다.
- ECS 클러스터 런타임 커버리지 탭에서 컨테이너 인스턴스 커버리지 필드는 Amazon ECS 클러스터와 연결된 컨테이너 인스턴스의 커버리지 상태를 나타냅니다.

  Amazon ECS 클러스터에 Fargate 작업만 포함된 경우 개수는 0/0으로 표시됩니다.
- Amazon ECS 클러스터가 보안 에이전트가 없는 Amazon EC2 인스턴스와 연결된 경우 Amazon ECS 클러스터도 비정상 커버리지 상태가 됩니다.

  관련 Amazon EC2 인스턴스의 커버리지 문제를 식별하고 해결하려면 Amazon EC2 인스턴스를 적용 범위 문제 해결 참조하십시오.

액세스 방법 중 하나를 선택하여 계정의 적용 범위 통계를 검토합니다.

Console

- AWS Management Console 로그인하고 https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
- 탐색 창에서 런타임 모니터링을 선택합니다.
- 런타임 커버리지 탭을 선택합니다.

- ECS 클러스터 런타임 커버리지 탭에서 클러스터 목록 테이블에 있는 각 Amazon ECS 클러스터의 커버리지 상태별로 집계된 커버리지 통계를 볼 수 있습니다.
  - 다음 열을 기준으로 클러스터 목록 테이블을 필터링할 수 있습니다.
    - 계정 ID
    - 클러스터 이름
    - 에이전트 관리 유형
    - 적용 범위 상태
- Amazon ECS 클러스터 중 하나라도 커버리지 상태가 비정상인 경우, Issue 열에는 비정상 상태의 이유에 대한 추가 정보가 포함됩니다.

  Amazon ECS 클러스터가 Amazon EC2 인스턴스와 연결되어 있는 경우, EC2 인스턴스 런타임 커버리지 탭으로 이동하여 클러스터 이름 필드를 기준으로 필터링하여 관련 문제를 확인하십시오.

API/CLI

- 고유한 유효한 탐지기 ID, 현재 지역 및 서비스 엔드포인트를 사용하여 ListCoverageAPI를 실행합니다. 이 API를 사용하여 인스턴스 목록을 필터링하고 정렬할 수 있습니다.
  - `CriterionKey`에 대한 다음 옵션 중 하나를 사용하여 예시 `filter-criteria`를 변경할 수 있습니다.
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
  - 다음 옵션을 사용하여 `sort-criteria`에서 예시 `AttributeName`을 변경할 수 있습니다.
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ECS_CLUSTER_NAME`
    - `UPDATED_AT`

      필드는 관련 Amazon ECS 클러스터에서 새 작업이 생성되거나 해당 적용 범위 상태가 변경될 때만 업데이트됩니다.

- *max-results*를 변경할 수 있습니다(최대 50개).
- 계정 및 현재 지역에 detectorId 맞는 항목을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- GetCoverageStatisticsAPI를 실행하여 를 기반으로 커버리지 집계 통계를 검색하십시오. statisticsType
  - 다음 옵션 중 하나를 사용하여 예시 statisticsType을 변경할 수 있습니다.
    - COUNT_BY_COVERAGE_STATUS— 커버리지 상태별로 집계된 ECS 클러스터의 커버리지 통계를 나타냅니다.
    - COUNT_BY_RESOURCE_TYPE— 목록에 있는 AWS 리소스 유형에 따라 집계된 커버리지 통계.
    - 명령에서 예시 filter-criteria를 변경할 수 있습니다. CriterionKey에 대해 다음 옵션을 사용할 수 있습니다.
      - ACCOUNT_ID
      - ECS_CLUSTER_NAME
      - COVERAGE_STATUS
      - MANAGEMENT_TYPE
      - INSTANCE_ID
    - 계정과 현재 지역에 detectorId 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

커버리지 문제에 대한 자세한 내용은 을 참조하십시오적용 범위 문제 해결.

적용 범위 상태 변경 알림 구성

Amazon ECS 클러스터의 커버리지 상태가 비정상으로 표시될 수 있습니다. 커버리지 상태가 언제 변경되는지 확인하려면 주기적으로 커버리지 상태를 모니터링하고 상태가 비정상으로 바뀌면 문제를 해결하는 것이 좋습니다. 또는 보장 상태가 비정상에서 건강으로 또는 기타 상태로 변경될 때 알림을 받도록 Amazon EventBridge 규칙을 생성할 수 있습니다. 기본적으로 계정의 EventBridge 버스에 이 내용을 GuardDuty 게시합니다.

샘플 알림 스키마

EventBridge 규칙적으로 사전 정의된 샘플 이벤트와 이벤트 패턴을 사용하여 커버리지 상태 알림을 받을 수 있습니다. EventBridge 규칙 생성에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 규칙 생성을 참조하십시오.

또한 다음 예시 알림 스키마를 사용하여 사용자 지정 이벤트 패턴을 생성할 수 있습니다. 계정에 대한 값을 바꿔야 합니다. Amazon ECS 클러스터의 커버리지 상태가 에서 `Healthy` 로 `Unhealthy` 변경될 때 알림을 받으려면 *`GuardDuty ### ## detail-type ######`* 합니다. 적용 범위 상태가 에서 `Unhealthy` 로 변경될 때 알림을 받으려면 의 값을 *`GuardDuty ### ##`* 정상 상태로 `detail-type` 바꾸십시오. `Healthy`

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
  "time": "event timestamp (string)",
  "region": "AWS ##",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
```

```
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

적용 범위 문제 해결

Amazon ECS 클러스터의 커버리지 상태가 비정상인 경우 Issue 열에서 이유를 확인할 수 있습니다.

다음 표에는 Fargate (Amazon ECS만 해당) 문제에 대한 권장 문제 해결 단계가 나와 있습니다. Amazon EC2 인스턴스 적용 범위 문제에 대한 자세한 내용은 Amazon 적용 범위 문제 해결 EC2 인스턴스를 참조하십시오.

문제 유형	추가 정보	권장 문제 해결 단계
상담원이 신고하지 않음	에이전트가 내 작업에 대해 보고하지 않음 TaskDefinition - '*TASK_DEFINITION* '	VPC 엔드포인트 구성이 올바른지 확인합니다. 조직에 SCP (서비스 제어 정책) 가 있는 경우 권한을 거부하지 않는지 확인하세요. guardduty:SendSecurityTelemetry 자세한 정보는 조직 서비스 제어 정책 검증을 참조하세요.
	VPC_ISSUE ; for task in TaskDefinition - ' *TASK_DEFINITION* '	추가 정보에서 VPC 문제 세부 정보를 확인하세요.
에이전트가 종료되었습니다.	ExitCode: EXIT_CODE 에 있는 작업의 경우 TaskDefinition - '*TASK_DEFINITION* '	추가 정보에서 문제 세부 정보를 확인하세요.

문제 유형	추가 정보	권장 문제 해결 단계
	##: 에서 작업을 수행하는 이유 TaskDefinition - ' *TASK_DEFINITION* '	
	ExitCode: 이유 EXIT_CODE 포함: 에 있는 작업의 경우 '*EXIT_CODE* ' TaskDefinition - '*TASK_DEFINITION* '	

	에이전트 종료: 원인:CannotPullContainerError : 풀 이미지 매니페스트가 재시도되었습니다...	작업 실행 역할에는 다음과 같은 Amazon Elastic 컨테이너 레지스트리 (Amazon ECR) 권한이 있어야 합니다.
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		자세한 정보는 ECR 권한 및 서브넷 세부 정보를 제공하십시오.을 참조하세요.
		Amazon ECR 권한을 추가한 후에는 작업을 다시 시작해야 합니다.
		문제가 지속되면 을 참조하십시오. AWS Step Functions 워크플로가 예기치 않게 실패합니다.

문제 유형	추가 정보	권장 문제 해결 단계
기타 또는 에이전트가 프로비저닝되지 않음	미확인 문제, 작업의 경우 `TaskDefinition - 'TASK_DEFINITION '`	다음 질문을 사용하여 문제의 근본 원인을 파악하십시오. • 런타임 모니터링을 활성화하기 전에 작업이 시작되었나요? Amazon ECS에서는 작업을 변경할 수 없습니다. 실행 중인 Fargate 작업의 런타임 동작을 평가하려면 Runtime Monitoring이 이미 활성화되어 있는지 확인한 다음 컨테이너 사이드카를 GuardDuty 추가하기 위해 작업을 다시 시작하십시오. • 지원되지 않는 서비스에서 작업을 시작했나요? 현재 런타임 모니터링은 에서 시작한 작업을 지원하지 않습니다. AWS CodePipeline • 이 작업은 런타임 모니터링을 활성화하기 전에 시작된 서비스 배포의 일부인가요? 그렇다면 서비스를 다시 시작하거나 서비스 업데이트의 단계를 `forceNewDeployment` 사용하여 서비스를 업데이트할 수 있습니다. UpdateService또는 를 사용할 수도 AWS CLI있습니다. • 런타임 모니터링에서 ECS 클러스터를 제외한 후 작업이 시작되었습니까? 사전 정의된 GuardDuty 태그를 `GuardDutyManaged` -에서 `true` `GuardDutyManaged` `false` -로

문제 유형	추가 정보	권장 문제 해결 단계
		GuardDuty 변경하면 ECS 클러스터의 런타임 이벤트가 수신되지 않습니다. • 작업이 누락되었나요? `TaskExecutionRole` ECR 저장소에서 GuardDuty 컨테이너를 다운로드할 수 있는 권한이 `TaskExecutionRole` GuardDuty 필요하므로 반드시 추가해야 합니다. 자세한 정보는 ECR 권한 및 서브넷 세부 정보를 제공하십시오.을 참조하세요. • 서비스에 이전 형식의 `taskArn` 작업이 포함되어 있나요? GuardDuty 런타임 모니터링은 이전 형식이 다음과 같은 작업에 대한 적용 범위를 지원하지 않습니다`taskArn`. Amazon ECS 리소스의 Amazon 리소스 이름 (ARN) 에 대한 자세한 내용은 Amazon 리소스 이름 (ARN) 및 ID를 참조하십시오.

Amazon EKS 클러스터 적용 범위

런타임 모니터링을 활성화하고 EKS용 GuardDuty 보안 에이전트 (추가 기능) 를 수동으로 또는 자동 에이전트 구성을 통해 설치한 후 EKS 클러스터의 적용 범위 평가를 시작할 수 있습니다.

내용

- 적용 범위 통계 검토
- 적용 범위 상태 변경 알림 구성
- EKS 적용 범위 문제 해결

적용 범위 통계 검토

자체 계정 또는 멤버 계정과 연결된 EKS 클러스터의 적용 범위 통계는 선택한 AWS 리전의 모든 EKS 클러스터에 대한 정상 EKS 클러스터 비율입니다. 다음 등식은 이를 다음과 같이 나타냅니다.

(정상 클러스터/모든 클러스터)*100

액세스 방법 중 하나를 선택하여 계정의 적용 범위 통계를 검토합니다.

Console

- AWS Management Console 로그인하고 https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다. GuardDuty
- 탐색 창에서 런타임 모니터링을 선택합니다.
- EKS 클러스터 실행 시간 적용 범위 탭을 선택합니다.
- EKS 클러스터 실행 시간 적용 범위 탭에서 클러스터 목록 테이블에 제공된 적용 범위 상태별로 집계된 적용 범위 통계를 볼 수 있습니다.
  - 다음 열을 기준으로 클러스터 목록 테이블을 필터링할 수 있습니다.
    - 클러스터 이름
    - 계정 ID
    - 에이전트 관리 유형
    - 적용 범위 상태
    - 추가 기능 버전
- 적용 범위 상태가 비정상인 EKS 클러스터가 있는 경우 문제 열에 비정상 상태의 이유에 대한 추가 정보가 포함될 수 있습니다.

API/CLI

- 고유한 유효한 탐지기 ID, 지역 및 서비스 엔드포인트로 ListCoverageAPI를 실행합니다. 이 API를 사용하여 클러스터 목록을 필터링 및 정렬할 수 있습니다.
  - `CriterionKey`에 대한 다음 옵션 중 하나를 사용하여 예시 `filter-criteria`를 변경할 수 있습니다.
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`

    - COVERAGE_STATUS
    - ADDON_VERSION
    - MANAGEMENT_TYPE
  - 다음 옵션을 사용하여 sort-criteria에서 예시 AttributeName을 변경할 수 있습니다.
    - ACCOUNT_ID
    - CLUSTER_NAME
    - COVERAGE_STATUS
    - ISSUE
    - ADDON_VERSION
    - UPDATED_AT
  - *max-results*를 변경할 수 있습니다(최대 50개).
  - 계정과 현재 지역에 detectorId 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- GetCoverageStatistics API를 실행하여 를 기반으로 커버리지 집계 통계를 검색하십시오. statisticsType
  - 다음 옵션 중 하나를 사용하여 예시 statisticsType을 변경할 수 있습니다.
    - COUNT_BY_COVERAGE_STATUS - 적용 범위 상태별로 집계된 EKS 클러스터의 적용 범위 통계를 나타냅니다.
    - COUNT_BY_RESOURCE_TYPE— 목록에 있는 AWS 리소스 유형에 따라 집계된 커버리지 통계.
    - 명령에서 예시 filter-criteria를 변경할 수 있습니다. CriterionKey에 대해 다음 옵션을 사용할 수 있습니다.
      - ACCOUNT_ID
      - CLUSTER_NAME
      - RESOURCE_TYPE
      - COVERAGE_STATUS

    - ADDON_VERSION
    - MANAGEMENT_TYPE
- 계정과 현재 지역에 detectorId 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

EKS 클러스터의 적용 범위 상태가 비정상인 경우 EKS 적용 범위 문제 해결 섹션을 참조하세요.

적용 범위 상태 변경 알림 구성

계정에 있는 EKS 클러스터의 적용 범위 상태가 비정상으로 표시될 수 있습니다. 적용 범위 상태가 비정상이 된 시점을 탐지하려면 주기적으로 적용 범위 상태를 모니터링하고 상태가 비정상인 경우 문제를 해결하는 것이 좋습니다. 또는 Amazon EventBridge 규칙을 생성하여 적용 범위 상태가 둘 Unhealthy 중 하나로 Healthy 또는 다른 상태로 변경될 때 알림을 받을 수 있습니다. 기본적으로 계정의 EventBridge버스에 이 내용을 GuardDuty 게시합니다.

샘플 알림 스키마

EventBridge 규칙적으로 사전 정의된 샘플 이벤트와 이벤트 패턴을 사용하여 커버리지 상태 알림을 받을 수 있습니다. EventBridge 규칙 생성에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 규칙 생성을 참조하십시오.

또한 다음 예시 알림 스키마를 사용하여 사용자 지정 이벤트 패턴을 생성할 수 있습니다. 계정에 대한 값을 바꿔야 합니다. Amazon EKS 클러스터의 커버리지 상태가 에서 Healthy 로 Unhealthy 변경될 때 알림을 받으려면 *GuardDuty ### ## detail-type ######* 합니다. 적용 범위 상태가 에서 Unhealthy 로 변경될 때 알림을 받으려면 의 값을 *GuardDuty ### ## detail-type* 정상으로 바꾸십시오. Healthy

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
  "time": "event timestamp (string)",
```

```
  "region": "AWS ##",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

EKS 적용 범위 문제 해결

EKS 클러스터의 커버리지 상태가 Unhealthy 인 경우 GuardDuty 콘솔의 Issue 열에서 또는 CoverageResource데이터 유형을 사용하여 해당 오류를 확인할 수 있습니다.

EKS 클러스터를 선택적으로 모니터링하기 위해 포함 또는 제외 태그를 사용하는 경우 태그 동기화에 시간이 걸릴 수 있습니다. 이는 연결된 EKS 클러스터의 적용 범위 상태에 영향을 미칠 수 있습니다. 해당 태그(포함 또는 제외)를 제거하고 다시 추가할 수 있습니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS 리소스 태깅을 참조하세요.

적용 범위 문제의 구조는 `Issue type:Extra information`입니다. 일반적으로 문제에는 선택 사항으로 추가 정보가 있으며, 특정 클라이언트 측 예외 또는 문제에 대한 설명이 포함될 수 있습니다. 추가 정보를 기반으로 다음 표는 EKS 클러스터의 커버리지 문제를 해결하기 위한 권장 단계를 제공합니다.

문제 유형(접두사)	추가 정보	권장 문제 해결 단계
애드온 생성 실패	`aws-guardduty-agent` 애드온은 클러스터	`aws-guardduty-agent` EKS 추가 기능 배포를

문제 유형(접두사)	추가 정보	권장 문제 해결 단계
	의 현재 클러스터 버전과 호환되지 않습니다. *ClusterName* 지정된 추가 기능이 지원되지 않습니다.	지원하는 Kubernetes 버전 중 하나를 사용하고 있는지 확인해야 합니다. 자세한 정보는 보안 에이전트가 지원하는 쿠버네티스 버전 GuardDuty 을 참조하세요. Kubernetes 버전 업데이트에 대한 자세한 내용은 Amazon EKS 클러스터 Kubernetes 버전 업데이트를 참조하세요.
애드온 생성 실패 애드온 업데이트 실패 애드온 상태 비정상	EKS 추가 기능 문제 - `AddonIssueCode` : `AddonIssueMessage`	특정 애드온 문제 코드의 권장 단계에 대한 자세한 내용은 을 참조하십시오. Troubleshooting steps for Addon creation/updatation error with Addon issue code 이 문제에서 발생할 수 있는 애드온 문제 코드 목록은 을 참조하십시오. AddonIssue
VPC 엔드포인트 생성 실패	*### VPC vPCID## VPC ##### ### #### ##*	런타임 모니터링은 이제 조직 내 공유 VPC 사용을 지원합니다. 계정이 모든 사전 요구 사항을 충족하는지 확인하세요. 자세한 정보는 공유 VPC 사용을 위한 사전 요구 사항을 참조하세요.

문제 유형(접두사)	추가 정보	권장 문제 해결 단계
	자동 에이전트 구성과 함께 공유 VPC를 사용하는 경우에만 공유 VPC *vPCID# ### ## ID 111122223333 ## ### ####, ## ### # ##* 또는 둘 다 활성화되어 있지 않습니다.	공유 VPC 소유자 계정은 하나 이상의 리소스 유형 (Amazon EKS 또는 Amazon ECS ()) 에 대해 런타임 모니터링 및 자동 에이전트 구성을 활성화해야 합니다.AWS Fargate자세한 정보는 런타임 모니터링과 관련된 사전 요구 사항 GuardDuty을 참조하세요.
	프라이빗 DNS를 활성화하려면 *vpcId*(서비스: Ec2, 상태 코드:400, 요청 ID: *a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*)에 대해 `enableDnsSupport` 및 `enableDnsHostnames` VPC 속성 모두 `true`로 설정되어야 합니다.	다음 `enableDnsSupport` 및 `enableDnsHostnames` VPC 속성이 `true`로 설정되어야 합니다. 자세한 내용을 알아보려면 VPC의 DNS 속성을 참조하세요. Amazon VPC 콘솔 (https://console.aws.amazon.com/vpc/)을 사용하여 Amazon VPC를 생성하는 경우 DNS 호스트 이름 활성화와 DNS 확인 활성화를 모두 선택해야 합니다. 자세한 내용은 VPC 구성 옵션을 참조하세요.

문제 유형(접두사)	추가 정보	권장 문제 해결 단계
공유 VPC 엔드포인트 삭제 실패	*## ID 111122223333, ## VPC VPCID, ### ## ID 5555555555# #### ## VPC ###### ### #### ####.*	잠재적 단계는 다음과 같습니다. • 공유 VPC 참가자 계정의 런타임 모니터링 상태를 비활성화해도 공유 VPC 엔드포인트 정책 및 소유자 계정에 있는 보안 그룹에는 영향을 미치지 않습니다. 공유 VPC 엔드포인트 및 보안 그룹을 삭제하려면 공유 VPC 소유자 계정에서 런타임 모니터링 또는 자동 에이전트 구성 상태를 비활성화해야 합니다. • 공유 VPC 참가자 계정은 공유 VPC 소유자 계정에 호스팅된 공유 VPC 엔드포인트 및 보안 그룹을 삭제할 수 없습니다.
로컬 EKS 클러스터	EKS 추가 기능은 로컬 Outpost 클러스터에서 지원되지 않습니다.	실행 불가. 자세한 내용은 AWS Outposts에 대한 Amazon EKS를 참조하세요.

문제 유형(접두사)	추가 정보	권장 문제 해결 단계
EKS 런타임 모니터링 활성화 권한이 부여되지 않음	(추가 정보를 표시할 수도 있고 표시하지 않을 수도 있음)	1. 이 문제에 대한 추가 정보가 제공된 경우 근본 원인을 수정하고 다음 단계를 따릅니다. 2. EKS 런타임 모니터링을 끄고 다시 켭니다. GuardDuty 에이전트가 자동으로 배포되든 GuardDuty 수동으로든 관계없이 배포되도록 하세요.
EKS 런타임 모니터링 활성화 리소스 프로비저닝 진행 중	(추가 정보를 표시할 수도 있고 표시하지 않을 수도 있음)	실행 불가. EKS 런타임 모니터링을 활성화한 후에는 리소스 프로비저닝 단계가 완료될 때까지 적용 범위 상태가 `Unhealthy` 로 지속될 수 있습니다. 적용 범위 상태는 정기적으로 모니터링 및 업데이트됩니다.
기타 (기타 문제)	인증 실패로 인한 오류	EKS 런타임 모니터링을 끄고 다시 켭니다. GuardDuty 에이전트가 자동으로 GuardDuty 또는 수동으로 배포되는지 확인하십시오.

애드온 생성 또는 업데이트 오류	문제 해결 단계
EKS 애드온 문제 -InsufficientNumberOfReplicas : 원하는 수의 복제본이 없어서 애드온이 비정상입니다.	문제 메시지를 사용하여 근본 원인을 식별하고 수정할 수 있습니다. 클러스터를 설명하는 것으로 시작할 수 있습니다. 예를 들어 포드 장애의 근본 원인을 식별하는 kubectl describe pods데 사용합니다. 근본 원인을 수정한 후 해당 단계 (애드온 생성 또는 업데이트) 를 다시 시도하세요.
EKS 애드온 문제 -AdmissionRequestDenied : 승인 웹훅이 요청을 "validate.kyverno.svc-fail" 거부함: 리소스 DaemonSet/amazon-guardduty/aws-guardduty-agent 위반에 대한 정책:::... restrict-image-registries autogen-validate-registries	1. Amazon EKS 클러스터 또는 보안 관리자는 애드온 업데이트를 차단하는 보안 정책을 검토해야 합니다. 2. 컨트롤러 (webhook) 를 비활성화하거나 컨트롤러가 Amazon EKS의 요청을 수락하도록 해야 합니다.
EKS 애드온 문제 -ConfigurationConflict : 적용하려고 할 때 충돌이 발견되었습니다. 충돌 해결 모드로 인해 계속되지 않습니다. Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image	애드온을 만들거나 업데이트할 때 충돌 OVERWRITE 해결 플래그를 제공하십시오. 이렇게 하면 쿠버네티스 API를 사용하여 쿠버네티스의 관련 리소스에 직접 적용한 모든 변경 사항을 덮어쓸 수 있습니다. 먼저 애드온을 삭제한 다음 다시 설치할 수 있습니다.

EKS 애드온 문제 - AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope	누락된 권한을 수동으로 추가해야 합니다. eks:addon-cluster-admin ClusterRoleBinding 에 eks:addon-cluster-admin 다음을 yaml 추가하세요.
	
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`

애드온 생성 또는 업데이트 오류	문제 해결 단계

	metadata:
	  name: eks:addon-cluster-admin
	subjects:
	- kind: User
	  name: eks:addon-manager
	  apiGroup: rbac.authorization.k8s.io
	roleRef:
	  kind: ClusterRole
	  name: cluster-admin
	  apiGroup: rbac.authorization.k8s.io
	--- 	
	
	이제 다음 명령을 yaml 사용하여 Amazon EKS 클러스터에 이를 적용할 수 있습니다.
	
	kubectl apply -f eks-addon-cluster-admin.yaml

EKS 애드온 문제 - AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label	컨트롤러를 비활성화하거나 컨트롤러가 Amazon EKS 클러스터의 요청을 수락하도록 해야 합니다. 애드온을 생성하거나 업데이트하기 전에 GuardDuty 네임스페이스를 생성하고 레이블을 붙일 수도 있습니다. owner

FAQ

내용

- Runtime Monitoring을 활성화하고, GuardDuty 보안 에이전트를 배포하고, 사전 요구 사항을 모두 Unhealthy 충족했는데도 내 리소스의 커버리지 상태가 표시되는 이유는 무엇입니까?
- 내 리소스의 런타임 커버리지 상태는 누가 볼 수 AWS 계정있습니까?

Runtime Monitoring을 활성화하고, GuardDuty 보안 에이전트를 배포하고, 사전 요구 사항을 모두 **Unhealthy** 충족했는데도 내 리소스의 커버리지 상태가 표시되는 이유는 무엇입니까?

자동 에이전트 구성을 통해 또는 수동으로 GuardDuty 보안 에이전트를 배포했거나 권장 단계에 따라 적용 범위 문제를 해결한 경우 적용 범위 상태가 정상화되는 데 몇 분 정도 걸릴 수 있습니다. 커버리지 상태를 주기적으로 확인하거나 커버리지 상태가 변경될 때 알림을 받도록 Amazon EventBridge (EventBridge) 을 구성할 수 있습니다.

내 리소스의 런타임 커버리지 상태는 누가 볼 수 AWS 계정있습니까?

멤버 계정 또는 독립형 계정으로 자신의 계정과 연결된 리소스의 적용 범위 통계를 볼 수 있습니다. 조직의 위임된 GuardDuty 관리자 계정으로서 사용자 계정과 연결된 리소스 및 조직에 속한 구성원 계정의 적용 범위 통계를 볼 수 있습니다.

CPU 및 메모리 모니터링 설정

런타임 모니터링을 활성화하고 클러스터의 커버리지 상태가 정상인지 평가한 후에는 인사이트 지표를 설정하고 볼 수 있습니다.

다음 항목은 에이전트의 CPU 및 메모리 한도를 기준으로 배포된 에이전트의 성능을 평가하는 데 도움이 될 수 있습니다. GuardDuty

Amazon ECS 클러스터에서 모니터링 설정

Amazon CloudWatch User Guide의 다음 단계는 에이전트의 CPU 및 메모리 한도를 기준으로 배포된 에이전트의 성능을 평가하는 데 도움이 될 수 있습니다. GuardDuty

1. Amazon ECS에서 클러스터 및 서비스 수준 메트릭을 위한 컨테이너 인사이트 설정
2. Amazon ECS 컨테이너 인사이트 지표

Amazon EKS 클러스터에서 모니터링 설정

GuardDuty 보안 에이전트가 배포되고 클러스터의 커버리지 상태가 정상으로 평가되면 컨테이너 인사이트 메트릭을 설정하고 볼 수 있습니다.

보안 에이전트의 성능을 평가하세요.

1. Amazon 사용 설명서에서 Amazon EKS 및 쿠버네티스에 컨테이너 인사이트 설정하기 CloudWatch

2. Amazon 사용 설명서의 Amazon EKS 및 쿠버네티스 컨테이너 인사이트 지표 CloudWatch 보안 에이전트 v1.5.0 이상을 사용하여 성능을 관리합니다.

보안 에이전트 v1.5.0 이상에서는 관련 GuardDuty 에이전트가 할당된 한도에 도달한 것으로 확인되면 특정 매개 변수를 구성할 수 있습니다. 자세한 정보는 EKS 애드온 파라미터 구성을 참조하세요.

를 사용하는 수집된 런타임 이벤트 유형 GuardDuty

GuardDuty 보안 에이전트는 위협 탐지 및 분석을 위해 다음 이벤트 유형을 수집하여 GuardDuty 백엔드로 전송합니다. GuardDuty 이러한 이벤트에 액세스할 수 있게 만들지는 않습니다. 잠재적 위협을 GuardDuty 탐지하고 Runtime Monitoring 검색 결과를 생성하는 경우 해당 검색 결과 세부 정보를 볼 수 있습니다. 수집된 이벤트 유형을 GuardDuty 사용하는 방법에 대한 자세한 내용은 을 참조하십시오서비스 개선을 위한 데이터 사용 거부.

프로세스 이벤트

필드 이름	설명
프로세스 이름	관찰된 프로세스의 이름.
프로세스 경로	프로세스 실행 파일의 절대 경로.
프로세스 ID	운영 체제에서 프로세스에 할당한 ID.
네임스페이스 PID	호스트 수준 PID 네임스페이스가 아닌 보조 PID 네임스페이스에 있는 프로세스의 프로세스 ID. 컨테이너 내부 프로세스의 경우 컨테이너 내부에서 관찰된 프로세스 ID.
프로세스 사용자 ID	프로세스를 실행한 사용자의 고유 ID입니다.
프로세스 UUID	가 프로세스에 할당한 고유 ID GuardDuty.
프로세스 GID	프로세스 그룹의 프로세스 ID입니다.
프로세스 EGID	프로세스 그룹의 유효 그룹 ID입니다.
프로세스 EUID	프로세스의 유효 사용자 ID입니다.

필드 이름	설명
프로세스 사용자 이름	프로세스를 실행한 사용자 이름.
프로세스 시작 시간	프로세스가 생성된 시간입니다. 이 필드는 UTC 날짜 문자열 형식(`2023-03-22T19:37:20.168Z`)입니다.
프로세스 실행 파일 SHA-256	프로세스 실행 파일의 SHA256 해시.
프로세스 스크립트 경로	실행된 스크립트 파일의 경로.
프로세스 환경 변수	프로세스에 제공된 환경 변수입니다. `LD_PRELOAD` 및 `LD_LIBRARY_PATH` 만 수집됩니다.
프로세스 현재 작업 디렉터리(PWD)	프로세스의 현재 작업 디렉터리입니다.
상위 프로세스	상위 프로세스의 프로세스 세부 정보. 상위 프로세스는 관찰된 프로세스를 만든 프로세스입니다.
커맨드 라인 인수 현재 이 필드는 리소스 유형에 해당하는 특정 에이전트 버전으로 제한됩니다. • GuardDuty 보안 에이전트 v1.0.0 이상을 사용하는 Fargate (Amazon ECS만 해당) • GuardDuty 보안 에이전트 v1.0.0 이상을 사용하는 Amazon EC2 인스턴스 • 보안 에이전트 v1.4.0 이상을 사용하는 Amazon EKS 클러스터 자세한 정보는 GuardDuty 에이전트 릴리스 기록을 참조하세요.	프로세스 실행 시 제공되는 명령줄 인수. 이 필드에는 민감한 고객 데이터가 포함될 수 있습니다.

컨테이너 이벤트

필드 이름	설명
컨테이너 이름	컨테이너의 이름입니다. 사용 가능한 경우 이 필드에는 레이블 `io.kubenetes.container.name` 값이 표시됩니다.
컨테이너 UID	컨테이너 런타임에서 할당한 컨테이너의 고유 ID.
컨테이너 런타임	컨테이너 실행에 사용되는 컨테이너 런타임(예: `docker` 또는 `containerd`).
컨테이너 이미지 ID	컨테이너 이미지의 ID입니다.
컨테이너 이미지 이름	컨테이너 이미지의 이름입니다.

AWS Fargate (Amazon ECS만 해당) 태스크 이벤트

필드 이름	설명
태스크 아마존 리소스 이름 (ARN)	태스크의 ARN입니다.
클러스터 이름	Amazon ECS 클러스터의 이름.
패밀리 이름	태스크 정의의 패밀리 이름. `family`는 작업을 시작하는 데 사용되는 작업 정의의 이름으로 사용됩니다.
서비스 이름	Amazon ECS 서비스의 이름 (작업이 서비스의 일부로 시작된 경우)
시작 유형	작업이 실행되는 인프라. 리소스 유형이 인 런타임 모니터링의 `ECSCluster` 경우 시작 유형은 `EC2` 또는 일 수 `FARGATE` 있습니다.

필드 이름	설명
CPU	태스크 정의에 명시된 바와 같이 태스크에서 사용하는 CPU 유닛 수입니다.

Kubernetes 포드 이벤트

필드 이름	설명
포드 ID	Kubernetes 포드의 ID입니다.
포드 이름	Kubernetes 포드의 이름입니다.
포드 네임스페이스	Kubernetes 워크로드가 속하는 Kubernetes 네임스페이스의 이름입니다.
Kubernetes 클러스터 이름	Kubernetes 클러스터의 이름입니다.

DNS 이벤트

필드 이름	설명
소켓 유형	통신 의미 체계를 나타내는 소켓의 유형입니다. 예를 들어 `SOCK_RAW`입니다.
주소 패밀리	주소와 관련된 통신 프로토콜을 나타냅니다. 예를 들어 주소 패밀리 `AF_INET`은 IPv4 프로토콜에 사용됩니다.
방향 ID	연결 방향의 ID입니다.
프로토콜 번호	레이어 4 프로토콜 번호(예: UDP의 경우 17, TCP의 경우 6).
DNS 원격 엔드포인트 IP	연결의 원격 IP입니다.
DNS 원격 엔드포인트 포트	연결의 포트 번호입니다.
DNS 로컬 엔드포인트 IP	연결의 로컬 IP입니다.

필드 이름	설명
DNS 로컬 엔드포인트 포트	연결의 포트 번호입니다.
DNS 페이로드	DNS 쿼리 및 응답이 포함된 DNS 패킷의 페이로드입니다.

열린 이벤트

필드 이름	설명
파일 경로	이 이벤트에서 열린 파일의 경로입니다.
플래그	읽기 전용, 쓰기 전용, 읽기-쓰기와 같은 파일 액세스 모드를 설명합니다.

모듈 이벤트 로드

필드 이름	설명
모듈 이름	커널에 로드된 모듈의 이름입니다.

Mprotect 이벤트

필드 이름	설명
주소 범위	액세스 보호가 수정된 주소 범위.
메모리 영역	스택 및 힙과 같은 프로세스 주소 공간의 영역을 지정합니다.
플래그	이 이벤트의 동작을 제어하는 옵션을 나타냅니다.

탑재 이벤트

필드 이름	설명
탑재 대상	탑재 소스가 탑재된 경로.
탑재 소스	탑재 대상에 탑재된 호스트의 경로.
파일 시스템 유형	탑재된 파일 시스템의 유형을 나타냅니다.
플래그	이 이벤트의 동작을 제어하는 옵션을 나타냅니다.

링크 이벤트

필드 이름	설명
링크 경로	하드 링크가 생성되는 경로입니다.
대상 경로	하드 링크가 가리키는 파일의 경로입니다.

심볼 링크 이벤트

필드 이름	설명
링크 경로	심볼 링크가 생성되는 경로입니다.
대상 경로	심볼 링크가 가리키는 파일의 경로입니다.

중복 이벤트

필드 이름	설명
이전 파일 설명자	열린 파일 객체를 나타내는 파일 설명자입니다.

필드 이름	설명
새 파일 설명자	이전 파일 설명자와 중복되는 새 파일 설명자입니다. 이전 파일 설명자와 새 파일 설명자는 모두 동일한 열린 파일 객체를 나타냅니다.
중복 원격 엔드포인트 IP	이전 파일 설명자로 표시되는 네트워크 소켓의 원격 IP 주소입니다. 이전 파일 설명자가 네트워크 소켓을 나타내는 경우에만 해당됩니다.
중복 원격 엔드포인트 포트	이전 파일 설명자로 표시되는 네트워크 소켓의 원격 포트입니다. 이전 파일 설명자가 네트워크 소켓을 나타내는 경우에만 해당됩니다.
중복 로컬 엔드포인트 IP	이전 파일 설명자로 표시되는 네트워크 소켓의 로컬 IP 주소입니다. 이전 파일 설명자가 네트워크 소켓을 나타내는 경우에만 해당됩니다.
중복 로컬 엔드포인트 포트	이전 파일 설명자로 표시되는 네트워크 소켓의 로컬 포트입니다. 이전 파일 설명자가 네트워크 소켓을 나타내는 경우에만 해당됩니다.

메모리 맵 이벤트

필드 이름	설명
파일 경로	메모리가 매핑되는 파일의 경로입니다.

소켓 이벤트

필드 이름	설명
Address family(주소 패밀리)	주소와 관련된 통신 프로토콜을 나타냅니다. 예를 들어 주소 패밀리 `AF_INET`은 IP 버전 4 프로토콜에 사용됩니다.

필드 이름	설명
소켓 유형	통신 의미 체계를 나타내는 소켓의 유형입니다. 예를 들어 SOCK_RAW입니다.
프로토콜 번호	주소 패밀리 내의 특정 프로토콜을 지정합니다. 대체로 주소 패밀리에는 단일 프로토콜이 있습니다. 예를 들어 주소 패밀리 AF_INET에는 IP 프로토콜만 있습니다.

연결 이벤트

필드 이름	설명
Address family(주소 패밀리)	주소와 관련된 통신 프로토콜을 나타냅니다. 예를 들어 주소 패밀리 AF_INET은 IPv4 프로토콜에 사용됩니다.
소켓 유형	통신 의미 체계를 나타내는 소켓의 유형입니다. 예를 들어 SOCK_RAW입니다.
프로토콜 번호	주소 패밀리 내의 특정 프로토콜을 지정합니다. 대체로 주소 패밀리에는 단일 프로토콜이 있습니다. 예를 들어 주소 패밀리 AF_INET에는 IP 프로토콜만 있습니다.
파일 경로	소켓 파일의 경로입니다(주소 패밀리가 AF_UNIX인 경우).
원격 엔드포인트 IP	연결의 원격 IP입니다.
원격 엔드포인트 포트	연결의 포트 번호입니다.
로컬 엔드포인트 IP	연결의 로컬 IP입니다.
로컬 엔드포인트 포트	연결의 포트 번호입니다.

프로세스 VM Readv 이벤트

필드 이름	설명
플래그	이 이벤트의 동작을 제어하는 옵션을 나타냅니다.
대상 PID	메모리를 읽는 프로세스의 프로세스 ID입니다.
대상 프로세스 UUID	대상 프로세스의 고유 ID입니다.
대상 실행 파일 경로	대상 프로세스 실행 파일의 절대 경로입니다.

프로세스 VM Writev 이벤트

필드 이름	설명
플래그	이 이벤트의 동작을 제어하는 옵션을 나타냅니다.
대상 PID	메모리를 쓰는 프로세스의 프로세스 ID입니다.
대상 프로세스 UUID	대상 프로세스의 고유 ID입니다.
대상 실행 파일 경로	대상 프로세스 실행 파일의 절대 경로입니다.

Ptrace 이벤트

필드 이름	설명
대상 PID	대상 프로세스의 프로세스 ID입니다.
대상 프로세스 UUID	대상 프로세스의 고유 ID입니다.
대상 실행 파일 경로	대상 프로세스 실행 파일의 절대 경로입니다.
플래그	이 이벤트의 동작을 제어하는 옵션을 나타냅니다.

바인드 이벤트

필드 이름	설명
주소 패밀리	주소와 관련된 통신 프로토콜을 나타냅니다. 예를 들어 주소 패밀리 AF_INET은 IPv4 프로토콜에 사용됩니다.
소켓 유형	통신 의미 체계를 나타내는 소켓의 유형입니다. 예를 들어 SOCK_RAW입니다.
프로토콜 번호	레이어 4 프로토콜 번호(예: UDP의 경우 17, TCP의 경우 6).
로컬 엔드포인트 IP	연결의 로컬 IP입니다.
로컬 엔드포인트 포트	연결의 포트 번호입니다.

리슨 이벤트

필드 이름	설명
주소 패밀리	주소와 관련된 통신 프로토콜을 나타냅니다. 예를 들어 주소 패밀리 AF_INET은 IPv4 프로토콜에 사용됩니다.
소켓 유형	통신 의미 체계를 나타내는 소켓의 유형입니다. 예를 들어 SOCK_RAW입니다.
프로토콜 번호	레이어 4 프로토콜 번호(예: UDP의 경우 17, TCP의 경우 6).
로컬 엔드포인트 IP	연결의 로컬 IP입니다.
로컬 엔드포인트 포트	연결의 포트 번호입니다.

이벤트 이름 변경

필드 이름	설명
파일 경로	파일 이름이 바뀐 경로

필드 이름	설명
대상	파일의 새 경로.

UID 이벤트 설정

필드 이름	설명
새 EUID	프로세스의 새로운 유효 사용자 ID.
새 UID	프로세스의 새 사용자 ID.

Chmod 이벤트

필드 이름	설명
파일 경로	이 이벤트를 호출하는 파일의 경로입니다.
파일 모드	관련 파일에 대한 업데이트된 액세스 권한.

Amazon ECR 리포지토리 호스팅 에이전트 GuardDuty

다음 섹션에는 Amazon EKS 및 Amazon ECS 클러스터에 GuardDuty 배포되는 보안 에이전트를 호스팅하는 Amazon Elastic Container 레지스트리 (Amazon ECR) 리포지토리가 나열되어 있습니다.

내용

- EKS 에이전트 버전 1.6.0 이상용 리포지토리
- EKS 에이전트 버전 1.5.0 이하용 리포지토리
- GuardDuty 에이전트용 리포지토리 AWS Fargate (Amazon ECS만 해당)

EKS 에이전트 버전 1.6.0 이상용 리포지토리

다음 표에는 Amazon EKS 애드온 에이전트 버전 (`aws-guardduty-agent`) 1.6.0 이상을 호스팅하는 Amazon ECR 리포지토리가 각각에 대해 나와 있습니다. AWS 리전

AWS 리전	Amazon ECR 리포지토리 URI
미국 서부(오레곤)	602401143452.dkr.ecr.us-west-2.amazonaws.com
유럽(파리)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
아시아 태평양(뭄바이)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
아시아 태평양(하이데라바드)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
캐나다(중부)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
캐나다 서부(캘거리)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
중동(UAE)	759879836304.dkr.ecr.me-central-1.amazonaws.com
유럽(런던)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
유럽(아일랜드)	602401143452.dkr.ecr.us-west-1.amazonaws.com
미국 동부(버지니아 북부)	602401143452.dkr.ecr.us-east-1.amazonaws.com
미국 동부(오하이오)	602401143452.dkr.ecr.us-east-2.amazonaws.com
유럽(아일랜드)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
남아메리카(상파울루)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
유럽(스톡홀름)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
유럽(프랑크푸르트)	602401143452.dkr.ecr.eu-central-1.amazonaws.com

AWS 리전	Amazon ECR 리포지토리 URI
유럽(취리히)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
아시아 태평양(싱가포르)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
아시아 태평양(시드니)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
아시아 태평양(자카르타)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
아시아 태평양(도쿄)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
아시아 태평양(서울)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
아시아 태평양(오사카)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
아시아 태평양(홍콩)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
중동(바레인)	759879836304.dkr.ecr.me-south-1.amazonaws.com
유럽(밀라노)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
유럽(스페인)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
아프리카(케이프타운)	877085696533.dkr.ecr.af-south-1.amazonaws.com
아시아 태평양(멜버른)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
이스라엘(텔아비브)	066635153087.dkr.ecr.il-central-1.amazonaws.com

EKS 에이전트 버전 1.5.0 이하용 리포지토리

다음 표에는 Amazon EKS 애드온 에이전트 버전 (aws-guardduty-agent) 1.5.0 및 이전 버전을 호스팅하는 Amazon ECR 리포지토리가 각각에 대해 나와 있습니다. AWS 리전

AWS 리전	Amazon ECR 리포지토리 URI
미국 서부(오레곤)	039403964562.dkr.ecr.us-west-2.amazonaws.com
유럽(파리)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
아시아 태평양(뭄바이)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
아시아 태평양(하이데라바드)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
캐나다(중부)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
중동(UAE)	601769779514.dkr.ecr.me-central-1.amazonaws.com
유럽(런던)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
유럽(아일랜드)	373421517865.dkr.ecr.us-west-1.amazonaws.com
미국 동부(버지니아 북부)	031903291036.dkr.ecr.us-east-1.amazonaws.com
미국 동부(오하이오)	591382732059.dkr.ecr.us-east-2.amazonaws.com
유럽(아일랜드)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
남아메리카(상파울루)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
유럽(스톡홀름)	366771026645.dkr.ecr.eu-north-1.amazonaws.com

AWS 리전	Amazon ECR 리포지토리 URI
유럽(프랑크푸르트)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
유럽(취리히)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
아시아 태평양(싱가포르)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
아시아 태평양(시드니)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
아시아 태평양(자카르타)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
아시아 태평양(도쿄)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
아시아 태평양(서울)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
아시아 태평양(오사카)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
아시아 태평양(홍콩)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
중동(바레인)	541829937850.dkr.ecr.me-south-1.amazonaws.com
유럽(밀라노)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
유럽(스페인)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
아프리카(케이프타운)	379032919888.dkr.ecr.af-south-1.amazonaws.com
아시아 태평양(멜버른)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com

AWS 리전	Amazon ECR 리포지토리 URI
이스라엘(텔아비브)	292660727137.dkr.ecr.il-central-1.amazonaws.com

GuardDuty 에이전트용 리포지토리 AWS Fargate (Amazon ECS만 해당)

다음 표에는 각 리포지토리의 GuardDuty 에이전트를 호스팅하는 Amazon ECR 리포지토리 (AWS Fargate Amazon ECS만 해당) 가 나와 있습니다. AWS 리전

AWS 리전	Amazon ECR 리포지토리 URI
미국 서부(오레곤)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate
유럽(파리)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(뭄바이)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(하이데라바드)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate
캐나다(중부)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate
중동(UAE)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate
유럽(런던)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate
유럽(아일랜드)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
미국 동부(버지니아 북부)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate

AWS 리전	Amazon ECR 리포지토리 URI
미국 동부(오하이오)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
유럽(아일랜드)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
남아메리카(상파울루)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate
유럽(스톡홀름)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
유럽(프랑크푸르트)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
유럽(취리히)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(싱가포르)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(시드니)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(자카르타)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(도쿄)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(서울)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(오사카)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(홍콩)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate

AWS 리전	Amazon ECR 리포지토리 URI
중동(바레인)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
유럽(밀라노)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
유럽(스페인)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
아프리카(케이프타운)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
아시아 태평양(멜버른)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate
이스라엘(텔아비브)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate

GuardDuty 에이전트 릴리스 기록

다음 섹션에서는 Amazon EC2 인스턴스, Amazon ECS 클러스터 및 Amazon EKS 클러스터에 배포되는 GuardDuty 에이전트의 릴리스 버전을 제공합니다.

GuardDuty Amazon EC2 인스턴스용 보안 에이전트

에이전트 버전	릴리스 정보	사용 가능 날짜
v1.1.0	Amazon EC2 인스턴스의 런타임 모니터링에서 GuardDuty 자동 에이전트 구성을 지원합니다. EC2 인스턴스용 런타임 모니터링의 일반 출시 발표와 함께 발표된 새로운 보안 신호 및 조사 결과를 지원합니다.	2024년 3월 26일

에이전트 버전	릴리스 정보	사용 가능 날짜
	전반적인 성능 개선.	
v1.0.2	최신 Amazon ECS AMI를 지원합니다.	2024년 2월 2일
v1.0.1	일반 성능 조정 및 개선 v1.0.2 이전에 릴리스된 에이전트 버전은 2024년 1월 31일 이후에 출시된 Amazon ECS AMI와 호환되지 않습니다.	2024년 1월 23일
v1.0.0	RPM 설치의 초기 릴리스. v1.0.2 이전에 릴리스된 에이전트 버전은 2024년 1월 31일 이후에 출시된 Amazon ECS AMI와 호환되지 않습니다.	2023년 11월 26일

공개 키, x86_64 RPM의 서명, arm64 RPM의 서명 및 Amazon S3 버킷에서 호스팅되는 RPM 스크립트에 대한 해당 액세스 링크는 다음 템플릿에서 구성할 수 있습니다. RPM 스크립트에 AWS 액세스하려면 AWS 리전, 계정 ID 및 에이전트 버전의 값을 바꾸십시오. GuardDuty 다음 템플릿에는 Amazon EC2 인스턴스용 최신 에이전트 버전이 포함되어 있습니다.

- 퍼블릭 키:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
```

- GuardDuty 보안 에이전트 RPM 서명:

  x86_64 RPM의 시그니처

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig
```

arm64 RPM의 시그니처

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.sig
```

- Amazon S3 버킷의 RPM 스크립트로 연결되는 링크에 액세스하십시오.

  x86_64 RPM용 액세스 링크

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm
  ```

  arm64 RPM을 위한 액세스 링크

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.rpm
  ```

AWS 리전	지역명	AWS 계정 ID
eu-west-1	유럽(아일랜드)	694911143906
us-east-1	미국 동부(버지니아 북부)	593207742271
us-east-2	미국 동부(오하이오)	733349766148
eu-west-3	유럽(파리)	665651866788
us-east-2	미국 동부(오하이오)	307168627858
eu-central-1	유럽(프랑크푸르트)	323658145986
ap-northeast-2	아시아 태평양(서울)	914738172881
eu-north-1	유럽(스톡홀름)	591436053604
ap-east-1	아시아 태평양(홍콩)	258348409381
me-south-1	중동(바레인)	536382113932
eu-west-2	유럽(런던)	892757235363

ap-northeast-1	아시아 태평양(도쿄)	533107202818
ap-southeast-1	아시아 태평양(싱가포르)	174946120834
ap-south-1	아시아 태평양(뭄바이)	251508486986
ap-southeast-3	아시아 태평양(자카르타)	510637619217
sa-east-1	남아메리카(상파울루)	758426053663
ap-northeast-3	아시아 태평양(오사카)	273192626886
eu-south-1	유럽(밀라노)	266869475730
af-south-1	아프리카(케이프타운)	197869348890
ap-southeast-2	아시아 태평양(시드니)	005257825471
me-central-1	중동(UAE)	000014521398
us-west-1	미국 서부(캘리포니아 북부)	684579721401
ca-central-1	캐나다(중부)	354763396469
ap-south-2	아시아 태평양(하이데라바드)	950823858135
eu-south-2	유럽(스페인)	919611009337
eu-central-2	유럽(취리히)	529164026651
ap-southeast-4	아시아 태평양(멜버른)	251357961535
il-central-1	이스라엘(텔아비브)	870907303882

GuardDuty 보안 에이전트 대상 AWS Fargate (Amazon ECS만 해당)

다음 표에는 Fargate용 GuardDuty 보안 에이전트의 릴리스 버전 기록이 나와 있습니다 (Amazon ECS만 해당).

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜
v1.2.0	x86_64(AMD64): sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93 Graviton(ARM64): sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd	일반 성능 조정 및 개선 사항	2024년 5월 31일
v1.1.0	x86_64(AMD64): sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657 Graviton(ARM64): sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7	새로운 보안 신호 및 조사 결과 지원 일반 성능 조정 및 개선	2024년 5월 1일
v1.0.1	x86_64(AMD64): sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68 Graviton(ARM64): sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	일반 성능 조정 및 개선	2024년 1월 26일

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜
v1.0.0	x86_64(AMD64): sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017 Graviton(ARM64): sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984	에 대한 GuardDuty 보안 에이전트의 초기 릴리스 AWS Fargate (Amazon ECS만 해당)	2023년 11월 26일

GuardDuty Amazon EKS 클러스터용 보안 에이전트

다음 표는 Amazon EKS 애드온 GuardDuty 에이전트의 릴리스 버전 기록을 보여줍니다.

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜	표준 지원 종료 1
v1.6.1	x86_64(AMD64): sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1 Graviton(ARM64): sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019	일반 성능 조정 및 개선	2024년 5월 14일	–
v1.6.0	x86_64(AMD64): sha256:7dabcbee30d8b053676752fbc19e89f77272d9	• EKS/EC2 리소스에 대한 GuardDuty	2024년 4월 29일	–

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜	표준 지원 종료 1
	a6a53cc93731f5872180ef9010 Graviton(ARM64): sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650	자동 에이전트 구성을 지원합니다. • 새로운 보안 신호 및 결과를 지원합니다. 자세한 내용은 를 사용하는 수집된 런타임 이벤트 유형 GuardDuty 및 런타임 모니터링 검색 유형 섹션을 참조하세요. • 일반 성능 조정 및 개선.		

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜	표준 지원 종료 1
v1.5.0	x86_64(AMD64): sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d Graviton(ARM64): sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6	• 일반 성능 조정 및 개선 • 새 이벤트 유형을 포함한 보안 개선 사항이 아래에 있습니다. 수집된 런타임 이벤트 유형 • CPU 사용과 관련된 성능 향상.	2024년 3월 7일	–
v1.4.1	x86_64(AMD64): sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c Graviton(ARM64): sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40	일반 성능 조정 및 개선	2024년 1월 16일	–

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜	표준 지원 종료 1
v1.4.0	x86_64(AMD64): sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f Graviton(ARM64): sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e	매니페스트 마운트 포인트는 더 나은 데이터 수집을 지원합니다. AppArmor 매니페스트에서의 구성 명령줄 인수 수집 일반 성능 튜닝 및 개선 사항	2023년 12월 21일	–
v1.3.1	x86_64(AMD64): sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29 Graviton(ARM64): sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd	중요 보안 패치 및 업데이트.	2023년 10월 23일	–

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜	표준 지원 종료 1
v1.3.0	x86_64(AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton(ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Ubuntu 플랫폼 지원 Kubernetes 버전 1.28 지원 일반 성능 향상 및 안정성 개선.	2023년 10월 5일	–
v1.2.0	x86_64(AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton(ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	AMD64 기반 인스턴스 외에도 v1.2.0에서 이제 ARM64 기반 인스턴스도 지원합니다. Bottlerocket에 대해 추가 및 확인된 지원 Kubernetes 버전 1.27 지원 일반 성능 향상 및 안정성 개선.	2023년 6월 16일	–

에이전트 버전	컨테이너 이미지	릴리스 정보	사용 가능 날짜	표준 지원 종료 1
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	보안 에이전트가 지원하는 쿠버네티스 버전 GuardDuty 외에 이 에이전트 릴리스는 Kubernetes 버전 1.26도 지원합니다. 일반 성능 향상 및 안정성 개선.	2023년 5월 2일	2024년 5월 14일
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Amazon EKS 추가 기능 에이전트의 초기 릴리스.	2023년 3월 30일	2024년 5월 14일

- [1] 표준 지원 종료일이 임박한 현재 에이전트 버전 업데이트에 대한 자세한 내용은 을 참조하십시오. 보안 에이전트를 수동으로 업데이트

리소스 비활성화 및 정리가 미치는 영향

이 섹션은 런타임 모니터링을 비활성화하거나 리소스 유형에 대해 GuardDuty 자동화된 에이전트 구성만 사용하지 않도록 선택한 AWS 계정 경우에 적용됩니다.

GuardDuty 자동 에이전트 구성 비활성화

GuardDuty 리소스에 배포된 보안 에이전트는 제거하지 않습니다. 하지만 보안 에이전트에 대한 업데이트 관리는 GuardDuty 중지됩니다.

GuardDuty 리소스 유형으로부터 런타임 이벤트를 계속 수신합니다. 사용 통계에 영향을 미치지 않도록 하려면 리소스에서 GuardDuty 보안 에이전트를 제거해야 합니다.

공유 VPC 엔드포인트를 AWS 계정 사용하든 사용하지 GuardDuty 않든 VPC 엔드포인트는 삭제되지 않습니다. 필요한 경우 VPC 엔드포인트를 수동으로 삭제해야 합니다.

런타임 모니터링 및 EKS 런타임 모니터링 비활성화

이 섹션은 다음 시나리오에 적용됩니다.

- EKS 런타임 모니터링을 별도로 활성화한 적이 없고 이제 런타임 모니터링을 비활성화했습니다.
- 런타임 모니터링과 EKS 런타임 모니터링을 모두 비활성화합니다. EKS 런타임 모니터링의 구성 상태가 확실하지 않은 경우 을 참조하십시오. EKS 런타임 모니터링 구성 상태 확인

위에 나열된 시나리오에 해당하는 경우 계정에서 GuardDuty 다음 조치를 취합니다.

- GuardDuty : 태그가 있는 VPC를 삭제합니다`GuardDutyManaged`. `true` 자동화된 보안 에이전트를 관리하기 GuardDuty 위해 만든 VPC입니다.
- GuardDuty 태그가 지정된 보안 그룹을 삭제합니다. `GuardDutyManaged` `true`
- 하나 이상의 참가자 계정에서 사용한 공유 VPC의 경우, VPC GuardDuty 엔드포인트나 공유 VPC 리소스와 연결된 보안 그룹을 삭제하지 않습니다.
- Amazon EKS 리소스의 경우 보안 GuardDuty 에이전트를 삭제합니다. 이는 수동으로 관리했는지 아니면 통해 관리했는지와 무관합니다. GuardDuty

  Amazon ECS 리소스의 경우 ECS 작업은 변경할 수 없으므로 해당 리소스에서 보안 에이전트를 제거할 GuardDuty 수 없습니다. 이는 수동 또는 자동으로 보안 에이전트를 관리하는 방식과는 별개입니다. GuardDuty 런타임 모니터링을 GuardDuty 비활성화하면 새 ECS 작업이 실행되기 시작할 때 사이드카 컨테이너를 연결하지 않습니다. Fargate-ECS 작업 사용에 대한 자세한 내용은 을 참조하십시오. Fargate와 런타임 모니터링이 작동하는 방식 (Amazon ECS만 해당)

  Amazon EC2 리소스의 경우 다음 조건을 충족하는 경우에만 모든 Systems Manager (SSM) 관리 Amazon EC2 인스턴스에서 보안 에이전트를 GuardDuty 제거합니다.

  - 리소스에는 제외 태그가 지정되지 않았습니다. `GuardDutyManaged` `false`
  - GuardDuty 인스턴스 메타데이터의 태그에 액세스할 권한이 있어야 합니다. 이 EC2 리소스의 경우 인스턴스 메타데이터의 태그에 대한 액세스는 Allow로 설정되어 있습니다.

보안 에이전트의 수동 관리를 중지할 때

GuardDuty 보안 에이전트를 배포하고 관리하는 데 사용하는 접근 방식에 관계없이 리소스의 런타임 이벤트 모니터링을 중지하려면 GuardDuty 보안 에이전트를 제거해야 합니다. 계정의 리소스 유

형에서 런타임 이벤트 모니터링을 중단하려는 경우 Amazon VPC 엔드포인트를 삭제할 수도 있습니다.

보안 에이전트 리소스를 정리하는 프로세스

Amazon VPC 엔드포인트 삭제

- 공유 VPC 없음 — 계정의 리소스를 더 이상 모니터링하지 않으려면 Amazon VPC 엔드포인트를 삭제해 보십시오.
- 공유 VPC 사용 — 공유 VPC 소유자 계정이 아직 사용 중인 공유 VPC 리소스를 삭제하면 공유 VPC 소유자 계정 및 참여 계정의 리소스에 대한 런타임 모니터링 (해당하는 경우 EKS Runtime Monitoring) 적용 범위 상태가 비정상이 될 수 있습니다. 적용 범위 상태에 대한 자세한 내용은 을 참조하십시오. 리소스의 런타임 커버리지 평가

자세한 내용은 인터페이스 엔드포인트 삭제를 참조하세요.

보안 그룹을 삭제하려면

- 공유 VPC 없음 — 계정의 리소스 유형을 더 이상 모니터링하지 않으려면 Amazon VPC와 연결된 보안 그룹을 삭제해 보십시오.
- 공유 VPC 사용 — 공유 VPC 소유자 계정이 보안 그룹을 삭제하면 공유 VPC와 연결된 보안 그룹을 현재 사용하고 있는 모든 참가자 계정, 공유 VPC 소유자 계정의 리소스 및 참여 계정에 대한 Runtime Monitoring 적용 범위 상태가 비정상이 될 수 있습니다. 자세한 정보는 리소스의 런타임 커버리지 평가을 참조하세요.

자세한 내용은 보안 그룹 삭제를 참조하십시오.

EKS 클러스터에서 GuardDuty 보안 에이전트를 제거하려면

더 이상 모니터링하지 않으려는 보안 에이전트를 EKS 클러스터에서 제거하려면 추가 기능 삭제를 참조하십시오.

EKS 추가 기능 에이전트를 제거해도 EKS 클러스터에서 `amazon-guardduty` 네임스페이스가 제거되지는 않습니다. `amazon-guardduty` 네임스페이스를 삭제하려면 Deleting a namespace를 참조하세요.

`amazon-guardduty`네임스페이스를 삭제하려면 (EKS 클러스터)

자동 에이전트 구성을 사용하지 않도록 설정해도 EKS 클러스터에서 `amazon-guardduty` 네임스페이스가 자동으로 제거되지는 않습니다. `amazon-guardduty` 네임스페이스를 삭제하려면 Deleting a namespace를 참조하세요.

아마존에서의 아마존 S3 보호 GuardDuty

S3 보호를 통해 Amazon은 객체 수준 API 작업이 포함된 Amazon Simple Storage Service (Amazon S3) 의 AWS CloudTrail 데이터 이벤트를 GuardDuty 모니터링하여 Amazon S3 버킷 내 데이터에 대한 잠재적 보안 위험을 식별할 수 있습니다.

GuardDuty AWS CloudTrail 관리 이벤트와 AWS CloudTrail S3 데이터 이벤트를 모두 모니터링하여 Amazon S3 리소스의 잠재적 위협을 식별합니다. 두 데이터 소스 모두 다양한 종류의 활동을 모니터링합니다. S3에 대한 CloudTrail 관리 이벤트의 예로는 Amazon S3 버킷을 나열하거나 구성하는 작업 (예:, `ListBuckets`,`DeleteBuckets`) 이 있습니다. `PutBucketReplication` S3에 대한 CloudTrail 데이터 이벤트의 예로는,, `GetObject`, `ListObjects`, `DeleteObject` 등의 객체 수준 API 작업이 있습니다. `PutObject`

GuardDuty Amazon을 활성화하면 CloudTrail 관리 이벤트 모니터링이 GuardDuty 시작됩니다. AWS 계정 S3 데이터 이벤트 로그인을 수동으로 활성화하거나 구성할 필요가 없습니다 AWS CloudTrail. Amazon GuardDuty 내에서 이 기능을 사용할 수 있는 모든 계정의 S3 보호 기능 (S3의 CloudTrail 데이터 이벤트를 모니터링) 을 언제든지 활성화할 수 있습니다. AWS 리전 이미 활성화된 GuardDuty 사용자는 30일 무료 평가 기간을 통해 처음으로 S3 보호를 활성화할 수 있습니다. AWS 계정 GuardDuty 처음으로 AWS 계정 활성화하는 경우 S3 Protection이 이미 활성화되어 있으며 이 30일 무료 평가판에 포함되어 있습니다. 자세한 정보는 비용 추정 GuardDuty 을 참조하세요.

에서 GuardDuty S3 보호를 활성화하는 것이 좋습니다. 이 기능을 활성화하지 않으면 Amazon S3 버킷을 완전히 모니터링할 수 없거나 S3 버킷에 저장된 데이터에 대한 의심스러운 액세스에 대한 결과를 생성할 수 없습니다. GuardDuty

S3 데이터 이벤트 GuardDuty 사용 방법

S3 데이터 이벤트 (S3 Protection) 를 활성화하면 모든 S3 버킷의 S3 데이터 이벤트 분석을 GuardDuty 시작하고 악의적이고 의심스러운 활동이 있는지 모니터링합니다. 자세한 정보는 AWS CloudTrail S3 용 데이터 이벤트을 참조하세요.

인증되지 않은 사용자가 S3 객체에 액세스하면 해당 S3 객체에 공개적으로 액세스할 수 있습니다. 따라서 에서는 이러한 요청을 처리하지 GuardDuty 않습니다. GuardDuty 유효한 IAM (AWS Identity and Access Management) 또는 AWS STS (AWS Security Token Service) 자격 증명을 사용하여 S3 객체에 대한 요청을 처리합니다.

S3 데이터 이벤트 모니터링을 기반으로 잠재적 위협을 GuardDuty 탐지하면 보안 탐지 결과를 생성합니다. Amazon S3 버킷에 대해 생성할 GuardDuty 수 있는 검색 결과 유형에 대한 자세한 내용은 을 참조하십시오GuardDuty S3 검색 유형.

S3 보호를 비활성화하면 S3 버킷에 저장된 데이터에 대한 S3 데이터 이벤트 모니터링이 GuardDuty 중지됩니다.

독립형 계정에 대한 S3 보호 구성

에 연결된 계정의 경우 콘솔 설정을 통해 이 프로세스를 자동화할 수 있습니다. AWS Organizations자세한 정보는 다중 계정 환경에서 S3 보호 구성을 참조하세요.

S3 보호 활성화 또는 비활성화

선호하는 액세스 방법을 선택하여 독립형 계정에 대해 S3 보호를 구성합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 S3 보호를 선택합니다.
3. S3 보호 페이지는 계정에 대한 S3 보호의 현재 상태를 제공합니다. 활성화 또는 비활성화를 선택하여 언제든지 S3 보호를 활성화 또는 비활성화할 수 있습니다.
4. 확인을 선택하여 선택 사항을 확인합니다.

API/CLI

1. 현재 리전의 유효한 탐지기 ID를 사용하고 `features` 객체 `name`을 `S3_DATA_EVENTS`로, `ENABLED` 또는 `DISABLED`로 설정하여 전달해 updateDetector를 실행하고 S3 보호를 활성화 또는 비활성화합니다.

   > **Note**
   >
   > 계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

2. 또는 를 사용할 수도 있습니다 AWS Command Line Interface. S3 보호를 활성화하려면 다음 명령을 실행하고 유효한 자체 탐지기 ID를 사용해야 합니다.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

S3 보호를 비활성화하려면 예시에서 ENABLED를 DISABLED로 바꿉니다.

다중 계정 환경에서 S3 보호 구성

다중 계정 환경에서는 위임된 GuardDuty 관리자 계정만 조직의 구성원 계정에 대해 S3 보호를 구성(활성화 또는 비활성화) 할 수 있습니다 AWS . GuardDuty 구성원 계정은 자신의 계정에서 이 구성을 수정할 수 없습니다. 위임된 GuardDuty 관리자 계정은 를 사용하여 AWS Organizations구성원 계정을 관리합니다. 위임된 GuardDuty 관리자 계정은 모든 계정에서 S3 Protection을 자동으로 활성화하거나, 새 계정만 활성화하거나, 조직 내 계정은 사용하지 않도록 선택할 수 있습니다. 자세한 정보는 AWS Organizations를 사용하여 계정 관리을 참조하세요.

위임된 GuardDuty 관리자 계정을 위한 S3 보호 구성

선호하는 액세스 방법을 선택하여 위임된 GuardDuty 관리자 계정에 대해 S3 보호를 구성하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   관리 계정 보안 인증 정보를 사용해야 합니다.
2. 탐색 창에서 S3 보호를 선택합니다.
3. S3 보호 페이지에서 편집을 선택합니다.
4. 다음 중 하나를 수행하십시오.

   모든 계정에 대해 활성화 사용

   - 모든 계정에 대해 활성화를 선택합니다. 그러면 조직에 가입한 새 GuardDuty 계정을 포함하여 AWS 조직의 모든 활성 계정에 대한 보호 계획이 활성화됩니다.
   - 저장을 선택합니다.

   수동으로 계정 구성 사용

   - 위임된 GuardDuty 관리자 계정 계정에만 보호 계획을 활성화하려면 계정 수동 구성을 선택합니다.

- 위임된 GuardDuty 관리자 계정 (이 계정) 섹션에서 활성화를 선택합니다.
- 저장을 선택합니다.

API/CLI

현재 지역의 위임된 GuardDuty 관리자 계정의 탐지기 ID를 사용하고 `features` 객체를 name or로 updateDetectorS3_DATA_EVENTS전달하여 실행합니다. `status` ENABLED DISABLED

또는 를 사용하여 AWS Command Line Interface S3 보호를 구성할 수 있습니다. *## ### # ### 12abc34d567e8fa901bc2d34e56789f0# ## ### ### ### ### ### ID# ### 555555555555# ### ### ### ID# #####. GuardDuty* AWS 계정 GuardDuty

사용자 계정 및 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오**detectorId**.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

조직의 모든 멤버 계정에 S3 보호 자동 활성화

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   관리자 계정 계정을 사용하여 로그인합니다.

2. 다음 중 하나를 수행하십시오.

   S3 보호 사용

   1. 탐색 창에서 S3 보호를 선택합니다.
   2. 모든 계정에 대해 활성화를 선택합니다. 이 작업을 통해 조직의 기존 계정과 새 계정 모두에 대해 S3 보호가 자동으로 활성화됩니다.
   3. 저장을 선택합니다.

> **Note**
>
> 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

계정 페이지 사용

1. 탐색 창에서 Accounts(계정)를 선택합니다.
2. 계정 페이지에서 초대 기준으로 계정 추가 전에 자동 활성화 기본 설정을 선택합니다.
3. 자동 활성화 기본 설정 관리 창의 S3 보호에서 모든 계정에 대해 활성화를 선택합니다.
4. 저장을 선택합니다.

모든 계정에 대해 활성화 옵션을 사용할 수 없는 경우 멤버 계정에서 S3 보호를 선택적으로 활성화 또는 비활성화 섹션을 참조하세요.

API/CLI

- 멤버 계정에 대해 S3 보호를 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.
- 다음 예시에서는 단일 멤버 계정에 S3 보호를 활성화하는 방법을 보여줍니다. *12abc34d567e8fa901bc2d34e56789f0# ### ### ### 11112222333# #### ### ## #. detector-id GuardDuty* S3 보호를 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

  계정 detectorId 및 현재 지역에 맞는 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

모든 기존 활성 멤버 계정에서 S3 보호 활성화

원하는 액세스 방법을 선택하여 조직의 모든 기존 활성 멤버 계정에 대해 S3 보호를 활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 AWS Management Console 로그인하고 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 S3 보호를 선택합니다.
3. S3 보호 페이지에서 구성의 현재 상태를 볼 수 있습니다. 활성 멤버 계정 섹션에서 작업을 선택합니다.
4. 작업 드롭다운 메뉴에서 기존의 모든 활성 멤버 계정에 대해 활성화를 선택합니다.
5. 확인을 선택합니다.

API/CLI

- 멤버 계정에 대해 S3 보호를 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 updateMemberDetectors API 작업을 간접적으로 호출합니다.
- 다음 예시에서는 단일 멤버 계정에 S3 보호를 활성화하는 방법을 보여줍니다. *12abc34d567e8fa901bc2d34e56789f0# ### ### ### 11112222333# #### ### ##*
  #. detector-id GuardDuty S3 보호를 비활성화하려면 ENABLED를 DISABLED로 바꿉니다.

  계정 detectorId 및 현재 지역에 맞는 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

새 멤버 계정에서 S3 보호 자동 활성화

원하는 액세스 방법을 선택하여 조직에 가입하는 새 계정에 대해 S3 보호를 활성화합니다.

Console

위임된 GuardDuty 관리자 계정은 콘솔을 통해 S3 보호 또는 계정 페이지를 사용하여 조직의 새 구성원 계정을 활성화할 수 있습니다.

새 멤버 계정에서 S3 보호 자동 활성화

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 다음 중 하나를 수행하십시오.
   - S3 보호 페이지 사용:
     1. 탐색 창에서 S3 보호를 선택합니다.
     2. S3 보호 페이지에서 편집을 선택합니다.
     3. 수동으로 계정 구성을 선택합니다.
     4. 새 멤버 계정에 대해 자동으로 활성화를 선택합니다. 이 단계를 통해 새 계정이 조직에 가입할 때마다 해당 계정에 대해 S3 보호가 자동으로 활성화됩니다. 조직이 위임한 GuardDuty 관리자 계정만 이 구성을 수정할 수 있습니다.
     5. 저장을 선택합니다.
   - 계정 페이지 사용:
     1. 탐색 창에서 Accounts(계정)를 선택합니다.
     2. 계정 페이지에서 자동 활성화 기본 설정을 선택합니다.
     3. 자동 활성화 기본 설정 관리 창의 S3 보호에서 새 계정에 대해 활성화를 선택합니다.

4. 저장을 선택합니다.

API/CLI

- 멤버 계정에 대해 S3 보호를 선택적으로 활성화 또는 비활성화하려면 자체 *### ID*를 사용하여 UpdateOrganizationConfiguration API 작업을 간접적으로 호출합니다.
- 다음 예시에서는 단일 멤버 계정에 S3 보호를 활성화하는 방법을 보여줍니다. 비활성화하려면 멤버 계정에서 RDS 보호를 선택적으로 활성화 또는 비활성화 섹션을 참조하세요. 조직에 가입한 새 계정(NEW), 모든 계정(ALL)에 대해 리전의 보호 플랜을 자동으로 활성화 또는 비활성화하거나 조직의 어떤 계정도 해당되지 않도록(NONE) 기본 설정을 설정합니다. 자세한 내용은 autoEnableOrganization구성원을 참조하십시오. 기본 설정에 따라 NEW를 ALL 또는 NONE으로 바꿔야 할 수 있습니다.

  계정 및 현재 지역의 계정을 detectorId 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

- 코드가 성공적으로 실행되면 빈 UnprocessedAccounts 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

멤버 계정에서 S3 보호를 선택적으로 활성화 또는 비활성화

원하는 액세스 방법을 선택하여 멤버 계정에 대해 S3 보호를 선택적으로 활성화 또는 비활성화합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용해야 합니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.

계정 페이지의 S3 보호 열에서 멤버 계정 상태를 검토합니다.

3. 선택적으로 S3 보호 활성화 또는 비활성화

   S3 보호를 구성할 계정을 선택합니다. 한 번에 여러 개의 계정을 선택할 수 있습니다. 보호 계획 편집 드롭다운 메뉴에서 S3Pro를 선택한 다음 적절한 옵션을 선택합니다.

API/CLI

멤버 계정에 대해 S3 보호를 선택적으로 활성화 또는 비활성화하려면 자체 탐지기 ID를 사용하여 updateMemberDetectors API 작업을 실행합니다. 다음 예시에서는 단일 멤버 계정에 S3 보호를 활성화하는 방법을 보여줍니다. 비활성화하려면 `true`를 `false`로 바꿉니다.

계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> 공백으로 구분된 계정 ID 목록을 전달할 수도 있습니다.

코드가 성공적으로 실행되면 빈 `UnprocessedAccounts` 목록이 반환됩니다. 계정의 탐지기 설정을 변경하는 데 문제가 있는 경우 해당 계정 ID가 문제 요약과 함께 나열됩니다.

> **Note**
>
> 스크립트를 사용하여 새 계정을 온보딩하고 새 계정에서 S3 보호를 비활성화하려는 경우 이 주제에서 설명하는 것과 같이 선택적 `dataSources` 객체를 사용하여 createDetector API 작업을 수정할 수 있습니다.

새 GuardDuty 계정에 대한 S3 보호를 자동으로 비활성화합니다.

> **Important**
>
> 기본적으로 S3 보호는 처음으로 AWS 계정 해당 조인에 GuardDuty 대해 자동으로 활성화됩니다.

새 계정을 GuardDuty 처음으로 활성화하는 GuardDuty 관리자 계정이고 S3 Protection이 기본적으로 활성화되지 않도록 하려면 선택적 `features` 객체를 createDetector사용하여 API 작업을 수정하여 비활성화할 수 있습니다. 다음 예에서는 AWS CLI 를 사용하여 S3 보호가 비활성화된 상태에서 새 GuardDuty 탐지기를 활성화합니다.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

S3 보호의 기능

AWS CloudTrail S3용 데이터 이벤트

데이터 영역 작업으로 알려진 데이터 이벤트를 통해 리소스에 또는 리소스 내에서 수행된 리소스 작업을 파악할 수 있습니다. 데이터 이벤트가 대량 활동인 경우도 많습니다.

GuardDuty 모니터링할 수 있는 S3의 CloudTrail 데이터 이벤트 예는 다음과 같습니다.

- `GetObject` API 작업
- `PutObject` API 작업
- `ListObjects` API 작업
- `DeleteObject` API 작업

GuardDuty 처음으로 활성화하면 S3 Protection이 기본적으로 활성화되며 30일 무료 평가 기간에도 포함됩니다. 하지만 이 기능은 선택 사항으로 언제든 모든 계정 또는 리전에 대해 활성화 또는 비활성화할 수 있습니다. 기능으로서 Amazon S3 구성에 대한 자세한 내용은 GuardDuty S3 보호 섹션을 참조하세요.

아마존 GuardDuty 조사 결과 이해

탐지 GuardDuty 결과는 네트워크 내에서 탐지된 잠재적 보안 문제를 나타냅니다. GuardDuty AWS 환경에서 예상치 못한 잠재적 악의적 활동이 탐지될 때마다 검색 결과를 생성합니다.

GuardDuty 콘솔의 GuardDuty 검색 결과 페이지에서 AWS CLI 또는 API 작업을 사용하여 결과를 보고 관리할 수 있습니다. 결과를 관리하는 방법에 대한 개요는 아마존 GuardDuty 조사 결과 관리 섹션을 참조하세요.

주제:

조사 결과 세부 정보

GuardDuty 조사 결과 내에서 사용할 수 있는 데이터 유형에 대해 알아보세요.

샘플 결과

테스트하거나 더 잘 이해할 수 있도록 샘플 결과를 생성하는 방법을 알아보세요 GuardDuty.

GuardDuty 결과 형식

GuardDuty 탐지 유형의 형식과 추적하는 GuardDuty 다양한 위협 목적을 이해하십시오.

결과 유형

사용 가능한 모든 검색 GuardDuty 결과를 유형별로 보고 검색하십시오. 각 결과 유형 항목에는 문제 해결을 위한 팁 및 제안 사항뿐만 아니라 해당 결과에 대한 설명이 포함되어 있습니다.

결과 세부 정보

Amazon GuardDuty 콘솔의 검색 결과 요약 섹션에서 검색 결과 세부 정보를 볼 수 있습니다. 결과 세부 정보는 결과 유형에 따라 달라집니다.

결과에 사용할 수 있는 정보의 종류를 결정하는 두 가지 기본 세부 정보가 있습니다. 첫 번째는 리소스 유형으로 `Instance`, `AccessKey`, `S3Bucket`, `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance` 또는 `Lambda`일 수 있습니다. 결과 정보를 결정하는 두 번째 세부 정보는 리소스 역할입니다. 리소스 역할은 액세스 키에 대해 `Target`일 수 있으며, 해당 리소스가 의심스러운 활동의 대상이었음을 의미합니다. 인스턴스 유형 결과의 경우 리소스 역할은 `Actor`일 수 있으며, 해당 리소스가 의심스러운 활동을 수행하는 작업자였음을 의미합니다. 이 주제에서는 결과에 대해 일반적으로 제공되는 몇 가지 세부 정보에 대해 설명합니다.

결과 개요

결과의 개요 섹션에는 다음 정보를 포함하여 결과의 가장 기본적으로 식별 가능한 특징이 포함되어 있습니다.

- 계정 ID — 이 검색 결과를 GuardDuty 생성하도록 유도한 활동이 발생한 AWS 계정의 ID입니다.
- 개수 — 이 패턴을 이 검색 결과 ID와 일치하는 활동을 집계한 GuardDuty 횟수입니다.
- 생성 날짜 - 이 결과가 처음 생성된 날짜와 시간입니다. 이 값이 업데이트된 시간과 다른 경우 활동이 여러 번 발생했으며 진행 중인 문제임을 나타냅니다.

> **Note**
>
> GuardDuty 콘솔의 검색 결과에 대한 타임스탬프는 현지 시간대로 표시되고 JSON 내보내기 및 CLI 출력에는 타임스탬프가 UTC로 표시됩니다.

- 결과 ID - 이 결과 유형 및 파라미터 집합에 대한 고유한 식별자입니다. 이 패턴과 일치하는 새로운 활동 발생은 동일한 ID로 집계됩니다.
- 결과 유형 - 결과를 트리거한 활동 유형을 나타내는 서식이 지정된 문자열입니다. 자세한 정보는 GuardDuty 결과 형식을 참조하세요.
- 지역 — 검색 결과가 생성된 AWS 지역입니다. 지원되는 리전에 대한 자세한 내용은 리전 및 엔드포인트 단원을 참조하십시오.
- 리소스 ID — 이 검색 결과를 GuardDuty 생성하도록 유도한 활동이 발생한 AWS 리소스의 ID입니다.
- 스캔 ID - GuardDuty 멀웨어 보호가 활성화된 경우의 검색 결과에 적용되는 것으로, 잠재적으로 손상된 EC2 인스턴스 또는 컨테이너 워크로드에 연결된 EBS 볼륨에서 실행되는 멀웨어 스캔의 식별자입니다. 자세한 정보는 맬웨어 보호 결과 세부 정보을 참조하세요.
- 심각도 - 결과에 할당된 심각도 수준(High, Medium 또는 Low)입니다. 자세한 정보는 GuardDuty 조사 결과의 심각도 수준을 참조하세요.
- 업데이트 시간 — 이 검색 결과가 GuardDuty 생성되도록 유도한 패턴과 일치하는 새 활동으로 이 검색 결과가 마지막으로 업데이트되었습니다.

Resource

영향을 받는 리소스는 시작 활동의 대상이 된 AWS 리소스에 대한 세부 정보를 제공합니다. 제공되는 정보는 리소스 유형과 작업 유형에 따라 달라집니다.

리소스 역할 — 검색을 시작한 AWS 리소스의 역할. 이 값은 TARGET 또는 ACTOR일 수 있으며, 리소스가 의심스러운 활동의 대상인지 아니면 의심스러운 활동을 수행한 작업자인지 여부를 나타냅니다.

리소스 유형 - 영향을 받은 리소스의 유형입니다. 여러 리소스가 관련된 경우 결과에는 여러 리소스 유형이 포함될 수 있습니다. 리소스 유형은 인스턴스, S3 버킷 AccessKey, ECS 클러스터, 컨테이너 KubernetesCluster, RDSDB 인스턴스 및 Lambda입니다. 리소스 유형에 따라 다른 결과 세부 정보가 제공됩니다. 리소스 옵션 탭을 선택하여 해당 리소스에 제공되는 세부 정보를 알아보세요.

Instance

인스턴스 세부 정보:

> **Note**
>
> 인스턴스가 이미 중지되었거나 교차 리전 API 호출 시 기본 API 호출이 다른 리전의 EC2 인스턴스에서 시작된 경우 일부 인스턴스 세부 정보가 누락될 수 있습니다.

- 인스턴스 ID - 검색 결과를 생성하도록 요청한 활동에 관련된 EC2 인스턴스의 ID입니다. GuardDuty
- 인스턴스 유형 - 결과와 관련이 있는 EC2 인스턴스의 유형입니다.
- 시작 시간 - 인스턴스가 시작된 날짜와 시간입니다.
- 아웃포스트 ARN — 의 아마존 리소스 이름 (ARN). AWS Outposts인스턴스에만 적용됩니다. AWS Outposts 자세한 내용은 AWS Outposts란 무엇입니까?를 참조하십시오.
- 보안 그룹 이름 - 관련 인스턴스에 연결된 보안 그룹의 이름입니다.
- 보안 그룹 ID – 관련 인스턴스에 연결된 보안 그룹의 ID입니다.
- 인스턴스 상태 – 대상 인스턴스의 현재 상태입니다.
- 가용 영역 – 관련 인스턴스가 위치한 AWS 리전 가용 영역입니다.
- 이미지 ID – 활동에 관여한 인스턴스를 빌드하는 데 사용되는 Amazon Machine Image의 ID입니다.
- 이미지 설명 – 활동에 관여한 인스턴스를 빌드하는 데 사용되는 Amazon Machine Image의 ID에 대한 설명입니다.
- 태그 - 이 리소스에 연결된 태그 목록(`key:value` 형식으로 나열됨)입니다.

AccessKey

액세스 키 세부 정보:

- 액세스 키 ID - 검색 결과를 GuardDuty 생성하라는 메시지가 표시된 활동에 참여한 사용자의 액세스 키 ID입니다.
- 주체 ID — 검색 결과 생성을 요청한 활동에 참여한 사용자의 주 ID입니다. GuardDuty
- 사용자 유형 — 검색 결과를 GuardDuty 생성하도록 요청한 활동에 참여한 사용자의 유형입니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- 사용자 이름 — 검색 결과를 GuardDuty 생성하라는 메시지가 표시된 활동에 참여한 사용자의 이름입니다.

S3Bucket

Amazon S3 버킷 세부 정보:

- 이름 – 결과에 관여한 버킷의 이름입니다.
- ARN - 결과에 관여한 버킷의 ARN입니다.
- 소유자 – 결과에 관여한 버킷을 소유한 사용자의 정식 사용자 ID입니다. 정식 사용자 ID에 대한 자세한 내용은 AWS account identifiers를 참조하세요.
- 유형 – 버킷 결과 유형으로, 대상 또는 소스가 될 수 있습니다.
- 기본 서버측 암호화 - 버킷에 대한 암호화 세부 정보입니다.
- 버킷 태그 - 이 리소스에 연결된 태그 목록(`key:value` 형식으로 나열됨)입니다.
- 유효한 권한 – 관여한 버킷이 공개적으로 노출되는지 여부를 나타내는 버킷에 대한 모든 유효한 권한 및 정책의 평가입니다. 값은 퍼블릭 또는 퍼블릭 아님이 될 수 있습니다.

EKSCluster

Kubernetes 클러스터 세부 정보:

- 이름 – Kubernetes 클러스터의 이름입니다.
- ARN - 클라이언트를 식별하는 ARN입니다.
- 생성 날짜 – 이 클러스터가 생성된 날짜와 시간입니다.

> **Note**
>
> GuardDuty 콘솔의 검색 결과에 대한 타임스탬프는 현지 시간대로 표시되고 JSON 내보내기 및 CLI 출력에는 타임스탬프가 UTC로 표시됩니다.

- VPC ID - 클러스터와 연결되는 VPC의 ID입니다.
- 상태 – 클러스터의 현재 상태입니다.
- 태그 – 클러스터를 분류하고 구성하는 데 도움이 되도록 클러스터에 적용하는 메타데이터입니다. 각 태그는 키와 값(선택 사항)으로 구성되며, `key:value` 형식으로 나열됩니다. 키와 값을 모두 정의해야 합니다.

  클러스터 태그는 클러스터에 연결된 다른 리소스로 전파되지 않습니다.

Kubernetes 워크로드 세부 정보:

- 유형 – Kubernetes 워크로드의 유형(예: 포드, 배포, 작업)입니다.
- 이름 - Kubernetes 워크로드의 이름입니다.
- Uid - Kubernetes 워크로드의 고유 ID입니다.
- 생성 날짜 - 이 워크로드가 생성된 날짜와 시간입니다.
- 레이블 - Kubernetes 워크로드에 연결된 키-값 쌍입니다.
- 컨테이너 - Kubernetes 워크로드의 일부로 실행되는 컨테이너의 세부 정보입니다.
- 네임스페이스 – 이 Kubernetes 네임스페이스에 속하는 워크로드입니다.
- 볼륨 – Kubernetes 워크로드에서 사용하는 볼륨입니다.
  - 호스트 경로 – 볼륨이 매핑되는 호스트 머신의 기존 파일 또는 디렉터리를 나타냅니다.
  - 이름 - 볼륨의 이름입니다.
- 포드 보안 컨텍스트 – 포드의 모든 컨테이너에 대한 권한 및 액세스 제어 설정을 정의합니다.
- 호스트 네트워크 – 포드가 Kubernetes 워크로드에 포함되는 경우 `true`로 설정됩니다.

Kubernetes 사용자 세부 정보:

- 그룹 - 결과를 생성한 활동에 관련된 사용자의 Kubernetes 역할 액세스 기반 제어(RBAC) 그룹입니다.
- ID - Kubernetes 사용자의 고유 ID입니다.

- 사용자 이름 - 결과를 생성한 활동에 관련된 Kubernetes 사용자의 이름입니다.
- 세션 이름 - Kubernetes RBAC 권한을 가진 IAM 역할을 맡은 엔터티입니다.

ECSCluster

ECS 클러스터 세부 정보:

- ARN - 클라이언트를 식별하는 ARN입니다.
- 이름 - 클러스터의 이름입니다.
- 상태 – 클러스터의 현재 상태입니다.
- 활성 서비스 개수 – `ACTIVE` 상태의 클러스터에서 실행 중인 서비스의 수입니다. 다음과 같은 방법으로 이러한 서비스를 볼 수 있습니다. ListServices
- 등록된 컨테이너 인스턴스 개수 – 클러스터에 등록된 컨테이너 인스턴스의 수입니다. 여기에는 `ACTIVE` 및 `DRAINING` 상태의 컨테이너 인스턴스가 모두 포함됩니다.
- 실행 중인 작업 개수 – `RUNNING` 상태인 클러스터의 작업 수입니다.
- 태그 – 클러스터를 분류하고 구성하는 데 도움이 되도록 클러스터에 적용하는 메타데이터입니다. 각 태그는 키와 값(선택 사항)으로 구성되며, `key:value` 형식으로 나열됩니다. 키와 값을 모두 정의해야 합니다.
- 컨테이너 - 작업과 관련된 컨테이너에 대한 세부 정보:
  - 컨테이너 이름 - 컨테이너의 이름입니다.
  - 컨테이너 이미지 - 컨테이너의 이미지입니다.
- 태스크 세부 정보 - 클러스터 내 태스크의 세부 정보입니다.
  - ARN - 작업의 Amazon 리소스 이름(ARN)입니다.
  - 정의 ARN - 태스크를 생성한 태스크 정의의 Amazon 리소스 이름(ARN)입니다.
  - 버전 - 작업의 버전 카운터입니다.
  - 태스크 생성 날짜 – 태스크가 생성되었을 때의 Unix 타임스탬프입니다.
  - 태스크 시작 시간 – 태스크가 시작되었을 때의 Unix 타임스탬프입니다.
  - 태스크 시작 – 태스크가 시작되었을 때 지정된 태그입니다.

Container

컨테이너 세부 정보:

- 컨테이너 런타임 – 컨테이너 실행에 사용되는 컨테이너 런타임(예: `docker` 또는 `containerd`)입니다.
- ID - 컨테이너 인스턴스 ID 또는 컨테이너 인스턴스의 전체 ARN 항목입니다.
- 이름 - 컨테이너의 이름입니다.

  사용 가능한 경우 이 필드에는 레이블 `io.kubenetes.container.name` 값이 표시됩니다.
- 이미지 - 컨테이너 인스턴스의 이미지입니다.
- 볼륨 마운트 – 컨테이너 볼륨 마운트 목록입니다. 컨테이너는 파일 시스템 아래에 볼륨을 탑재할 수 있습니다.
- 보안 컨텍스트 – 컨테이너 보안 컨텍스트는 컨테이너의 권한 및 액세스 제어 설정을 정의합니다.
- 프로세스 세부 정보 – 결과와 관련된 프로세스의 세부 정보를 설명합니다.

RDSDBInstance

RDSDBInstance 세부 정보:

> **Note**
>
> 이 리소스는 데이터베이스 인스턴스와 관련된 RDS 보호 결과에 제공됩니다.

- 데이터베이스 인스턴스 ID — 검색과 관련된 데이터베이스 인스턴스와 관련된 GuardDuty 식별자입니다.
- 엔진 - 결과에 관여한 데이터베이스 인스턴스의 데이터베이스 엔진 이름입니다. 가능한 값은 Aurora MySQL-Compatible 또는 Aurora PostgreSQL-Compatible입니다.
- 엔진 버전 - 검색과 관련된 데이터베이스 엔진 GuardDuty 버전입니다.
- 데이터베이스 클러스터 ID - 검색과 관련된 데이터베이스 인스턴스 ID를 포함하는 데이터베이스 클러스터의 GuardDuty 식별자입니다.
- 데이터베이스 인스턴스 ARN — 검색과 관련된 데이터베이스 인스턴스를 식별하는 ARN입니다. GuardDuty

Lambda

Lambda 함수 세부 정보

- 함수 이름 – 결과와 관련된 Lambda 함수의 이름입니다.

- 함수 버전 – 결과와 관련된 Lambda 함수의 버전입니다.
- 함수 설명 – 결과와 관련된 Lambda 함수의 설명입니다.
- 함수 ARN – 결과와 관련된 Lambda 함수의 Amazon 리소스 이름(ARN)입니다.
- 개정 ID – Lambda 함수 버전의 개정 ID입니다.
- 역할 - 결과와 관련된 Lambda 함수의 실행 역할입니다.
- VPC 구성 - Lambda 함수와 연결된 VPC ID, 보안 그룹 및 서브넷 ID를 포함한 Amazon VPC 구성입니다.
- VPC ID - 결과와 관련된 Lambda 함수와 연결된 Amazon VPC의 ID입니다.
- 서브넷 ID - Lambda 함수와 관련된 서브넷의 ID입니다.
- 보안 그룹 – 관련 Lambda 함수에 연결된 보안 그룹입니다. 여기에는 보안 그룹 이름과 그룹 ID가 포함됩니다.
- 태그 - 이 리소스에 연결된 태그 목록(`key:value` 형식으로 나열됨)입니다.

RDS 데이터베이스(DB) 사용자 세부 정보

> **Note**
>
> 이 섹션은 에서 RDS 보호 기능을 활성화한 경우의 검색 결과에 적용됩니다. GuardDuty 자세한 정보는 GuardDuty RDS 보호을 참조하세요.

GuardDuty 검색 결과는 손상 가능성이 있는 데이터베이스의 다음과 같은 사용자 및 인증 세부 정보를 제공합니다.

- 사용자 - 변칙적인 로그인 시도에 사용된 사용자 이름입니다.
- 애플리케이션 - 변칙적인 로그인 시도에 사용되는 애플리케이션 이름입니다.
- 데이터베이스 - 변칙적인 로그인 시도와 관련된 데이터베이스 인스턴스의 이름입니다.
- SSL - 네트워크에 사용되는 보안 소켓 계층(SSL)의 버전입니다.
- 인증 방법 – 결과와 관련된 사용자가 사용하는 인증 방법입니다.

런타임 모니터링: 검색 결과 세부 정보

> **Note**
>
> 이러한 세부 정보는 다음 중 하나를 GuardDuty 생성하는 경우에만 사용할 수 런타임 모니터링 검색 유형 있습니다.

이 섹션에는 프로세스 세부 정보 및 필요한 컨텍스트와 같은 런타임 세부 정보가 포함되어 있습니다. 프로세스 세부 정보는 관찰된 프로세스에 관한 정보를 설명하고 런타임 컨텍스트는 잠재적으로 의심스러운 활동에 관한 추가 정보를 설명합니다.

프로세스 세부 정보

- 이름 - 프로세스의 이름입니다.
- 실행 파일 경로 – 프로세스 실행 파일의 절대 경로입니다.
- 실행 파일 SHA-256 – 프로세스 실행 파일의 SHA256 해시입니다.
- 네임스페이스 PID – 호스트 수준 PID 네임스페이스가 아닌 보조 PID 네임스페이스에 있는 프로세스의 ID입니다. 컨테이너 내부 프로세스의 경우 컨테이너 내부에서 관찰된 프로세스 ID입니다.
- 현재 작업 디렉터리 – 프로세스의 현재 작업 디렉터리입니다.
- 프로세스 ID – 운영 체제에서 프로세스에 할당한 ID입니다.
- 시작 시간 – 프로세스가 시작된 시간입니다. UTC 날짜 문자열 형식 (`2023-03-22T19:37:20.168Z`)입니다.
- UUID — 에서 프로세스에 할당한 고유 ID입니다. GuardDuty
- 상위 UUID – 상위 프로세스의 고유 ID입니다. 이 ID는 에서 상위 프로세스에 할당합니다. GuardDuty
- 사용자 - 프로세스를 실행한 사용자입니다.
- 사용자 ID – 프로세스를 실행한 사용자의 ID입니다.
- 유효한 사용자 ID – 이벤트 시점에서 프로세스의 유효 사용자 ID입니다.
- 계보 - 프로세스의 상위 항목에 관한 정보입니다.
  - 프로세스 ID – 운영 체제에서 프로세스에 할당한 ID입니다.
  - UUID — 에서 프로세스에 할당한 고유 ID입니다. GuardDuty
  - 실행 파일 경로 – 프로세스 실행 파일의 절대 경로입니다.
  - 유효한 사용자 ID – 이벤트 시점에서 프로세스의 유효 사용자 ID입니다.

- 상위 UUID – 상위 프로세스의 고유 ID입니다. 이 ID는 에서 상위 프로세스에 할당합니다. GuardDuty
- 시작 시간 – 프로세스가 시작된 시간입니다.
- 네임스페이스 PID – 호스트 수준 PID 네임스페이스가 아닌 보조 PID 네임스페이스에 있는 프로세스의 ID입니다. 컨테이너 내부 프로세스의 경우 컨테이너 내부에서 관찰된 프로세스 ID입니다.
- 사용자 ID – 프로세스를 실행한 사용자의 사용자 ID입니다.
- 이름 – 프로세스의 이름입니다.

런타임 컨텍스트

다음 필드에서 생성된 결과에는 해당 결과 유형과 관련된 필드만 포함될 수 있습니다.

- 탑재 소스 – 컨테이너에 탑재된 호스트의 경로입니다.
- 탑재 대상 – 호스트 디렉터리에 매핑되는 컨테이너의 경로입니다.
- 파일 시스템 유형 – 탑재된 파일 시스템의 유형을 나타냅니다.
- 플래그 - 이 결과와 관련된 이벤트의 동작을 제어하는 옵션을 나타냅니다.
- 수정 프로세스 – 런타임에 컨테이너 내에서 바이너리, 스크립트 또는 라이브러리를 만들거나 수정한 프로세스에 관한 정보입니다.
- 수정 날짜 – 프로세스가 런타임에 컨테이너 내에서 바이너리, 스크립트 또는 라이브러리를 만들거나 수정한 타임스탬프입니다. 이 필드는 UTC 날짜 문자열 형식(`2023-03-22T19:37:20.168Z`)입니다.
- 라이브러리 경로 – 로드된 새 라이브러리의 경로입니다.
- LD 로드 이전 값 – `LD_PRELOAD` 환경 변수의 값입니다.
- 소켓 경로 – 액세스된 Docker 소켓의 경로입니다.
- runC 바이너리 경로 – `runc` 바이너리의 경로입니다.
- 릴리스 에이전트 경로 - `cgroup` 릴리스 에이전트 파일의 경로입니다.
- 명령줄 예제 — 잠재적으로 의심스러운 활동과 관련된 명령줄의 예입니다.
- 도구 범주 - 도구가 속한 범주입니다. 예로는 백도어 툴, 펜테스트 툴, 네트워크 스캐너, 네트워크 스니퍼 등이 있습니다.
- 도구 이름 — 의심스러울 수 있는 도구의 이름.
- 스크립트 경로 — 검색 결과를 생성한 실행된 스크립트의 경로입니다.
- 위협 파일 경로 - 위협 인텔리전스 세부 정보가 발견된 의심스러운 경로입니다.

- 서비스 이름 - 비활성화된 보안 서비스의 이름입니다.

EBS 볼륨 스캔 세부 정보

> **Note**
>
> 이 섹션은 GuardDuty -initiated 멀웨어 스캔을 활성화했을 때 발견된 결과에 적용됩니다. GuardDuty 멀웨어 보호

EBS 볼륨 스캔은 잠재적으로 손상된 EC2 인스턴스 또는 컨테이너 워크로드에 연결된 EBS 볼륨에 관한 세부 정보를 제공합니다.

- 스캔 ID – 맬웨어 스캔의 식별자입니다.
- 스캔 시작 시간 – 맬웨어 스캔이 시작된 날짜와 시간입니다.
- 스캔 완료 시간 – 맬웨어 스캔이 완료된 날짜와 시간입니다.
- 트리거 검색 ID — 이 맬웨어 검사를 시작한 GuardDuty 검색 결과의 검색 ID입니다.
- 소스 - 가능한 값은 `Bitdefender` 및 `AWS`입니다.
- 스캔 탐지 – 각 맬웨어 스캔의 세부 정보 및 결과를 전체적으로 볼 수 있습니다.
  - 스캔한 항목 수 - 스캔한 파일의 총 수입니다. `totalGb`, `files` 및 `volumes` 등의 세부 정보를 제공합니다.
  - 위협이 탐지된 항목 수 – 스캔 중에 탐지된 악성 `files`의 총 수입니다.
  - 최고 심각도 위협 세부 정보 – 스캔 중에 탐지된 최고 심각도 위협의 세부 정보 및 악성 파일 수입니다. `severity`, `threatName` 및 `count` 등의 세부 정보를 제공합니다.
  - 이름 기준 탐지된 위협 – 모든 심각도 수준으로 위협이 그룹화된 컨테이너 요소입니다. `itemCount`, `uniqueThreatNameCount`, `shortened` 및 `threatNames` 등의 세부 정보를 제공합니다.

맬웨어 보호 결과 세부 정보

> **Note**
>
> 이 섹션은 GuardDuty 시작 멀웨어 검사를 활성화했을 때 발견된 결과에 적용됩니다. GuardDuty 멀웨어 보호

맬웨어 보호 스캔에서 맬웨어를 탐지하면 콘솔(https://console.aws.amazon.com/guardduty/)의 결과 페이지에서 해당 결과를 선택하여 스캔 세부 정보를 볼 수 있습니다. 멀웨어 보호 검색 결과의 심각도는 검색 결과의 심각도에 따라 달라집니다. GuardDuty

> **Note**
>
> `GuardDutyFindingDetected` 태그는 스냅샷에 맬웨어가 포함되어 있음을 나타냅니다.

세부 정보 패널의 탐지된 위협 섹션에서 다음 정보가 제공됩니다.

- 이름 - 탐지별로 파일을 그룹화하여 얻은 위협의 이름입니다.
- 심각도 - 탐지된 위협의 심각도입니다.
- 해시 - 파일의 SHA-256 해시입니다.
- 파일 경로 – EBS 볼륨에서 악성 파일의 위치입니다.
- 파일 이름 – 위협이 탐지된 파일의 이름입니다.
- 볼륨 ARN – 스캔한 EBS 볼륨의 ARN입니다.

세부 정보 패널의 맬웨어 스캔 세부 정보 섹션에서 다음 정보가 제공됩니다.

- 스캔 ID – 맬웨어 스캔의 스캔 ID입니다.
- 스캔 시작 시간 - 스캔이 시작된 날짜와 시간입니다.
- 스캔 완료 시간 – 스캔이 완료된 날짜와 시간입니다.
- 스캔된 파일 – 스캔한 파일 및 디렉터리의 총 수입니다.
- 스캔한 총 GB – 프로세스 중 스캔한 스토리지의 양입니다.
- 트리거 검색 ID - 이 멀웨어 검사를 시작한 GuardDuty 검색 결과의 검색 ID입니다.
- 세부 정보 패널의 볼륨 세부 정보 섹션에서 다음 정보가 제공됩니다.
  - 볼륨 ARN – 볼륨의 Amazon 리소스 이름(ARN)입니다.
  - 스냅샷 ARN - EBS 볼륨 스냅샷의 ARN입니다.
  - 상태 - 볼륨의 스캔 상태(예: `Running`, `Skipped`, `Completed`)입니다.
  - 암호화 유형 – 볼륨을 암호화하는 데 사용된 암호화 유형입니다. 예를 들어 `CMCMK`입니다.
  - 디바이스 이름 – 디바이스의 이름입니다. 예를 들어 `/dev/xvda`입니다.

작업

결과의 작업은 결과를 트리거한 활동 유형에 대한 세부 정보를 제공합니다. 사용 가능한 정보는 작업 유형에 따라 다릅니다.

작업 유형 – 결과 활동 유형입니다. 이 값은 NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST, AWS_API_CALL 또는 RDS_LOGIN_ATTEMPT일 수 있습니다. 사용 가능한 정보는 작업 유형에 따라 다릅니다.

- NETWORK_CONNECTION - 확인된 EC2 인스턴스와 원격 호스트 사이에 네트워크 트래픽을 교환했음을 나타냅니다. 이 작업 유형은 다음과 같은 추가 정보를 보유합니다.
  - 연결 방향 — 검색 결과를 GuardDuty 생성하라는 메시지가 표시된 활동에서 관찰된 네트워크 연결 방향입니다. 다음 값 중 하나일 수 있습니다.
    - INBOUND - 원격 호스트가 사용자 계정에서 확인된 EC2 인스턴스의 로컬 포트에 대한 연결을 시작했다는 의미입니다.
    - OUTBOUND - 확인된 EC2 인스턴스가 원격 호스트에 대한 연결을 시작했음을 나타냅니다.
    - UNKNOWN — 연결 방향을 결정할 GuardDuty 수 없음을 나타냅니다.
  - 프로토콜 - 검색 결과를 GuardDuty 생성하라는 메시지를 표시한 활동에서 관찰된 네트워크 연결 프로토콜입니다.
  - 로컬 IP – 결과를 트리거한 트래픽의 기존 소스 IP 주소입니다. 이 정보는 트래픽이 흐르는 중간 계층의 IP 주소와 결과를 트리거한 트래픽의 원래 소스 IP 주소를 구별하는 데 사용할 수 있습니다. 예를 들어 EKS 포드가 실행 중인 인스턴스의 IP 주소가 아닌 EKS 포드의 IP 주소입니다.
  - 차단됨 - 대상 포트가 차단되었는지 여부를 나타냅니다.
- PORT_PROBE - 원격 호스트가 확인된 EC2 인스턴스를 여러 곳의 열린 포트에서 탐색했음을 나타냅니다. 이 작업 유형은 다음과 같은 추가 정보를 보유합니다.
  - 로컬 IP – 결과를 트리거한 트래픽의 기존 소스 IP 주소입니다. 이 정보는 트래픽이 흐르는 중간 계층의 IP 주소와 결과를 트리거한 트래픽의 원래 소스 IP 주소를 구별하는 데 사용할 수 있습니다. 예를 들어 EKS 포드가 실행 중인 인스턴스의 IP 주소가 아닌 EKS 포드의 IP 주소입니다.
  - 차단됨 - 대상 포트가 차단되었는지 여부를 나타냅니다.
- DNS_REQUEST - 식별된 EC2 인스턴스에서 도메인 이름을 쿼리했다는 의미입니다. 이 작업 유형은 다음과 같은 추가 정보를 보유합니다.
  - 프로토콜 — 검색 결과를 GuardDuty 생성하라는 메시지를 표시한 활동에서 관찰된 네트워크 연결 프로토콜입니다.
  - 차단됨 - 대상 포트가 차단되었는지 여부를 나타냅니다.

- AWS_API_CALL - AWS API가 간접적으로 호출되었음을 나타냅니다. 이 작업 유형은 다음과 같은 추가 정보를 보유합니다.
  - API - 호출되어 검색 결과를 GuardDuty 생성하라는 메시지가 표시된 API 작업의 이름입니다.

    > **Note**
    >
    > 이러한 작업에는 AWS CloudTrail로 캡처한 비 API 이벤트도 포함될 수 있습니다. 자세한 내용은 에서 캡처한 비 API 이벤트를 참조하십시오. CloudTrail

  - 사용자 에이전트 - API 요청한 사용자 에이전트입니다. 이 값은 호출이 에서 이루어졌는지, AWS 서비스 AWS Management Console, AWS SDK 또는 에서 이루어졌는지 알려줍니다. AWS CLI
  - 오류 코드 – API 호출 실패로 인해 결과가 트리거된 경우 해당 호출에 대한 오류 코드가 표시됩니다.
  - 서비스 이름 - 결과를 트리거한 API 호출을 시도한 서비스의 DNS 이름입니다.
- RDS_LOGIN_ATTEMPT - 원격 IP 주소에서 잠재적으로 손상된 데이터베이스에 대해 로그인 시도가 이루어졌음을 나타냅니다.
  - IP 주소 – 잠재적으로 의심스러운 로그인 시도에 사용된 원격 IP 주소입니다.

작업자 또는 대상

Resource role이 `TARGET`인 경우 결과에 작업자 섹션이 있습니다. 이는 리소스가 의심스러운 활동의 대상이 되었음을 나타내며 작업자 섹션에는 리소스를 대상으로 한 엔터티에 대한 세부 정보가 포함됩니다.

Resource role이 `ACTOR`인 경우 결과에 대상 섹션이 있습니다. 이는 리소스가 원격 호스트에 대한 의심스러운 활동에 관여했음을 나타내며, 이 섹션에는 리소스가 대상으로 한 IP 또는 도메인에 대한 정보가 포함됩니다.

작업자 또는 대상 섹션에서 제공되는 정보는 다음과 같습니다.

- 제휴 — 원격 API 호출자의 AWS 계정이 사용자 환경과 관련이 있는지 여부에 대한 세부 정보입니다. GuardDuty 이 값이 `true`인 경우 API 호출자가 어떤 방식으로 계정과 연결되어 있으며, `false`인 경우 API 호출자가 환경 외부에 있습니다.
- 원격 계정 ID - 최종 네트워크에서 리소스에 액세스하는 데 사용된 아웃바운드 IP 주소를 소유한 계정 ID입니다.
- IP 주소 - 검색 결과를 GuardDuty 생성하라는 메시지가 표시된 활동과 관련된 IP 주소입니다.

- 위치 - 검색 결과를 GuardDuty 생성하라는 메시지가 표시된 활동과 관련된 IP 주소의 위치 정보입니다.
- 조직 — 검색 결과를 GuardDuty 생성하도록 요청한 활동과 관련된 IP 주소의 ISP 조직 정보입니다.
- 포트 — 검색 결과를 GuardDuty 생성하도록 요청한 활동과 관련된 포트 번호입니다.
- 도메인 — 검색 결과를 GuardDuty 생성하도록 요청한 활동과 관련된 도메인입니다.
- 접미사가 있는 도메인 — 검색 결과를 GuardDuty 생성하도록 유도했을 가능성이 있는 활동에 관련된 두 번째 및 최상위 도메인입니다. 최상위 및 두 번째 수준 도메인 목록은 공개 접미사 목록을 참조하십시오.

추가 정보

모든 결과의 추가 정보 섹션에는 다음 정보가 포함될 수 있습니다.

- 위협 목록 이름 - 탐지 결과를 GuardDuty 생성하도록 요청한 활동과 관련된 IP 주소 또는 도메인 이름을 포함하는 위협 목록의 이름입니다.
- 샘플 - 샘플 결과인지 여부를 나타내는 true 또는 false 값입니다.
- 보관됨 - 결과가 보관되었는지 여부를 나타내는 true 또는 false 값입니다.
- 비정상 - 기록상 관찰된 적 없는 활동의 세부 정보입니다. 여기에는 비정상(이전까지 관찰되지 않은) 사용자, 위치, 시간, 버킷, 로그인 동작 또는 ASN 조직이 포함될 수 있습니다.
- 비정상적 프로토콜 - 탐지 결과를 GuardDuty 생성하라는 메시지를 표시한 활동과 관련된 네트워크 연결 프로토콜입니다.
- 에이전트 세부 정보 – AWS 계정의 EKS 클러스터에 현재 배포되어 있는 보안 에이전트에 관한 세부 정보입니다. 이는 EKS 런타임 모니터링 결과 유형에만 적용됩니다.
  - 에이전트 버전 — GuardDuty 보안 에이전트의 버전입니다.
  - 에이전트 ID — GuardDuty 보안 에이전트의 고유 식별자입니다.

증거

위협 인텔리전스에 기반한 결과에는 다음 정보가 포함된 증거 섹션이 있습니다.

- 위협 인텔리전스 세부 정보 - 인식된 항목이 `Threat name` 표시되는 위협 목록의 이름입니다.
- 위협 이름 - 위협과 관련된 멀웨어 계열 또는 기타 식별자의 이름입니다.
- 탐지 결과를 생성한 파일의 위협 파일 SHA256 - SHA256.

변칙적 동작

로 끝나는 검색 결과 유형은 해당 검색 결과가 GuardDuty 예외 항목 탐지 기계 학습 (ML) 모델에 의해 생성된 것임을 AnomalousBehavior나타냅니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 전략과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다.

요청을 호출한 CloudTrail 사용자 ID에 대해 API 요청의 어떤 요소가 비정상적인지에 대한 세부 정보는 검색 결과 세부 정보에서 확인할 수 있습니다. ID는 CloudTrail UserIdentity 요소에 의해 정의되며 가능한 값은,,,, 또는 입니다`Root`. `IAMUser` `AssumedRole` `FederatedUser` `AWSAccount` `AWSService`

API 활동과 관련된 모든 GuardDuty 검색 결과에 대해 제공되는 세부 정보 외에도 검색 AnomalousBehavior결과에는 다음 섹션에 요약된 추가 세부 정보가 있습니다. 이러한 세부 정보는 콘솔에서 볼 수 있으며 검색 결과의 JSON에서도 제공됩니다.

- 비정상 API - 결과와 관련된 주요 API 요청과 가까운 사용자 ID에 의해 간접적으로 호출된 API 요청 목록입니다. 이 창은 API 이벤트의 세부 정보를 다음 방식으로 추가 세분화합니다.
  - 첫 번째 나열된 API는 위험이 가장 높은 것으로 관찰된 활동과 관련된 API 요청인 주요 API입니다. 이 API는 결과를 트리거한 API로, 결과 유형의 공격 단계와 관련이 있습니다. 이 API는 콘솔의 작업 섹션과 결과의 JSON에 자세히 설명되어 있는 API이기도 합니다.
  - 나열된 다른 모든 API는 주요 API 근처에서 관찰되어 나열된 사용자 ID에서의 추가 변칙 API입니다. 목록에서 API가 하나뿐인 경우 ML 모델은 해당 사용자 ID의 추가 API 요청을 변칙으로 식별하지 않았습니다.
  - API 목록은 API 호출 완료 여부 또는 API 호출 실패(오류 응답 수신) 여부에 따라 구분됩니다. 수신된 오류 응답 유형은 호출에 실패한 각 API 위에 나열됩니다. 가능한 오류 응답 유형은 `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` 및 `operation not permitted`입니다.
  - API는 관련 서비스에 따라 분류됩니다.

> **Note**
>
> 보다 많은 컨텍스트를 위해 API 기록을 선택하여 최상위 API에 대한 세부 정보를 최대 20개까지 볼 수 있으며, 주로 사용자 ID와 계정 내 모든 사용자 모두에게 표시됩니다. API는 계정 내에서 사용되는 빈도에 따라 드문(한 달에 1회 미만), 이따금씩(한 달에 몇 회) 또는 자주(매일에서 매주 사용)로 표시됩니다.

- 비정상적인 동작(계정) - 이 섹션에서는 계정에서 프로파일링된 동작에 대한 추가 세부 정보를 제공합니다. 이 패널에서 추적되는 정보는 다음과 같습니다.
  - ASN 조직 - 변칙적인 API 호출이 이루어진 ASN 조직입니다.
  - 사용자 이름 - 변칙적인 API 호출을 한 사용자의 이름입니다.
  - User Agent - 변칙적인 API 호출을 하는 데 사용된 사용자 에이전트입니다. 사용자 에이전트는 호출에 사용된 메서드입니다(예: `aws-cli` 또는 `Botocore`).
  - 사용자 유형 - 변칙적인 API 호출을 한 사용자의 유형입니다. 가능한 값은 `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` 또는 `ROLE`입니다.
  - 버킷 - 액세스 중인 S3 버킷의 이름입니다.
- 비정상적인 동작(사용자 ID) - 이 섹션에서는 결과와 관련된 사용자 ID의 프로파일링된 동작에 대한 추가 세부 정보를 제공합니다. 특정 행동이 기록된 것으로 식별되지 않는 경우, 이는 GuardDuty ML 모델에서 교육 기간 내에 이 사용자 ID가 이러한 방식으로 API를 호출하는 것을 본 적이 없다는 의미입니다. 사용자 ID에 관하여 다음 추가 세부 정보가 제공됩니다.
  - ASN 조직 - 변칙적인 API 호출이 이루어진 ASN 조직입니다.
  - User Agent - 변칙적인 API 호출을 하는 데 사용된 사용자 에이전트입니다. 사용자 에이전트는 호출에 사용된 메서드입니다(예: `aws-cli` 또는 `Botocore`).
  - 버킷 - 액세스 중인 S3 버킷의 이름입니다.
- 비정상적인 동작(버킷) - 이 섹션에서는 결과와 관련된 S3 버킷의 프로파일링된 동작에 관한 추가 세부 정보를 제공합니다. 행동이 기록된 것으로 식별되지 않으면 GuardDuty ML 모델이 교육 기간 내에 이 버킷에 대한 API 호출을 이전에 본 적이 없다는 뜻입니다. 이 섹션에서 추적되는 정보는 다음과 같습니다.
  - ASN 조직 - 변칙적인 API 호출이 이루어진 ASN 조직입니다.
  - 사용자 이름 - 변칙적인 API 호출을 한 사용자의 이름입니다.
  - User Agent - 변칙적인 API 호출을 하는 데 사용된 사용자 에이전트입니다. 사용자 에이전트는 호출에 사용된 메서드입니다(예: `aws-cli` 또는 `Botocore`).
  - 사용자 유형 - 변칙적인 API 호출을 한 사용자의 유형입니다. 가능한 값은 `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` 또는 `ROLE`입니다.

> **Note**
>
> 동작 기록에 대한 추가 컨텍스트의 경우 비정상적인 동작(계정), 사용자 ID 또는 버킷 섹션에서 동작 기록을 선택하여 계정 내에서 사용되는 빈도에 따라 드문(한 달에 1회 미만), 이따끔

씩(한 달에 몇 회) 또는 자주(매일에서 매주 사용) 범주 각각에 대해 계정에서 예상되는 동작에 관한 세부 정보를 확인합니다.

- 비정상적인 동작(데이터베이스) - 이 섹션에서는 결과와 관련된 데이터베이스 인스턴스의 프로파일링된 동작에 관한 추가 세부 정보를 제공합니다. 행동이 기록으로 식별되지 않으면 GuardDuty ML 모델에서 교육 기간 내에 이러한 방식으로 이 데이터베이스 인스턴스에 로그인을 시도한 적이 없다는 의미입니다. 결과 패널의 이 섹션에서 추적되는 정보는 다음과 같습니다.
  - 사용자 이름 - 변칙적인 로그인 시도에 사용된 사용자 이름입니다.
  - ASN Org - 변칙적인 로그인 시도가 이루어진 ASN 조직입니다.
  - 애플리케이션 이름 - 변칙적인 로그인 시도에 사용되는 애플리케이션 이름입니다.
  - 데이터베이스 이름 - 변칙적인 로그인 시도와 관련된 데이터베이스 인스턴스의 이름입니다.

  > **Note**
  >
  > 동작 기록 섹션은 연결된 데이터베이스에 대해 이전에 관찰된 사용자 이름, ASN Orgs, 애플리케이션 이름 및 데이터베이스 이름에 관한 추가 컨텍스트를 제공합니다. 각 고유 값에는 로그인 성공 이벤트에서 이 값이 관찰된 횟수를 나타내는 관련 카운트가 있습니다.

- 비정상적인 동작(계정 Kubernetes 클러스터, Kubernetes 네임스페이스 및 Kubernetes 사용자 이름) - 이 섹션에서는 해당 결과와 관련된 Kubernetes 클러스터 및 네임스페이스의 프로파일링된 동작에 관한 추가 세부 정보를 제공합니다. 특정 동작이 기록으로 식별되지 않으면 GuardDuty ML 모델이 이전에 이 계정, 클러스터, 네임스페이스 또는 사용자 이름을 이런 방식으로 관찰한 적이 없음을 의미합니다. 결과 패널의 이 섹션에서 추적되는 정보는 다음과 같습니다.
  - 사용자 이름 - 결과와 관련된 Kubernetes API를 호출한 사용자입니다.
  - 가장한 사용자 – `username`으로 가장한 사용자입니다.
  - 네임스페이스 - 작업이 발생한 Amazon EKS 클러스터 내의 Kubernetes 네임스페이스입니다.
  - 사용자 에이전트 – Kubernetes API 호출과 관련된 사용자 에이전트입니다. 사용자 에이전트는 호출에 사용된 메서드입니다(예: `kubectl`).
  - API - Amazon EKS 클러스터 내에서 `username`에 의해 호출된 Kubernetes API입니다.
  - ASN 정보 - 호출한 사용자의 IP 주소와 관련된 ASN 정보(예: 조직 및 ISP)입니다.
  - 요일 - Kubernetes API 호출이 이루어진 요일입니다.
  - 권한[1] – `username`에서 Kubernetes API를 사용할 수 있는지 여부를 나타내기 위해 액세스 여부를 확인하는 Kubernetes 동사 및 리소스입니다.

- 서비스 계정 이름[1] – 워크로드에 ID를 제공하는 Kubernetes 워크로드와 관련된 서비스 계정입니다.
- 레지스트리[1] – Kubernetes 워크로드에 배포된 컨테이너 이미지와 관련된 컨테이너 레지스트리입니다.
- 이미지[1] – 관련 태그 및 다이제스트 없이 Kubernetes 워크로드에 배포된 컨테이너 이미지입니다.
- 이미지 접두사 구성[1] – 이미지를 사용하는 컨테이너에 대해 컨테이너 및 워크로드 보안 구성이 활성화된 이미지 접두사입니다(예: `hostNetwork` 또는 `privileged`).
- 주체 이름[1] – `RoleBinding` 또는 `ClusterRoleBinding`의 참조 역할에 바인딩된 주체(예: `user`, `group` 또는 `serviceAccountName`)입니다.
- 역할 이름[1] – 역할 또는 `roleBinding` API의 생성 또는 수정과 관련된 역할의 이름입니다.

S3 볼륨 기반 이상

이 섹션에서는 S3 볼륨 기반 이상에 관한 컨텍스트 정보를 자세히 설명합니다. 볼륨 기반 결과(Exfiltration:S3/AnomalousBehavior)는 사용자가 S3 버킷에 대해 수행한 비정상적인 수의 S3 API 호출을 모니터링하며, 이는 잠재적 데이터 유출 가능성을 나타냅니다. 볼륨 기반 이상 결과에 대해 다음 S3 API 호출이 모니터링됩니다.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

다음 지표는 IAM 엔터티가 S3 버킷에 액세스할 때 일반적인 동작의 기준을 세우는 데 도움이 됩니다. 데이터 유출을 탐지하기 위해 볼륨 기반 이상 탐지 결과는 일반적인 동작 기준과 비교하여 모든 활동을 평가합니다. 비정상적인 동작(사용자 ID), 관찰된 볼륨(사용자 ID) 및 관찰된 볼륨(버킷) 섹션에서 동작 기록을 선택하여 다음 지표를 확인합니다.

- 지난 24시간 동안 영향을 받는 S3 버킷과 연결된 IAM 사용자 또는 IAM 역할(무엇이 호출되었는지에 따라 다름)에 의해 간접적으로 호출된 `s3-api-name` API 호출 수입니다.
- 지난 24시간 동안 모든 S3 버킷과 연결된 IAM 사용자 또는 IAM 역할(무엇이 호출되었는지에 따라 다름)에 의해 간접적으로 호출된 `s3-api-name` API 호출 수입니다.
- 지난 24시간 동안 영향을 받는 S3 버킷과 연결된 모든 IAM 사용자 또는 IAM 역할(무엇이 호출되었는지에 따라 다름)의 `s3-api-name` API 호출 수입니다.

RDS 로그인 활동 기반 이상

이 섹션서는 비정상적 작업자의 로그인 시도 횟수를 자세히 설명하고 로그인 시도 결과에 따라 그룹화됩니다. RDS 보호 결과 유형에서 로그인 이벤트에서 비정상적인 `successfulLoginCount`, `failedLoginCount` 및 `incompleteConnectionCount` 패턴을 모니터링하여 변칙적인 동작을 식별합니다.

- successfulLoginCount— 이 카운터는 특이한 행위자가 데이터베이스 인스턴스에 성공적으로 연결한 횟수 (로그인 속성의 올바른 조합) 의 합계를 나타냅니다. 로그인 속성에는 사용자 이름, 암호 및 데이터베이스 이름이 포함됩니다.
- failedLoginCount— 이 카운터는 데이터베이스 인스턴스에 대한 연결을 설정하는 데 실패한 (실패) 로그인 시도 횟수의 합계를 나타냅니다. 이는 사용자 이름, 암호 또는 데이터베이스 이름과 같은 로그인 조합의 속성 중 하나 이상이 잘못되었음을 나타냅니다.
- incompleteConnectionCount— 이 카운터는 성공 또는 실패로 분류할 수 없는 연결 시도 횟수를 나타냅니다. 데이터베이스가 응답을 제공하기 전에 이러한 연결은 닫힙니다. 데이터베이스 포트가 연결되어 있지만 데이터베이스로 정보가 전송되지 않는 포트 스캔, 로그인 시도 성공 또는 실패 전에 연결이 중단된 경우를 예로 들 수 있습니다.

GuardDuty 결과 형식

GuardDuty는 AWS 환경에서 의심스럽거나 예기치 않은 행동을 탐지할 때 결과를 생성합니다. 결과는 GuardDuty에서 발견한 잠재적 보안 문제에 대한 세부 정보를 포함한 알림입니다. 결과 세부 정보에는 발생한 문제, 의심되는 활동과 관련된 AWS 리소스, 문제의 활동이 발생한 시점에 대한 정보와 기타 정보가 포함되어 있습니다.

조사 결과 세부 정보의 가장 유용한 정보 중 하나는 조사 결과 유형입니다. 조사 결과 유형의 용도는 잠재적인 보안 문제에 대한 간결하면서도 읽기 쉬운 설명을 제공하는 것입니다. 예를 들어 GuardDuty Recon:EC2/PortProbeUnprotectedPort 결과 유형은 AWS 환경의 어느 지점에서 EC2 인스턴스에 잠재적 공격자가 탐색 중인 보호되지 않는 포트가 있음을 신속하게 알려줍니다.

GuardDuty는 생성한 다양한 결과 유형에 다음 형식을 사용합니다.

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

이 형식의 각 부분은 결과 유형의 한 측면을 나타냅니다. 이러한 측면에는 다음과 같은 설명이 있습니다.

- ThreatPurpose - 위협, 공격 유형 또는 잠재적 공격 단계의 주요 목적을 설명합니다. GuardDuty 위협 목적의 전체 목록은 다음 섹션을 참조하세요.

- ResourceTypeAffected - 이 결과에서 공격의 잠재적인 대상으로 식별된 AWS 리소스를 설명합니다. 현재 GuardDuty는 EC2, S3, IAM 및 EKS 리소스에 대한 결과를 생성할 수 있습니다.
- ThreatFamilyName - GuardDuty가 탐지하는 전반적인 위협 또는 잠재적인 악성 활동을 설명합니다. 예를 들어 NetworkPortUnusual의 값은 GuardDuty 결과에서 식별된 EC2 인스턴스에 해당 결과에서 식별된 특정 원격 포트에 대한 이전 통신 내역이 없음을 나타냅니다.
- DetectionMechanism - GuardDuty가 결과를 탐지한 방법을 설명합니다. 이는 일반적인 결과 유형의 변형 또는 GuardDuty가 특정 메커니즘을 사용하여 탐지한 결과를 나타내는 데 사용할 수 있습니다. 예를 들어 Backdoor:EC2/DenialOfService.Tcp는 TCP를 통해 서비스 거부(DoS)가 탐지되었음을 나타냅니다. UDP 변형은 Backdoor:EC2/DenialOfService.Udp입니다.

  .Custom 값은 GuardDuty가 사용자 지정 위협 목록을 기반으로 결과를 탐지했음을 나타내고, .Reputation은 GuardDuty가 도메인 평판 점수 모델을 사용하여 결과를 탐지했음을 나타냅니다.
- Artifact - 악성 활동에 사용된 도구가 소유한 특정 리소스를 설명합니다. 예를 들어 결과 유형 CryptoCurrency:EC2/BitcoinTool.B!DNS에서 DNS EC2 인스턴스가 알려진 비트코인 관련 도메인과 통신 중임을 나타냅니다.

Threat Purposes

GuardDuty에서 위협 목적은 위협, 공격 유형 또는 잠재적 공격 단계의 주요 목적을 설명합니다. 예를 들어 Backdoor와 같은 일부 위협 목적은 공격 유형을 나타냅니다. 그러나 Impact와 같은 일부 위협 목적은 MITRE ATT&CK 전략과 연계되어 있습니다. MITRE ATT&CK 전략은 적의 공격 주기에서 서로 다른 단계를 나타냅니다. 현재 GuardDuty 릴리스에서 ThreatPurpose는 다음 값을 가질 수 있습니다.

Backdoor

이 값은 해당 공격이 AWS 리소스를 손상시키고 변조하였으며 악의적인 활동에 대한 추가 지침을 수신하도록 홈 명령 및 제어(C&C) 서버에 접속할 수 있음을 나타냅니다.

동작

이 값은 GuardDuty에서 관련 AWS 리소스에 대해 설정된 기준과 다른 활동 또는 활동 패턴을 탐지했음을 나타냅니다.

CredentialAccess

이 값은 GuardDuty가 공격자가 환경에서 계정 ID 또는 암호와 같은 보안 인증 정보를 훔치는 데 사용할 수 있는 활동 패턴을 탐지했음을 나타냅니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

Cryptocurrency

이 값은 GuardDuty가 환경의 AWS 리소스가 암호화폐와 관련된 소프트웨어(예: 비트코인)를 호스팅하고 있음을 탐지했음을 나타냅니다.

DefenseEvasion

이 값은 GuardDuty가 공격자가 환경에 침투하는 동안 탐지를 피하기 위해 사용할 수 있는 활동 또는 활동 패턴을 탐지했음을 나타냅니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

Discovery

이 값은 GuardDuty에서 공격자가 시스템 및 내부 네트워크에 대한 지식을 넓히는 데 사용할 수 있는 활동 또는 활동 패턴을 탐지했음을 나타냅니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

Execution

이 값은 공격자가 네트워크를 탐색하거나 데이터를 훔치기 위해 악성 코드 실행을 시도할 수 있음을 GuardDuty에서 탐지했음을 나타냅니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

Exfiltration

이 값은 GuardDuty에서 공격자가 네트워크에서 데이터를 훔치려고 할 때 사용할 수 있는 활동 또는 활동 패턴을 탐지했음을 나타냅니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

Impact

이 값은 GuardDuty에서 공격자가 시스템 및 데이터를 조작, 방해 또는 파괴하려고 시도하는 중임을 보여주는 활동 또는 활동 패턴을 탐지했음을 나타냅니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

InitialAccess

이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

Pentest

때때로 AWS 리소스의 소유자 또는 이들의 공인 대리인이 전반적으로 허용적인 개방형 보안 그룹 또는 액세스 키와 같은 취약성을 찾기 위해 AWS 애플리케이션에 대해 테스트를 의도적으로 실행합니다. 이러한 침투 테스트는 공격자가 취약한 리소스를 찾아내기 전에 해당 리소스를 파악하여 제재하기 위해 수행됩니다. 하지만 권한이 있는 침투 테스터가 사용하는 일부 도구는 무료로 사용할 수 있으므로 무단 사용자 또는 공격자가 탐색 테스트를 실행할 수 있습니다. GuardDuty는 이러한 활동 이면의 진정한 의도까지는 파악할 수 없지만 Pentest 값은 GuardDuty에서 이러한 활동을

탐지했고 알려진 침투 테스트에서 생성한 활동과 유사하므로 잠재적인 공격일 수 있음을 나타내며, 네트워크의 악의적인 탐색을 나타낼 수 있습니다.

Persistence

이 값은 GuardDuty에서 공격자가 초기 액세스 경로가 차단된 경우에도 시스템에 대한 액세스를 시도하고 유지하기 위해 사용할 수 있는 활동 또는 활동 패턴을 탐지했음을 나타냅니다. 기존 사용자의 손상된 보안 인증 정보를 통해 액세스 권한을 획득한 후 새 IAM 사용자를 생성하는 것이 여기에 포함될 수 있습니다. 기존 사용자의 보안 인증 정보가 삭제되면 공격자는 기존 이벤트의 일부로 탐지되지 않은 새 사용자에 대한 액세스를 유지하게 됩니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

정책

이 값은 AWS 계정에서 권장되는 보안 모범 사례에 반하는 행동을 보이고 있음을 나타냅니다.

PrivilegeEscalation

이 값은 AWS 환경 내의 관련 주체가 공격자가 네트워크에 대해 더 높은 수준의 권한을 얻기 위해 활용할 수 있는 행동을 보이고 있음을 알려줍니다. 이 위협 목적은 MITRE ATT&CK 전략을 기반으로 합니다.

Recon

이 값은 네트워크 정찰을 수행할 때 공격자가 액세스 범위를 넓히거나 리소스를 활용하는 방법을 결정하는 데 사용할 수 있는 활동 또는 활동 패턴을 GuardDuty에서 탐지했음을 나타냅니다. 예를 들어 이 활동에는 포트를 조사하고, 사용자, 데이터베이스 테이블을 나열하는 등의 방법으로 AWS 환경의 취약성을 파악하는 활동이 포함될 수 있습니다.

Stealth

이 값은 공격자가 행동을 적극적으로 숨기려고 함을 나타냅니다. 예를 들어 익명화 프록시 서버를 사용하면 활동의 실제 특성을 파악하는 것이 무척 어려울 수 있습니다.

Trojan

이 값은 공격이 조용히 악의적인 활동을 수행하는 트로이 목마 프로그램을 사용 중임을 의미합니다. 때때로 이 소프트웨어는 일반적인 프로그램으로 보이기도 합니다. 사용자가 실수로 이 소프트웨어를 실행할 때도 있고, 취약성을 악용하여 이 소프트웨어가 자동으로 실행될 수도 있습니다.

UnauthorizedAccess

이 값은 권한 없는 개인의 의심되는 활동 또는 의심되는 활동 패턴을 GuardDuty에서 탐지했음을 나타냅니다.

에서 샘플 결과 생성 GuardDuty

Amazon에서 샘플 결과를 생성하면 생성할 GuardDuty 수 있는 다양한 검색 결과를 시각화하고 이해하는 GuardDuty 데 도움이 됩니다. 샘플 검색 결과를 생성할 때 현재 검색 결과 목록을 지원되는 각 검색 결과 유형별로 하나의 샘플 검색 결과로 GuardDuty 채웁니다.

생성된 샘플은 자리표시자 값으로 채워진 근삿값입니다. 이러한 샘플은 사용자 환경의 실제 결과와 다르게 보일 수 있지만 이를 사용하여 CloudWatch 이벤트 또는 필터와 같은 다양한 구성을 테스트할 수 있습니다. GuardDuty 결과 유형에 대해 제공되는 값의 목록은 결과 유형 표에 나열되어 있습니다.

시뮬레이션된 활동을 기반으로 몇 가지 일반적인 결과를 환경 내에 생성하려면 다음 일반적인 GuardDuty 결과 자동 생성 단원을 참조하십시오.

GuardDuty 콘솔 또는 API를 통해 샘플 결과 생성

선호하는 액세스 방법을 선택하여 샘플 결과를 생성합니다.

> **Note**
>
> 콘솔 방법은 각 결과 유형 중 하나를 생성합니다. 단일 샘플 결과는 API를 통해서만 생성할 수 있습니다.

Console

다음 절차를 수행하여 샘플 조사 결과를 생성합니다. 이 프로세스는 각 검색 유형에 대해 하나의 샘플 GuardDuty 검색 결과를 생성합니다.

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. [Settings] 페이지의 [Sample findings] 아래에서 [Generate sample findings]를 선택합니다.
4. 탐색 창에서 결과를 선택합니다. 샘플 결과는 현재 결과 페이지에 접두사 [SAMPLE]과 함께 표시됩니다.

API/CLI

CreateSampleFindingsAPI를 통해 모든 검색 유형과 일치하는 단일 샘플 GuardDuty 검색 결과를 생성할 수 있습니다. 검색 유형에 사용할 수 있는 값은 결과 유형 표에 나열되어 있습니다.

이는 CloudWatch 이벤트 규칙을 테스트하거나 결과를 기반으로 자동화하는 데 유용합니다. 다음 예시에서는 AWS CLI를 사용하여 `Backdoor:EC2/DenialOfService.Tcp` 유형에 대한 단일 샘플 결과를 만드는 방법을 보여줍니다.

계정과 현재 지역에 `detectorId` 맞는 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

이러한 방법을 통해 생성된 샘플 결과의 제목은 콘솔에서 항상 [SAMPLE]로 시작합니다. 샘플 결과의 경우 결과 JSON 세부 정보의 additionalInfo 섹션에 `"sample": true` 값이 있습니다.

일반적인 GuardDuty 결과 자동 생성

다음 스크립트를 사용하여 몇 가지 일반적인 GuardDuty 결과를 자동으로 생성할 수 있습니다. guardduty-tester.template은 배스천 호스트, AWS CloudFormation SSH를 통해 액세스할 수 있는 테스터 Amazon EC2 인스턴스, 두 개의 대상 EC2 인스턴스가 있는 격리된 환경을 만드는 데 사용합니다. 그런 다음 guardduty_tester.sh 를 실행하여 테스터 EC2 인스턴스, 대상 Windows EC2 인스턴스 및 대상 Linux EC2 인스턴스 간의 상호 작용을 시작하여 다섯 가지 유형의 일반적인 공격을 시뮬레이션하여 탐지하고 생성된 결과를 통해 알려줄 수 있습니다. GuardDuty

1. 사전 요구 사항으로 guardduty-tester.template 및 guardduty_tester.sh 를 실행하려는 계정 및 GuardDuty 지역에서 활성화해야 합니다. GuardDuty시작하기 GuardDuty활성화에 대한 자세한 내용은 을 참조하십시오.

   또한 이러한 스크립트를 실행할 각 리전에서 새 EC2 키 페어를 생성하거나 기존 EC2 키 페어를 사용해야 합니다. 이 EC2 키 페어는 새 스택을 생성하는 데 사용하는 guardduty-tester.template 스크립트에서 파라미터로 사용됩니다. CloudFormation 키 페어 생성에 대한 자세한 내용은 Amazon EC2 키 페어를 참조하세요.
2. guardduty-tester.template을 사용하여 새 스택을 생성합니다. CloudFormation 스택 생성에 대한 자세한 지침은 스택 생성을 참조하세요. guardduty-tester.template을 실행하기 전에 새 스택을 식별할 스택 이름, 스택을 실행할 가용 영역, EC2 인스턴스를 시작하는 데 사용할 수 있는 키 페어와 같은 파라미터의 값으로 수정합니다. 그런 다음 해당 프라이빗 키를 사용하여 SSH를 통해 EC2 인스턴스에 액세스할 수 있습니다.

   guardduty-tester.template은 실행 및 완료하는 데 약 10분이 걸립니다. 환경을 생성하고 guardduty_tester.sh를 테스터 EC2 인스턴스에 복사합니다.

3. AWS CloudFormation 콘솔에서 새 실행 스택 옆의 체크박스를 선택합니다. AWS CloudFormation 표시된 일련의 탭 중에서 출력 탭을 선택합니다. Bastion Host와 테스터 EC2 인스턴스에 할당된 IP 주소를 기록합니다. SSH를 통해 테스터 EC2 인스턴스에 액세스하려면 이러한 IP 주소가 모두 필요합니다.
4. ~/.ssh/config 파일에 다음 항목을 생성하여 Bastion Host를 통해 인스턴스에 로그인합니다.

```
Host bastion
        HostName {Elastic IP Address of Bastion}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
Host tester
        ForwardAgent yes
        HostName {Local IP Address of RedTeam Instance}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
        ProxyCommand ssh bastion nc %h %p
        ServerAliveInterval 240
```

   이제 $ ssh tester를 호출하여 대상 EC2 인스턴스에 로그인할 수 있습니다. 배스천 호스트를 통한 EC2 인스턴스 구성 및 연결에 대한 자세한 내용은 https://aws.amazon.com/blogs/security/securely-connect-to-linux - - instances-running-in-a /를 참조하십시오. private-amazon-vpc
5. 테스터 EC2 인스턴스에 연결한 후 guardduty_tester.sh 를 실행하여 테스터와 대상 EC2 인스턴스 간의 상호 작용을 시작하고, 공격을 시뮬레이션하고, 결과를 생성합니다. GuardDuty

GuardDuty 조사 결과의 심각도 수준

각 GuardDuty 탐지 결과에는 보안 엔지니어가 판단한 바에 따라 탐지 결과가 네트워크에 미칠 수 있는 잠재적 위험을 반영하는 지정된 심각도 수준과 값이 있습니다. 심각도 값은 1.0~8.9 범위 내에 있을 수 있으며, 값이 높을수록 심각도 위험도 높아짐을 의미합니다. 조사 결과로 강조된 잠재적 보안 문제에 대한 대응을 결정하는 데 도움이 되도록 이 범위를 심각도 높음, 중간, 낮음 심각도 수준으로 GuardDuty 세분화하십시오.

> **Note**
>
> 값 0과 9.0~10.0은 향후에 사용하기 위해 예약되어 있습니다.

다음은 조사 결과에 대해 현재 정의된 심각도 수준 및 값과 각 GuardDuty 결과에 대한 일반적인 권장 사항입니다.

심각도 수준	값 범위
높음	7.0 - 8.9
높음 심각도 수준은 문제의 리소스(EC2 인스턴스 또는 IAM 사용자 로그인 보안 인증 정보 세트)가 손상되었고 무단 액세스에 적극적으로 사용되고 있음을 나타냅니다. 결과에서 높음 심각도로 명시된 보안 문제를 우선적으로 처리하고 즉시 해결 단계를 수행하여 더 이상 리소스가 무단으로 사용되지 못하도록 하는 것이 좋습니다. 예를 들어, EC2 인스턴스를 정리 또는 종료하거나 IAM 보안 인증 정보를 교체합니다. 자세한 내용은 해결 단계를 참조하십시오.	
Medium	4.0 - 6.9
중간 심각도 수준은 일반적으로 관찰된 동작에서 벗어나는 의심스러운 활동을 나타내며 사용 사례에 따라 리소스가 손상되었을 수 있습니다. 가급적 빨리 관련된 리소스를 조사하는 것이 좋습니다. 해결 단계는 리소스 및 결과 그룹에 따라 다르지만, 일반적으로 활동이 승인되고 사용 사례와 일치하는지 확인해야 합니다. 원인을 식별할 수 없거나 활동이 승인되었는지 확인할 수 없는 경우, 리소스가 손상된 것으로 간주하고 해결 단계를 수행하여 리소스를 보호해야 합니다. 다음은 중간 수준 결과를 검토할 때 고려해야 할 몇 가지 사항입니다. • 권한이 있는 사용자가 리소스의 동작을 변경한(예: 정상 트래픽보다 높은 트래픽 허용 또는 새로운 포트에서의 통신 활성화) 새 소프트웨어를 설치했는지 확인합니다. • 권한이 있는 사용자가 제어판 설정을 변경했는지 확인합니다(예: 보안 그룹 설정 변경). • 관련된 리소스에 대해 바이러스 백신 스캔을 실행해 권한이 없는 소프트웨어를 감지합니다. • 관련된 IAM 역할, 사용자, 그룹 또는 자격 증명 세트에 연결된 권한을 확인합니다. 이러한 권한이 변경 또는 교체되었을 수 있습니다.	
낮음	1.0 - 3.9
낮음 심각도 수준은 네트워크가 손상되지 않은 의심스러운 활동(예: 포트 검색 또는 침입 시도 실패)이 시도되었음을 나타냅니다.	

심각도 수준	값 범위
즉각적인 권장 조치는 없지만 누군가가 네트워크의 취약점을 찾고 있음을 나타낼 수 있으므로 이 정보를 기록해 두는 것이 좋습니다.	

GuardDuty 집계 결과 찾기

모든 검색 결과는 동적입니다. 즉, 동일한 보안 문제와 관련된 새로운 활동이 GuardDuty 감지되면 새 결과를 생성하는 대신 원래 결과를 새 정보로 업데이트합니다. 이러한 동작을 통해 여러 개의 유사한 보고서를 살펴볼 필요 없이 진행 중인 문제를 식별하고 이미 알고 있는 보안 문제로 인한 전반적인 노이즈를 줄일 수 있습니다.

예를 들어 `UnauthorizedAccess:EC2/SSHBruteForce` 결과의 경우 인스턴스에 대한 다중 액세스 시도가 동일한 결과 ID로 집계되므로 결과의 세부 정보에서 카운트 수가 증가합니다. 이는 결과가 인스턴스(즉, 인스턴스의 SSH 포트가 이러한 유형의 활동에 대해 제대로 보호되지 않음을 나타내는 경우)와 관련한 단일 보안 문제를 나타내기 때문입니다. 하지만 사용자 환경의 새 인스턴스를 대상으로 하는 SSH 액세스 활동이 GuardDuty 탐지되면 고유한 검색 결과 ID로 새 검색 결과를 생성하여 새 리소스와 관련된 보안 문제가 있음을 알려줍니다.

결과 집계 시, 해당 활동에서 가장 최근에 발생한 정보로 업데이트됩니다. 즉, 위의 예에서 인스턴스가 새로운 작업자의 무차별 암호 대입 시도 대상인 경우 검색 세부 정보는 가장 최근 소스에 대한 원격 IP를 반영하기 위해 업데이트되며 이전 정보가 교체됩니다. 개별 활동 시도에 대한 전체 정보는 사용자 CloudTrail 또는 VPC 흐름 로그에서 계속 확인할 수 있습니다.

기존 검색 결과를 집계하는 대신 새 검색 결과를 GuardDuty 생성하라는 알림을 보내는 기준은 검색 결과 유형에 따라 다릅니다. 각 결과 유형의 집계 기준은 계정 내의 고유한 보안 문제를 가장 잘 파악할 수 있도록 보안 엔지니어가 결정합니다.

결과 찾기 및 분석 GuardDuty

다음 절차를 사용하여 GuardDuty 결과를 보고 분석하십시오.

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. Findings(결과)를 선택한 후 특정 결과를 선택하여 세부 정보를 확인합니다.

   각 결과에 대한 세부 정보는 결과 유형, 관련된 리소스 및 활동 특성에 따라 다릅니다. 사용 가능한 결과 필드에 대한 자세한 내용은 결과 세부 정보 단원을 참조하십시오.

3. (선택 사항) 결과를 보관하려면 결과 목록에서 원하는 결과를 선택한 후 작업 메뉴를 선택합니다. 그런 다음 Archive(보관)를 선택합니다.

   보관된 결과는 현재 드롭다운에서 보관됨을 선택하여 볼 수 있습니다.

   현재 GuardDuty 회원 계정의 GuardDuty 사용자는 결과를 보관할 수 없습니다.

   > **Important**
   >
   > 위의 절차를 사용하여 결과를 수동으로 보관하는 경우 이 결과(보관 완료 후 생성된)의 후속 발생이 현재 결과 목록에 추가됩니다. 이 결과를 현재 목록에서 절대 보지 않으려면 자동 보관할 수 있습니다. 자세한 정보는 억제 규칙을 참조하세요.

4. (선택 사항) 결과를 다운로드하려면 결과 목록에서 원하는 결과를 선택한 후 Actions(작업) 메뉴를 선택합니다. 그런 다음 내보내기를 선택합니다. 결과를 내보내기하는 경우 전체 JSON 문서를 볼 수 있습니다.

   > **Note**
   >
   > 어떤 경우에는 특정 결과가 생성된 후 오탐이라는 사실을 알게 GuardDuty 됩니다. GuardDuty 검색 결과의 JSON에 신뢰도 필드를 제공하고 값을 0으로 설정합니다. GuardDuty 이렇게 하면 이러한 결과를 무시해도 된다는 것을 알 수 있습니다.

결과 유형

새로 추가되거나 사용 중지된 검색 결과 유형을 포함하여 GuardDuty 검색 결과 유형의 중요한 변경 사항에 대한 자세한 내용은 을 참조하십시오. 아마존의 문서 기록 GuardDuty

현재는 사용 중지된 결과 유형에 대한 자세한 내용은 사용 중지된 결과 유형 섹션을 참조하세요.

GuardDuty EC2 검색 유형

다음 결과는 Amazon EC2 리소스에만 해당되며 항상 리소스 유형이 `Instance`입니다. 결과의 심각도 및 세부 정보는 EC2 인스턴스가 의심스러운 활동의 대상인지 또는 작업자가 해당 활동을 수행 중인지 여부를 나타내는 리소스 역할에 따라 다릅니다.

여기에 나열된 결과에는 해당 결과 유형을 생성하는 데 사용된 데이터 소스 및 모델이 포함됩니다. 데이터 소스 및 모델에 대한 자세한 내용은 기본 데이터 소스 섹션을 참조하세요.

> **Note**
>
> 인스턴스가 이미 종료되었거나 다른 리전의 EC2 인스턴스에서 시작된 교차 리전 API 호출의 일부로 기본 API 호출이 이루어진 경우 일부 EC2 결과에 대해 인스턴스 세부 정보가 누락될 수 있습니다.

모든 EC2 결과의 경우 해당 리소스를 검토하여 예상대로 작동하는지 확인하는 것이 좋습니다. 활동이 승인된 경우 억제 규칙 또는 신뢰할 수 있는 IP 목록을 사용하여 해당 리소스에 대한 오탐지 알림을 방지할 수 있습니다. 활동이 예기치 않게 발생한 경우, 보안을 유지하는 가장 좋은 방법은 인스턴스가 손상되었다고 가정하고 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결에 설명된 작업을 수행하는 것입니다.

주제

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts

- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce

- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

EC2 인스턴스가 알려진 명령 및 제어 서버와 연결된 IP를 쿼리하는 중입니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경 내에 알려진 명령 및 제어(C&C) 서버와 연결된 IP를 쿼리하는 인스턴스가 있음을 알립니다. 나열된 인스턴스는 손상되었을 수 있습니다. 명령 및 제어(C&C) 서버는 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다.

봇넷은 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스(PC, 서버, 모바일 디바이스 및 사물 인터넷 디바이스 포함)의 모음입니다. 일반적으로 봇넷은 맬웨어를 분산하고 부적절한 정보(예: 신용카드 번호)를 수집합니다. 봇넷의 용도와 구조에 따라 C&C 서버가 DDoS(분산 서비스 거부) 공격을 시작하는 명령을 실행할 수도 있습니다.

> **Note**
>
> 쿼리된 IP가 log4j와 관련된 경우 관련 결과의 필드에 다음 값이 포함됩니다.
>
> - 서비스. 추가 정보. threatListName = 아마존
> - service.additionalInfo.threatName = Log4j Related

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/C&CActivity.B!DNS

EC2 인스턴스가 알려진 명령 및 제어 서버와 연결된 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경 내에 알려진 명령 및 제어(C&C) 서버와 연결된 도메인 이름을 쿼리하는 인스턴스가 있음을 알립니다. 나열된 인스턴스는 손상되었을 수 있습니다. 명령 및 제어(C&C) 서버는 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다.

봇넷은 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스(PC, 서버, 모바일 디바이스 및 사물 인터넷 디바이스 포함)의 모음입니다. 일반적으로 봇넷은 맬웨어를 분산하고 부적절한 정보(예: 신용카드 번호)를 수집합니다. 봇넷의 용도와 구조에 따라 C&C 서버가 DDoS(분산 서비스 거부) 공격을 시작하는 명령을 실행할 수도 있습니다.

> **Note**
>
> 쿼리된 도메인 이름이 log4j와 관련된 경우 관련 결과의 필드에 다음 값이 포함됩니다.
>
> - 서비스. 추가 정보. threatListName = 아마존
> - service.additionalInfo.threatName = Log4j Related

> **Note**
>
> 이 검색 유형을 GuardDuty 생성하는 방법을 테스트하려면 인스턴스 (Linux 또는 `dig` `nslookup` Windows용 사용) 에서 테스트 도메인에 대해 DNS 요청을 보낼 수 `guarddutyc2activityb.com` 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/DenialOfService.Dns

EC2 인스턴스가 DNS 프로토콜을 통한 DoS(Denial of Service) 공격 수행에 사용 중이라고 볼 수 있는 방식으로 동작하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 대용량의 아웃바운드 DNS 트래픽을 생성 중인 나열된 EC2 인스턴스가 있음을 알립니다. 이는 나열된 인스턴스가 손상되어 DNS 프로토콜을 사용하여 denial-of-service DoS 공격을 수행하는 데 사용되고 있음을 의미할 수 있습니다.

> **Note**
>
> 이 조사 결과는 DoS 공격의 주요 대상인 공개적으로 라우팅이 가능한 IP 주소에 대한 DoS 공격만 감지합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/DenialOfService.Tcp

EC2 인스턴스가 TCP 프로토콜을 통한 DoS(Denial of Service) 공격 수행에 사용 중이라고 볼 수 있는 방식으로 동작하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 대용량의 아웃바운드 TCP 트래픽을 생성 중인 나열된 EC2 인스턴스가 있음을 알립니다. 이는 인스턴스가 손상되어 TCP 프로토콜을 사용하여 denial-of-service DoS 공격을 수행하는 데 사용되고 있음을 의미할 수 있습니다.

> **Note**
>
> 이 조사 결과는 DoS 공격의 주요 대상인 공개적으로 라우팅이 가능한 IP 주소에 대한 DoS 공격만 감지합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/DenialOfService.Udp

EC2 인스턴스가 UDP 프로토콜을 통한 DoS(Denial of Service) 공격 수행에 사용 중이라고 볼 수 있는 방식으로 동작하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 대용량의 아웃바운드 UDP 트래픽을 생성 중인 나열된 EC2 인스턴스가 있음을 알립니다. 이는 나열된 인스턴스가 손상되어 UDP 프로토콜을 사용하여 denial-of-service DoS 공격을 수행하는 데 사용되고 있음을 의미할 수 있습니다.

> **Note**
>
> 이 조사 결과는 DoS 공격의 주요 대상인 공개적으로 라우팅이 가능한 IP 주소에 대한 DoS 공격만 감지합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

EC2 인스턴스가 TCP 포트에서 UDP 프로토콜을 통한 DoS(Denial of Service) 공격 수행에 사용 중이라고 볼 수 있는 방식으로 동작하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 일반적으로 TCP 통신에 사용되는 포트를 대상으로 대량의 아웃바운드 UDP 트래픽을 생성 중인 나열된 EC2 인스턴스가 있음을 알립니다. 이는 나열된 인스턴스가 손상되어 TCP 포트에서 UDP 프로토콜을 사용하여 denial-of-service (DoS) 공격을 수행하는 데 사용되고 있음을 의미할 수 있습니다.

> **Note**
>
> 이 조사 결과는 DoS 공격의 주요 대상인 공개적으로 라우팅이 가능한 IP 주소에 대한 DoS 공격만 감지합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/DenialOfService.UnusualProtocol

EC2 인스턴스가 특이한 프로토콜을 통한 DoS(Denial of Service) 공격 수행에 사용 중이라고 볼 수 있는 방식으로 동작하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 일반적으로 EC2 인스턴스에서 사용하지 않는 특이한 프로토콜 유형의 대량 아웃바운드 트래픽을 생성 중인 나열된 EC2 인스턴스가 있음을 알립니다(예: Internet Group Management Protocol). 이는 인스턴스가 손상되어 비정상적인 프로토콜을 사용하여 DoS denial-of-service (DoS) 공격을 수행하는 데 사용되고 있음을 의미할 수 있습니다. 이 조사 결과는 DoS 공격의 주요 대상인 공개적으로 라우팅이 가능한 IP 주소에 대한 DoS 공격만 감지합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/Spambot

EC2 인스턴스가 포트 25의 원격 호스트와 통신하여 비정상적인 동작을 보이고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 나열된 EC2 인스턴스가 포트 25의 원격 호스트와 통신하고 있음을 알립니다. EC2 인스턴스에 포트 25에서의 이전 통신 내역이 없기 때문에 이 동작은 비정상적입니다. 포트 25는 일반적으로 메일 서버에서 SMTP 통신을 위해 사용합니다. 이 결과는 EC2 인스턴스가 스팸 발송에 사용됨으로 인해 손상되었을 수 있음을 나타냅니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Behavior:EC2/NetworkPortUnusual

EC2 인스턴스가 비정상적인 서버 포트의 원격 호스트와 통신하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 나열된 EC2 인스턴스가 설정된 기준과 다른 방식으로 동작하고 있음을 알립니다. 이 EC2 인스턴스에는 해당 원격 포트에서 통신한 이전 내역이 없습니다.

> **Note**
>
> EC2 인스턴스가 포트 389 또는 포트 1389에서 통신한 경우 관련 결과 심각도가 높음으로 수정되고, 결과 필드에 다음 값이 포함됩니다.
>
> - service.additionalInfo.context = Possible log4j callback

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Behavior:EC2/TrafficVolumeUnusual

EC2 인스턴스가 원격 호스트에 대해 비정상적으로 큰 네트워크 트래픽을 생성하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 나열된 EC2 인스턴스가 설정된 기준과 다른 방식으로 동작하고 있음을 알립니다. 이 EC2 인스턴스에는 해당 원격 호스트로 이렇게 많은 양의 트래픽을 보낸 이전 내역이 없습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

CryptoCurrency:EC2/BitcoinTool.B

EC2 인스턴스가 암호 화폐 관련 활동과 연결된 IP 주소를 쿼리하는 중입니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 비트코인 또는 기타 암호화폐 관련 활동과 연결된 IP 주소를 쿼리하는 나열된 EC2 인스턴스가 있음을 알립니다. 비트코인은 다른 통화, 제품, 서비스와 교환할 수 있는 세계적인 암호화폐 및 디지털 결제 시스템입니다. 비트코인은 비트코인 채굴에 따른 보상으로, 공격자들의 많은 관심을 받고 있습니다.

해결 권장 사항:

이 EC2 인스턴스를 사용하여 암호화폐를 채굴 또는 관리하거나 이 인스턴스가 블록체인 활동에 관여한 경우, 이 결과는 환경에 대한 예상된 활동일 수 있습니다. AWS 환경에서 이러한 경우 이 결과에 대

한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `CryptoCurrency:EC2/BitcoinTool.B` 값을 사용해야 합니다. 두 번째 필터 기준은 블록체인 활동에 관여한 인스턴스의 인스턴스 ID여야 합니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 단원을 참조하십시오.

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 가능성이 높습니다. 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 단원을 참조하십시오.

CryptoCurrency:EC2/BitcoinTool.B!DNS

EC2 인스턴스가 암호 화폐 관련 활동과 연결된 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경에 비트코인 또는 기타 암호화폐 관련 활동과 연결된 도메인 이름을 쿼리하는 나열된 EC2 인스턴스가 있음을 알립니다. 비트코인은 다른 통화, 제품, 서비스와 교환할 수 있는 세계적인 암호화폐 및 디지털 결제 시스템입니다. 비트코인은 비트코인 채굴에 따른 보상으로, 공격자들의 많은 관심을 받고 있습니다.

해결 권장 사항:

이 EC2 인스턴스를 사용하여 암호화폐를 채굴 또는 관리하거나 이 인스턴스가 블록체인 활동에 관여한 경우, 이 결과는 환경에 대한 예상된 활동일 수 있습니다. AWS 환경에서 이러한 경우 이 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `CryptoCurrency:EC2/BitcoinTool.B!DNS` 값을 사용해야 합니다. 두 번째 필터 기준은 블록체인 활동에 관여한 인스턴스의 인스턴스 ID여야 합니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 단원을 참조하십시오.

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 가능성이 높습니다. 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 단원을 참조하십시오.

DefenseEvasion:EC2/UnusualDNSResolver

Amazon EC2 인스턴스가 비정상적인 퍼블릭 DNS 해석기와 통신하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 Amazon EC2 인스턴스가 기준 동작과 다른 방식으로 동작하고 있음을 알립니다. 이 EC2 인스턴스에는 최근에 이 퍼블릭 DNS 해석기와 통신한 기록이 없습니다. GuardDuty 콘솔의 검색 결과 세부 정보 패널의 Unormaly 필드는 쿼리된 DNS 확인자에 대한 정보를 제공할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

DefenseEvasion:EC2/UnusualDoHActivity

Amazon EC2 인스턴스가 비정상적인 HTTPS를 통한 DNS(DoH) 통신을 수행하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 Amazon EC2 인스턴스가 설정된 기준과 다른 방식으로 동작하고 있음을 알립니다. 이 EC2 인스턴스에는 이 퍼블릭 DoH 서버와의 최근 HTTPS를 통한 DNS(DoH) 통신 기록이 없습니다. 결과 세부 정보의 비정상적 필드는 쿼리된 DoH 서버에 관한 정보를 제공할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

DefenseEvasion:EC2/UnusualDoTActivity

Amazon EC2 인스턴스가 비정상적인 TLS를 통한 DNS(DoT) 통신을 수행하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 나열된 EC2 인스턴스가 설정된 기준과 다른 방식으로 동작하고 있음을 알립니다. 이 EC2 인스턴스에는 이 퍼블릭 DoT 서버와의 최근 DNS over TLS(DoT) 통신 기록이 없습니다. 결과 세부 정보 패널의 비정상적 필드는 쿼리된 DoT 서버에 관한 정보를 제공할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Impact:EC2/AbusedDomainRequest.Reputation

EC2 인스턴스가 알려진 악용된 도메인과 연결된 평판이 낮은 도메인 이름을 쿼리하고 있습니다.

기본 심각도: 중간

- 데이터 소스: DNS 로그

이 결과는 AWS 환경 내에 나열된 Amazon EC2 인스턴스가 알려진 악용된 도메인 또는 IP 주소와 연결된 평판이 낮은 도메인 이름을 쿼리하고 있음을 알립니다. 악용된 도메인의 예로는 동적 DNS 공급자뿐 아니라 무료 하위 도메인 등록을 제공하는 최상위 도메인 이름(TLD) 및 2단계 도메인 이름(2LD) 등이 있습니다. 위협 작업자는 이러한 서비스를 활용하여 무료로 또는 저렴한 비용으로 도메인을 등록하는 경향이 있습니다. 이 범주에서 평판이 낮은 도메인은 등록 기관의 파킹 IP 주소로 확인되는 만료된 도메인일 수도 있으며, 그에 따라 더 이상 활성화되지 않을 수도 있습니다. 파킹 IP에서 등록 기관은 어떤 서비스와도 연결되지 않은 도메인의 트래픽을 전달합니다. 위협 작업자가 일반적으로 이러한 등록 기관 또는 서비스를 C&C 및 맬웨어 배포에 사용하기 때문에 나열된 Amazon EC2 인스턴스가 손상될 수 있습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Impact:EC2/BitcoinDomainRequest.Reputation

EC2 인스턴스가 암호화폐 관련 활동과 연결된 평판이 낮은 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경에 비트코인 또는 기타 암호화폐 관련 활동과 연결된 평판이 낮은 도메인 이름을 쿼리하는 Amazon EC2 인스턴스가 있음을 알립니다. 비트코인은 다른 통화, 제품, 서비스와 교환할 수 있는 세계적인 암호화폐 및 디지털 결제 시스템입니다. 비트코인은 비트코인 채굴에 따른 보상으로, 공격자들의 많은 관심을 받고 있습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

해결 권장 사항:

이 EC2 인스턴스를 사용하여 암호화폐를 채굴 또는 관리하거나 이 인스턴스가 블록체인 활동에 관여한 경우, 이 결과는 환경에 대한 예상된 활동을 나타낼 수 있습니다. AWS 환경에서 이러한 경우 이 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `Impact:EC2/BitcoinDomainRequest.Reputation` 값을 사용해야 합니다. 두 번째 필터 기준은 블록체인 활동에 관여한 인스턴스의 인스턴스 ID여야 합니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 단원을 참조하십시오.

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 가능성이 높습니다. 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 단원을 참조하십시오.

Impact:EC2/MaliciousDomainRequest.Reputation

EC2 인스턴스가 알려진 악성 도메인과 연결된 평판이 낮은 도메인 이름을 쿼리하고 있습니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경 내에 나열된 Amazon EC2 인스턴스가 알려진 악성 도메인 또는 IP 주소와 연결된 평판이 낮은 도메인 이름을 쿼리하고 있음을 알립니다. 예를 들어 도메인이 알려진 싱크홀 IP 주소와 연결되어 있을 수 있습니다. 싱크홀 도메인은 이전에 위협 작업자가 통제한 도메인으로, 이러한 도메인에 대한 요청은 인스턴스 손상을 나타낼 수 있습니다. 이러한 도메인은 알려진 악성 캠페인 또는 도메인 생성 알고리즘과도 상관관계가 있을 수 있습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Impact:EC2/PortSweep

EC2 인스턴스가 다수의 IP 주소에서 포트를 탐색하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 나열된 EC2 인스턴스가 다수의 공개적으로 라우팅 가능한 IP 주소에서 포트를 탐색하고 있음을 알립니다. 이러한 유형의 활동은 일반적으로 악용할 취약한 호스트를 찾는 데 사용됩니다. GuardDuty 콘솔의 검색 결과 세부 정보 패널에는 가장 최근의 원격 IP 주소만 표시됩니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Impact:EC2/SuspiciousDomainRequest.Reputation

EC2 인스턴스의 수명 또는 적은 사용으로 인해 의심스러운 평판이 낮은 도메인 이름을 쿼리하고 있습니다.

기본 심각도: 낮음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경 내에 나열된 Amazon EC2 인스턴스가 악성인 것으로 의심되는 평판이 낮은 도메인 이름을 쿼리하고 있음을 알려줍니다. 이 도메인의 특성은 이전에 관찰된 악성 도메인과 일치했지만, 당사의 평판 모델에서는 알려진 위협과 확실한 상관관계를 파악할 수 없었습니다. 이러한 도메인은 대체로 새로 관찰되었거나 트래픽이 적습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Impact:EC2/WinRMBruteForce

EC2 인스턴스가 아웃바운드 Windows 원격 관리 무차별 암호 대입 공격을 수행하고 있습니다.

기본 심각도: 낮음*

> **Note**
>
> EC2 인스턴스가 무차별 암호 대입 공격 대상인 경우 이 결과는 심각도가 낮습니다. 무차별 암호 대입 공격을 수행하는 데 작업자가 EC2 인스턴스를 사용하고 있다면 이 결과는 심각도가 높습니다.

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에서 나열된 EC2 인스턴스가 Windows 기반 시스템의 Windows 원격 관리 서비스 액세스하고자 Windows 원격 관리(WinRM) 무차별 암호 대입 공격을 수행하고 있음을 알려줍니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Recon:EC2/PortProbeEMRUnprotectedPort

알려진 악의적 호스트에서 탐색 중인 보호되지 않는 EMR 관련 포트가 EC2 인스턴스에 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 사용자 환경의 클러스터에 속하는 나열된 EC2 인스턴스의 EMR 관련 민감한 포트가 보안 그룹, ACL (액세스 제어 목록) 또는 Linux IPtables와 같은 호스트 방화벽에 의해 차단되지 않았음을 알려줍니다. AWS 또한 이 발견은 인터넷상의 알려진 스캐너가 이 포트를 적극적으로 검색하고 있다는 사실도 알려줍니다. 포트 8088(YARN 웹 UI 포트)과 같이 이 결과를 트리거할 수 있는 포트는 잠재적으로 원격 코드 실행에 사용될 수 있습니다.

해결 권장 사항:

클러스터의 포트에 대한 인터넷으로부터의 개방 액세스를 차단하고, 액세스 범위를 이러한 포트에 대한 액세스를 요구하는 특정 IP 주소로만 제한하는 것을 고려해야 합니다. 자세한 내용은 EMR 클러스터의 보안 그룹을 참조하십시오.

Recon:EC2/PortProbeUnprotectedPort

알려진 악의적 호스트에서 탐색 중인 보호되지 않는 포트가 EC2 인스턴스에 있습니다.

기본 심각도: 낮음*

> **Note**
>
> 이 결과의 기본 심각도는 낮음입니다. 하지만 프로브 대상 포트를 Elasticsearch (9200 또는 9300) 에서 사용하는 경우 검색 결과의 심각도가 높습니다.

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경 내에 나열된 EC2 인스턴스가 보안 그룹, 액세스 제어 목록(ACL) 또는 호스트상의 방화벽(예: Linux IPTables)으로 차단되지 않고 있으며 인터넷에서 알려진 스캐너가 해당 포트를 적극적으로 탐색하고 있음을 나타냅니다.

보호되지 않은 것으로 식별된 포트가 22 또는 3389인데 이러한 포트를 사용하여 인스턴스에 연결하는 경우에도 회사 네트워크 IP 주소 공간의 IP 주소에 대해서만 이러한 포트에 액세스할 수 있도록 허용하여 노출을 제한할 수 있습니다. Linux의 포트 22에 대한 액세스를 제한하려면 Linux 인스턴스의 인바운드 트래픽 권한 부여 단원을 참조하십시오. Windows의 포트 3389에 대한 액세스를 제한하려면 Windows 인스턴스의 인바운드 트래픽 권한 부여 단원을 참조하십시오.

GuardDuty 포트 443과 80에 대해서는 이 검색 결과를 생성하지 않습니다.

해결 권장 사항:

인스턴스가 웹 서버를 호스팅하는 경우와 같이 의도적으로 노출되는 경우가 있을 수 있습니다. AWS 환경에서 이러한 경우 이 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `Recon:EC2/PortProbeUnprotectedPort` 값을 사용해야 합니다. 두 번째 필터 기준은 Bastion Host로 사용되는 인스턴스와 일치해야 합니다. 이러한 도구를 호스팅하는 인스턴스에서 식별 가능한 기준에 따라 인스턴스 이미지 ID 속성 또는 태그 값 속성을 사용할 수 있습니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 섹션을 참조하세요.

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 가능성이 높습니다. 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 단원을 참조하십시오.

Recon:EC2/Portscan

EC2 인스턴스가 원격 호스트에 대한 아웃바운드 포트 스캔을 수행하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경에 단기간에 여러 포트에 대한 연결을 시도하는 가능한 포트 스캔 공격과 관련된 나열된 EC2 인스턴스가 있음을 알려줍니다. 포트 스캔 공격의 목적은 개방 포트를 찾아 머신이 실행 중인 서비스를 파악하고 해당 머신의 운영 체제를 식별하는 것입니다.

해결 권장 사항:

이러한 결과는 환경의 EC2 인스턴스에 취약성 평가 애플리케이션이 배포된 경우 오탐지일 수 있습니다. 이러한 애플리케이션은 포트 스캔을 수행하여 잘못 구성된 열린 포트에 대해 알리기 때문입니다. AWS 환경에서 이러한 경우 이 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `Recon:EC2/Portscan` 값을 사용해야 합니다. 두 번째 필터 기준은 이러한 취약성 평가 도구를 호스팅하는 인스턴스와 일치해야 합니다. 이러한 도구를 호스팅하는 인스턴스에서 식별 가능한 기준에 따라 Instance image ID 속성 또는 Tag 값 속성을 사용할 수 있습니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 섹션을 참조하세요.

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 가능성이 높습니다. 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 단원을 참조하십시오.

Trojan:EC2/BlackholeTraffic

EC2 인스턴스가 블랙홀로 알려진 원격 호스트의 IP 주소와 통신을 시도하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 나열된 EC2 인스턴스가 블랙홀(또는 싱크홀) IP 주소와의 통신을 시도하다가 손상되었을 수 있음을 알려줍니다. 블랙홀은 데이터가 의도한 수신자에게 도달하지 않았음을 소스에 알리지 않고 수신 트래픽 또는 발신 트래픽을 자동으로 취소하는 네트워크의 위치입니다. 블랙홀 IP 주소는 실행되고 있지 않은 호스트 머신 또는 호스트가 할당되지 않은 주소를 지정합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/BlackholeTraffic!DNS

EC2 인스턴스가 블랙홀 IP 주소로 리디렉션 중인 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 중간

- 데이터 소스: DNS 로그

이 결과는 AWS 환경의 나열된 EC2 인스턴스가 블랙홀 IP 주소로 리디렉션 중인 도메인 이름을 쿼리하기 때문에 손상되었을 수 있음을 알려줍니다. 블랙홀은 데이터가 의도한 수신자에게 도달하지 않았음을 소스에 알리지 않고 수신 트래픽 또는 발신 트래픽을 자동으로 취소하는 네트워크의 위치입니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/DGADomainRequest.B

EC2 인스턴스가 알고리즘을 통해 생성된 도메인을 쿼리하는 중입니다. 이러한 도메인은 일반적으로 맬웨어에서 사용되며 손상된 EC2 인스턴스의 표시일 수 있습니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경에 도메인 생성 알고리즘(DGA) 도메인을 쿼리하려고 하는 나열된 EC2 인스턴스가 있음을 알려줍니다. 이 EC2 인스턴스는 손상되었을 수 있습니다.

DGA는 C&C(명령 및 제어) 서버와의 랑데부 지점으로 사용할 수 있는 많은 수의 도메인 이름을 정기적으로 생성하는 데 사용됩니다. 명령 및 제어(C&C) 서버는 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스 모음인 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다. 감염된 컴퓨터가 업데이트 또는 명령을 수신하기 위해 매일 도메인 이름 중 일부에 접속을 시도하기 때문에 잠재적인 랑데부 지점이 많으면 봇넷을 효율적으로 종료하기가 어렵습니다.

> **Note**
>
> 이 결과는 고급 휴리스틱을 통한 도메인 이름 분석을 토대로 하며, 따라서 위협 인텔리전스 피드에 포함되지 않은 새로운 DGA 도메인이 발견될 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/DGADomainRequest.C!DNS

EC2 인스턴스가 알고리즘을 통해 생성된 도메인을 쿼리하는 중입니다. 이러한 도메인은 일반적으로 맬웨어에서 사용되며 손상된 EC2 인스턴스의 표시일 수 있습니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경에 도메인 생성 알고리즘(DGA) 도메인을 쿼리하려고 하는 나열된 EC2 인스턴스가 있음을 알려줍니다. 이 EC2 인스턴스는 손상되었을 수 있습니다.

DGA는 C&C(명령 및 제어) 서버와의 랑데부 지점으로 사용할 수 있는 많은 수의 도메인 이름을 정기적으로 생성하는 데 사용됩니다. 명령 및 제어(C&C) 서버는 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스 모음인 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다. 감염된 컴퓨터가 업데이트 또는 명령을 수신하기 위해 매일 도메인 이름 중 일부에 접속을 시도하기 때문에 잠재적인 랑데부 지점이 많으면 봇넷을 효율적으로 종료하기가 어렵습니다.

> **Note**
>
> 이 결과는 GuardDuty 의 위협 인텔리전스 피드의 알려진 DGA 도메인을 기반으로 합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/DNSDataExfiltration

EC2 인스턴스가 DNS 쿼리를 통해 데이터를 유출시키고 있습니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경에 아웃바운드 데이터 전송에 DNS 쿼리를 사용하는 맬웨어를 실행 중인 나열된 EC2 인스턴스가 있음을 알려줍니다. 이러한 유형의 데이터 전송은 인스턴스 손상을 나타내며 데이터 유출로 이어질 수 있습니다. DNS 트래픽은 일반적으로 방화벽으로 차단되지 않습니다. 예를 들어, 손상된 EC2 인스턴스에 있는 맬웨어는 데이터(예: 신용카드 번호)를 DNS 쿼리로 인코딩해 공격자가 제어하는 원격 DNS 서버로 전송할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/DriveBySourceTraffic!DNS

EC2 인스턴스가 드라이브 바이(Drive-By) 다운로드 공격의 알려진 소스인 원격 호스트의 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경의 나열된 EC2 인스턴스가 드라이브 바이 다운로드 공격의 알려진 소스인 원격 호스트의 도메인 이름을 쿼리하기 때문에 손상되었을 수 있음을 알려줍니다. 인터넷에서 이러한 컴퓨터 소프트웨어의 의도치 않은 다운로드로 인해 바이러스, 스파이웨어 또는 맬웨어가 자동으로 설치될 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/DropPoint

EC2 인스턴스가 맬웨어를 통해 캡처된 자격 증명 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 IP 주소와 통신을 시도하는 중입니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 EC2 인스턴스가 맬웨어를 통해 캡처된 보안 인증 정보 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 IP 주소와 통신을 시도 중임을 알립니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/DropPoint!DNS

EC2 인스턴스가 맬웨어를 통해 캡처된 자격 증명 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 중간

- 데이터 소스: DNS 로그

이 결과는 AWS 환경의 EC2 인스턴스가 맬웨어를 통해 캡처된 보안 인증 정보 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 도메인 이름을 쿼리하는 중임을 알립니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Trojan:EC2/PhishingDomainRequest!DNS

EC2 인스턴스가 피싱 공격과 관련된 도메인을 쿼리하는 중입니다. 이 EC2 인스턴스는 손상되었을 수 있습니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경에 피싱 공격과 관련된 도메인을 쿼리하려고 하는 EC2 인스턴스가 있음을 알려줍니다. 피싱 도메인은 개인이 개인 식별 정보, 은행 및 신용 카드 세부 정보, 암호 등의 중요한 데이터 제공을 유도하기 위해 합법적인 기관으로 위장한 사람이 설정한 도메인입니다. EC2 인스턴스에서 피싱

웹 사이트에 저장된 민감한 데이터를 검색하려고 하거나 피싱 웹 사이트를 설정하려고 할 수 있습니다. 이 EC2 인스턴스는 손상되었을 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

EC2 인스턴스가 사용자 지정 위협 목록에 있는 IP 주소에 연결하고 있습니다.

기본 심각도: 중간

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 EC2 인스턴스가 사용자가 업로드한 위협 목록에 포함된 IP 주소를 사용하여 통신 중임을 알려줍니다. GuardDuty에서 위험 목록은 알려진 악성 IP 주소로 이루어져 있습니다. GuardDuty에서는 업로드된 위협 목록을 기반으로 결과를 생성합니다. 이 결과를 생성하는 데 사용된 위협 목록은 결과의 세부 정보에 나열됩니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

UnauthorizedAccess:EC2/MetadataDNSRebind

EC2 인스턴스가 인스턴스 메타데이터 서비스로 확인되는 DNS 조회를 수행하고 있습니다.

기본 심각도: 높음

- 데이터 소스: DNS 로그

이 결과는 AWS 환경에 EC2 메타데이터 IP 주소(169.254.169.254)로 확인되는 도메인을 쿼리하는 EC2 인스턴스가 있음을 알려줍니다. 이러한 종류의 DNS 쿼리는 인스턴스가 DNS 리바인딩 기술의 대

상임을 나타낼 수 있습니다. 이 기술은 인스턴스와 연결된 IAM 보안 인증 정보를 포함하여 EC2 인스턴스의 메타데이터를 가져오는 데 사용할 수 있습니다.

DNS 리바인딩은 URL의 도메인 이름이 EC2 메타데이터 IP 주소(169.254.169.254)로 확인되는 URL의 리턴 데이터를 로드하도록 EC2 인스턴스에서 실행 중인 애플리케이션을 속이는 작업이 포함됩니다. 이렇게 하면 애플리케이션에서 EC2 메타데이터에 액세스하여 공격자가 사용 가능하도록 만듭니다.

EC2 인스턴스가 URL을 삽입할 수 있도록 취약한 애플리케이션을 실행 중인 경우 또는 다른 누군가가 EC2 인스턴스에서 실행 중인 웹 브라우저에서 URL에 액세스하는 경우에만 DNS 리바인딩을 사용하여 EC2 메타데이터에 액세스할 수 있습니다.

해결 권장 사항:

이 결과에 대한 응답으로, EC2 인스턴스에서 실행 중인 취약한 애플리케이션이 있는지 여부 또는 다른 누군가가 브라우저를 사용하여 결과에서 확인된 도메인에 액세스했는지 여부를 평가해야 합니다. 근본 원인이 취약한 애플리케이션인 경우, 취약성을 수정해야 합니다. 누군가 식별된 도메인을 검색한 경우 도메인을 차단하거나 사용자 액세스를 방지해야 합니다. 결과가 위의 경우 중 하나와 관련된 것으로 확인된다면 EC2 인스턴스와 연결된 세션을 취소하세요.

일부 AWS 고객이 의도적으로 메타데이터 IP 주소를 권한 DNS 서버의 도메인 이름에 매핑합니다. 환경에서 이러한 경우 이 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `UnauthorizedAccess:EC2/MetaDataDNSRebind` 값을 사용해야 합니다. 두 번째 필터 조건은 DNS request domain(DNS 요청 도메인)이어야 하며 값은 메타데이터 IP 주소(169.254.169.254)에 매핑한 도메인과 일치해야 합니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 단원을 참조하십시오.

UnauthorizedAccess:EC2/RDPBruteForce

EC2 인스턴스가 RDP 무차별 암호 대입 공격에 관여했습니다.

기본 심각도: 낮음*

> **Note**
>
> EC2 인스턴스가 무차별 암호 대입 공격 대상인 경우 이 결과는 심각도가 낮습니다. 무차별 암호 대입 공격을 수행하는 데 작업자가 EC2 인스턴스를 사용하고 있다면 이 결과는 심각도가 높습니다.

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 EC2 인스턴스가 Windows 기반 시스템의 RDP 서비스에 대한 암호를 얻기 위한 목적으로 무차별 암호 대입 공격에 관여했음을 알려줍니다. 이는 AWS 리소스에 대한 무단 액세스를 나타낼 수 있습니다.

해결 권장 사항:

인스턴스의 리소스 역할이 `ACTOR`인 경우, 인스턴스가 RDP 무차별 암호 대입 공격을 수행하는 데 사용되었음을 나타냅니다. 이 인스턴스가 `Target`으로 나열된 IP 주소에 접속해야 하는 정당한 이유가 없는 경우, 인스턴스가 손상되었다고 가정하고 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션의 작업을 수행하는 것이 좋습니다.

인스턴스의 리소스 역할이 `TARGET`인 경우에는 보안 그룹, ACL 또는 방화벽을 통해 신뢰할 수 있는 IP에 대해서만 RDP 포트를 보호하여 이 결과에 명시된 문제를 해결할 수 있습니다. 자세한 내용은 Tips for securing your EC2 instances(Linux)를 참조하세요.

UnauthorizedAccess:EC2/SSHBruteForce

EC2 인스턴스가 SSH 무차별 암호 대입 공격에 관여했습니다.

기본 심각도: 낮음*

> **Note**
>
> 무차별 암호 대입 공격이 EC2 인스턴스 중 하나를 표적으로 할 경우 이 결과는 심각도가 낮습니다. EC2 인스턴스가 무차별 암호 대입 공격을 수행하는 데 사용되고 있다면 이 결과는 심각도가 높습니다.

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 EC2 인스턴스가 Linux 기반 시스템의 SSH 서비스에 대한 암호를 얻기 위한 목적으로 행해진 무차별 암호 대입 공격에 관여했음을 알려줍니다. 이는 AWS 리소스에 대한 무단 액세스를 나타낼 수 있습니다.

> **Note**
>
> 이 조사 결과는 포트 22에서 트래픽을 모니터링 중인 만을 통해 생성된 것입니다. 다른 포트를 사용하도록 SSH 서비스를 구성한 경우, 이 조사 결과는 생성되지 않습니다.

해결 권장 사항:

무차별 암호 대입 시도의 대상이 Bastion Host인 경우 이는 AWS 환경에서 예상되는 동작일 수 있습니다. 이 경우 이 결과에 대해 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `UnauthorizedAccess:EC2/SSHBruteForce` 값을 사용해야 합니다. 두 번째 필터 기준은 Bastion Host로 사용되는 인스턴스와 일치해야 합니다. 이러한 도구를 호스팅하는 인스턴스에서 식별 가능한 기준에 따라 인스턴스 이미지 ID 속성 또는 태그 값 속성을 사용할 수 있습니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 섹션을 참조하세요.

이 활동이 환경에서 예기치 않게 발생했고 인스턴스의 인스턴스 역할이 `TARGET`인 경우에는 보안 그룹, ACL 또는 방화벽을 통해 신뢰할 수 있는 IP에 대해서만 SSH 포트를 보호하여 이 결과에 명시된 문제를 해결할 수 있습니다. 자세한 내용은 Tips for securing your EC2 instances(Linux)를 참조하세요.

인스턴스의 리소스 역할이 `ACTOR`인 경우, 인스턴스가 SSH 무차별 암호 대입 공격을 수행하는 데 사용되었음을 나타냅니다. 이 인스턴스가 `Target`으로 나열된 IP 주소에 접속해야 하는 정당한 이유가 없는 경우, 인스턴스가 손상되었다고 가정하고 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션의 작업을 수행하는 것이 좋습니다.

UnauthorizedAccess:EC2/TorClient

EC2 인스턴스가 Tor Guard 또는 Authority 노드에 연결하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 EC2 인스턴스가 Tor Guard 또는 Authority 노드에 연결함을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, Tor Guards 및 Authority 노드는 Tor 네트워크의 첫 번째 게이트웨이 역할을 합니다. 이 트래픽은 EC2 인스턴스가 손상되어 Tor 네트워크에서 클라이언트 역할을 하고 있음을 나타냅니다. 이는 공격자의 실제 신원을 숨기려는 의도를 갖고 AWS 리소스에 무단으로 액세스하려 함을 나타낼 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

UnauthorizedAccess:EC2/TorRelay

EC2 인스턴스가 Tor 릴레이로 Tor 네트워크에 연결하고 있습니다.

기본 심각도: 높음

- 데이터 소스: VPC 흐름 로그

이 결과는 AWS 환경의 EC2 인스턴스가 Tor 네트워크에 Tor 릴레이 역할을 수행하는 방식으로 연결함을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, Tor는 한 Tor 릴레이에서 다른 릴레이로 클라이언트의 불법 가능성이 있는 트래픽을 전달함으로써 통신의 익명성을 높입니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결을(를) 참조하세요.

GuardDuty IAM 검색 유형

다음 결과는 IAM 엔터티 및 액세스 키에만 해당되며 항상 리소스 유형이 `AccessKey`입니다. 결과의 심각도 및 세부 정보는 결과 유형에 따라 다릅니다.

여기에 나열된 결과에는 해당 결과 유형을 생성하는 데 사용된 데이터 소스 및 모델이 포함됩니다. 자세한 설명은 기본 데이터 소스 섹션을 참조하세요.

모든 IAM 관련 결과에 대해서는 해당 엔터티를 검사하여 엔터티의 권한이 최소 권한 모범 사례를 따르는지 확인하는 것이 좋습니다. 예상하지 못한 활동인 경우 보안 인증 정보가 손상되었을 수 있습니다. 결과 해결에 대한 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

주제

- CredentialAccess:IAMUser/AnomalousBehavior

- DefenseEvasion:IAMUser/AnomalousBehavior
- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

AWS 환경에 대한 액세스 권한을 얻는 데 사용된 API가 비정상적인 방식으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 관찰되는 API는 일반적으로 공격자가 환경의 암호, 사용자 이름 및 액세스 키를 수집하려고 시도하는 공격의 보안 인증 정보 액세스 단계와 관련이 있습니다. 이 범주의 API는 `GetPasswordData`, `GetSecretValue` 및 `GenerateDbAuthToken`입니다.

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

DefenseEvasion:IAMUser/AnomalousBehavior

방어 조치를 우회하는 데 사용된 API가 변칙적인 방식으로 간접 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 관찰된 API는 일반적으로 공격자가 자신의 흔적을 감추고 탐지를 피하려는 방어 우회 전략과 관련이 있습니다. 이 범주의 API는 일반적으로 delete, disable 또는 stop 작업입니다(예: `DeleteFlowLogs`, `DisableAlarmActions` 또는 `StopLogging`).

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Discovery:IAMUser/AnomalousBehavior

리소스를 검색하는 데 일반적으로 사용되는 API가 변칙적인 방식으로 간접 호출되었습니다.

기본 심각도: 낮음

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 관찰된 API는 일반적으로 공격자가 사용자 AWS 환경이 광범위한 공격에 취약한지 여부를 판단하기 위해 정보를 수집하는 공격의 탐지 단계와 관련이 있습니다. 이 범주의 API는 일반적으로 get, describe 또는 list 작업입니다(예: `DescribeInstances`, `GetRolePolicy` 또는 `ListAccessKeys`).

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에서 변칙 요청으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Exfiltration:IAMUser/AnomalousBehavior

AWS 환경에서 데이터를 수집하는 데 일반적으로 사용되는 API가 비정상적인 방식으로 호출되었습니다.

기본 심각도: 높음

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 관찰된 API는 일반적으로 공격자가 탐지를 피하기 위해 패키징 및 암호화를 사용하여 네트워크에서 데이터를 수집하려는 유출 전략과 관련이 있습니다. 이 결과 유형의 API는 management(control-plane) 작업만 있으며, 대체로 S3, 스냅샷 및 데이터베이스와 관련이 있습니다(예: `PutBucketReplication`, `CreateSnapshot` 또는 `RestoreDBInstanceFromDBSnapshot`).

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Impact:IAMUser/AnomalousBehavior

AWS 환경의 데이터나 프로세스를 변조하는 데 일반적으로 사용되는 API가 변칙적인 방식으로 호출되었습니다.

기본 심각도: 높음

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 관찰된 API는 일반적으로 공격자가 운영을 방해하고 계정의 데이터를 조작, 방해 또는 파괴하려는 공격 전략과 관련이 있습니다. 이 결과 유형의 API는 일반적으로 delete, update 또는 put 작업입니다(예: `DeleteSecurityGroup`, `UpdateUser` 또는 `PutBucketPolicy`).

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

InitialAccess:IAMUser/AnomalousBehavior

AWS 환경에 대한 무단 액세스를 얻기 위해 일반적으로 사용되는 API가 변칙적인 방식으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 관찰되는 API는 일반적으로 공격자가 환경의 액세스 설정을 시도하는 공격의 초기 액세스 단계와 관련이 있습니다. 이 범주의 API는 일반적으로 get token 또는 session 작업입니다(예: `GetFederationToken`, `StartSession` 또는 `GetAuthorizationToken`).

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

PenTest:IAMUser/KaliLinux

Kali Linux 시스템에서 API가 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 Kali Linux를 실행하는 컴퓨터가 사용자 환경에 나열된 AWS 계정에 속하는 자격 증명을 사용하여 API 호출을 수행하고 있음을 알려줍니다. Kali Linux는 보안 전문가가 패치가 필요한 EC2 인스턴스의 약점을 식별하기 위해 널리 사용하는 침투 테스트 도구입니다. 또한 공격자는 이 도구를 사용하여 EC2 구성 취약점을 찾아 사용자 환경에 무단으로 액세스합니다. AWS

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

PenTest:IAMUser/ParrotLinux

Parrot Security Linux 머신에서 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 Parrot Security Linux를 실행하는 시스템이 사용자 환경에 나열된 AWS 계정에 속하는 자격 증명을 사용하여 API 호출을 수행하고 있음을 알려줍니다. Parrot Security Linux는 보안 전문가가 패치가 필요한 EC2 인스턴스의 약점을 식별하기 위해 널리 사용하는 침투 테스트 도구입니다. 또한 공격자는 이 도구를 사용하여 EC2 구성 약점을 찾아 사용자 환경에 무단으로 액세스합니다. AWS

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

PenTest:IAMUser/PentooLinux

Pentoo Linux 머신에서 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 Pentoo Linux를 실행하는 컴퓨터가 사용자 환경에 나열된 AWS 계정에 속하는 자격 증명을 사용하여 API 호출을 수행하고 있음을 알려줍니다. Pentoo Linux는 보안 전문가가 패치가 필요한 EC2

인스턴스의 약점을 식별하기 위해 널리 사용하는 침투 테스트 도구입니다. 또한 공격자는 이 도구를 사용하여 EC2 구성 약점을 찾아 사용자 환경에 무단으로 액세스합니다. AWS

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Persistence:IAMUser/AnomalousBehavior

AWS 환경에 대한 무단 액세스를 유지하는 데 일반적으로 사용되는 API가 변칙적인 방식으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 일반적으로 관찰되는 API는 공격자가 환경에 대한 액세스 권한을 획득하고 이를 유지하려고 하는 지속성 전략과 관련이 있습니다. 이 범주의 API는 일반적으로 create, import 또는 modify 작업입니다(예: `CreateAccessKey`, `ImportKeyPair` 또는 `ModifyInstanceAttribute`).

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Policy:IAMUser/RootCredentialUsage

루트 사용자 보안 인증 정보를 사용하여 API가 간접적으로 호출되었습니다.

기본 심각도: 낮음

- 데이터 소스: CloudTrail 관리 이벤트 또는 데이터 이벤트 CloudTrail

이 결과는 환경에서 나열된 AWS 계정 의 루트 사용자 로그인 보안 인증 정보가 AWS 서비스 요청에 사용되고 있음을 알려줍니다. 사용자는 루트 사용자 로그인 자격 증명을 사용하여 AWS 서비스에 액세스하지 않는 것이 좋습니다. 대신 AWS Security Token Service (STS) 의 최소 권한 임시 자격 증명을 사용하여 AWS 서비스에 액세스해야 합니다. AWS STS 가 지원되지 않는 상황에서는 IAM 사용자 보안 인증 정보가 권장됩니다. 자세한 내용은 IAM 모범 사례 단원을 참조하십시오.

> **Note**
>
> 계정에 대해 S3 위협 탐지가 활성화된 경우 AWS 계정의 루트 사용자 로그인 보안 인증 정보를 사용하여 S3 리소스에서 S3 데이터 플레인 작업을 실행하려는 시도에 대한 응답으로 이 결과가 생성될 수 있습니다. 사용된 API 호출은 결과 세부 정보에 나열됩니다. S3 위협 탐지가 활성화되지 않은 경우 이 결과는 이벤트 로그 API에 의해서만 트리거될 수 있습니다. S3 위협 탐지에 대한 자세한 내용은 S3 보호를 참조하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

PrivilegeEscalation:IAMUser/AnomalousBehavior

AWS 환경에 대한 높은 수준의 권한을 얻기 위해 일반적으로 사용되는 API가 변칙적인 방식으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 계정에서 변칙적인 API 요청이 관찰되었음을 알려줍니다. 이 결과에는 단일 사용자 자격 증명 근처에서 이루어진 단일 API 또는 일련의 관련 API 요청이 포함될 수 있습니다. 관찰된 API는 일반적으로 공격자가 환경에 대해 더 높은 수준의 권한을 얻으려고 시도하는 권한 상승 전략과 관련이 있

습니다. 이 범주의 API에는 일반적으로 IAM 정책, 역할 및 사용자를 변경하는 작업이 포함됩니다(예: `AssociateIamInstanceProfile`, `AddUserToGroup` 또는 `PutUserPolicy`).

이 API 요청은 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Recon:IAMUser/MaliciousIPCaller

알려진 악의적인 IP 주소에서 API가 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 환경 내 계정의 AWS 리소스를 나열 또는 설명할 수 있는 API 작업이 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 공격자는 더 중요한 자격 증명을 찾거나 이미 보유한 자격 증명의 기능을 파악하기 위해 훔친 자격 증명을 사용하여 이러한 유형의 AWS 리소스 정찰을 수행할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Recon:IAMUser/MaliciousIPCaller.Custom

알려진 악의적인 IP 주소에서 API가 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 환경 내 계정의 AWS 리소스를 나열 또는 설명할 수 있는 API 작업이 사용자 지정 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 사용된 위협 목록은 결과의 세부 정보에 나열됩니다. 공격자는 더 중요한 자격 증명을 찾거나 이미 보유한 자격 증명의 기능을 파악하기 위해 도난당한 자격 증명을 사용하여 이러한 유형의 AWS 리소스 정찰을 수행할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Recon:IAMUser/TorIPCaller

Tor 출구 노드(Tor exit node) IP 주소에서 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 환경 내 계정의 AWS 리소스를 나열 또는 설명할 수 있는 API 작업이 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 공격자는 Tor를 사용하여 자신의 실제 정체를 숨길 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail 로깅이 비활성화되었습니다.

기본 심각도: 낮음

- 데이터 소스: CloudTrail 관리 이벤트

이 발견을 통해 AWS 환경 내 CloudTrail 트레일이 비활성화되었음을 알 수 있습니다. 이는 공격자가 악의적인 의도로 AWS 리소스에 대한 액세스 권한을 얻으려고 하는 동시에 자신의 활동 흔적을 덮어 없

애기 위해 로깅을 비활성화한 시도일 수 있습니다. 이 조사 결과는 추적이 성공적으로 삭제되거나 업데이트되었을 때 트리거될 수 있습니다. 연결된 트레일에서 로그를 저장하는 S3 버킷을 성공적으로 삭제해도 이 검색 결과가 트리거될 수 있습니다. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Stealth:IAMUser/PasswordPolicyChange

계정 암호 정책이 취약합니다.

기본 심각도: 낮음*

> **Note**
> 이 결과의 심각도는 암호 정책 변경의 심각도에 따라 낮음, 보통 또는 높음일 수 있습니다.

- 데이터 소스: CloudTrail 관리 이벤트

사용자 AWS 환경 내에 나열된 AWS 계정의 계정 암호 정책이 약화되었습니다. 예를 들어, 정책이 삭제되었거나, 문자를 몇 개만 요구하거나, 기호 및 숫자를 요구하지 않거나, 암호 만료 기간 연장을 요구하도록 수정되었습니다. 이 결과는 AWS 계정 암호 정책을 업데이트하거나 삭제하려는 시도에 의해서도 발생할 수 있습니다. AWS 계정 암호 정책은 IAM 사용자에게 설정할 수 있는 암호 종류를 제어하는 규칙을 정의합니다. 암호 정책이 약할수록 기억하기 쉽고 추측하기 쉬워 보안 위험을 일으킬 수 있는 암호 생성을 허용합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

전 세계에서 여러 번의 성공적인 콘솔 로그인이 관찰되었습니다.

기본 심각도: 중간

- 데이터 소스: 관리 이벤트 CloudTrail

이 조사 결과는 다양한 지역에서 동시에 동일한 IAM 사용자에 대한 여러 번의 성공적인 콘솔 로그인이 관찰되었음을 알려 줍니다. 이러한 변칙적이고 위험한 액세스 위치 패턴은 리소스에 대한 무단 액세스 가능성이 있음을 나타냅니다. AWS

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

인스턴스 시작 역할을 통해 EC2 인스턴스에 대해 단독으로 생성된 보안 인증 정보가 AWS내 다른 계정에서 사용 중입니다.

기본 심각도: 높음*

> **Note**
>
> 이 결과의 기본 심각도는 높음입니다. 하지만 AWS 환경과 관련된 계정에서 API를 호출한 경우 심각도는 보통입니다.

- 데이터 소스: CloudTrail 관리 이벤트 또는 S3 데이터 이벤트

이 결과는 연결된 EC2 인스턴스가 실행되고 있는 계정과 다른 AWS 계정이 소유한 IP 주소에서 API를 호출하는 데 EC2 인스턴스 자격 증명이 사용되는 경우를 알려줍니다.

AWS 임시 자격 증명을 생성한 엔티티 (예: AWS 애플리케이션, EC2 또는 Lambda) 외부에 임시 자격 증명을 재배포하는 것은 권장하지 않습니다. 하지만 권한이 있는 사용자는 EC2 인스턴스에서 자격 증명을 내보내 합법적으로 API를 호출할 수 있습니다. `remoteAccountDetails.Affiliated`필드가 인 경우 `True` 해당 환경과 연결된 계정에서 API를 호출한 것입니다. AWS 잠재적인 공격을 배제하고 활동의 적법성을 확인하려면 이러한 자격 증명이 할당된 IAM 사용자에게 문의하십시오.

> **Note**
>
> 원격 계정에서 지속적인 활동을 GuardDuty 관찰하면 머신 러닝 (ML) 모델이 이를 예상된 동작으로 식별합니다. 따라서 GuardDuty 해당 원격 계정에서의 활동에 대한 결과 생성이 중단됩니다. GuardDuty 다른 원격 계정의 새로운 행동에 대한 결과를 계속 생성하고 시간이 지남에 따라 행동이 변화함에 따라 학습된 원격 계정을 재평가할 것입니다.

해결 권장 사항:

이 결과에 따라 다음 워크플로를 사용하여 어떤 방법을 사용할지 결정할 수 있습니다.

1. `service.action.awsApiCallAction.remoteAccountDetails.accountId` 필드에서 관련된 원격 계정을 식별합니다.
2. 다음으로, 해당 계정이 현재 GuardDuty 환경과 연계되어 있는지 `service.action.awsApiCallAction.remoteAccountDetails.affiliated` 현장에서 확인해 보세요.
3. 계정이 연결되어 있는 경우 원격 계정 소유자와 EC2 인스턴스 보안 인증 정보 소유자에게 문의하여 조사합니다.
4. 계정이 제휴되지 않은 경우 먼저 해당 계정이 조직에 연결되어 있지만 GuardDuty 다중 계정 설정의 일부가 아니거나 계정에서 아직 활성화되지 않았는지 GuardDuty 여부를 평가하십시오. 그렇지 않은 경우 EC2 보안 인증 정보 소유자에게 문의하여 원격 계정에서 이러한 보안 인증 정보를 사용할 수 있는 사용 사례가 있는지 확인합니다.
5. 보안 인증 정보의 소유자가 원격 계정을 알지 못하는 경우 AWS내에서 활동하는 위협 작업자가 보안 인증 정보를 침해했을 수 있습니다. 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결에서 권장하는 단계를 통해 환경을 보호해야 합니다. 또한 AWS 신뢰 및 안전 팀에 악용 보고서를 제출하여 원격 계정에 대한 조사를 시작할 수 있습니다. AWS Trust and Safety에 신고를 제출할 때는 결과의 전체 JSON 세부 정보를 포함해야 합니다.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

인스턴스 시작 역할을 통해 EC2 인스턴스에 대해 단독으로 생성된 자격 증명이 외부 IP 주소에서 사용 중입니다.

기본 심각도: 높음

- 데이터 소스: CloudTrail 관리 이벤트 또는 S3 데이터 이벤트

이 결과는 외부의 호스트가 사용자 환경의 EC2 인스턴스에 생성된 임시 AWS 자격 증명을 사용하여 AWS API 작업을 실행하려고 AWS 시도했음을 알려줍니다. AWS 목록에 있는 EC2 인스턴스가 손상되었을 수 있으며 이 인스턴스의 임시 자격 증명이 외부의 원격 호스트로 유출되었을 수 있습니다. AWS AWS 임시 자격 증명을 생성한 엔티티 (예: AWS 애플리케이션, EC2 또는 Lambda) 외부에 임시 자격 증명을 재배포하는 것은 권장하지 않습니다. 하지만 권한이 있는 사용자는 EC2 인스턴스에서 자격 증명을 내보내 합법적으로 API를 호출할 수 있습니다. 잠재적 공격을 배제하고 활동의 적법성을 확인하려면 결과에 있는 원격 IP의 인스턴스 보안 인증 정보의 사용이 예상된 것인지 검증하세요.

> **Note**
>
> 원격 계정에서 지속적인 활동을 GuardDuty 관찰하면 머신 러닝 (ML) 모델은 이를 예상된 동작으로 식별합니다. 따라서 GuardDuty 해당 원격 계정에서의 활동에 대한 결과 생성이 중단됩니다. GuardDuty 다른 원격 계정의 새로운 행동에 대한 결과를 계속 생성하고 시간이 지남에 따라 행동이 변화함에 따라 학습된 원격 계정을 재평가할 것입니다.

해결 권장 사항:

이 결과는 네트워킹이 인터넷 트래픽을 라우팅하도록 구성되어 VPC 인터넷 게이트웨이(IGW)가 아닌 온프레미스 게이트웨이에서 나가는 경우에 생성됩니다. AWS Outposts 또는 VPC VPN 연결을 사용하는 것과 같은 일반적인 구성으로 인해 트래픽이 이러한 방식으로 라우팅될 수 있습니다. 예상된 동작인 경우 억제 규칙을 사용하고 두 개의 필터 기준으로 구성된 규칙을 만드는 것이 좋습니다. 첫 번째 기준은 결과 유형으로 `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`이어야 합니다. 두 번째 필터 기준은 온프레미스 인터넷 게이트웨이의 IP 주소 또는 CIDR 범위를 포함하는 API 호출자 IPv4 주소입니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙 단원을 참조하십시오.

> **Note**
>
> 외부 소스로부터 지속적인 활동을 GuardDuty 관찰하면 머신 러닝 모델은 이를 예상된 동작으로 식별하고 해당 소스의 활동에 대한 결과 생성을 중단합니다. GuardDuty 계속해서 다른 출처에서 새로운 행동에 대한 결과를 도출하고 시간이 지남에 따라 행동이 변화함에 따라 학습된 출처를 재평가할 것입니다.

이 활동이 예기치 않게 발생한 경우 자격 증명이 손상되었을 수 있습니다. 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 단원을 참조하십시오.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

알려진 악의적인 IP 주소에서 API가 호출되었습니다.

기본 심각도: 중간

- 데이터 출처: CloudTrail 관리 이벤트

이 탐지 결과는 알려진 악성 IP 주소에서 API 작업 (예: EC2 인스턴스 시작, 새 IAM 사용자 생성 또는 AWS 권한 수정 시도) 이 호출되었음을 알려줍니다. 이는 환경 내 AWS 리소스에 대한 무단 액세스를 의미할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

사용자 지정 위협 목록의 IP 주소에서 API를 호출했습니다.

기본 심각도: 중간

- 데이터 소스: CloudTrail 관리 이벤트

이 탐지 결과는 업로드한 위협 목록에 포함된 IP 주소에서 API 작업 (예: EC2 인스턴스 시작, 새 IAM 사용자 생성 또는 AWS 권한 수정 시도) 이 호출되었음을 알려줍니다. 위협 목록은 알려진 악성 IP 주소로 구성됩니다. 이는 환경 내 AWS 리소스에 대한 무단 액세스를 의미할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 설명은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

UnauthorizedAccess:IAMUser/TorIPCaller

Tor 출구 노드(Tor exit node) IP 주소에서 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: CloudTrail 관리 이벤트

이 결과는 Tor 출구 노드 IP 주소에서 API 작업(예: EC2 인스턴스를 시작, 새 IAM 사용자를 생성 또는 AWS 권한을 수정하려는 시도)이 간접적으로 호출되었음을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 신원을 숨기려는 의도를 갖고 AWS 리소스에 무단으로 액세스하려 함을 나타낼 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS을(를) 참조하세요.

EKS 감사 로그 찾기 유형

다음 결과는 Kubernetes 리소스에만 해당되며 항상 resource_type이 `EKSCluster`입니다. 결과의 심각도 및 세부 정보는 결과 유형에 따라 다릅니다.

모든 Kubernetes 유형 결과에 대해 해당 리소스를 검토하여 활동이 예상된 것인지 또는 잠재적으로 악의적일 수 있는지 확인하는 것이 좋습니다. 발견으로 식별된 손상된 Kubernetes 리소스를 수정하는 방법에 대한 지침은 을 참조하십시오. GuardDuty EKS 감사 로그 모니터링 결과 해결

> **Note**
>
> 이러한 결과 생성의 원인이 된 활동이 예상된 활동일 경우 향후 알림을 방지하기 위해 억제 규칙 추가를 고려해 보세요.

주제

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller

- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> 쿠버네티스 버전 1.14 이전에는 그룹이 기본적으로 연결되어 있었습니다. `system:unauthenticated` `system:discovery` `system:basic-user` ClusterRoles 이 연결로 인해 익명 사용자의 의도하지 않은 액세스가 허용될 수 있습니다. 클러스터 업데이트를 통해 이러한 권한을 철회되지 않습니다. 클러스터를 버전 1.14 이상으로 업데이트한 경우에도 이러한 권한은 계속 활성화될 수 있습니다. `system:unauthenticated` 그룹에서 이러한 권한을 분리하는 것이 좋습니다. 이러한 권한 취소에 대한 지침은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오.

CredentialAccess:Kubernetes/MaliciousIPCaller

Kubernetes 클러스터의 보안 인증 정보나 보안 암호에 액세스하는 데 일반적으로 사용되는 API가 알려진 악성 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 API 작업이 간접적으로 호출되었음을 알려줍니다. 관찰되는 API는 일반적으로 공격자가 Kubernetes 클러스터의 암호, 사용자 이름 및 액세스 키를 수집하려고 시도하는 공격의 보안 인증 정보 액세스 전략과 관련이 있습니다.

해결 권장 사항:

사용자가 *`KubernetesUserDetails`* 섹션의 결과에 다음과 같다고 보고한 경우*`system:anonymous`*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Kubernetes 클러스터의 보안 인증 정보나 보안 암호에 액세스하는 데 일반적으로 사용되는 API가 사용자 지정 위협 목록에서 간접적으로 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 API 작업이 사용자가 업로드한 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이 결과와 관련된 위협 목록은 결과 세부 정보의 추가 정보 섹션에 나열됩니다. 관찰되는 API는 일반적으로 공격자가 Kubernetes 클러스터의 암호, 사용자 이름 및 액세스 키를 수집하려고 시도하는 공격의 보안 인증 정보 액세스 전략과 관련이 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우 Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. *system:anonymous* 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

인증되지 않은 사용자가 Kubernetes 클러스터의 보안 인증 정보나 보안 암호에 액세스하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 높음

- 특징: EKS 감사 로그

이 결과는 `system:anonymous` 사용자가 API 작업을 성공적으로 간접 호출했음을 알려줍니다. `system:anonymous`의 API 호출이 인증되지 않았습니다. 관찰되는 API는 일반적으로 공격자가 Kubernetes 클러스터의 암호, 사용자 이름 및 액세스 키를 수집하려고 시도하는 공격의 보안 인증 정보 액세스 전략과 관련이 있습니다. 이 활동은 결과에 보고된 API 작업에서 익명 또는 인증되지 않은 액세스가 허용되고 다른 작업에서 허용될 수 있음을 나타냅니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

해결 권장 사항:

클러스터의 `system:anonymous` 사용자에게 부여된 권한을 검사하고 모든 권한이 필요한지 여부를 확인해야 합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자의 액세스를 철회하고 공격자가

클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오.

자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

CredentialAccess:Kubernetes/TorIPCaller

Kubernetes 클러스터의 보안 인증 정보나 보안 암호에 액세스하는 데 일반적으로 사용되는 API가 알려진 Tor 출구 노드 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 API 작업이 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 관찰되는 API는 일반적으로 공격자가 Kubernetes 클러스터의 암호, 사용자 이름 및 액세스 키를 수집하려고 시도하는 공격의 보안 인증 정보 액세스 전략과 관련이 있습니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 신원을 숨기려는 의도를 갖고 Kubernetes 클러스터 리소스에 무단으로 액세스하려 함을 나타낼 수 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

DefenseEvasion:Kubernetes/MaliciousIPCaller

방어 조치를 우회하는 데 일반적으로 사용되는 API가 알려진 악성 IP 주소에서 간접 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 API 작업이 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 자신의 행동을 감추고 탐지를 피하려는 방어 우회 전략과 관련이 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

방어 조치를 우회하는 데 일반적으로 사용되는 API가 사용자 지정 위협 목록의 IP 주소에서 간접 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 API 작업이 사용자가 업로드한 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이 결과와 관련된 위협 목록은 결과 세부 정보의 추가 정보 섹션에 나열됩니다. 관찰된 API는 일반적으로 공격자가 자신의 행동을 감추고 탐지를 피하려는 방어 우회 전략과 관련이 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

인증되지 않은 사용자가 방어 조치를 우회하는 데 일반적으로 사용되는 API를 간접 호출했습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 `system:anonymous` 사용자가 API 작업을 성공적으로 간접 호출했음을 알려줍니다. `system:anonymous`의 API 호출이 인증되지 않았습니다. 관찰된 API는 일반적으로 공격자가 자신의 행동을 감추고 탐지를 피하려는 방어 우회 전략과 관련이 있습니다. 이 활동은 결과에 보고된 API 작업에서 익명 또는 인증되지 않은 액세스가 허용되고 다른 작업에서 허용될 수 있음을 나타냅니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

해결 권장 사항:

클러스터의 `system:anonymous` 사용자에게 부여된 권한을 검사하고 모든 권한이 필요한지 여부를 확인해야 합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자의 액세스를 철회하고 공격자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오.

자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

DefenseEvasion:Kubernetes/TorIPCaller

방어 조치를 우회하는 데 일반적으로 사용되는 API가 Tor 출구 노드 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 API 작업이 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 자신의 행동을 감추고 탐지를 피하려는 방어 우회 전략과 관련이 있습니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 신원을 숨기려는 의도를 갖고 Kubernetes 클러스터에 무단으로 액세스하려 함을 나타낼 수 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Discovery:Kubernetes/MaliciousIPCaller

Kubernetes 클러스터에서 리소스를 검색하는 데 일반적으로 사용되는 API가 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 API 작업이 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 Kubernetes 클러스터가 광범위한 공격에 취약한지 판단하기 위해 정보를 수집하는 공격의 발견 단계에서 사용됩니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Kubernetes 클러스터에서 리소스를 검색하는 데 일반적으로 사용되는 API가 사용자 지정 위협 목록의 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 API가 사용자가 업로드한 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이 결과와 관련된 위협 목록은 결과 세부 정보의 추가 정보 섹션에 나열됩니다. 관찰된 API는 일반적으로 공격자가 Kubernetes 클러스터가 광범위한 공격에 취약한지 판단하기 위해 정보를 수집하는 공격의 발견 단계에서 사용됩니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Discovery:Kubernetes/SuccessfulAnonymousAccess

인증되지 않은 사용자가 Kubernetes 클러스터에서 리소스를 검색하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 `system:anonymous` 사용자가 API 작업을 성공적으로 간접 호출했음을 알려줍니다. `system:anonymous`의 API 호출이 인증되지 않았습니다. 관찰된 API는 일반적으로 공격자가 Kubernetes 클러스터에 관한 정보를 수집하는 공격의 발견 단계와 관련이 있습니다. 이 활동은 결과에 보고된 API 작업에서 익명 또는 인증되지 않은 액세스가 허용되고 다른 작업에서 허용될 수 있음을 나타냅니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

해결 권장 사항:

클러스터의 `system:anonymous` 사용자에게 부여된 권한을 검사하고 모든 권한이 필요한지 여부를 확인해야 합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자의 액세스를 철회하고 공격자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오.

자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Discovery:Kubernetes/TorIPCaller

Kubernetes 클러스터에서 리소스를 검색하는 데 일반적으로 사용되는 API가 Tor 출구 노드 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 API 작업이 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 Kubernetes 클러스터가 광범위한 공격에 취약한지 판단하기 위해 정보를 수집하는 공격의 발견 단계에서 사용됩니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 신원을 숨기려는 의도를 갖고 Kubernetes 클러스터에 무단으로 액세스하려 함을 나타낼 수 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우 Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. *system:anonymous* 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Execution:Kubernetes/ExecInKubeSystemPod

kube-system 네임스페이스 내에 있는 포드 내부에서 명령이 실행되었습니다.

기본 심각도: 중간

- 특징: EKS 감사 로그

이 결과는 Kubernetes exec API를 사용하여 kube-system 네임스페이스 내의 포드에서 명령이 실행되었음을 알려줍니다. kube-system 네임스페이스는 기본 네임스페이스로, 주로 kube-dns 및

kube-proxy와 같은 시스템 수준 구성 요소에 사용됩니다. kube-system 네임스페이스의 포드 또는 컨테이너 내에서 명령을 실행하는 경우는 매우 드물며, 의심스러운 활동을 나타낼 수 있습니다.

해결 권장 사항:

이 명령이 예기치 않게 실행된 경우 명령을 실행하는 데 사용된 사용자 ID의 보안 인증 정보가 손상되었을 수 있습니다. 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Impact:Kubernetes/MaliciousIPCaller

Kubernetes 클러스터에 있는 리소스를 변조하는 데 일반적으로 사용되는 API가 알려진 악성 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 높음

- 특징: EKS 감사 로그

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 API 작업이 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 환경 내의 데이터를 조작, 방해 또는 파괴하려고 하는 영향 전술과 관련이 있습니다. AWS

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Impact:Kubernetes/MaliciousIPCaller.Custom

Kubernetes 클러스터에 있는 리소스를 변조하는 데 일반적으로 사용되는 API가 사용자 지정 위협 목록의 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 API 작업이 사용자가 업로드한 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이 결과와 관련된 위협 목록은 결과 세부 정보의 추가 정보 섹션에 나열됩니다. 관찰된 API는 일반적으로 공격자가 환경 내의 데이터를 조작, 방해 또는 파괴하려고 하는 영향 전술과 관련이 있습니다. AWS

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Impact:Kubernetes/SuccessfulAnonymousAccess

인증되지 않은 사용자가 Kubernetes 클러스터에 있는 리소스를 변조하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 system:anonymous 사용자가 API 작업을 성공적으로 간접 호출했음을 알려줍니다. system:anonymous의 API 호출이 인증되지 않았습니다. 관찰된 API는 일반적으로 공격자가 클러스터에 있는 리소스를 변조하는 공격의 영향 단계와 관련이 있습니다. 이 활동은 결과에 보고된 API 작업에서 익명 또는 인증되지 않은 액세스가 허용되고 다른 작업에서 허용될 수 있음을 나타냅니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

해결 권장 사항:

클러스터의 system:anonymous 사용자에게 부여된 권한을 검사하고 모든 권한이 필요한지 여부를 확인해야 합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자의 액세스를 철회하고 공격자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오.

자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Impact:Kubernetes/TorIPCaller

Kubernetes 클러스터에 있는 리소스를 변조하는 데 일반적으로 사용되는 API가 Tor 출구 노드 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 API 작업이 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 AWS 환경의 데이터를 조작, 방해 또는 파괴하려는 공격 전략과 관련이 있습니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 신원을 숨기려는 의도를 갖고 Kubernetes 클러스터에 무단으로 액세스하려 함을 나타낼 수 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Persistence:Kubernetes/ContainerWithSensitiveMount

내부에 탑재된 민감한 외부 호스트 경로에서 컨테이너가 시작되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 `volumeMounts` 섹션에서 쓰기 액세스를 보유한 민감한 호스트 경로를 포함한 구성에서 컨테이너가 시작되었음을 알려줍니다. 이로 인해 민감한 호스트 경로가 컨테이너 내부에서 액세스 및 쓰기가 가능합니다. 이 기법은 공격자가 호스트의 파일 시스템에 대한 액세스 권한을 얻는 데 일반적으로 사용됩니다.

해결 권장 사항:

이 컨테이너의 시작이 예상치 못한 동작인 경우 컨테이너 시작에 사용된 사용자 ID의 보안 인증 정보가 손상되었을 수 있습니다. 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

이 컨테이너의 시작이 예상된 동작인 경우 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 필드를 기반으로 하는 필터 기준으로 구성된 억제 규칙을 사용하는 것이 좋습니다. 필터 기준에서 `imagePrefix` 필드는 결과에 지정된 `imagePrefix`와 같아야 합니다. 억제 규칙 작성에 대한 자세한 내용은 억제 규칙을 참조하세요.

Persistence:Kubernetes/MaliciousIPCaller

Kubernetes 클러스터의 리소스에 대한 영구 액세스를 획득하는 데 일반적으로 사용되는 API가 알려진 악성 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 중간

- 특징: EKS 감사 로그

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 API 작업이 간접적으로 호출되었음을 알려줍니다. 일반적으로 관찰되는 API는 공격자가 Kubernetes 클러스터에 대한 액세스 권한을 획득하고 이를 유지하려고 하는 지속성 전략과 관련이 있습니다.

해결 권장 사항:

사용자가 *`KubernetesUserDetails`* 섹션의 결과에 다음과 같다고 보고한 경우*`system:anonymous`*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Kubernetes 클러스터의 리소스에 대한 영구 액세스를 획득하는 데 일반적으로 사용되는 API가 알려진 사용자 지정 위협 목록의 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 API 작업이 사용자가 업로드한 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이 결과와 관련된 위협 목록은 결과 세부 정보의 추가 정보 섹션에 나열됩니다. 일반적으로 관찰되는 API는 공격자가 Kubernetes 클러스터에 대한 액세스 권한을 획득하고 이를 유지하려고 하는 지속성 전략과 관련이 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Persistence:Kubernetes/SuccessfulAnonymousAccess

인증되지 않은 사용자가 Kubernetes 클러스터에 대한 상위 수준 권한을 획득하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 `system:anonymous` 사용자가 API 작업을 성공적으로 간접 호출했음을 알려줍니다. `system:anonymous`의 API 호출이 인증되지 않았습니다. 관찰된 API는 일반적으로 공격자가 클러스터에 대한 액세스 권한을 획득하고 이를 유지하려고 하는 지속성 전략과 관련이 있습니다. 이 활동은 결과에 보고된 API 작업에서 익명 또는 인증되지 않은 액세스가 허용되고 다른 작업에서 허용될 수 있음을 나타냅니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

해결 권장 사항:

클러스터의 `system:anonymous` 사용자에게 부여된 권한을 검사하고 모든 권한이 필요한지 여부를 확인해야 합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자의 액세스를 철회하고 공격자가

클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오.

자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Persistence:Kubernetes/TorIPCaller

Kubernetes 클러스터의 리소스에 대한 영구 액세스를 획득하는 데 일반적으로 사용되는 API가 Tor 출구 노드 IP 주소에서 간접적으로 호출되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 API 작업이 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 일반적으로 관찰되는 API는 공격자가 Kubernetes 클러스터에 대한 액세스 권한을 획득하고 이를 유지하려고 하는 지속성 전략과 관련이 있습니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 ID를 숨기려는 의도로 AWS 리소스에 무단으로 액세스했음을 의미할 수 있습니다.

해결 권장 사항:

사용자가 *KubernetesUserDetails* 섹션의 결과에 다음과 같다고 보고한 경우*system:anonymous*, Amazon EKS 사용 설명서의 Amazon EKS 보안 모범 사례의 지침에 따라 익명 사용자에게 API 호출이 허용된 이유를 조사하고 필요한 경우 권한을 취소하십시오. 사용자가 인증된 사용자인 경우 해당 활동이 적법한지 또는 악의적인지 여부를 조사해 확인합니다. 악의적인 활동인 경우 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Kubernetes 클러스터의 관리자 권한이 기본 서비스 계정에 부여되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 Kubernetes 클러스터의 네임스페이스에 대한 기본 서비스 계정에 관리자 권한이 부여되었음을 알려줍니다. Kubernetes는 클러스터의 모든 네임스페이스에 대해 기본 서비스 계정을 생성합니다. 다른 서비스 계정에 명시적으로 연결되지 않은 포드에 기본 서비스 계정을 자격 증명으로 자동 할당합니다. 기본 서비스 계정에 관리자 권한이 있는 경우 의도치 않게 관리자 권한을 사용하여 포드가 시작될 수 있습니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

해결 권장 사항:

기본 서비스 계정을 사용하여 포드에 권한을 부여해서는 안 됩니다. 대신 각 워크로드에 전용 서비스 계정을 생성하고 필요에 따라 해당 계정에 권한을 부여해야 합니다. 이 문제를 해결하려면 모든 포드와 워크로드에 전용 서비스 계정을 생성하고 포드와 워크로드를 업데이트하여 기본 서비스 계정에서 전용 계정으로 마이그레이션해야 합니다. 이후 기본 서비스 계정에서 관리자 권한을 제거해야 합니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Policy:Kubernetes/AnonymousAccessGranted

`system:anonymous` 사용자에게 Kubernetes 클러스터에 대한 API 권한이 부여되었습니다.

기본 심각도: 높음

- 특징: EKS 감사 로그

이 결과는 Kubernetes 클러스터의 사용자가 `ClusterRoleBinding` 또는 `RoleBinding`을 성공적으로 생성하여 사용자 `system:anonymous`에 역할을 바인딩했음을 알려줍니다. 이를 통해 역할에서 허용하는 API 작업에 대해 인증되지 않은 액세스가 가능합니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

해결 권장 사항:

클러스터의 `system:anonymous` 사용자 또는 `system:unauthenticated` 그룹에 부여된 권한을 검사하여 불필요한 익명 액세스를 철회해야 합니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오. 권한이 악의적으로 부여된 경우 권한이 부여된 사용자의 액세스를 철회하고 공격자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Policy:Kubernetes/ExposedDashboard

Kubernetes 클러스터의 대시보드가 인터넷에 노출되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 클러스터의 Kubernetes 대시보드가 로드 밸런서 서비스에 의해 인터넷에 노출되었음을 알려줍니다. 대시보드가 노출되면 인터넷에서 클러스터의 관리 인터페이스에 액세스할 수 있고 공격자가 존재할 수 있는 인증 및 액세스 제어 허점을 악용할 수 있습니다.

해결 권장 사항:

Kubernetes 대시보드에 강력한 인증 및 권한 부여가 시행되도록 해야 합니다. 또한 네트워크 액세스 제어를 구현하여 특정 IP 주소에서의 대시보드 액세스를 제한해야 합니다.

자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Policy:Kubernetes/KubeflowDashboardExposed

Kubernetes 클러스터의 Kubeflow 대시보드가 인터넷에 노출되었습니다.

기본 심각도: 중간

- 특징: EKS 감사 로그

이 결과는 클러스터의 Kubeflow 대시보드가 로드 밸런서 서비스에 의해 인터넷에 노출되었음을 알려줍니다. Kubeflow 대시보드가 노출되면 인터넷에서 Kubeflow 환경의 관리 인터페이스에 액세스할 수 있고 공격자가 존재할 수 있는 인증 및 액세스 제어 허점을 악용할 수 있습니다.

해결 권장 사항:

Kubeflow 대시보드에 강력한 인증 및 권한 부여가 시행되도록 해야 합니다. 또한 네트워크 액세스 제어를 구현하여 특정 IP 주소에서의 대시보드 액세스를 제한해야 합니다.

자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

루트 수준 액세스 권한이 있는 컨테이너가 Kubernetes 클러스터에서 시작되었습니다.

기본 심각도: 중간

- 특징: EKS 감사 로그

이 결과는 Kubernetes 클러스터에서 권한이 있는 컨테이너가 이전에 클러스터에서 권한이 있는 컨테이너를 시작하는 데 사용된 적이 없는 이미지를 사용하여 Kubernetes 클러스터에서 시작되었음을 알려줍니다. 권한이 있는 컨테이너는 호스트에 대한 루트 수준 액세스 권한을 갖습니다. 공격자는 권한 상승 전략으로 권한이 있는 컨테이너를 시작하여 호스트에 대한 액세스 권한을 획득하고 호스트를 손상시킬 수 있습니다.

해결 권장 사항:

이 컨테이너의 시작이 예상치 못한 동작인 경우 컨테이너 시작에 사용된 사용자 ID의 보안 인증 정보가 손상되었을 수 있습니다. 사용자의 액세스를 철회하고 클러스터에서 공격자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

보안 암호에 액세스하는 데 일반적으로 사용되는 Kubernetes API가 변칙적인 방식으로 간접 호출되었습니다.

기본 심각도: 중간

- 특징: EKS 감사 로그

이 결과는 민감한 클러스터 보안 암호를 검색하는 변칙적인 API 작업을 클러스터의 Kubernetes 사용자가 간접적으로 호출했음을 알려줍니다. 관찰된 API는 일반적으로 클러스터 내에서 권한 상승 및 추가 액세스로 이어질 수 있는 보안 인증 정보 액세스 전략과 관련이 있습니다. 이 동작이 예상되지 않는 경우 구성 실수이거나 AWS 자격 증명이 손상되었기 때문일 수 있습니다.

관찰된 API는 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 이상 API로 식별되었습니다. ML 모델은 EKS 클러스터 내의 모든 사용자 API 활동을 평가하고 승인되지 않은 사용자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 사용한 사용자 에이

전트, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

클러스터의 Kubernetes 사용자에게 부여된 권한을 검사하고 모든 권한이 필요한지 여부를 확인해야 합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자 액세스를 철회하고 승인되지 않은 사용자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

지나치게 허용된 역할 RoleBinding 또는 ClusterRoleBinding 민감한 네임스페이스가 Kubernetes 클러스터에서 생성되거나 수정되었습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 하지만 a가 OR와 ClusterRoleBinding 관련된 경우 RoleBinding 심각도가 높습니다. ClusterRoles `admin` `cluster-admin`

- 기능: EKS 감사 로그

이 결과는 Kubernetes 클러스터의 사용자가 `RoleBinding` 또는 `ClusterRoleBinding`을 생성하여 사용자를 관리자 권한이 있는 역할 또는 민감한 네임스페이스에 바인딩했음을 알려줍니다. 이 동작이 예상되지 않는 경우 구성 실수이거나 AWS 자격 증명이 손상되었기 때문일 수 있습니다.

관찰된 API는 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 이상 API로 식별되었습니다. ML 모델은 EKS 클러스터 내의 모든 사용자 API 활동을 평가합니다. 또한 이 ML 모델은 승인되지 않은 사용자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. 또한 ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 사용한 사용자 에이전트, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

Kubernetes 사용자에게 부여된 권한을 검사합니다. 이러한 권한은 `RoleBinding` 및 `ClusterRoleBinding`과 관련된 역할 및 주체에 정의되어 있습니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자 액세스를 철회하고 승인되지 않은 사용자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

Execution:Kubernetes/AnomalousBehavior.ExecInPod

포드 내에서 명령이 변칙적으로 실행되었습니다.

기본 심각도: 중간

- 기능: EKS 감사 로그

이 결과는 Kubernetes exec API를 사용하여 포드에서 명령이 실행되었음을 알려줍니다. Kubernetes exec API를 사용하면 포드에서 임의의 명령을 실행할 수 있습니다. 사용자, 네임스페이스 또는 포드에서 이러한 동작이 예상되지 않는 경우 구성 실수이거나 AWS 자격 증명이 손상된 것일 수 있습니다.

관찰된 API는 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 이상 API로 식별되었습니다. ML 모델은 EKS 클러스터 내의 모든 사용자 API 활동을 평가합니다. 또한 이 ML 모델은 승인되지 않은 사용자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. 또한 ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 사용한 사용자 에이전트, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

이 명령이 예기치 않게 실행된 경우 명령을 실행하는 데 사용된 사용자 ID의 보안 인증 정보가 손상되었을 수 있습니다. 사용자 액세스를 철회하고 클러스터에서 승인되지 않은 사용자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

권한이 있는 컨테이너를 사용하여 워크로드가 변칙적인 방식으로 시작되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 Amazon EKS 클러스터의 권한이 있는 컨테이너를 사용하여 워크로드가 시작되었음을 알려줍니다. 권한이 있는 컨테이너는 호스트에 대한 루트 수준 액세스 권한을 갖습니다. 승인되지 않은 사용자는 권한 상승 전략으로 권한이 있는 컨테이너를 시작하여 우선 호스트에 대한 액세스 권한을 획득하고 이후 이를 손상시킬 수 있습니다.

관찰된 컨테이너 생성 또는 수정은 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 비정상으로 식별되었습니다. ML 모델은 EKS 클러스터 내의 모든 사용자 API 및 컨테이너 이미지 활동을 평가합니다. 또한 이 ML 모델은 승인되지 않은 사용자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. 또한 ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 사용한 사용자 에이전트, 계정에서 관찰된 컨테이너 이미지, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

이 컨테이너의 시작이 예상치 못한 동작인 경우 컨테이너 시작에 사용된 사용자 ID의 보안 인증 정보가 손상되었을 수 있습니다. 사용자 액세스를 철회하고 클러스터에서 승인되지 않은 사용자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

이 컨테이너의 시작이 예상된 동작인 경우 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 필드를 기반으로 하는 필터 기준으로 구성된 억제 규칙을 사용하는 것이 좋습니다. 필터 기준에서 `imagePrefix` 필드는 결과에 지정된 `imagePrefix` 필드와 값이 같아야 합니다. 자세한 정보는 억제 규칙을 참조하세요.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

민감한 호스트 경로가 워크로드 내에 탑재된 상태에서 워크로드가 변칙적인 방식으로 배포되었습니다.

기본 심각도: 높음

- 기능: EKS 감사 로그

이 결과는 volumeMounts 섹션에 민감한 호스트 경로가 포함된 컨테이너에서 워크로드가 시작되었음을 알려줍니다. 이로 인해 민감한 호스트 경로가 컨테이너 내부에서 액세스 및 쓰기가 가능할 수 있습니다. 이 기법은 승인되지 않은 사용자가 호스트의 파일 시스템에 대한 액세스 권한을 얻는 데 일반적으로 사용됩니다.

관찰된 컨테이너 생성 또는 수정은 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 비정상으로 식별되었습니다. ML 모델은 EKS 클러스터 내의 모든 사용자 API 및 컨테이너 이미지 활동을 평가합니다. 또한 이 ML 모델은 승인되지 않은 사용자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. 또한 ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 사용한 사용자 에이전트, 계정에서 관찰된 컨테이너 이미지, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

이 컨테이너의 시작이 예상치 못한 동작인 경우 컨테이너 시작에 사용된 사용자 ID의 보안 인증 정보가 손상되었을 수 있습니다. 사용자 액세스를 철회하고 클러스터에서 승인되지 않은 사용자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

이 컨테이너의 시작이 예상된 동작인 경우 resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix 필드를 기반으로 하는 필터 기준으로 구성된 억제 규칙을 사용하는 것이 좋습니다. 필터 기준에서 imagePrefix 필드는 결과에 지정된 imagePrefix 필드와 값이 같아야 합니다. 자세한 정보는 억제 규칙을 참조하세요.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

워크로드가 변칙적인 방식으로 시작되었습니다.

기본 심각도: 낮음*

> **Note**
>
> 기본 심각도는 낮음입니다. 하지만 워크로드에 알려진 침투 테스트 도구와 같이 잠재적으로 의심스러운 이미지 이름 또는 시작 시 잠재적으로 의심스러운 명령(예: reverse shell 명령)을 실행하는 컨테이너가 포함된 경우 이 결과 유형의 심각도는 중간으로 간주됩니다.

- 기능: EKS 감사 로그

이 결과는 Kubernetes 워크로드가 Amazon EKS 클러스터 내에서 API 활동, 새 컨테이너 이미지 또는 위험한 워크로드 구성과 같은 변칙적인 방식으로 생성 또는 수정되었음을 알려줍니다. 승인되지 않은 사용자는 전략적으로 컨테이너를 시작하여 임의 코드를 실행해 우선 호스트에 대한 액세스 권한을 획득하고 이후 이를 손상시킬 수 있습니다.

관찰된 컨테이너 생성 또는 수정은 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 비정상으로 식별되었습니다. ML 모델은 EKS 클러스터 내의 모든 사용자 API 및 컨테이너 이미지 활동을 평가합니다. 또한 이 ML 모델은 승인되지 않은 사용자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. 또한 ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 사용한 사용자 에이전트, 계정에서 관찰된 컨테이너 이미지, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

이 컨테이너의 시작이 예상치 못한 동작인 경우 컨테이너 시작에 사용된 사용자 ID의 보안 인증 정보가 손상되었을 수 있습니다. 사용자 액세스를 철회하고 클러스터에서 승인되지 않은 사용자의 변경 사항을 되돌립니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

이 컨테이너의 시작이 예상된 동작인 경우 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 필드를 기반으로 하는 필터 기준으로 구성된 억제 규칙을 사용하는 것이 좋습니다. 필터 기준에서 `imagePrefix` 필드는 결과에 지정된 `imagePrefix` 필드와 값이 같아야 합니다. 자세한 정보는 억제 규칙을 참조하세요.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

매우 허용적인 역할이거나 비정상적인 방식으로 생성 또는 ClusterRole 수정되었습니다.

기본 심각도: 낮음

- 기능: EKS 감사 로그

이 결과는 Amazon EKS 클러스터의 Kubernetes 사용자가 변칙적인 API 작업을 호출하여 과도한 권한을 가진 `Role` 또는 `ClusterRole`을 생성했음을 알려줍니다. 작업자는 강력한 권한이 있는 역할 생성을 사용하여 관리자와 유사한 기본 역할을 사용하지 않고 탐지를 피할 수 있습니다. 과도한 권한은 권한 상승, 원격 코드 실행, 잠재적으로 네임스페이스나 클러스터에 대한 통제로 이어질 수 있습니다. 이러한 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

관찰된 API는 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 비정상으로 식별되었습니다. ML 모델은 Amazon EKS 클러스터 내의 모든 사용자 API 활동을 평가하고 승인되지 않은 사용자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. 또한 ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 사용한 사용자 에이전트, 계정에서 관찰된 컨테이너 이미지, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

`Role` 또는 `ClusterRole`에 정의된 권한을 검사하여 모든 권한이 필요한지 확인하고 최소 권한 원칙을 준수합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자 액세스를 철회하고 승인되지 않은 사용자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

사용자가 변칙적인 방식으로 액세스 권한을 확인했습니다.

기본 심각도: 낮음

- 기능: EKS 감사 로그

이 결과는 Kubernetes 클러스터의 사용자가 권한 상승 및 원격 코드 실행으로 이어질 수 있는 알려진 강력한 권한의 허용 여부를 확인했음을 알려줍니다. 예를 들어 사용자의 권한을 확인하는 데 사용되는 일반적인 명령은 `kubectl auth can-i`입니다. 이 동작이 예상된 동작이 아닌 경우 구성 실수이거나 보안 인증 정보가 손상되었기 때문일 수 있습니다.

관찰된 API는 GuardDuty 이상 탐지 기계 학습 (ML) 모델에 의해 비정상으로 식별되었습니다. ML 모델은 Amazon EKS 클러스터 내의 모든 사용자 API 활동을 평가하고 승인되지 않은 사용자가 사용한 기

법과 관련된 이상 이벤트를 식별합니다. 또한 ML 모델은 요청을 보낸 사용자, 요청을 보낸 위치, 확인된 권한, 사용자가 작업하는 네임스페이스 등 API 작업의 여러 요소를 추적합니다. 콘솔의 검색 결과 세부 정보 패널에서 특이한 API 요청 세부 정보를 찾을 수 있습니다. GuardDuty

해결 권장 사항:

Kubernetes 사용자에게 부여된 권한을 검사하고 모든 권한이 필요한지 여부를 확인해야 합니다. 권한이 실수로 또는 악의적으로 부여된 경우 사용자 액세스를 철회하고 승인되지 않은 사용자가 클러스터에 적용한 변경 사항을 되돌려야 합니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

AWS 자격 증명이 손상된 경우 을 참조하십시오잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS.

Lambda 보호 결과 유형

이 섹션에서는 AWS Lambda 리소스에 고유하고 `resourceType`이 `Lambda`인 결과 유형에 대해 설명합니다. 모든 Lambda 결과의 경우 해당 리소스를 검토하고 예상대로 작동하는지 확인하는 것이 좋습니다. 활동이 승인된 경우 억제 규칙 또는 신뢰할 수 있는 IP 및 위협 목록을 사용하여 해당 리소스에 대한 오탐지 알림을 방지할 수 있습니다.

예상치 않은 활동인 경우 보안 모범 사례는 Lambda가 잠재적으로 침해되었다고 가정하고 해결 권장 사항을 따르는 것입니다.

주제

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Lambda 함수가 알려진 명령 및 제어 서버와 연결된 IP 주소를 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Lambda 네트워크 활동 모니터링

이 결과는 AWS 환경 내에 알려진 명령 및 제어(C&C) 서버와 연결된 IP 주소를 쿼리하는 Lambda 함수가 있음을 알립니다. 생성된 결과와 관련된 Lambda 함수가 잠재적으로 침해되었습니다. C&C 서버는 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다.

봇넷은 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스(PC, 서버, 모바일 디바이스 및 사물 인터넷 디바이스 포함)의 모음입니다. 일반적으로 봇넷은 맬웨어를 분산하고 부적절한 정보(예: 신용카드 번호)를 수집합니다. 봇넷의 용도와 구조에 따라 C&C 서버가 분산 서비스 거부를 시작하는 명령을 실행할 수도 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 Lambda 함수가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Lambda 함수 수정 섹션을 참조하세요.

CryptoCurrency:Lambda/BitcoinTool.B

Lambda 함수가 암호화폐 관련 활동과 연결된 IP 주소를 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Lambda 네트워크 활동 모니터링

이 결과는 AWS 환경에 비트코인 또는 기타 암호화폐 관련 활동과 연결된 IP 주소를 쿼리하는 Lambda 함수가 있음을 알립니다. 위협 작업자는 악의적으로 승인되지 않은 암호화폐 채굴로 용도를 변경하기 위해 Lambda 함수를 제어하려고 할 수 있습니다.

해결 권장 사항:

이 Lambda 함수를 사용하여 암호화폐를 채굴 또는 관리하거나 이 함수가 블록체인 활동에 관여한 경우, 환경에 대한 예상된 활동일 수 있습니다. AWS 환경에서 이러한 경우 이 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 CryptoCurrency:Lambda/BitcoinTool.B 값이 있는 결과 유형 속성을 사용해야 합니다. 두 번째 필터 기준은 블록체인 활동과 관련된 함수의 Lambda 함수 이름이어야 합니다. 억제 규칙 작성에 대한 내용은 억제 규칙을 참조하세요.

이 활동이 예기치 않게 발생한 경우 Lambda 함수가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Lambda 함수 수정 섹션을 참조하세요.

Trojan:Lambda/BlackholeTraffic

Lambda 함수가 블랙홀로 알려진 원격 호스트의 IP 주소와 통신을 시도합니다.

기본 심각도: 중간

- 특성: Lambda 네트워크 활동 모니터링

이 결과는 AWS 환경 내에 나열된 Lambda 함수가 블랙홀(또는 싱크홀)의 IP 주소와 통신을 시도하고 있음을 알려줍니다. 블랙홀은 데이터가 의도한 수신자에게 도달하지 않았음을 소스에 알리지 않고 수신 트래픽 또는 발신 트래픽을 자동으로 취소하는 네트워크의 위치입니다. 블랙홀 IP 주소는 실행되고 있지 않은 호스트 머신 또는 호스트가 할당되지 않은 주소를 지정합니다. 나열된 Lambda 함수가 잠재적으로 손상되었습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 Lambda 함수가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Lambda 함수 수정 섹션을 참조하세요.

Trojan:Lambda/DropPoint

Lambda 함수가 맬웨어를 통해 캡처된 자격 증명 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 IP 주소와 통신을 시도하는 중입니다.

기본 심각도: 중간

- 특성: Lambda 네트워크 활동 모니터링

이 결과는 AWS 환경 내에 나열된 Lambda 함수가 맬웨어를 통해 캡처된 보안 인증 정보 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 IP 주소와 통신을 시도 중임을 알립니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 Lambda 함수가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Lambda 함수 수정 섹션을 참조하세요.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Lambda 함수가 사용자 지정 위협 목록에 있는 IP 주소에 연결하고 있습니다.

기본 심각도: 중간

- 특성: Lambda 네트워크 활동 모니터링

이 결과는 AWS 환경의 Lambda 함수가 사용자가 업로드한 위협 목록에 포함된 IP 주소를 사용하여 통신 중임을 알려줍니다. GuardDuty에서 위협 목록은 알려진 악성 IP 주소로 구성됩니다. GuardDuty는 업로드된 위협 목록을 기반으로 결과를 생성합니다. GuardDuty 콘솔의 결과 세부 정보에서 위협 목록의 세부 정보를 볼 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 Lambda 함수가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Lambda 함수 수정 섹션을 참조하세요.

UnauthorizedAccess:Lambda/TorClient

Lambda 함수가 Tor Guard 또는 Authority 노드에 연결됩니다.

기본 심각도: 높음

- 특성: Lambda 네트워크 활동 모니터링

이 결과는 AWS 환경의 Lambda 함수가 Tor Guard 또는 Authority 노드에 연결 중임을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, Tor Guards 및 Authority 노드는 Tor 네트워크의 첫 번째 게이트웨이 역할을 합니다. 이 트래픽은 이 Lambda 함수가 잠재적으로 손상되었음을 나타낼 수 있습니다. 이제 Tor 네트워크에서 클라이언트 역할을 하고 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 Lambda 함수가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Lambda 함수 수정 섹션을 참조하세요.

UnauthorizedAccess:Lambda/TorRelay

Lambda 함수가 Tor 네트워크에 Tor 릴레이로 연결됩니다.

기본 심각도: 높음

- 특성: Lambda 네트워크 활동 모니터링

이 결과는 AWS 환경의 Lambda 함수가 Tor 네트워크에 Tor 릴레이 역할을 수행하는 방식으로 연결 중임을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, Tor는 한 Tor 릴레이에서 다른 릴레이로 클라이언트의 불법 가능성이 있는 트래픽을 전달함으로써 익명 통신을 가능하게 합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 Lambda 함수가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Lambda 함수 수정 섹션을 참조하세요.

맬웨어 보호 결과 유형

GuardDuty 멀웨어 보호는 EC2 인스턴스 또는 컨테이너 워크로드 스캔 중에 탐지된 모든 위협에 대한 단일 멀웨어 보호 탐지 기능을 제공합니다. 결과에는 스캔 중에 발견된 총 탐지 수가 포함되고, 심각도에 따라 탐지된 상위 32개 위협에 대한 세부 정보가 제공됩니다. 다른 GuardDuty 탐지 결과와 달리 멀웨어 보호 결과는 동일한 EC2 인스턴스 또는 컨테이너 워크로드를 다시 스캔해도 업데이트되지 않습니다.

맬웨어를 탐지한 각 스캔에 대해 새로운 맬웨어 보호 결과가 생성됩니다. 멀웨어 보호 탐지 결과에는 검색 결과를 생성한 해당 검사와 이 검사를 시작한 검색 결과에 대한 정보가 포함됩니다. GuardDuty 이를 통해 의심스러운 동작을 탐지된 맬웨어와 쉽게 연관시킬 수 있습니다.

> **Note**
>
> 컨테이너 워크로드에서 악의적인 활동을 GuardDuty 탐지한 경우 멀웨어 보호는 EC2 수준의 탐지 결과를 생성하지 않습니다.

다음 결과는 GuardDuty 멀웨어 보호에만 해당됩니다.

주제

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile

- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

EC2 인스턴스에서 악성 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 스캔이 사용자 AWS 환경 내에 나열된 EC2 인스턴스에서 하나 이상의 악성 파일을 탐지했음을 나타냅니다. 이 나열된 인스턴스는 손상되었을 수 있습니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 정보는 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결을 참조하세요.

Execution:ECS/MaliciousFile

ECS 클러스터에서 악성 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 스캔이 컨테이너 워크로드에서 ECS 클러스터에 속하는 하나 이상의 악성 파일을 탐지했음을 나타냅니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 ECS 클러스터에 속한 컨테이너가 손상되었을 수 있습니다. 자세한 정보는 잠재적으로 손상된 ECS 클러스터의 문제 해결을 참조하세요.

Execution:Kubernetes/MaliciousFile

Kubernetes 클러스터에서 악성 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 스캔이 Kubernetes 클러스터에 속하는 컨테이너 워크로드에서 하나 이상의 악성 파일을 탐지했음을 나타냅니다. EKS 관리형 클러스터인 경우 결과 세부 정보에는 영향을 받는 EKS 리소스에 대한 추가 정보가 제공됩니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 컨테이너 워크로드가 손상되었을 수 있습니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Execution:Container/MaliciousFile

독립형 컨테이너에서 악성 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 검사에서 컨테이너 워크로드에서 하나 이상의 악성 파일을 탐지했으며 클러스터 정보는 식별되지 않았음을 나타냅니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 컨테이너 워크로드가 손상되었을 수 있습니다. 자세한 정보는 잠재적으로 손상되었을 수 있는 독립형 컨테이너의 문제 해결을 참조하세요.

Execution:EC2/SuspiciousFile

EC2 인스턴스에서 의심스러운 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 검사에서 EC2 인스턴스에서 하나 이상의 의심스러운 파일을 탐지했음을 나타냅니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

`SuspiciousFile` 유형 탐지는 영향을 받는 리소스에 애드웨어, 스파이웨어 또는 이중 용도 도구와 같은 잠재적으로 원치 않는 프로그램이 존재함을 나타냅니다. 이러한 프로그램은 리소스에 부정적인 영향을 미치거나 공격자가 악의적인 용도로 사용할 수 있습니다. 예를 들어 공격자는 네트워크 도구를 합법적으로 또는 악의적으로 사용하여 리소스를 손상시키려는 해킹 도구로 사용할 수 있습니다.

의심스러운 파일이 탐지되면 해당 환경에서 탐지된 파일을 볼 수 있을 것으로 예상하는지 평가하십시오. AWS 예상하지 못한 파일인 경우 다음 섹션의 해결 권장 사항을 따르세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 정보는 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결을 참조하세요.

Execution:ECS/SuspiciousFile

ECS 클러스터에서 의심스러운 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 검사에서 ECS 클러스터에 속한 컨테이너에서 하나 이상의 의심스러운 파일을 탐지했음을 나타냅니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

`SuspiciousFile` 유형 탐지는 영향을 받는 리소스에 애드웨어, 스파이웨어 또는 이중 용도 도구와 같은 잠재적으로 원치 않는 프로그램이 존재함을 나타냅니다. 이러한 프로그램은 리소스에 부정적인

영향을 미치거나 공격자가 악의적인 용도로 사용할 수 있습니다. 예를 들어 공격자는 네트워크 도구를 합법적으로 또는 악의적으로 사용하여 리소스를 손상시키려는 해킹 도구로 사용할 수 있습니다.

의심스러운 파일이 탐지되면 해당 환경에서 탐지된 파일을 볼 수 있을 것으로 예상하는지 평가하십시오. AWS 예상하지 못한 파일인 경우 다음 섹션의 해결 권장 사항을 따르세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 ECS 클러스터에 속한 컨테이너가 손상되었을 수 있습니다. 자세한 정보는 잠재적으로 손상된 ECS 클러스터의 문제 해결을 참조하세요.

Execution:Kubernetes/SuspiciousFile

Kubernetes 클러스터에서 의심스러운 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 스캔이 Kubernetes 클러스터에 속한 컨테이너에서 하나 이상의 의심스러운 파일을 탐지했음을 나타냅니다. EKS 관리형 클러스터인 경우 결과 세부 정보에는 영향을 받는 EKS에 대한 추가 정보가 제공됩니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

`SuspiciousFile` 유형 탐지는 영향을 받는 리소스에 애드웨어, 스파이웨어 또는 이중 용도 도구와 같은 잠재적으로 원치 않는 프로그램이 존재함을 나타냅니다. 이러한 프로그램은 리소스에 부정적인 영향을 미치거나 공격자가 악의적인 용도로 사용할 수 있습니다. 예를 들어 공격자는 네트워크 도구를 합법적으로 또는 악의적으로 사용하여 리소스를 손상시키려는 해킹 도구로 사용할 수 있습니다.

의심스러운 파일이 탐지되면 해당 환경에서 탐지된 파일을 볼 수 있을 것으로 예상되는지 평가하십시오. AWS 예상하지 못한 파일인 경우 다음 섹션의 해결 권장 사항을 따르세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 컨테이너 워크로드가 손상되었을 수 있습니다. 자세한 정보는 EKS 감사 로그 모니터링 결과 해결을 참조하세요.

Execution:Container/SuspiciousFile

독립형 컨테이너에서 의심스러운 파일이 탐지되었습니다.

기본 심각도: 탐지된 위협에 따라 다릅니다.

- 기능: EBS 멀웨어 보호

이 결과는 GuardDuty 멀웨어 보호 검사에서 클러스터 정보가 없는 컨테이너에서 하나 이상의 의심스러운 파일을 탐지했음을 나타냅니다. 자세한 내용은 결과 세부 정보의 탐지된 위협 섹션을 참조하세요.

`SuspiciousFile` 유형 탐지는 영향을 받는 리소스에 애드웨어, 스파이웨어 또는 이중 용도 도구와 같은 잠재적으로 원치 않는 프로그램이 존재함을 나타냅니다. 이러한 프로그램은 리소스에 부정적인 영향을 미치거나 공격자가 악의적인 용도로 사용할 수 있습니다. 예를 들어 공격자는 네트워크 도구를 합법적으로 또는 악의적으로 사용하여 리소스를 손상시키려는 해킹 도구로 사용할 수 있습니다.

의심스러운 파일이 탐지되면 해당 환경에서 탐지된 파일을 볼 수 있을 것으로 예상되는지 평가하십시오 AWS . 예상하지 못한 파일인 경우 다음 섹션의 해결 권장 사항을 따르세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 컨테이너 워크로드가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 독립형 컨테이너의 문제 해결을(를) 참조하세요.

GuardDuty RDS 보호 결과 유형

GuardDuty RDS 보호는 데이터베이스 인스턴스에서 변칙적 로그인 동작을 탐지합니다. 다음 결과는 지원되는 Amazon Aurora 데이터베이스에 해당되며 리소스 유형은 `RDSDBInstance`입니다. 결과의 심각도 및 세부 정보는 결과 유형에 따라 다릅니다.

주제

- CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin
- CredentialAccess:RDS/TorIPCaller.FailedLogin

- Discovery:RDS/TorIPCaller

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

사용자가 변칙적 방식으로 계정의 RDS 데이터베이스에 성공적으로 로그인했습니다.

기본 심각도: 가변적

> **Note**
>
> 이 결과와 관련된 변칙적 동작에 따라 기본 심각도는 낮음, 중간, 높음일 수 있습니다.
>
> - 낮음 - 이 결과와 관련된 사용자 이름이 프라이빗 네트워크에 연결된 IP 주소에서 로그인한 경우.
> - 중간 - 이 결과와 관련된 사용자 이름이 퍼블릭 IP 주소에서 로그인한 경우.
> - 높음 - 액세스 정책이 지나치게 허용적인 듯한 퍼블릭 IP 주소에서의 일관적인 로그인 시도 실패 패턴 있는 경우.

- 특성: RDS 로그인 활동 모니터링

이 결과는 AWS 환경의 RDS 데이터베이스에서 변칙적인 로그인 성공이 관찰되었음을 알려줍니다. 이는 이전에 보지 못한 사용자가 처음으로 RDS 데이터베이스에 로그인했음을 나타낼 수 있습니다. 일반적인 시나리오는 개별 사용자가 아닌 애플리케이션에 의해 프로그래밍 방식으로 내부 사용자가 데이터베이스에 로그인한 것입니다.

이 로그인 성공은 GuardDuty 이상 탐지 기계 학습(ML) 모델에 의해 이상으로 식별되었습니다. ML 모델은 지원되는 Amazon Aurora 데이터베이스의 모든 데이터베이스 로그인 이벤트를 평가하고 공격자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 사용된 특정 데이터베이스 연결 세부 정보 등 RDS 로그인 활동의 다양한 요소를 추적합니다. 비정상적일 수 있는 로그인 이벤트에 대한 자세한 내용은 RDS 로그인 활동 기반 이상 섹션을 참조하세요.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 관련 데이터베이스 사용자의 암호를 변경하고 이상 사용자가 수행한 활동에 대해 제공된 감사 로그를 검토하는 것이 좋습니다. 중간 및 높음 심

각도 결과는 데이터베이스에 대한 액세스 정책이 지나치게 허용적이고 사용자 보안 인증 정보가 노출 또는 손상되었을 가능성을 나타낼 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 성공적인 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

계정의 RDS 데이터베이스에서 한 번 이상의 비정상적인 로그인 실패 시도가 관찰되었습니다.

기본 심각도: 낮음

- 특성: RDS 로그인 활동 모니터링

이 결과는 AWS 환경의 RDS 데이터베이스에서 변칙적인 로그인 실패가 한 번 이상 관찰되었음을 알려줍니다. 퍼블릭 IP 주소에서의 로그인 시도 실패는 계정의 RDS 데이터베이스가 악의적인 공격자의 무차별 대입 공격을 받았음을 의미할 수 있습니다.

이러한 로그인 실패는 GuardDuty 이상 탐지 기계 학습(ML) 모델에 의해 이상으로 식별되었습니다. ML 모델은 지원되는 Amazon Aurora 데이터베이스의 모든 데이터베이스 로그인 이벤트를 평가하고 공격자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 사용된 특정 데이터베이스 연결 세부 정보 등 RDS 로그인 활동의 다양한 요소를 추적합니다. 비정상적일 수 있는 RDS 로그인 활동에 대한 자세한 내용은 RDS 로그인 활동 기반 이상 섹션을 참조하세요.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 데이터베이스가 공개적으로 노출되었거나 데이터베이스에 대한 액세스 정책이 지나치게 허용적일 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 실패한 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

일관적으로 비정상적인 로그인 시도 실패 패턴 이후 사용자가 퍼블릭 IP 주소를 사용하여 계정의 RDS 데이터베이스에 변칙적인 방식으로 로그인했습니다.

기본 심각도: 높음

- 특성: RDS 로그인 활동 모니터링

이 결과는 AWS 환경의 RDS 데이터베이스에서 무차별 암호 대입 성공을 의미하는 변칙적인 로그인이 관찰되었음을 알려줍니다. 변칙적 로그인에 성공하기 전에는 일관적으로 비정상적인 로그인 시도 실패가 있었습니다. 이는 계정의 RDS 데이터베이스와 연결된 사용자 및 암호가 손상되었을 수 있으며, 잠재적으로 악의적인 공격자가 RDS 데이터베이스에 액세스했을 수 있음을 나타냅니다.

이 무차별 암호 대입 로그인 성공은 GuardDuty 이상 탐지 기계 학습(ML) 모델에 의해 이상으로 식별되었습니다. ML 모델은 지원되는 Amazon Aurora 데이터베이스의 모든 데이터베이스 로그인 이벤트를 평가하고 공격자가 사용한 기법과 관련된 이상 이벤트를 식별합니다. ML 모델은 요청한 사용자, 요청이 이루어진 위치, 사용된 특정 데이터베이스 연결 세부 정보 등 RDS 로그인 활동의 다양한 요소를 추적합니다. 비정상적일 수 있는 RDS 로그인 활동에 대한 자세한 내용은 RDS 로그인 활동 기반 이상 섹션을 참조하세요.

해결 권장 사항:

이 활동은 데이터베이스 보안 인증 정보가 노출 또는 손상되었을 수 있음을 나타냅니다. 관련 데이터베이스 사용자의 암호를 변경하고 잠재적으로 침해되었을 수 있는 사용자가 수행한 활동에 대해 제공된 감사 로그를 검토하는 것이 좋습니다. 비정상적인 로그인 시도 실패의 일관적인 패턴은 데이터베이스에 대한 액세스 정책이 지나치게 허용적이거나 데이터베이스가 공개적으로 노출되었을 수도 있음을 나타냅니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 성공적인 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

사용자가 알려진 악성 IP 주소를 사용하여 계정의 RDS 데이터베이스에 로그인했습니다.

기본 심각도: 높음

- 특성: RDS 로그인 활동 모니터링

이 결과는 AWS 환경에서 알려진 악의적 활동과 관련된 IP 주소로부터 성공적인 RDS 로그인 활동이 발생했음을 알려줍니다. 이는 계정의 RDS 데이터베이스와 연결된 사용자 및 암호가 손상되었을 수 있으며, 잠재적으로 악의적인 공격자가 RDS 데이터베이스에 액세스했을 수 있음을 나타냅니다.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 사용자 보안 인증 정보가 노출 또는 손상되었을 수 있습니다. 관련 데이터베이스 사용자의 암호를 변경하고 침해된 사용자가 수행한 활동에 대해 제공된 감사 로그를 검토하는 것이 좋습니다. 또한 이 활동은 데이터베이스에 대한 액세스 정책이 지나치게 허용적이거나 데이터가 공개적으로 노출되었음을 나타낼 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 성공적인 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

알려진 악성 활동과 연결된 IP 주소가 계정의 RDS 데이터베이스에 로그인을 시도했지만 실패했습니다.

기본 심각도: 중간

- 특성: RDS 로그인 활동 모니터링

이 결과는 알려진 악성 활동과 연결된 IP 주소가 AWS 환경의 RDS 데이터베이스에 로그인을 시도했지만 올바른 사용자 이름이나 암호를 입력하지 못했음을 알려줍니다. 이는 잠재적으로 악의적인 공격자가 계정의 RDS 데이터베이스 손상을 시도하고 있을 가능성을 나타냅니다.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 데이터베이스에 대한 액세스 정책이 지나치게 허용적이거나 데이터베이스가 공개적으로 노출되었을 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 실패한 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

Discovery:RDS/MaliciousIPCaller

알려진 악성 활동과 연결된 IP 주소가 계정의 RDS 데이터베이스를 탐색했지만 인증 시도는 이루어지지 않았습니다.

기본 심각도: 중간

- 특성: RDS 로그인 활동 모니터링

이 결과는 악성 활동과 연결된 IP 주소에서 AWS 환경의 RDS 데이터베이스를 탐색했지만 로그인 시도는 이루어지지 않았음을 알려줍니다. 이는 잠재적으로 악의적인 공격자가 공개적으로 액세스할 수 있는 인프라를 찾고 있음을 의미할 수 있습니다.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 데이터베이스에 대한 액세스 정책이 지나치게 허용적이거나 데이터베이스가 공개적으로 노출되었을 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 실패한 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

사용자가 Tor 출구 노드 IP 주소에서 계정의 RDS 데이터베이스에 로그인했습니다.

기본 심각도: 높음

- 특성: RDS 로그인 활동 모니터링

이 결과는 사용자가 Tor 출구 노드 IP 주소에서 AWS 환경의 RDS 데이터베이스에 성공적으로 로그인했음을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어입니다. 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 익명 사용자의 실제 신원을 숨기려는 의도를 갖고 계정의 RDS 리소스에 무단으로 액세스함을 나타낼 수 있습니다.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 사용자 보안 인증 정보가 노출 또는 손상되었을 수 있습니다. 관련 데이터베이스 사용자의 암호를 변경하고 침해된 사용자가 수행한 활동에 대해 제공된 감사 로그를 검토하는 것이 좋습니다. 또한 이 활동은 데이터베이스에 대한 액세스 정책이 지나치게 허용적이거나 데이터가 공개적으로 노출되었음을 나타낼 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 성공적인 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Tor IP 주소에서 계정의 RDS 데이터베이스에 로그인을 시도했지만 실패했습니다.

기본 심각도: 중간

- 특성: RDS 로그인 활동 모니터링

이 결과는 Tor 출구 노드 IP 주소에서 AWS 환경의 RDS 데이터베이스에 로그인을 시도했지만 올바른 사용자 이름이나 암호를 입력하지 못했음을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어입니다. 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 익명 사용자의 실제 신원을 숨기려는 의도를 갖고 계정의 RDS 리소스에 무단으로 액세스함을 나타낼 수 있습니다.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 데이터베이스에 대한 액세스 정책이 지나치게 허용적이거나 데이터베이스가 공개적으로 노출되었을 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 실패한 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

Discovery:RDS/TorIPCaller

Tor 종료 노드 IP 주소에서 계정의 RDS 데이터베이스를 탐색했지만 인증 시도는 없었습니다.

기본 심각도: 중간

- 특성: RDS 로그인 활동 모니터링

이 결과는 Tor 출구 노드 IP 주소에서 AWS 환경의 RDS 데이터베이스를 탐색했지만 로그인 시도는 이루어지지 않았음을 알려줍니다. 이는 잠재적으로 악의적인 공격자가 공개적으로 액세스할 수 있는 인프라를 찾고 있음을 의미할 수 있습니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어입니다. 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 잠재적으로 악의적인 공격자의 실제 신원을 숨기려는 의도를 갖고 계정의 RDS 리소스에 무단으로 액세스함을 나타낼 수 있습니다.

해결 권장 사항:

관련 데이터베이스에서 이 활동이 예상치 않게 발생한 경우 데이터베이스에 대한 액세스 정책이 지나치게 허용적이거나 데이터베이스가 공개적으로 노출되었을 수 있습니다. 데이터베이스를 프라이빗 VPC에 배치하고, 필요한 소스의 트래픽만 허용하도록 보안 그룹 규칙을 제한하는 것이 좋습니다. 자세한 내용은 실패한 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결 섹션을 참조하세요.

런타임 모니터링 검색 유형

Amazon은 Amazon EKS 클러스터, Fargate 및 Amazon ECS 워크로드, Amazon EC2 인스턴스의 Amazon EC2 호스트 및 컨테이너의 운영 체제 수준 동작을 기반으로 다음과 같은 런타임 모니터링 결과를 GuardDuty 생성하여 잠재적 위협을 표시합니다.

> **Note**
>
> Runtime Monitoring 결과 유형은 호스트에서 수집된 런타임 로그를 기반으로 합니다. 로그에는 악의적인 작업자가 제어할 수 있는 파일 경로와 같은 필드가 포함되어 있습니다. 또한 이러한 필드는 런타임 컨텍스트를 제공하기 위해 조사 결과에 포함됩니다. GuardDuty GuardDuty 콘솔 외부에서 런타임 모니터링 결과를 처리할 때는 검색 결과 필드를 삭제해야 합니다. 예를 들어 웹 페이지에 표시할 때 결과 필드를 HTML로 인코딩할 수 있습니다.

주제

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS

- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

CryptoCurrency:Runtime/BitcoinTool.B

Amazon EC2 인스턴스 또는 컨테이너가 암호화폐 관련 활동과 연결된 IP 주소를 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경에 암호화폐 관련 활동과 연결된 IP 주소를 쿼리하는 나열된 EC2 인스턴스 또는 컨테이너가 있음을 알립니다. 위협 작업자는 악의적으로 승인되지 않은 암호화폐 채굴로 용도를 변경하기 위해 컴퓨팅 리소스를 제어하려고 할 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 리소스 유형을 확인하세요. GuardDuty

해결 권장 사항:

이 EC2 인스턴스 또는 컨테이너를 사용하여 암호화폐를 채굴 또는 관리하거나 이 중 하나가 블록체인 활동에 관여한 경우, CryptoCurrency:Runtime/BitcoinTool.B 결과는 환경에 대한 예상된 활동을 나타낼 수 있습니다. 사용자 AWS 환경에서 이런 경우에는 이 검색 결과에 대한 금지 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 필터 기준에는 결과 유형 속성과 `CryptoCurrency:Runtime/BitcoinTool.B` 값을 사용해야 합니다. 두 번째 필터 기준은 암호화폐 또는 블록체인 관련 활동에 관여한 인스턴스의 인스턴스 ID 또는 컨테이너의 컨테이너 이미지 ID여야 합니다. 자세한 내용은 억제 규칙을 참조하세요.

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Backdoor:Runtime/C&CActivity.B

Amazon EC2 인스턴스 또는 컨테이너가 알려진 명령 및 제어 서버와 연결된 IP를 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경 내에 알려진 명령 및 제어(C&C) 서버와 연결된 IP를 쿼리하는 나열된 EC2 인스턴스 또는 컨테이너가 있음을 알립니다. 나열된 인스턴스 또는 컨테이너가 잠재적으로 손상되었을 수 있습니다. 명령 및 제어(C&C) 서버는 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다.

봇넷은 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스(PC, 서버, 모바일 디바이스 및 사물 인터넷 디바이스 포함)의 모음입니다. 일반적으로 봇넷은 맬웨어를

분산하고 부적절한 정보(예: 신용카드 번호)를 수집합니다. 봇넷의 용도와 구조에 따라 C&C 서버가 DDoS(분산 서비스 거부) 공격을 시작하는 명령을 실행할 수도 있습니다.

> **Note**
>
> 쿼리된 IP가 log4j와 관련된 경우 관련 결과의 필드에 다음 값이 포함됩니다.
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

UnauthorizedAccess:Runtime/TorRelay

Amazon EC2 인스턴스 또는 컨테이너가 Tor 릴레이로 Tor 네트워크에 연결하고 있습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 사용자 AWS 환경의 EC2 인스턴스 또는 컨테이너가 Tor 릴레이 역할을 한다는 것을 암시하는 방식으로 Tor 네트워크에 연결하고 있음을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, Tor는 한 Tor 릴레이에서 다른 릴레이로 클라이언트의 불법 가능성이 있는 트래픽을 전달함으로써 통신의 익명성을 높입니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하세요. GuardDuty

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

UnauthorizedAccess:Runtime/TorClient

Amazon EC2 인스턴스 또는 컨테이너가 Tor Guard 또는 Authority 노드에 연결하고 있습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 사용자 AWS 환경의 EC2 인스턴스 또는 컨테이너가 Tor Guard 또는 Authority 노드에 연결되고 있음을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, Tor Guards 및 Authority 노드는 Tor 네트워크의 첫 번째 게이트웨이 역할을 합니다. 이 트래픽은 잠재적으로 EC2 인스턴스 또는 컨테이너가 손상되어 Tor 네트워크에서 클라이언트 역할을 하고 있음을 나타냅니다. 이 발견은 공격자의 실제 신원을 숨기려는 의도로 AWS 리소스에 무단으로 액세스했음을 의미할 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 침해된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Trojan:Runtime/BlackholeTraffic

Amazon EC2 인스턴스 또는 컨테이너가 블랙홀로 알려진 원격 호스트의 IP 주소와 통신을 시도하고 있습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 검색 결과는 나열된 EC2 인스턴스 또는 사용자 AWS 환경의 컨테이너가 블랙홀 (또는 싱크홀) 의 IP 주소와 통신을 시도하기 때문에 손상되었을 수 있음을 알려줍니다. 블랙홀은 데이터가 의도한 수신자에게 도달하지 않았음을 소스에 알리지 않고 수신 트래픽 또는 발신 트래픽을 자동으로 취소하는 네트워크의 위치입니다. 블랙홀 IP 주소는 실행되고 있지 않은 호스트 머신 또는 호스트가 할당되지 않은 주소를 지정합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Trojan:Runtime/DropPoint

Amazon EC2 인스턴스 또는 컨테이너가 맬웨어를 통해 캡처된 자격 증명 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 IP 주소와 통신을 시도하는 중입니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 검색 결과는 사용자 AWS 환경의 EC2 인스턴스 또는 컨테이너가 멀웨어로 캡처한 자격 증명 및 기타 도용 데이터를 보관하는 것으로 알려진 원격 호스트의 IP 주소와 통신을 시도하고 있음을 알려줍니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Amazon EC2 인스턴스 또는 컨테이너가 암호화폐 활동과 연결된 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경에 비트코인 또는 기타 암호화폐 관련 활동과 연결된 도메인 이름을 쿼리하는 나열된 EC2 인스턴스 또는 컨테이너가 있음을 알립니다. 위협 작업자는 악의적으로 승인되지 않은 암호화폐 채굴로 용도를 변경하기 위해 컴퓨팅 리소스를 제어하려고 할 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 EC2 인스턴스 또는 컨테이너를 사용하여 암호화폐를 채굴 또는 관리하거나 이 중 하나가 블록체인 활동에 관여한 경우, CryptoCurrency:Runtime/BitcoinTool.B!DNS 결과는 환경에 대한 예상된 활동일 수 있습니다. 사용자 AWS 환경에서 이런 경우에는 이 검색 결과에 대한 금지 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `CryptoCurrency:Runtime/BitcoinTool.B!DNS` 값을 사용해야 합니다. 두 번째 필터 기준은 암호화폐 또는 블록체인 활동에 관여한 인스턴스의 인스턴스 ID 또는 컨테이너의 컨테이너 이미지 ID여야 합니다. 자세한 내용은 억제 규칙을 참조하세요.

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Backdoor:Runtime/C&CActivity.B!DNS

Amazon EC2 인스턴스 또는 컨테이너가 알려진 명령 및 제어 서버와 연결된 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경 내에 알려진 명령 및 제어(C&C) 서버와 연결된 도메인 이름을 쿼리하는 나열된 EC2 인스턴스 또는 컨테이너가 있음을 알립니다. 나열된 EC2 인스턴스 또는 컨테이너가 손상되었을 수 있습니다. 명령 및 제어(C&C) 서버는 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다.

봇넷은 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스(PC, 서버, 모바일 디바이스 및 사물 인터넷 디바이스 포함)의 모음입니다. 일반적으로 봇넷은 맬웨어를 분산하고 부적절한 정보(예: 신용카드 번호)를 수집합니다. 봇넷의 용도와 구조에 따라 C&C 서버가 DDoS(분산 서비스 거부) 공격을 시작하는 명령을 실행할 수도 있습니다.

> **Note**
>
> 쿼리된 도메인 이름이 log4j와 관련된 경우 관련 결과의 필드에 다음 값이 포함됩니다.
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> 이 검색 유형이 어떻게 GuardDuty 생성되는지 테스트하려면 인스턴스 (`dig`Linux용 또는 `nslookup` Windows용) 에서 테스트 도메인을 `guarddutyc2activityb.com` 대상으로 DNS 요청을 보낼 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 GuardDuty 콘솔의 검색 결과 패널에서 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Trojan:Runtime/BlackholeTraffic!DNS

Amazon EC2 인스턴스 또는 컨테이너가 블랙홀 IP 주소로 리디렉션 중인 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 결과는 AWS 환경의 나열된 EC2 인스턴스 또는 컨테이너가 블랙홀 IP 주소로 리디렉션 중인 도메인 이름을 쿼리하기 때문에 손상되었을 수 있음을 알려줍니다. 블랙홀은 데이터가 의도한 수신자에게 도달하지 않았음을 소스에 알리지 않고 수신 트래픽 또는 발신 트래픽을 자동으로 취소하는 네트워크의 위치입니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Trojan:Runtime/DropPoint!DNS

Amazon EC2 인스턴스 또는 컨테이너가 맬웨어를 통해 캡처된 자격 증명 및 기타 도난 데이터를 보관하고 있는 것으로 알려진 원격 호스트의 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 검색 결과는 사용자 AWS 환경의 EC2 인스턴스 또는 컨테이너가 멀웨어로 캡처한 자격 증명 및 기타 도용 데이터를 보관하는 것으로 알려진 원격 호스트의 도메인 이름을 쿼리하고 있음을 알려줍니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Trojan:Runtime/DGADomainRequest.C!DNS

Amazon EC2 인스턴스 또는 컨테이너가 알고리즘을 통해 생성된 도메인을 쿼리하는 중입니다. 이러한 도메인은 일반적으로 맬웨어에서 사용되며 EC2 인스턴스 또는 컨테이너의 손상을 나타낼 수 있습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경에 도메인 생성 알고리즘(DGA) 도메인을 쿼리하려고 하는 나열된 EC2 인스턴스 또는 컨테이너가 있음을 알려줍니다. 리소스가 손상되었을 수 있습니다.

DGA는 C&C(명령 및 제어) 서버와의 랑데부 지점으로 사용할 수 있는 많은 수의 도메인 이름을 정기적으로 생성하는 데 사용됩니다. 명령 및 제어(C&C) 서버는 일반적인 유형의 맬웨어에 감염되어 해당 맬웨어의 제어를 받는 인터넷 연결 디바이스 모음인 봇넷의 멤버에게 명령을 발행하는 컴퓨터입니다. 감염된 컴퓨터가 업데이트 또는 명령을 수신하기 위해 매일 도메인 이름 중 일부에 접속을 시도하기 때문에 잠재적인 랑데부 지점이 많으면 봇넷을 효율적으로 종료하기가 어렵습니다.

> **Note**
>
> 이 결과는 GuardDuty 위협 인텔리전스 피드의 알려진 DGA 도메인을 기반으로 합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 침해된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Trojan:Runtime/DriveBySourceTraffic!DNS

Amazon EC2 인스턴스 또는 컨테이너가 드라이브 바이 다운로드 공격의 알려진 소스인 원격 호스트의 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경의 나열된 EC2 인스턴스 또는 컨테이너가 드라이브 바이 다운로드 공격의 알려진 소스인 원격 호스트의 도메인 이름을 쿼리하기 때문에 손상되었을 수 있음을 알려줍니다. 인터넷에서

이러한 컴퓨터 소프트웨어의 의도치 않은 다운로드로 인해 바이러스, 스파이웨어 또는 맬웨어가 자동으로 설치될 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Trojan:Runtime/PhishingDomainRequest!DNS

Amazon EC2 인스턴스 또는 컨테이너가 피싱 공격과 관련된 도메인을 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경에 피싱 공격과 관련된 도메인을 쿼리하려고 하는 EC2 인스턴스 또는 컨테이너가 있음을 알려줍니다. 피싱 도메인은 개인이 개인 식별 정보, 은행 및 신용 카드 세부 정보, 암호 등의 중요한 데이터 제공을 유도하기 위해 합법적인 기관으로 위장한 사람이 설정한 도메인입니다. EC2 인스턴스 또는 컨테이너에서 피싱 웹 사이트에 저장된 민감한 데이터를 검색하려고 하거나 피싱 웹 사이트를 설정하려고 할 수 있습니다. EC2 인스턴스 또는 컨테이너가 손상되었을 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Impact:Runtime/AbusedDomainRequest.Reputation

Amazon EC2 인스턴스 또는 컨테이너가 알려진 악용된 도메인과 연결된 평판이 낮은 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 결과는 AWS 환경 내에 나열된 EC2 인스턴스 또는 컨테이너가 알려진 악용된 도메인 또는 IP 주소와 연결된 평판이 낮은 도메인 이름을 쿼리하고 있음을 알립니다. 악용된 도메인의 예로는 동적 DNS 공급자뿐 아니라 무료 하위 도메인 등록을 제공하는 최상위 도메인 이름(TLD) 및 2단계 도메인 이름(2LD) 등이 있습니다. 위협 작업자는 이러한 서비스를 활용하여 무료로 또는 저렴한 비용으로 도메인을 등록하는 경향이 있습니다. 이 범주에서 평판이 낮은 도메인은 등록 기관의 파킹 IP 주소로 확인되는 만료된 도메인일 수도 있으며, 그에 따라 더 이상 활성화되지 않을 수도 있습니다. 파킹 IP에서 등록 기관은 어떤 서비스와도 연결되지 않은 도메인의 트래픽을 전달합니다. 위협 작업자가 일반적으로 이러한 등록 기관 또는 서비스를 C&C 및 맬웨어 배포에 사용하기 때문에 나열된 Amazon EC2 인스턴스 또는 컨테이너가 손상될 수 있습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Impact:Runtime/BitcoinDomainRequest.Reputation

Amazon EC2 인스턴스 또는 컨테이너가 암호화폐 관련 활동과 연결된 평판이 낮은 도메인 이름을 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경에 비트코인 또는 기타 암호화폐 관련 활동과 연결된 평판이 낮은 도메인 이름을 쿼리하는 나열된 EC2 인스턴스 또는 컨테이너가 있음을 알립니다. 위협 작업자는 악의적으로 승인되지 않은 암호화폐 채굴로 용도를 변경하기 위해 컴퓨팅 리소스를 제어하려고 할 수 있습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 EC2 인스턴스 또는 컨테이너를 사용하여 암호화폐를 채굴 또는 관리하거나 이러한 리소스가 블록체인 활동에 관여한 경우, 결과는 환경에 대한 예상된 활동을 나타낼 수 있습니다. 사용자 AWS 환경에서 이런 경우에는 이 검색 결과에 대한 금지 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 필터 기준에는 결과 유형 속성과 `Impact:Runtime/BitcoinDomainRequest.Reputation` 값을 사용해야 합니다. 두 번째 필터 기준은 암호화폐 또는 블록체인 관련 활동에 관여한 인스턴스의 인스턴스 ID 또는 컨테이너의 컨테이너 이미지 ID여야 합니다. 자세한 내용은 억제 규칙을 참조하세요.

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Impact:Runtime/MaliciousDomainRequest.Reputation

Amazon EC2 인스턴스 또는 컨테이너가 알려진 악성 도메인과 연결된 평판이 낮은 도메인을 쿼리하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 AWS 환경 내에 나열된 EC2 인스턴스 또는 컨테이너가 알려진 악성 도메인 또는 IP 주소와 연결된 평판이 낮은 도메인 이름을 쿼리하고 있음을 알립니다. 예를 들어 도메인이 알려진 싱크홀 IP 주소와 연결되어 있을 수 있습니다. 싱크홀 도메인은 이전에 위협 작업자가 통제한 도메인으로, 이러한 도메인에 대한 요청은 인스턴스 손상을 나타낼 수 있습니다. 이러한 도메인은 알려진 악성 캠페인 또는 도메인 생성 알고리즘과도 상관관계가 있을 수 있습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Amazon EC2 인스턴스 또는 컨테이너의 수명 또는 적은 사용으로 인해 의심스러운 평판이 낮은 도메인 이름을 쿼리하고 있습니다.

기본 심각도: 낮음

- 특성: Runtime Monitoring

이 결과는 AWS 환경 내에 나열된 EC2 인스턴스 또는 컨테이너가 악성인 것으로 의심되는 평판이 낮은 도메인 이름을 쿼리하고 있음을 알려줍니다. 이 도메인의 특성은 이전에 관찰된 악성 도메인과 일치했지만, 당사의 평판 모델에서는 알려진 위협과 확실한 상관관계를 파악할 수 없었습니다. 이러한 도메인은 대체로 새로 관찰되었거나 트래픽이 적습니다.

평판이 낮은 도메인은 평판 점수 모델을 기반으로 합니다. 이 모델은 도메인의 특성을 평가하고 순위를 매겨 악성일 가능성을 판단합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Amazon EC2 인스턴스 또는 컨테이너가 인스턴스 메타데이터 서비스로 확인되는 DNS 조회를 수행하고 있습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

> **Note**
>
> 현재 이 검색 유형은 AMD64 아키텍처에서만 지원됩니다.

이 검색 결과는 사용자 AWS 환경의 EC2 인스턴스 또는 컨테이너가 EC2 메타데이터 IP 주소(169.254.169.254) 로 확인되는 도메인을 쿼리하고 있음을 알려줍니다. 이러한 종류의 DNS 쿼리는 인스턴스가 DNS 리바인딩 기술의 대상임을 나타낼 수 있습니다. 이 기술은 인스턴스와 연결된 IAM 보안 인증 정보를 포함하여 EC2 인스턴스의 메타데이터를 가져오는 데 사용할 수 있습니다.

DNS 리바인딩은 URL의 도메인 이름이 EC2 메타데이터 IP 주소(`169.254.169.254`)로 확인되는 URL의 리턴 데이터를 로드하도록 EC2 인스턴스에서 실행 중인 애플리케이션을 속이는 작업이 포함됩니다. 이렇게 하면 애플리케이션에서 EC2 메타데이터에 액세스하여 공격자가 사용 가능하도록 만듭니다.

EC2 인스턴스가 URL을 삽입할 수 있도록 취약한 애플리케이션을 실행 중인 경우 또는 다른 누군가가 EC2 인스턴스에서 실행 중인 웹 브라우저에서 URL에 액세스하는 경우에만 DNS 리바인딩을 사용하여 EC2 메타데이터에 액세스할 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 결과에 대한 응답으로, EC2 인스턴스 또는 컨테이너에서 실행 중인 취약한 애플리케이션이 있는지 여부 또는 다른 누군가가 브라우저를 사용하여 결과에서 확인된 도메인에 액세스했는지 여부를 평가해야 합니다. 근본 원인이 취약한 애플리케이션인 경우 취약성을 수정합니다. 누군가 식별된 도메인을 검색한 경우 도메인을 차단하거나 사용자 액세스를 방지합니다. 결과가 위의 경우 중 하나와 관련된 것으로 확인된다면 EC2 인스턴스와 연결된 세션을 취소하세요.

일부 AWS 고객은 메타데이터 IP 주소를 신뢰할 수 있는 DNS 서버의 도메인 이름에 의도적으로 매핑합니다. 환경에서 이러한 경우 이 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 필터 기준에는 결과 유형 속성과 `UnauthorizedAccess:Runtime/MetaDataDNSRebind` 값을 사용해야 합니다. 두 번째 필터 기준은 컨테이너의 DNS 요청 도메인 또는 컨테이너 이미지 ID여야 합니다. DNS 요청 도메인 값은 메타데이터 IP 주소(`169.254.169.254`)에 매핑한 도메인과 일치해야 합니다. 억제 규칙 작성에 대한 내용은 억제 규칙을 참조하세요.

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Execution:Runtime/NewBinaryExecuted

컨테이너에서 새로 생성되었거나 최근에 수정된 바이너리 파일이 실행되었습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 결과는 컨테이너에서 새로 생성되었거나 최근에 수정된 바이너리 파일이 실행되었음을 알려줍니다. 런타임 시 컨테이너를 변경할 수 없도록 유지하는 것이 가장 좋으며, 컨테이너의 수명 동안 바이너리 파일, 스크립트 또는 라이브러리를 생성 또는 수정해서는 안 됩니다. 이 동작은 컨테이너에 대한 액세스 권한을 획득한 악의적인 공격자가 잠재적 침해의 일환으로 멀웨어 또는 기타 소프트웨어를 다운로드하고 실행했음을 나타냅니다. 이러한 유형의 활동은 침해의 징후일 수 있지만 일반적인 사용 패턴이기도 합니다. 따라서 GuardDuty 는 메커니즘을 사용하여 이 활동의 의심스러운 인스턴스를 식별하고 의심스러운 인스턴스에 대해서만 이 검색 유형을 생성합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 침해된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 리소스 유형을 확인하세요. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

PrivilegeEscalation:Runtime/DockerSocketAccessed

컨테이너 내부의 프로세스가 Docker 소켓을 사용하여 Docker 대몬과 통신하고 있습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

Docker 소켓은 Docker 대몬(`dockerd`)이 클라이언트와 통신하는 데 사용하는 Unix 도메인 소켓입니다. 클라이언트는 Docker 소켓을 통해 Docker 대몬과 통신하여 컨테이너를 생성하는 등의 다양한 작업을 수행할 수 있습니다. 컨테이너 프로세스가 Docker 소켓에 액세스하는 것으로 의심됩니다. 컨테이너 프로세스는 Docket 소켓과 통신하고 권한이 있는 컨테이너를 생성하여 컨테이너를 이스케이프하고 호스트 수준의 액세스 권한을 얻을 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

PrivilegeEscalation:Runtime/RuncContainerEscape

RunC를 통한 컨테이너 이스케이프 시도가 감지되었습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

RunC는 Docker 및 Containerd와 같은 고수준 컨테이너 런타임에서 컨테이너를 생성하고 실행하는 데 사용하는 저수준 컨테이너 런타임입니다. RunC는 컨테이너를 생성하는 저수준 작업을 수행해야 하므로 항상 루트 권한으로 실행됩니다. 위협 행위자는 RunC 바이너리의 취약성을 수정하거나 악용하여 호스트 수준의 액세스 권한을 얻을 수 있습니다.

이 발견은 RunC 바이너리의 수정과 다음과 같은 RunC 취약성을 악용하려는 잠재적 시도를 탐지합니다.

- CVE-2019-5736— 악용에는 컨테이너 내에서 RunC 바이너리를 덮어쓰는 것이 CVE-2019-5736 포함됩니다. 이 검색 결과는 RunC 바이너리가 컨테이너 내부 프로세스에 의해 수정될 때 호출됩니다.
- CVE-2024-21626— 악용에는 현재 작업 디렉토리 (CWD) 또는 컨테이너를 열린 파일 디스크립터로 설정하는 것이 CVE-2024-21626 포함됩니다. `/proc/self/fd/FileDescriptor` 예를 들어, 현재 작업 디렉터리가 있는 컨테이너 프로세스가 탐지되면 이 검색 결과가 `/proc/self/fd/` 호출됩니다. `/proc/self/fd/7`

이 결과는 악의적인 행위자가 다음 유형의 컨테이너 중 하나에서 악용을 시도했음을 나타낼 수 있습니다.

- 공격자 제어 이미지가 포함된 새 컨테이너.
- 호스트 수준 RunC 바이너리에 대한 쓰기 권한으로 행위자가 액세스할 수 있었던 기존 컨테이너입니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하세요. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

CGroups 릴리스 에이전트를 통한 컨테이너 이스케이프 시도가 감지되었습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 결과는 제어 그룹(cgroup) 릴리스 에이전트 파일을 수정하려는 시도가 탐지되었음을 알려줍니다. Linux는 제어 그룹(cgroup)을 사용하여 프로세스 컬렉션의 리소스 사용을 제한, 처리 및 격리합니다. 각 cgroup에는 cgroup 내부의 프로세스가 종료될 때 Linux에서 실행하는 스크립트인 릴리스 에이전트 파일(`release_agent`)이 있습니다. 릴리스 에이전트 파일은 항상 호스트 수준에서 실행됩니다. 컨테이너 내부의 위협 작업자는 cgroup에 속하는 릴리스 에이전트 파일에 임의의 명령을 작성하여 호스트로 이스케이프할 수 있습니다. 해당 cgroup 내부의 프로세스가 종료되면 해당 작업자가 작성한 명령이 실행됩니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하세요. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

DefenseEvasion:Runtime/ProcessInjection.Proc

proc 파일 시스템을 사용한 프로세스 주입이 컨테이너 또는 Amazon EC2 인스턴스에서 탐지되었습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

프로세스 주입은 위협 작업자가 프로세스에 코드를 주입하여 방어를 우회하고 잠재적으로 권한을 상승시키는 데 사용하는 기법입니다. proc 파일 시스템(procfs)은 프로세스의 가상 메모리를 파일로 표시하는 Linux의 특수 파일 시스템입니다. 해당 파일의 경로는 `/proc/PID/mem`으로, `PID`는 프로세스의 고유한 ID입니다. 위협 작업자는 이 파일에 쓰고 프로세스에 코드를 삽입할 수 있습니다. 이 결과는 이 파일에 대한 잠재적 쓰기 시도를 식별합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스 유형이 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

ptrace 시스템 호출을 사용한 프로세스 주입이 컨테이너 또는 Amazon EC2 인스턴스에서 탐지되었습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

프로세스 주입은 위협 작업자가 프로세스에 코드를 주입하여 방어를 우회하고 잠재적으로 권한을 상승시키는 데 사용하는 기법입니다. 프로세스는 ptrace 시스템 호출을 사용하여 다른 프로세스에 코드를 주입할 수 있습니다. 이 결과는 ptrace 시스템 호출을 사용하여 프로세스에 코드를 주입하려는 잠재적 시도를 식별합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스 유형이 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

컨테이너 또는 Amazon EC2 인스턴스에서 가상 메모리에 직접 쓰기를 통한 프로세스 주입이 탐지되었습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

프로세스 주입은 위협 작업자가 프로세스에 코드를 주입하여 방어를 우회하고 잠재적으로 권한을 상승시키는 데 사용하는 기법입니다. 프로세스는 `process_vm_writev`와 같은 시스템 호출을 사용하여 다른 프로세스의 가상 메모리에 코드를 직접 주입할 수 있습니다. 이 결과는 프로세스의 가상 메모리에 쓰기 위한 시스템 호출을 사용하여 프로세스에 코드를 주입하려는 잠재적 시도를 식별합니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 GuardDuty 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스 유형이 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Execution:Runtime/ReverseShell

컨테이너 또는 Amazon EC2 인스턴스의 프로세스가 리버스 쉘을 생성했습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

리버스 쉘은 대상 호스트에서 작업자의 호스트로 시작되는 연결에서 생성된 쉘 세션입니다. 이는 작업자의 호스트에서 대상 호스트로 시작되는 일반 쉘과는 반대 방향입니다. 위협 작업자는 대상에 대한 초기 액세스 권한을 획득한 후 리버스 쉘을 생성하여 대상에 명령을 실행합니다. 이 결과는 리버스 쉘을 생성하려는 잠재적 시도를 식별합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스 유형이 손상되었을 수 있습니다.

DefenseEvasion:Runtime/FilelessExecution

컨테이너 또는 Amazon EC2 인스턴스의 프로세스가 메모리에서 코드를 실행하고 있습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 결과는 디스크의 메모리 내 실행 파일을 사용하여 프로세스가 실행되는 상황을 알립니다. 이는 파일 시스템 스캔 기반 탐지를 우회하기 위해 악성 실행 파일을 디스크에 쓰는 것을 방지하는 일반적인 방어 우회 기법입니다. 이 기법은 맬웨어에서 사용되지만 일부 합법적인 사용 사례도 있습니다. 예제 중 하나는 컴파일된 코드를 메모리에 쓰고 메모리에서 실행하는 just-in-time (JIT) 컴파일러입니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 패널에서 리소스 유형을 확인하세요. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Impact:Runtime/CryptoMinerExecuted

컨테이너 또는 Amazon EC2 인스턴스가 암호화폐 채굴 활동과 연결된 바이너리 파일을 실행하는 중입니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 검색 결과는 사용자 AWS 환경의 컨테이너 또는 EC2 인스턴스가 암호화폐 채굴 활동과 관련된 바이너리 파일을 실행하고 있음을 알려줍니다. 위협 작업자는 악의적으로 승인되지 않은 암호화폐 채굴로 용도를 변경하기 위해 컴퓨팅 리소스를 제어하려고 할 수 있습니다.

런타임 에이전트는 여러 리소스 유형의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 결과 패널에서 리소스 유형을 확인하세요. GuardDuty

해결 권장 사항:

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 GuardDuty 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하고 을 참조하십시오런타임 모니터링 결과 수정.

Execution:Runtime/NewLibraryLoaded

새로 생성되거나 최근에 수정된 라이브러리가 컨테이너 내부의 프로세스에 의해 로드되었습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

이 결과는 라이브러리가 런타임 중에 컨테이너 내부에서 생성 또는 수정되었고 컨테이너 내부에서 실행 중인 프로세스에 의해 로드되었음을 알려줍니다. 런타임 시 컨테이너를 변경할 수 없도록 유지하고, 컨테이너의 수명 동안 바이너리 파일, 스크립트 또는 라이브러리를 생성 또는 수정할 수 없도록 하는 것이 좋습니다. 새로 생성하거나 수정된 라이브러리를 컨테이너에 로드하는 것은 의심스러운 활동을 의미할 수 있습니다. 이 동작은 악의적인 작업자가 컨테이너에 대한 액세스 권한을 획득하고 잠재적 침해의 일환으로 맬웨어 또는 기타 소프트웨어를 다운로드하고 실행했음을 나타냅니다. 이러한 유형의 활동은 손상의 징후일 수 있지만 일반적인 사용 패턴이기도 합니다. 따라서 GuardDuty 는 메커니즘을 사용하여 이 활동의 의심스러운 인스턴스를 식별하고 의심스러운 인스턴스에 대해서만 이 검색 유형을 생성합니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하세요. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

컨테이너 내부의 프로세스가 런타임 시 호스트 파일 시스템을 탑재했습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

여러 컨테이너 이스케이프 기법에는 런타임 시 컨테이너 내부에 호스트 파일 시스템을 탑재하는 과정이 포함됩니다. 이 결과는 컨테이너 내부의 프로세스가 호스트 파일 시스템을 탑재하려고 시도했을 가능성이 있음을 알려주며, 이는 호스트로 이스케이프하려는 시도를 의미할 수 있습니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 GuardDuty 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

PrivilegeEscalation:Runtime/UserfaultfdUsage

프로세스에서 **`userfaultfd`** 시스템 호출을 사용하여 사용자 공간의 페이지 장애를 처리했습니다.

기본 심각도: 중간

- 특성: Runtime Monitoring

대체로 페이지 장애는 커널 공간의 커널에서 처리합니다. 하지만 `userfaultfd` 시스템 호출을 통해 프로세스에서 사용자 공간에 있는 파일 시스템의 페이지 장애를 처리할 수 있습니다. 이는 사용자 공간 파일 시스템 구현을 가능하게 하는 유용한 기능입니다. 반대로 잠재적으로 악의적인 프로세스가 사용자 공간에서 커널을 중단시키는 데 사용될 수도 있습니다. `userfaultfd` 시스템 호출을 사용하여 커널을 중단하는 것은 커널 교착 조건을 악용하는 동안 교착 기간을 연장하기 위한 일반적인 악용 기법입니다. `userfaultfd` 사용은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서의 의심스러운 활동을 나타낼 수 있습니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 GuardDuty 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하세요.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Execution:Runtime/SuspiciousTool

컨테이너 또는 Amazon EC2 인스턴스가 보안 테스트 참여와 같은 불쾌한 보안 시나리오에서 자주 사용되는 바이너리 파일 또는 스크립트를 실행하고 있습니다.

기본 심각도: 가변적

이 발견의 심각도는 탐지된 의심스러운 도구가 이중 용도로 간주되는지 아니면 오용으로만 사용되는지에 따라 높거나 낮을 수 있습니다.

- 특성: Runtime Monitoring

이 발견은 사용자 환경 내의 EC2 인스턴스 또는 컨테이너에서 의심스러운 도구가 실행되었음을 알려줍니다. AWS 여기에는 백도어 도구, 네트워크 스캐너, 네트워크 스니퍼라고도 하는 침입 테스트 작업에 사용되는 도구가 포함됩니다. 이러한 도구는 모두 무해한 상황에서도 사용할 수 있지만 악의적인 의도를 가진 위협 행위자들도 자주 사용합니다. 공격적인 보안 도구를 관찰하면 관련 EC2 인스턴스 또는 컨테이너가 손상되었음을 알 수 있습니다.

GuardDuty 관련 런타임 활동 및 컨텍스트를 검사하여 관련 활동 및 컨텍스트가 잠재적으로 의심스러운 경우에만 이 결과를 생성하도록 합니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Execution:Runtime/SuspiciousCommand

Amazon EC2 인스턴스 또는 컨테이너에서 손상을 나타내는 의심스러운 명령이 실행되었습니다.

기본 심각도: 가변적

관찰된 악성 패턴의 영향에 따라 이 탐지 유형의 심각도는 낮음, 보통 또는 높을 수 있습니다.

- 특성: Runtime Monitoring

이 발견은 의심스러운 명령이 실행되었음을 알려주며, Amazon EC2 인스턴스 또는 AWS 사용자 환경의 컨테이너가 손상되었음을 나타냅니다. 이는 의심스러운 출처에서 파일을 다운로드한 후 실행했거나, 실행 중인 프로세스의 명령줄에 알려진 악성 패턴이 표시되었음을 의미할 수 있습니다. 이는 또한 시스템에서 멀웨어가 실행되고 있음을 나타냅니다.

GuardDuty 관련 런타임 활동 및 컨텍스트를 검사하여 관련 활동 및 컨텍스트가 잠재적으로 의심스러운 경우에만 이 결과를 생성하도록 합니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

DefenseEvasion:Runtime/SuspiciousCommand

나열된 Amazon EC2 인스턴스 또는 컨테이너에서 명령이 실행되면 방화벽이나 필수 시스템 서비스와 같은 Linux 방어 메커니즘을 수정하거나 비활성화하려고 시도합니다.

기본 심각도: 가변적

수정되거나 비활성화된 방어 메커니즘에 따라 이 검색 유형의 심각도는 높음, 중간 또는 낮을 수 있습니다.

- 특성: Runtime Monitoring

이 검색 결과는 로컬 시스템의 보안 서비스로부터 공격을 숨기려는 명령이 실행되었음을 알려줍니다. 여기에는 Unix 방화벽 비활성화, 로컬 IP 테이블 수정, crontab 항목 제거, 로컬 서비스 비활성화 또는 기능 인수와 같은 작업이 포함됩니다. `LDPreload` 모든 수정은 매우 의심스러우며 잠재적 손상의 징후가 될 수 있습니다. 따라서 이러한 메커니즘은 시스템의 추가 손상을 감지하거나 방지합니다.

GuardDuty 관련 런타임 활동 및 컨텍스트를 검사하여 관련 활동 및 컨텍스트가 잠재적으로 의심스러운 경우에만 이 결과를 생성하도록 합니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

DefenseEvasion:Runtime/PtraceAntiDebugging

컨테이너 또는 Amazon EC2 인스턴스의 프로세스가 ptrace 시스템 호출을 사용하여 디버깅 방지 조치를 실행했습니다.

기본 심각도: 낮음

- 특성: Runtime Monitoring

이 결과는 Amazon EC2 인스턴스 또는 AWS 환경 내의 컨테이너에서 실행 중인 프로세스가 옵션과 함께 ptrace 시스템 호출을 사용했음을 보여줍니다. `PTRACE_TRACEME` 이 활동으로 인해 연결된 디버거가 실행 중인 프로세스에서 분리됩니다. 연결된 디버거가 없으면 아무 효과가 없습니다. 그러나 활동 자체가 의심을 불러일으키고 있습니다. 이는 시스템에서 멀웨어가 실행되고 있음을 의미할 수 있습니다. 멀웨어는 분석을 회피하기 위해 디버그 방지 기술을 자주 사용하며, 이러한 기법은 런타임에 탐지될 수 있습니다.

GuardDuty 관련 런타임 활동 및 컨텍스트를 검사하여 관련 활동 및 컨텍스트가 잠재적으로 의심스러운 경우에만 이 결과를 생성하도록 합니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 정보는 런타임 모니터링 결과 수정을 참조하세요.

Execution:Runtime/MaliciousFileExecuted

알려진 악성 실행 파일이 Amazon EC2 인스턴스 또는 컨테이너에서 실행되었습니다.

기본 심각도: 높음

- 특성: Runtime Monitoring

이 발견은 알려진 악성 실행 파일이 Amazon EC2 인스턴스 또는 환경 내의 컨테이너에서 실행되었음을 알려줍니다. AWS 이는 인스턴스 또는 컨테이너가 잠재적으로 손상되었으며 멀웨어가 실행되었음을 나타내는 강력한 지표입니다.

멀웨어는 분석을 회피하기 위해 디버그 방지 기술을 자주 사용하며, 이러한 기법은 런타임에 탐지될 수 있습니다.

GuardDuty 관련 런타임 활동 및 컨텍스트를 검사하여 관련 활동 및 컨텍스트가 잠재적으로 의심스러운 경우에만 이 결과를 생성하도록 합니다.

런타임 에이전트는 여러 리소스의 이벤트를 모니터링합니다. 영향을 받는 리소스를 식별하려면 콘솔의 검색 결과 세부 정보에서 리소스 유형을 확인하십시오. GuardDuty

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 리소스가 손상되었을 수 있습니다. 자세한 내용은 런타임 모니터링 결과 수정을(를) 참조하세요.

GuardDuty S3 검색 유형

다음 결과는 Amazon S3 리소스에만 해당되며, 데이터 소스가 S3용 데이터 **S3Bucket** **AccessKey** 이벤트인지 또는 CloudTrail 데이터 소스가 CloudTrail 관리 이벤트인지를 리소스 유형으로 지정합니다. 결과의 심각도 및 세부 정보는 결과 유형 및 버킷과 연결된 권한에 따라 다릅니다.

여기에 나열된 결과에는 해당 결과 유형을 생성하는 데 사용된 데이터 소스 및 모델이 포함됩니다. 데이터 소스 및 모델에 대한 자세한 내용은 기본 데이터 소스 섹션을 참조하세요.

> **Important**
>
> S3에 대한 CloudTrail 데이터 소스의 데이터 이벤트 검색 결과는 S3 보호를 활성화한 경우에만 생성됩니다 GuardDuty. S3 보호는 2020년 7월 31일 이후에 생성된 모든 계정에서 기본적으로 활성화됩니다. S3 보호 활성화 또는 비활성화 방법에 대한 내용은 아마존에서의 아마존 S3 보호 GuardDuty 섹션을 참조하세요.

모든 S3Bucket 유형 결과의 경우 해당 버킷에 대한 권한과 결과에 관련된 모든 사용자의 권한을 검사하는 것이 좋습니다. 예기치 않은 활동인 경우 잠재적으로 손상된 S3 버킷 수정에서 설명하는 해결 권장 사항을 참조하세요.

주제

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

S3 객체를 검색하는 데 일반적으로 사용되는 API가 변칙적인 방식으로 간접 호출되었습니다.

기본 심각도: 낮음

- 데이터 소스: S3의 CloudTrail 데이터 이벤트

이 결과는 IAM 엔터티가 환경에서 S3 버킷을 검색하기 위한 S3 API(예: `ListObjects`)를 간접적으로 호출했음을 알려줍니다. 이러한 유형의 활동은 공격자가 정보를 수집하여 사용자 AWS 환경이 광범위

한 공격에 취약한지 여부를 판단하는 공격의 검색 단계와 관련이 있습니다. IAM 엔터티가 비정상적인 방식으로 API를 간접 호출했기 때문에 이 활동은 의심스럽습니다. 예를 들어 이전 기록이 없는 IAM 엔터티가 S3 API를 간접적으로 호출하거나, IAM 엔터티가 비정상적인 위치에서 S3 API를 호출합니다.

이 API는 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에서 변칙 API로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API, 요청된 버킷 및 API 호출 수 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Discovery:S3/MaliciousIPCaller

AWS 환경에서 리소스를 검색하는 데 일반적으로 사용되는 S3 API가 알려진 악성 IP 주소에서 호출되었습니다.

기본 심각도: 높음

- 데이터 소스: CloudTrail S3의 데이터 이벤트

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 S3 API 작업이 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 환경에 대한 정보를 수집하는 공격의 탐지 단계와 관련이 있습니다 AWS . 예를 들면 `GetObjectAcl`나 `ListObjects`와 같습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Discovery:S3/MaliciousIPCaller.Custom

사용자 지정 위협 목록의 IP 주소에서 S3 API를 간접적으로 호출했습니다.

기본 심각도: 높음

- 데이터 소스: S3용 CloudTrail 데이터 이벤트

이 결과는 S3 API(예: `GetObjectAcl` 또는 `ListObjects`)가 사용자가 업로드한 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이 결과와 관련된 위협 목록은 결과 세부 정보의 추가 정보 섹션에 나열됩니다. 이 활동 유형은 일반적으로 공격자가 AWS 환경이 광범위한 공격에 취약한지 판단하기 위해 정보를 수집하는 공격의 발견 단계와 관련이 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Discovery:S3/TorIPCaller

Tor 출구 노드 IP 주소에서 S3 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: S3의 CloudTrail 데이터 이벤트

이 결과는 S3 API(예: `GetObjectAcl` 또는 `ListObjects`)가 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이러한 유형의 활동은 공격자가 정보를 수집하여 사용자 AWS 환경이 광범위한 공격에 취약한지 여부를 판단하는 공격의 검색 단계와 관련이 있습니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 ID를 숨기려는 의도로 AWS 리소스에 무단으로 액세스했음을 의미할 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Exfiltration:S3/AnomalousBehavior

IAM 엔터티가 의심스러운 방식으로 S3 API를 간접적으로 호출했습니다.

기본 심각도: 높음

- 데이터 소스: CloudTrail S3의 데이터 이벤트

이 결과는 IAM 엔터티가 S3 버킷과 관련되고 해당 엔터티의 설정된 기준과 다른 활동임을 알려줍니다. 이 활동에 사용되는 API 호출은 공격자가 데이터 수집을 시도하는 공격의 유출 단계와 관련이 있습니다. IAM 엔터티가 비정상적인 방식으로 API를 간접 호출했기 때문에 이 활동은 의심스럽습니다. 예를 들어 이전 기록이 없는 IAM 엔터티가 S3 API를 간접적으로 호출하거나, IAM 엔터티가 비정상적인 위치에서 S3 API를 호출합니다.

이 API는 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에서 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API, 요청된 버킷 및 API 호출 수 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Exfiltration:S3/MaliciousIPCaller

AWS 환경에서 데이터를 수집하는 데 일반적으로 사용되는 S3 API가 알려진 악성 IP 주소에서 호출되었습니다.

기본 심각도: 높음

- 데이터 소스: CloudTrail S3의 데이터 이벤트

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 S3 API 작업이 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 네트워크에서 데이터를 수집하려는 유출 전략과 관련이 있습니다. 예를 들면 `GetObject`나 `CopyObject`와 같습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Impact:S3/AnomalousBehavior.Delete

IAM 엔터티가 의심스러운 방식으로 데이터를 삭제하는 S3 API를 간접적으로 호출했습니다.

기본 심각도: 높음

- 데이터 소스: S3의 CloudTrail 데이터 이벤트

이 결과는 사용자 AWS 환경의 IAM 엔티티가 S3 버킷과 관련된 API 호출을 수행하고 있으며 이 동작은 해당 엔티티의 설정된 기준과 다르다는 것을 알려줍니다. 이 활동에 사용된 API 호출은 데이터 삭제를 시도하는 공격과 관련이 있습니다. IAM 엔터티가 비정상적인 방식으로 API를 간접 호출했기 때문에 이 활동은 의심스럽습니다. 예를 들어 이전 기록이 없는 IAM 엔터티가 S3 API를 간접적으로 호출하거나, IAM 엔터티가 비정상적인 위치에서 S3 API를 호출합니다.

이 API는 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 이상 API로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API, 요청된 버킷 및 API 호출 수 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

S3 버킷의 콘텐츠를 감사하여 이전 객체 버전을 복원할 수 있는지 또는 복원해야 하는지 판단하는 것이 좋습니다.

Impact:S3/AnomalousBehavior.Permission

액세스 제어 목록(ACL) 권한을 설정할 때 일반적으로 사용되는 API가 변칙적인 방식으로 간접 호출되었습니다.

기본 심각도: 높음

- 데이터 소스: S3의 데이터 이벤트 CloudTrail

이 결과는 사용자 AWS 환경의 IAM 엔티티가 나열된 S3 버킷의 버킷 정책 또는 ACL을 변경했음을 알려줍니다. 이 변경으로 인해 S3 버킷이 인증된 모든 사용자에게 공개적으로 노출될 수 있습니다. AWS

이 API는 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 변칙으로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API, 요청된 버킷 및 API 호출 수 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

S3 버킷의 콘텐츠를 감사하여 예기치 않게 공개 액세스가 허용된 객체가 없는지 확인하는 것이 좋습니다.

Impact:S3/AnomalousBehavior.Write

IAM 엔터티가 의심스러운 방식으로 데이터를 쓰는 S3 API를 간접적으로 호출했습니다.

기본 심각도: 중간

- 데이터 소스: S3의 데이터 이벤트 CloudTrail

이 결과는 사용자 AWS 환경의 IAM 엔티티가 S3 버킷과 관련된 API 호출을 수행하고 있으며 이 동작은 해당 엔티티의 설정된 기준과 다르다는 것을 알려줍니다. 이 활동에 사용된 API 호출은 데이터 쓰기를 시도하는 공격과 관련이 있습니다. IAM 엔터티가 비정상적인 방식으로 API를 간접 호출했기 때문에 이 활동은 의심스럽습니다. 예를 들어 이전 기록이 없는 IAM 엔터티가 S3 API를 간접적으로 호출하거나, IAM 엔터티가 비정상적인 위치에서 S3 API를 호출합니다.

이 API는 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델에 의해 이상 API로 식별되었습니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. 요청한 사용자, 요청이 이루어진 위치, 요청된 특정 API, 요청된 버킷 및 API 호출 수 등 API 요청의 다양한 요소를 추적합니다. 요청을 간접적으로 호출한 사용자 ID에서 API 요청의 어떤 요소가 비정상적인지에 관한 세부 정보는 결과 세부 정보에서 확인할 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

S3 버킷의 콘텐츠를 감사하여 이 API 호출로 악의적이거나 승인되지 않은 데이터를 쓰지 않았는지 확인하는 것이 좋습니다.

Impact:S3/MaliciousIPCaller

AWS 환경의 데이터나 프로세스를 변조하는 데 일반적으로 사용되는 S3 API가 알려진 악성 IP 주소에서 호출되었습니다.

기본 심각도: 높음

- 데이터 소스: CloudTrail S3의 데이터 이벤트

이 결과는 알려진 악성 활동과 관련된 IP 주소에서 S3 API 작업이 간접적으로 호출되었음을 알려줍니다. 관찰된 API는 일반적으로 공격자가 환경 내의 데이터를 조작, 방해 또는 파괴하려고 하는 충격 전술과 관련이 있습니다. AWS 예를 들면 `PutObject`나 `PutObjectAcl`와 같습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

PenTest:S3/KaliLinux

Kali Linux 머신에서 S3 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: S3용 데이터 이벤트 CloudTrail

이 결과는 Kali Linux를 실행하는 시스템이 사용자 계정에 AWS 속한 자격 증명을 사용하여 S3 API를 호출하고 있음을 알려줍니다. 자격 증명이 손상되었을 수 있습니다. Kali Linux는 보안 전문가가 패치가 필요한 EC2 인스턴스의 약점을 식별하기 위해 널리 사용하는 침투 테스트 도구입니다. 또한 공격자는 이 도구를 사용하여 EC2 구성 취약점을 찾아 사용자 환경에 대한 무단 액세스를 확보합니다. AWS

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

PenTest:S3/ParrotLinux

Parrot Security Linux 머신에서 S3 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: S3의 CloudTrail 데이터 이벤트

이 결과는 Parrot Security Linux를 실행하는 시스템이 사용자 계정에 AWS 속한 자격 증명을 사용하여 S3 API를 호출하고 있음을 알려줍니다. 자격 증명이 손상되었을 수 있습니다. Parrot Security Linux는 보안 전문가가 패치가 필요한 EC2 인스턴스의 약점을 식별하기 위해 널리 사용하는 침투 테스트 도구입니다. 또한 공격자가 이 도구를 사용하여 EC2 구성의 약점을 찾아 AWS 환경에 대한 무단 액세스 권한을 얻기도 합니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

PenTest:S3/PentooLinux

Pentoo Linux 머신에서 S3 API가 간접적으로 호출되었습니다.

기본 심각도: 중간

- 데이터 소스: S3용 CloudTrail 데이터 이벤트

이 결과는 Pentoo Linux를 실행하는 컴퓨터가 사용자 계정에 AWS 속한 자격 증명을 사용하여 S3 API를 호출하고 있음을 알려줍니다. 자격 증명이 손상되었을 수 있습니다. Pentoo Linux는 보안 전문가가 패치가 필요한 EC2 인스턴스의 약점을 식별하기 위해 널리 사용하는 침투 테스트 도구입니다. 또한 공격자는 이 도구를 사용하여 EC2 구성 약점을 찾아 사용자 환경에 무단으로 액세스합니다. AWS

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Policy:S3/AccountBlockPublicAccessDisabled

IAM 엔터티가 계정에서 S3 퍼블릭 액세스 차단을 비활성화하는 데 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 낮음

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 Amazon S3 퍼블릭 액세스 차단이 계정 수준에서 비활성화되었음을 알려줍니다. S3 퍼블릭 액세스 차단이 활성화된 경우 데이터의 우발적인 공개 노출을 방지하기 위한 보안 조치로 버킷의 정책 또는 액세스 제어 목록(ACL)을 필터링하는 데 사용됩니다.

일반적으로 버킷 또는 버킷의 객체에 대한 퍼블릭 액세스를 허용하기 위해 계정에서 S3 퍼블릭 액세스 차단이 해제됩니다. 계정에 대해 S3 퍼블릭 액세스 차단이 비활성화되면 버킷에 대한 액세스는 개별 버킷에 적용된 정책, ACL 또는 버킷 수준의 퍼블릭 액세스 차단 설정에 의해 제어됩니다. 버킷이 반드시 공개적으로 공유되는 것은 아니지만 버킷에 적용된 권한을 감사하여 적절한 액세스 수준을 제공하는지 확인해야 합니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Policy:S3/BucketAnonymousAccessGranted

IAM 보안 주체가 버킷 정책 또는 ACL을 변경하여 인터넷에 S3 버킷에 대한 액세스 권한을 부여했습니다.

기본 심각도: 높음

- 데이터 소스: CloudTrail 관리 이벤트

이 결과는 IAM 엔터티가 해당 버킷의 버킷 정책 또는 ACL을 변경했기 때문에 나열된 S3 버킷이 인터넷에서 공개적으로 액세스할 수 있게 되었음을 알려줍니다. 정책 또는 ACL 변경이 탐지되면 Zelkova 기반의 자동 추론을 사용하여 버킷에 공개적으로 액세스할 수 있는지 확인합니다.

> **Note**
>
> 버킷의 ACL 또는 버킷 정책이 명시적 거부 또는 모두 거부로 구성된 경우 이 결과는 버킷의 현재 상태를 반영하지 않을 수 있습니다. 이 결과에는 S3 버킷에 대해 활성화되었을 수 있는 S3 퍼블릭 액세스 차단 설정이 반영되지 않습니다. 이 경우 결과의 `effectivePermission` 값은 `UNKNOWN`으로 표시됩니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Policy:S3/BucketBlockPublicAccessDisabled

IAM 엔터티가 버킷에서 S3 퍼블릭 액세스 차단을 비활성화하는 데 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 낮음

- 데이터 소스: CloudTrail 관리 이벤트

이 결과는 퍼블릭 액세스 차단이 나열된 S3 버킷에서 비활성화되었음을 알려줍니다. 활성화된 경우 S3 퍼블릭 액세스 차단은 데이터의 우발적인 공개 노출을 방지하기 위한 보안 조치로 버킷에 적용된 정책 또는 액세스 제어 목록(ACL)을 필터링하는 데 사용됩니다.

일반적으로 버킷 또는 버킷 내 객체에 대한 퍼블릭 액세스를 허용하기 위해 S3 퍼블릭 액세스 차단이 해제됩니다. S3 퍼블릭 액세스 차단이 버킷에서 비활성화되면 버킷에 대한 액세스는 여기에 적용된 정책 또는 ACL에서 제어합니다. 즉, 버킷이 공개적으로 공유되는 것이 아니라, 버킷에 적용된 정책 및 ACL을 감사하여 해당 권한이 적용되었는지 확인해야 합니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Policy:S3/BucketPublicAccessGranted

IAM 보안 주체가 버킷 정책 또는 ACL을 변경하여 모든 AWS 사용자에게 S3 버킷에 대한 공개 액세스 권한을 부여했습니다.

기본 심각도: 높음

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 IAM 엔티티가 해당 S3 버킷의 버킷 정책 또는 ACL을 변경했기 때문에 나열된 S3 버킷이 모든 인증된 AWS 사용자에게 공개적으로 노출되었음을 알려줍니다. 정책 또는 ACL 변경이 탐지되면 Zelkova 기반의 자동 추론을 사용하여 버킷에 공개적으로 액세스할 수 있는지 확인합니다.

> **Note**
>
> 버킷의 ACL 또는 버킷 정책이 명시적 거부 또는 모두 거부로 구성된 경우 이 결과는 버킷의 현재 상태를 반영하지 않을 수 있습니다. 이 결과에는 S3 버킷에 대해 활성화되었을 수 있는 S3 퍼블릭 액세스 차단 설정이 반영되지 않습니다. 이 경우 결과의 `effectivePermission` 값은 `UNKNOWN`으로 표시됩니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

Stealth:S3/ServerAccessLoggingDisabled

S3 서버 액세스 로깅이 버킷에 대해 비활성화되었습니다.

기본 심각도: 낮음

- 데이터 소스: 관리 이벤트 CloudTrail

이 결과는 AWS 환경 내 버킷에 대해 S3 서버 액세스 로깅이 비활성화되었음을 알려줍니다. 비활성화하면 식별된 S3 버킷에 액세스하려는 시도에 대한 웹 요청 로그가 생성되지 않지만, 버킷에 대한 S3 관리 API 호출 (예:) 은 계속 추적됩니다. DeleteBucket 이 CloudTrail 버킷에 대해 S3 데이터 이벤트 로깅이 활성화된 경우에도 버킷 내 객체에 대한 웹 요청은 계속 추적됩니다. 로깅 비활성화는 탐지를 우회하기 위해 권한이 없는 사용자가 사용하는 기법입니다. S3 로그에 대한 자세한 내용은 S3 서버 액세스 로깅 및 S3 로깅 옵션을 참조하세요.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

사용자 지정 위협 목록의 IP 주소에서 S3 API를 간접적으로 호출했습니다.

기본 심각도: 높음

- 데이터 소스: CloudTrail S3의 데이터 이벤트

이 결과는 S3 API 작업(예: `PutObject` 또는 `PutObjectAcl`)이 사용자가 업로드한 위협 목록에 포함된 IP 주소에서 간접적으로 호출되었음을 알려줍니다. 이 결과와 관련된 위협 목록은 결과 세부 정보의 추가 정보 섹션에 나열됩니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 정보는 잠재적으로 손상된 S3 버킷 수정을 참조하세요.

UnauthorizedAccess:S3/TorIPCaller

Tor 출구 노드 IP 주소에서 S3 API가 간접적으로 호출되었습니다.

기본 심각도: 높음

- 데이터 소스: S3의 CloudTrail 데이터 이벤트

이 결과는 S3 API 작업(예: `PutObject` 또는 `PutObjectAcl`)이 Tor 출구 노드 IP 주소에서 간접적으로 호출되었음을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이 발견은 공격자의 실제 신원을 숨기려는 의도로 AWS 리소스에 무단으로 액세스했음을 의미할 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 내용은 잠재적으로 손상된 S3 버킷 수정을(를) 참조하세요.

사용 중지된 결과 유형

결과는 GuardDuty에서 발견한 잠재적 보안 문제에 대한 세부 정보를 포함한 알림입니다. 새로 추가되었거나 수명 종료된 결과 유형을 포함하여 GuardDuty 결과 유형에 대한 중요한 변화에 대한 내용은 아마존의 문서 기록 GuardDuty을 참조하십시오.

다음 결과 유형은 사용이 중지되어 GuardDuty에서 더 이상 생성하지 않습니다.

> **Important**
>
> 사용 중지된 GuardDuty 결과 유형은 다시 활성화할 수 없습니다.

주제

- Exfiltration:S3/ObjectRead.Unusual
- Impact:S3/PermissionsModification.Unusual
- Impact:S3/ObjectDelete.Unusual
- Discovery:S3/BucketEnumeration.Unusual
- Persistence:IAMUser/NetworkPermissions

- Persistence:IAMUser/ResourcePermissions
- Persistence:IAMUser/UserPermissions
- PrivilegeEscalation:IAMUser/AdministrativePermissions
- Recon:IAMUser/NetworkPermissions
- Recon:IAMUser/ResourcePermissions
- Recon:IAMUser/UserPermissions
- ResourceConsumption:IAMUser/ComputeResources
- Stealth:IAMUser/LoggingConfigurationModified
- UnauthorizedAccess:IAMUser/ConsoleLogin
- UnauthorizedAccess:EC2/TorIPCaller
- Backdoor:EC2/XORDDOS
- Behavior:IAMUser/InstanceLaunchUnusual
- CryptoCurrency:EC2/BitcoinTool.A
- UnauthorizedAccess:IAMUser/UnusualASNCaller

Exfiltration:S3/ObjectRead.Unusual

IAM 엔터티가 의심스러운 방식으로 S3 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

- 데이터 소스: S3에 대한 CloudTrail 데이터 이벤트

이 결과는 AWS 환경의 IAM 엔터티가 S3 버킷과 관련되고 해당 엔터티의 설정된 기준과 다른 API 호출을 수행하고 있음을 알려줍니다. 이 활동에 사용되는 API 호출은 공격자가 데이터 수집을 시도하는 공격의 유출 단계와 관련이 있습니다. IAM 엔터티가 API를 간접적으로 호출한 방식이 비정상적이었기

때문에 이 활동은 의심스럽습니다. 이 IAM 엔터티가 이전에 이러한 유형의 API를 호출한 기록이 없거나 API가 비정상적인 위치에서 간접적으로 호출된 경우를 예로 들 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 내용은 잠재적으로 손상된 S3 버킷 수정 섹션을 참조하세요.

Impact:S3/PermissionsModification.Unusual

IAM 엔터티가 하나 이상의 S3 리소스에 대한 권한을 수정하기 위해 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 IAM 엔터티가 AWS 환경에 있는 하나 이상의 버킷 또는 객체에 대한 권한을 수정하도록 설계된 API 호출을 수행하고 있음을 알려줍니다. 공격자가 계정 외부에서 정보가 공유되도록 이 작업을 수행할 수 있습니다. IAM 엔터티가 API를 간접적으로 호출한 방식이 비정상적이었기 때문에 이 활동은 의심스럽습니다. 이 IAM 엔터티가 이전에 이러한 유형의 API를 호출한 기록이 없거나 API가 비정상적인 위치에서 간접적으로 호출된 경우를 예로 들 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 내용은 잠재적으로 손상된 S3 버킷 수정 섹션을 참조하세요.

Impact:S3/ObjectDelete.Unusual

IAM 엔터티가 S3 버킷의 데이터를 삭제하는 데 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 AWS 환경의 특정 IAM 엔터티가 버킷 자체를 삭제하여 목록에 있는 S3 버킷의 데이터를 삭제하도록 설계된 API 호출을 수행하고 있음을 알려줍니다. IAM 엔터티가 API를 간접적으로 호출한 방식이 비정상적이었기 때문에 이 활동은 의심스럽습니다. 이 IAM 엔터티가 이전에 이러한 유형의 API를 호출한 기록이 없거나 API가 비정상적인 위치에서 간접적으로 호출된 경우를 예로 들 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 내용은 잠재적으로 손상된 S3 버킷 수정 섹션을 참조하세요.

Discovery:S3/BucketEnumeration.Unusual

IAM 엔터티가 네트워크 내에서 S3 버킷을 검색하는 데 사용되는 S3 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 IAM 엔터티가 환경에서 S3 버킷을 검색하기 위한 S3 API(예: `ListBuckets`)를 간접적으로 호출했음을 알려줍니다. 이 활동 유형은 일반적으로 공격자가 AWS 환경이 광범위한 공격에 취약한지 판단하기 위해 정보를 수집하는 공격의 발견 단계와 관련이 있습니다. IAM 엔터티가 API를 간접적으로 호출한 방식이 비정상적이었기 때문에 이 활동은 의심스럽습니다. 이 IAM 엔터티가 이전에 이러한 유형의 API를 호출한 기록이 없거나 API가 비정상적인 위치에서 간접적으로 호출된 경우를 예로 들 수 있습니다.

해결 권장 사항:

관련 보안 주체에 대해 이 활동이 예상치 않은 활동인 경우 보안 인증 정보가 노출되었거나 S3 권한이 충분히 제한적이지 않은 것일 수 있습니다. 자세한 내용은 잠재적으로 손상된 S3 버킷 수정 섹션을 참조하세요.

Persistence:IAMUser/NetworkPermissions

IAM 엔터티가 AWS 계정에서의 보안 그룹, 라우팅 및 ACL에 대한 네트워크 액세스 권한을 변경하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 AWS 환경의 특정 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 사용자)가 설정된 기준과 다른 행동을 보이고 있음을 나타냅니다. 이 보안 주체에게는 이 API의 이전 호출 내역이 없습니다.

이 결과는 보안 주체가 이전에 호출한 적이 없는 `CreateSecurityGroup` API를 간접적으로 호출하는 경우와 같이 의심스러운 상황에서 네트워크 구성 설정이 변경될 때 트리거됩니다. 공격자가 EC2 인스턴스에 대한 액세스를 개선하기 위해서 다양한 포트의 인바운드 트래픽을 허용하는 보안 그룹 변경을 시도하는 경우가 종종 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Persistence:IAMUser/ResourcePermissions

보안 주체가 AWS 계정에서 다양한 리소스의 보안 액세스 정책을 변경하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 AWS 환경의 특정 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 사용자)가 설정된 기준과 다른 행동을 보이고 있음을 나타냅니다. 이 보안 주체에게는 이 API의 이전 호출 내역이 없습니다.

이 결과는 AWS 리소스에 연결된 정책 또는 권한의 변경이 탐지될 때 트리거됩니다(예: AWS 환경의 보안 주체가 이전에 호출한 적이 없는 `PutBucketPolicy` API를 간접적으로 호출하는 경우). 예를 들어 Amazon S3와 같은 일부 서비스는 하나 이상의 보안 주체에 리소스 액세스를 허용하는 리소스 연결 권한을 지원합니다. 보안 인증 정보가 도난당한 상태에서 공격자는 리소스에 연결된 정책을 변경하여 리소스에 대한 액세스를 획득할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Persistence:IAMUser/UserPermissions

보안 주체가 AWS 계정에서 IAM 사용자, 그룹 또는 정책을 추가, 변경 또는 삭제하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 AWS 환경의 특정 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 사용자)가 설정된 기준과 다른 행동을 보이고 있음을 나타냅니다. 이 보안 주체에게는 이 API의 이전 호출 내역이 없습니다.

이 결과는 AWS 환경의 보안 주체가 이전에 간접적으로 호출한 적이 없는 `AttachUserPolicy` API를 간접 호출하는 경우와 같이 AWS 환경의 사용자 관련 권한이 의심스럽게 변경된 경우 트리거됩니다.

공격자는 기존 액세스 지점이 폐쇄된 경우에도 훔친 보안 인증 정보를 사용하여 새 사용자를 만들거나, 기존 사용자에게 액세스 정책을 추가하거나, 액세스 키를 만들어 계정에 대한 액세스를 극대화할 수 있습니다. 예를 들어 계정 소유자가 특정 IAM 사용자 또는 암호의 도난을 파악하고 계정에서 삭제할 수 있습니다. 하지만 허위로 만든 관리자 보안 주체가 생성한 다른 사용자는 삭제되지 않을 수 있으므로 공격자가 해당 AWS 계정에 액세스할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

PrivilegeEscalation:IAMUser/AdministrativePermissions

한 보안 주체가 본인에게 과도하게 허용적인 정책을 할당하려고 시도했습니다.

기본 심각도: 낮음*

> **Note**
>
> 권한 에스컬레이션 시도가 실패했다면 이 결과의 심각도는 낮은 수준이며 권한 에스컬레이션 시도가 성공했다면 중간 수준입니다.

이 결과는 사용자의 AWS 환경의 특정 IAM 엔터티가 권한 에스컬레이션 공격을 의미할 수 있는 행동을 보이고 있음을 나타냅니다. IAM 사용자 또는 역할이 자신에게 매우 허용적인 정책을 할당하려고 시도할 때 이 결과가 트리거됩니다. 해당 사용자 또는 역할이 관리 권한을 보유해야 하는 경우가 아니라면 이는 사용자의 자격 증명이 손상되었거나 역할의 권한이 적절히 구성되지 않았음을 나타냅니다.

공격자는 기존 액세스 지점이 폐쇄된 경우에도 훔친 보안 인증 정보를 사용하여 새 사용자를 만들거나, 기존 사용자에게 액세스 정책을 추가하거나, 액세스 키를 만들어 계정에 대한 액세스를 극대화할 수 있습니다. 예를 들어 계정의 소유자는 특정 IAM 사용자의 로그인 보안 인증 정보가 도난당했음을 인지하고 이를 계정에서 삭제할 수 있습니다. 하지만 부정하게 생성된 관리 보안 주체가 생성한 다른 사용자를 삭제할 수 없어 공격자가 여전히 AWS 계정에 액세스가 가능할 수도 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Recon:IAMUser/NetworkPermissions

보안 주체가 AWS 계정에서의 보안 그룹, 라우팅 및 ACL에 대한 네트워크 액세스 권한을 변경하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 AWS 환경의 특정 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 사용자)가 설정된 기준과 다른 행동을 보이고 있음을 나타냅니다. 이 보안 주체에게는 이 API의 이전 호출 내역이 없습니다.

의심스러운 상황에서 AWS 계정의 리소스 액세스 권한이 탐색될 때 결과가 트리거됩니다. 예를 들어 보안 주체가 이전에 호출한 적이 없는 `DescribeInstances` API를 간접적으로 호출했습니다. 공격자는 도난당한 보안 인증 정보를 사용하여 가치 있는 보안 인증 정보를 찾거나 이미 보유한 보안 인증 정보의 능력을 판단하도록 일종의 AWS 리소스 정찰을 수행할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Recon:IAMUser/ResourcePermissions

보안 주체가 AWS 계정에서 다양한 리소스의 보안 액세스 정책을 변경하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 AWS 환경의 특정 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 사용자)가 설정된 기준과 다른 행동을 보이고 있음을 나타냅니다. 이 보안 주체에게는 이 API의 이전 호출 내역이 없습니다.

의심스러운 상황에서 AWS 계정의 리소스 액세스 권한이 탐색될 때 결과가 트리거됩니다. 예를 들어 보안 주체가 이전에 호출한 적이 없는 `DescribeInstances` API를 간접적으로 호출했습니다. 공격자는 도난당한 보안 인증 정보를 사용하여 가치 있는 보안 인증 정보를 찾거나 이미 보유한 보안 인증 정보의 능력을 판단하도록 일종의 AWS 리소스 정찰을 수행할 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Recon:IAMUser/UserPermissions

보안 주체가 AWS 계정에서 IAM 사용자, 그룹 또는 정책을 추가, 변경 또는 삭제하는 데 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

의심스러운 상황에서 AWS 환경의 사용자 권한이 탐색될 때 결과가 트리거됩니다. 예를 들어 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 IAM 사용자)가 이전에 간접적으로 호출한 적이 없는 `ListInstanceProfilesForRole` API를 호출했습니다. 공격자는 도난당한 보안 인증 정보를 사용하여 가치 있는 보안 인증 정보를 찾거나 이미 보유한 보안 인증 정보의 능력을 판단하도록 일종의 AWS 리소스 정찰을 수행할 수 있습니다.

이 결과는 AWS 환경의 특정 보안 주체가 설정된 기준과 다른 행동을 보이고 있음을 나타냅니다. 이 보안 주체에게는 이러한 방법으로 이 API의 이전 호출 내역이 없습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

ResourceConsumption:IAMUser/ComputeResources

보안 주체가 EC2 인스턴스와 같은 컴퓨팅 리소스를 시작하는 데 일반적으로 사용되는 API를 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

의심스러운 상황에서 AWS 환경 내에 나열된 계정에서 EC2 인스턴스가 시작될 때 결과가 트리거됩니다. 이 결과는 AWS 환경의 특정 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 사용자)가 설정된 기준과 다른 행동을 보이고 있음을 나타냅니다. 이전에 간접적으로 호출한 적이 없는 `RunInstances` API의 호출을 예로 들 수 있습니다. 공격자가 도난당한 자격 증명을 사용하여 컴퓨팅 시간을 훔치는 신호일 수 있습니다(암호 화폐 마이닝 또는 암호 크래킹이 목적일 수 있음). 또한 공격자가 AWS 환경의 EC2 인스턴스와 그 자격 증명을 사용하여 계정 액세스를 유지하는 신호일 수도 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

Stealth:IAMUser/LoggingConfigurationModified

보안 주체가 CloudTrail 로깅 중단, 기존 로그 삭제, AWS 계정 내 활동 흔적 제거에 일반적으로 사용되는 API를 간접적으로 호출했습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

이 결과는 의심스러운 상황에서 환경 내 AWS 계정의 로깅 구성이 수정될 때 트리거됩니다. 이 결과는 AWS 환경의 특정 보안 주체(AWS 계정 루트 사용자, IAM 역할 또는 사용자)가 설정된 기준과 다른 행동을 보이고 있음을 알려줍니다. 이전에 간접적으로 호출한 적이 없는 `StopLogging` API의 간접 호출을 예로 들 수 있습니다. 이는 공격자가 활동 흔적을 제거함으로써 공격을 덮으려는 시도의 신호일 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

UnauthorizedAccess:IAMUser/ConsoleLogin

AWS 계정 내 보안 주체의 비정상적인 콘솔 로그인이 탐지되었습니다.

기본 심각도: 중간*

> **Note**
>
> 이 결과의 기본 심각도는 중간입니다. 그러나 인스턴스에서 생성된 임시 AWS 보안 인증 정보를 사용하여 API가 간접적으로 호출되는 경우 결과의 심각도는 높음입니다.

의심스러운 상황에서 콘솔 로그인이 감지될 때 이 결과가 트리거됩니다. 예를 들어, 이러한 이전 작업 내역이 없는 보안 주체가 한 번도 사용하지 않은 클라이언트 또는 비정상적인 위치에서 ConsoleLogin API를 호출했습니다. 이는 도난당한 자격 증명이 AWS 계정 액세스를 얻는 데 사용 중이거나 유효한 사용자가 유효하지 않거나 안전도가 낮은 방법(예를 들어, 승인된 VPN을 통하지 않는 방법)으로 계정에 액세스하는 신호일 수 있습니다.

이 결과는 AWS 환경의 특정 보안 주체가 설정된 기준과 다른 행동을 보이고 있음을 알려줍니다. 이 보안 주체는 이 특정 위치에서 이 클라이언트 애플리케이션을 사용하여 로그인 활동을 한 이전 내역이 없습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

UnauthorizedAccess:EC2/TorIPCaller

EC2 인스턴스가 Tor 출구 노드로부터 인바운드 연결을 수신하고 있습니다.

기본 심각도: 중간

이 결과는 AWS 환경의 EC2 인스턴스가 Tor 출구 노드로부터 인바운드 연결을 받는다는 것을 알려줍니다. Tor는 익명 통신을 활성화하기 위한 소프트웨어로, 통신을 암호화하고 일련의 네트워크 노드 간 릴레이를 통해 통신을 무작위로 반송합니다. 마지막 Tor 노드를 출구 노드라고 합니다. 이는 공격자의 실제 신원을 숨기려는 의도를 갖고 AWS 리소스에 무단으로 액세스하려 함을 나타낼 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Backdoor:EC2/XORDDOS

EC2 인스턴스가 Xor DDos 맬웨어와 연관된 IP 주소와의 통신을 시도합니다.

기본 심각도: 높음

이 결과는 AWS 환경에 Xor DDos 맬웨어와 연관된 IP 주소와의 통신을 시도하는 EC2 인스턴스가 있음을 알립니다. 이 EC2 인스턴스는 손상되었을 수 있습니다. XOR DDoS는 Linux 시스템을 가로채는 트로이 목마 맬웨어입니다. 이 맬웨어는 시스템에 대한 액세스 권한을 얻기 위해 무차별 암호 대입 공격을 실행하여 Linux의 SSH(Secure Shell)에 대한 암호를 찾습니다. SSH 자격 증명을 획득하여 로그인에 성공한 이후 이 맬웨어는 루트 사용자 권한을 사용하여 XOR DDoS를 다운로드하고 설치하는 스크립트를 실행합니다. 그런 다음 봇넷의 일부로 사용되어 다른 대상에 대한 분산 서비스 거부 공격(DDoS)을 시작합니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

Behavior:IAMUser/InstanceLaunchUnusual

사용자가 비정상적인 유형의 EC2 인스턴스를 시작했습니다.

기본 심각도: 높음

이 결과는 AWS 환경의 특정 사용자가 설정된 기준과 다른 행동을 보이고 있음을 알려줍니다. 이 사용자에게는 이전에 이 유형의 EC2 인스턴스를 시작한 내역이 없습니다. 로그인 보안 인증 정보가 손상되었을 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

CryptoCurrency:EC2/BitcoinTool.A

EC2 인스턴스가 비트코인 마이닝 풀과 통신하고 있습니다.

기본 심각도: 높음

이 결과는 AWS 환경의 EC2 인스턴스가 비트코인 채굴 풀과 통신함을 알려줍니다. 암호 화폐 마이닝 분야에서 마이닝 도구는 블록 해결에 기여한 작업량에 따라 보상을 분할하기 위해 네트워크를 통해 처리 능력을 공유하는 마이너별 리소스 풀링입니다. 비트코인 마이닝에 이 EC2 인스턴스를 사용하지 않는 경우 EC2 인스턴스가 손상되었을 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 인스턴스가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

UnauthorizedAccess:IAMUser/UnusualASNCaller

비정상 네트워크의 IP 주소에서 API가 호출되었습니다.

기본 심각도: 높음

이 조사 결과는 특정 활동이 비정상적인 네트워크의 IP 주소에서 호출되었다고 사용자에게 알립니다. 이 네트워크는 해당 사용자의 이전 AWS 사용 내역을 통해 관찰된 적이 없습니다. 이러한 활동 중에는 콘솔 로그인을 비롯해 EC2 인스턴스를 시작하거나, 새로운 IAM 사용자를 생성하거나, AWS 권한을 수정하려는 시도 등이 포함됩니다. 이는 AWS 리소스에 대한 무단 액세스를 나타낼 수 있습니다.

해결 권장 사항:

이 활동이 예기치 않게 발생한 경우 보안 인증 정보가 손상되었을 수 있습니다. 자세한 내용은 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS 섹션을 참조하세요.

리소스 유형별 결과

다음 페이지는 검색 결과와 관련된 리소스 유형별로 분류되어 있습니다 GuardDuty .

- EC2 결과 유형
- 런타임 모니터링 검색 유형
- IAM 결과 유형
- EKS 감사 로그 검색 유형
- Lambda 보호 결과 유형
- 맬웨어 보호 결과 유형
- RDS 보호 결과 유형
- S3 결과 유형

결과 테이블

다음 테이블에는 해당하는 경우 기본 데이터 소스 또는 기능별로 정렬된 모든 활성 결과 유형이 나와 있습니다. 다음 결과 유형 중 일부의 경우 심각도가 가변적일 수 있으며, 이는 별표(*)로 표시되어 있습니다. 결과 유형의 가변적 심각도에 대한 자세한 내용은 해당 결과 유형의 구체적인 설명을 참조하세요.

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail S3의 데이터 이벤트	낮음
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail S3의 데이터 이벤트	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail S3의 데이터 이벤트	중간
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
PenTest:S3/KaliLinux	Amazon S3	CloudTrail S3의 데이터 이벤트	중간
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail S3의 데이터 이벤트	중간
PenTest:S3/PentooLinux	Amazon S3	CloudTrail S3의 데이터 이벤트	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3의 데이터 이벤트	높음
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail 관리 이벤트	중간
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail 매니지먼트 이벤트	중간
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail 매니지먼트 이벤트	낮음
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail 매니지먼트 이벤트	높음
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail 매니지먼트 이벤트	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail 매니지먼트 이벤트	중간
PenTest:IAMUser/KaliLinux	IAM	CloudTrail 매니지먼트 이벤트	중간
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail 매니지먼트 이벤트	중간
PenTest:IAMUser/PentooLinux	IAM	CloudTrail 매니지먼트 이벤트	중간
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail 매니지먼트 이벤트	중간
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail 매니지먼트 이벤트	낮음*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail 매니지먼트 이벤트	높음*

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail 매니지먼트 이벤트	낮음
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail 매니지먼트 이벤트	높음
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail 매니지먼트 이벤트	낮음
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail 매니지먼트 이벤트	높음
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail 매니지먼트 이벤트	중간
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail 매니지먼트 이벤트	중간
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 매니지먼트 이벤트	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Recon:IAMUser/TorIPCaller	IAM	CloudTrail 매니지먼트 이벤트	중간
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail 매니지먼트 이벤트	낮음
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail 매니지먼트 이벤트	낮음
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail 매니지먼트 이벤트	중간
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail 매니지먼트 이벤트	중간
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 매니지먼트 이벤트	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail 매니지먼트 이벤트	중간
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail S3의 관리 이벤트 또는 CloudTrail 데이터 이벤트	낮음
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail S3의 관리 이벤트 또는 CloudTrail 데이터 이벤트	높음
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNS 로그	높음
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNS 로그	높음
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNS 로그	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNS 로그	높음
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNS 로그	높음
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNS 로그	낮음
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNS 로그	중간
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNS 로그	높음
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNS 로그	높음
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNS 로그	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNS 로그	높음
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNS 로그	중간
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNS 로그	높음
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNS 로그	높음
Execution:Container/MaliciousFile	컨테이너	EBS 멀웨어 보호	탐지된 위협에 따라 다름
Execution:Container/SuspiciousFile	컨테이너	EBS 멀웨어 보호	탐지된 위협에 따라 다름
Execution:EC2/MaliciousFile	EC2	EBS 멀웨어 보호	탐지된 위협에 따라 다름
Execution:EC2/SuspiciousFile	EC2	EBS 멀웨어 보호	탐지된 위협에 따라 다름
Execution:ECS/MaliciousFile	ECS	EBS 멀웨어 보호	탐지된 위협에 따라 다름

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Execution:ECS/SuspiciousFile	ECS	EBS 멀웨어 보호	탐지된 위협에 따라 다름
Execution:Kubernetes/MaliciousFile	Kubernetes	EBS 멀웨어 보호	탐지된 위협에 따라 다름
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBS 멀웨어 보호	탐지된 위협에 따라 다름
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKS 감사 로그	중간
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 감사 로그	높음
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 감사 로그	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 감사 로그	높음
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKS 감사 로그	높음
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 감사 로그	높음
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 감사 로그	높음
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 감사 로그	높음
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKS 감사 로그	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKS 감사 로그	낮음
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 감사 로그	중간
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 감사 로그	중간
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 감사 로그	중간
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKS 감사 로그	중간
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKS 감사 로그	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKS 감사 로그	중간
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKS 감사 로그	낮음
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 감사 로그	높음
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 감사 로그	높음
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 감사 로그	높음
Impact:Kubernetes/TorIPCaller	Kubernetes	EKS 감사 로그	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKS 감사 로그	중간
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 감사 로그	중간
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 감사 로그	중간
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 감사 로그	높음
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKS 감사 로그	중간
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKS 감사 로그	높음
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKS 감사 로그	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKS 감사 로그	중간
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKS 감사 로그	중간
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKS 감사 로그	중간*
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKS 감사 로그	낮음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKS 감사 로그	높음
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKS 감사 로그	높음
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	EKS 감사 로그	중간
Backdoor:Lambda/C&CActivity.B	Lambda	Lambda 네트워크 활동 모니터링	높음
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Lambda 네트워크 활동 모니터링	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Trojan:Lambda/BlackholeTraffic	Lambda	Lambda 네트워크 활동 모니터링	중간
Trojan:Lambda/DropPoint	Lambda	Lambda 네트워크 활동 모니터링	중간
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Lambda 네트워크 활동 모니터링	중간
UnauthorizedAccess:Lambda/TorClient	Lambda	Lambda 네트워크 활동 모니터링	높음
UnauthorizedAccess:Lambda/TorRelay	Lambda	Lambda 네트워크 활동 모니터링	높음
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	낮음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	높음
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	가변적*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	중간
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	높음
CredentialAccess:RDS/TorIPCaller.FailedLogin	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	중간
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Discovery:RDS/MaliciousIPCaller	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	중간
Discovery:RDS/TorIPCaller	지원되는 Amazon Aurora 데이터베이스	RDS 로그인 활동 모니터링	중간
Backdoor:Runtime/C&CActivity.B	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
Backdoor:Runtime/C&CActivity.B!DNS	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
CryptoCurrency:Runtime/BitcoinTool.B	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
CryptoCurrency:Runtime/BitcoinTool.B!DNS	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
DefenseEvasion:Runtime/FilelessExecution	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
DefenseEvasion:Runtime/ProcessInjection.Proc	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
DefenseEvasion:Runtime/ProcessInjection.Ptrace	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
DefenseEvasion:Runtime/PtraceAntiDebugging	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	낮음
DefenseEvasion:Runtime/SuspiciousCommand	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
Execution:Runtime/MaliciousFileExecuted	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
Execution:Runtime/NewBinaryExecuted	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Execution:Runtime/NewLibraryLoaded	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Execution:Runtime/SuspiciousCommand	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	변수
Execution:Runtime/SuspiciousTool	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	변수
Execution:Runtime/ReverseShell	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
Impact:Runtime/AbusedDomainRequest.Reputation	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Impact:Runtime/BitcoinDomainRequest.Reputation	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
Impact:Runtime/CryptoMinerExecuted	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Impact:Runtime/MaliciousDomainRequest.Reputation	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Impact:Runtime/SuspiciousDomainRequest.Reputation	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	낮음
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
PrivilegeEscalation:Runtime/DockerSocketAccessed	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
PrivilegeEscalation:Runtime/RuncContainerEscape	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
PrivilegeEscalation:Runtime/UserfaultfdUsage	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Trojan:Runtime/BlackholeTraffic	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Trojan:Runtime/BlackholeTraffic!DNS	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Trojan:Runtime/DropPoint	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Trojan:Runtime/DGADomainRequest.C!DNS	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
Trojan:Runtime/DriveBySourceTraffic!DNS	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Trojan:Runtime/DropPoint!DNS	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	중간
Trojan:Runtime/PhishingDomainRequest!DNS	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
UnauthorizedAccess:Runtime/MetadataDNSRebind	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
UnauthorizedAccess:Runtime/TorClient	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
UnauthorizedAccess:Runtime/TorRelay	인스턴스, EKS 클러스터, ECS 클러스터 또는 컨테이너	Runtime Monitoring	높음
Backdoor:EC2/C&CActivity.B	EC2	VPC 흐름 로그	높음
Backdoor:EC2/DenialOfService.Dns	EC2	VPC 흐름 로그	높음
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC 흐름 로그	높음

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
Backdoor:EC2/DenialOfService.Udp	EC2	VPC 흐름 로그	높음
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC 흐름 로그	높음
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC 흐름 로그	높음
Backdoor:EC2/Spambot	EC2	VPC 흐름 로그	중간
Behavior:EC2/NetworkPortUnusual	EC2	VPC 흐름 로그	중간
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC 흐름 로그	중간
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC 흐름 로그	높음
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC 흐름 로그	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
DefenseEvasion:EC2/UnusualDoHActivity	EC2	VPC 흐름 로그	중간
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC 흐름 로그	중간
Impact:EC2/PortSweep	EC2	VPC 흐름 로그	높음
Impact:EC2/WinRMBruteForce	EC2	VPC 흐름 로그	낮음*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC 흐름 로그	높음
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC 흐름 로그	낮음*
Recon:EC2/Portscan	EC2	VPC 흐름 로그	중간
Trojan:EC2/BlackholeTraffic	EC2	VPC 흐름 로그	중간
Trojan:EC2/DropPoint	EC2	VPC 흐름 로그	중간

찾기 유형	리소스 유형	기본 데이터 소스/기능	결과 심각도
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC 흐름 로그	중간
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC 흐름 로그	낮음*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC 흐름 로그	낮음*
UnauthorizedAccess:EC2/TorClient	EC2	VPC 흐름 로그	높음
UnauthorizedAccess:EC2/TorRelay	EC2	VPC 흐름 로그	높음

아마존 GuardDuty 조사 결과 관리

GuardDuty 결과를 정렬, 저장 및 관리하는 데 도움이 되는 몇 가지 중요한 기능을 제공합니다. 이러한 특성을 사용하면 결과를 특정 AWS 환경에 맞게 조정하고, 가치가 낮은 결과로 인한 노이즈를 줄이고, 환경에 대한 특정 위협에 집중할 수 있습니다. 이 페이지의 주제를 검토하여 이러한 기능을 사용하여 연구 GuardDuty 결과의 가치를 높이는 방법을 알아보십시오.

주제:

요약 대시보드

GuardDuty콘솔에서 사용할 수 있는 요약 대시보드의 구성 요소에 대해 알아보세요.

조사 결과 필터링

지정한 기준에 따라 GuardDuty 결과를 필터링하는 방법을 알아보세요.

억제 규칙

제외 규칙을 통해 결과 GuardDuty 알림을 받는 결과를 자동으로 필터링하는 방법을 알아보세요. 억제 규칙은 필터를 기반으로 결과를 자동으로 보관합니다.

신뢰할 수 있는 IP 목록 및 위협 목록 사용

공개적으로 라우팅할 수 있는 IP 주소를 기반으로 IP 목록 및 위협 목록을 사용하여 GuardDuty 모니터링 범위를 사용자 지정합니다. 신뢰할 수 있는 IP 목록은 신뢰할 수 있는 것으로 간주되는 IP에서 DNS가 아닌 결과가 생성되지 않도록 하는 반면, 위협 인텔 목록은 사용자 정의 IP의 GuardDuty 활동을 경고하게 합니다.

결과 내보내기

생성된 결과를 Amazon S3 버킷으로 내보내 90일의 결과 보존 기간이 지난 기록을 유지할 수 있습니다. GuardDuty 이 기록 데이터를 사용하여 계정의 잠재적인 의심스러운 활동을 추적하고 권장 수정 단계가 성공적이었는지 평가하십시오.

Amazon CloudWatch Events를 사용하여 GuardDuty 결과에 대한 사용자 지정 응답 생성

Amazon CloudWatch 이벤트를 통해 GuardDuty 결과에 대한 자동 알림을 설정합니다. CloudWatch 이벤트를 통해 다른 작업을 자동화하여 결과에 응답하는 데 도움이 되도록 할 수도 있습니다.

멀웨어 보호 검사 중 리소스를 건너뛰는 이유와 CloudWatch 로그 이해

GuardDuty 멀웨어 방지 CloudWatch 로그를 감사하는 방법과 검사 과정에서 영향을 받은 Amazon EC2 인스턴스 또는 Amazon EBS 볼륨을 건너뛰었을 수 있는 이유에 대해 알아보십시오.

GuardDuty 맬웨어 보호에서 오탐지 보고

GuardDuty 멀웨어 보호에서의 오탐지 경험과 오탐지 위협 탐지를 신고하는 방법에 대해 알아보십시오.

요약 대시보드

요약 대시보드는 현재 지역에서 생성된 GuardDuty 결과를 집계하여 AWS 계정 보여줍니다. 현재 대시보드는 최대 5,000개의 결과를 지원합니다. 하지만 GuardDuty 콘솔의 조사 결과 페이지 또는 또는 를 사용하여 모든 검색 결과의 세부 정보를 볼 수 있습니다. GetFindingsListFindings

> **Note**
>
> 조사 결과 요약은 GuardDuty 콘솔 https://console.aws.amazon.com/guardduty/ 을 통해서만 확인할 수 있습니다.

다음 섹션은 대시보드 액세스 및 구성 요소를 이해하는 데 도움이 됩니다.

내용

- 요약 대시보드 액세스
- 요약 대시보드 이해
- 요약 대시보드에 피드백 제공

요약 대시보드 액세스

GuardDuty 콘솔의 요약 대시보드에는 현재 지역에서 생성된 최대 5,000개의 GuardDuty 검색 결과가 통합된 보기로 표시됩니다.

요약 대시보드 액세스

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다. 콘솔을 열면 요약 대시보드가 GuardDuty 표시됩니다.
3. 기본적으로 요약은 오늘 날짜에 대해 표시됩니다. GuardDuty콘솔은 지난 2일, 지난 7일 및 지난 30일의 요약을 볼 수 있는 옵션을 제공합니다. 기본 시간 범위를 변경하려면 개요 창 위에 있는 드롭다운에서 옵션 중 하나를 선택합니다.

4. 데이터 필터링

   - 결과가 가장 많은 계정, 결과가 가장 많은 리소스, 발생 빈도가 가장 적은 결과 위젯을 통해 결과의 심각도를 기반으로 데이터를 필터링할 수 있습니다.
   - 결과가 가장 많은 리소스 위젯을 사용하면 영향을 받을 수 있는 리소스 유형을 기준으로 데이터를 필터링할 수도 있습니다.

     멤버 계정은 자신의 계정에 속하는 잠재적으로 영향을 받을 수 있는 리소스의 세부 정보를 볼 수 있습니다. GuardDuty 관리자 계정이고 잠재적으로 영향을 받을 수 있는 리소스의 세부 정보를 보려면 연결된 구성원 계정의 자격 증명을 사용하여 GuardDuty 콘솔을 여십시오.

5. 보호 플랜 적용 범위

   보호 플랜 적용 범위는 GuardDuty 조직에서 활성화된 구성원 계정의 수를 제공합니다. 통계는 위임된 GuardDuty 관리자만 볼 수 있습니다.

요약 대시보드 이해

요약 대시보드에는 다음 섹션에 집계된 데이터가 표시됩니다. 요약을 보고 이해하려면 먼저 콘솔 상단의 리전 선택기에서 원하는 AWS 리전 을 선택합니다. 또한 개요 창 위에 있는 드롭다운 메뉴에서 원하는 시간 범위를 선택했는지 확인합니다. 선택한 파라미터에 대한 결과가 생성되지 않으면 어떤 위젯에서도 데이터가 제공되지 않습니다.

최대 5,000개의 검색 결과 중에서 GuardDuty 검색 결과가 가장 많은 계정, 검색 결과가 가장 많은 리소스, 가장 자주 발생하는 검색 결과가 있는 리소스, 가장 적게 발생하는 검색 결과가 있는 요약 대시보드에는 상위 5개 결과를 기반으로 데이터가 표시됩니다. 더 깊이 분석하려면 GuardDuty 콘솔의 조사 결과 페이지를 참조하십시오.

개요

이 섹션은 다음 데이터를 제공합니다.

- 총 결과: 현재 리전의 계정에서 생성된 총 결과 수를 나타냅니다.
- 높은 심각도 조사 결과: 현재 지역에서 심각도 수준이 높은 GuardDuty 검색 결과의 수를 나타냅니다.
- 결과가 있는 리소스: 결과와 관련되어 있고 손상되었을 수 있는 리소스의 수를 나타냅니다.
- 결과가 있는 계정: 하나 이상의 결과가 생성된 계정 수를 나타냅니다. 독립형 계정인 경우 이 필드의 값은 1입니다.

지난 7일 및 지난 30일 기간의 경우 개요 패널에는 각각 주별(WoW) 또는 월별(MoM)로 생성된 결과의 백분율 차이가 표시될 수 있습니다. 이전 주 또는 달에 결과가 생성되지 않았고 비교할 데이터가 없는 경우 백분율 차이를 확인하지 못할 수도 있습니다.

GuardDuty 관리자 계정인 경우 이 모든 필드는 조직의 모든 구성원 계정에 대한 요약 데이터를 제공합니다.

심각도별 결과

이 섹션에는 선택한 시간 범위에 대한 총 결과 수가 포함된 막대 차트가 표시됩니다. 선택한 시간 범위 내의 특정 날짜에 생성되어 심각도가 낮음, 중간 또는 높음인 결과 수를 볼 수 있습니다.

가장 일반적인 결과 유형

이 섹션에서는 현재 지역에서 생성된 최대 5,000개의 검색 GuardDuty 결과에서 관찰된 가장 일반적인 검색 결과 유형 5개를 원형 차트로 보여줍니다. 이 원형 차트에서 각 섹터를 마우스로 가리키면 다음 데이터가 표시됩니다.

- 결과 수: 선택한 시간 범위에서 이 결과가 생성된 횟수를 나타냅니다.
- 심각도: 결과의 심각도 수준(예: 보통, 높음)을 나타냅니다.
- 백분율: 원형 차트에서 이 결과 유형의 비율을 나타냅니다.
- 최종 생성: 이 결과 유형이 마지막으로 생성된 이후 경과된 시간을 나타냅니다.

결과가 가장 많은 계정

이 섹션은 다음 데이터를 제공합니다.

- 계정: 검색 결과가 생성된 AWS 계정 ID를 나타냅니다.
- 결과 수: 이 계정 ID에 대해 결과가 생성된 횟수를 나타냅니다.
- 최종 생성: 이 결과 유형이 이 계정 ID에서 마지막으로 생성된 이후 경과된 시간을 나타냅니다.
- 심각도 높음: 기본적으로 심각도가 높은 결과 유형에 대한 데이터가 표시됩니다. 이 필드에 사용할 수 있는 옵션은 심각도 높음, 심각도 중간 및 모든 심각도입니다.

결과가 있는 리소스

이 섹션은 다음 데이터를 제공합니다.

- 리소스: 영향을 받을 수 있는 리소스 유형을 나타내고, 이 리소스가 계정에 속한 경우 빠른 링크에 액세스하여 리소스 세부 정보를 볼 수 있습니다. GuardDuty 관리자 계정인 경우 이 자원이 속한 구성원

계정의 자격 증명으로 GuardDuty 콘솔에 액세스하여 영향을 받을 수 있는 리소스의 세부 정보를 볼 수 있습니다.

- 계정: 이 리소스가 속한 AWS 계정 ID를 나타냅니다.
- 결과 수: 이 리소스가 결과와 연관된 횟수를 나타냅니다.
- 최종 생성: 이 리소스와 연관된 결과 유형이 마지막으로 생성된 이후 경과된 시간을 나타냅니다.
- 모든 리소스 유형: 기본적으로 모든 리소스 유형에 대한 데이터가 표시됩니다. 드롭다운을 사용하여 인스턴스 AccessKey, Lambda 등과 같은 특정 리소스 유형에 대한 데이터를 볼 수 있습니다.
- 심각도 높음: 기본적으로 심각도가 높은 결과 유형에 대한 데이터가 표시됩니다. 드롭다운을 사용하여 다른 심각도에 대한 데이터를 볼 수 있습니다. 사용할 수 있는 옵션은 심각도 높음, 심각도 중간 및 모든 심각도입니다.

발생 빈도가 가장 적은 결과

이 섹션에서는 사용자 환경에서 자주 생성되지 않는 검색 유형에 대한 세부 정보를 제공합니다. AWS 이 인사이트는 환경의 새로운 위협 패턴을 조사하고 이에 대한 조치를 취하는 데 도움이 될 수 있습니다. 표에는 다음 데이터가 제공됩니다.

- 결과 유형: 결과 유형 이름을 나타냅니다.
- 결과 수: 선택한 시간 범위에서 이 결과 유형이 생성된 횟수를 나타냅니다.
- 최종 생성: 이 결과 유형이 마지막으로 생성된 이후 경과된 시간을 나타냅니다.
- 심각도 높음: 기본적으로 심각도가 높은 결과 유형에 대한 데이터가 표시됩니다. 이 필드에 사용할 수 있는 옵션은 심각도 높음, 심각도 중간 및 모든 심각도입니다.

보호 플랜 적용 범위

이 섹션은 조직에 속하며 현재 하나 이상의 기능 및 추가 기능 (해당하는 경우) 구성을 활성화한 활성 구성원 계정의 수를 제공합니다 AWS 리전.

위임된 GuardDuty 관리자만 조직 내 구성원 계정에 대한 통계를 볼 수 있습니다. 기능이 구성되지 않은 경우 작업 열에서 구성을 선택합니다.

새 AWS 조직을 만드는 경우 전체 조직에 대한 통계를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

요약 대시보드에 피드백 제공

GuardDuty 요약 대시보드의 유용성, 기능 및 성능에 대한 피드백을 제공하도록 권장합니다. 이렇게 하면 대시보드 개선에 도움이 됩니다.

요약 대시보드에 피드백 제공

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다. GuardDuty콘솔을 열면 요약 대시보드가 표시됩니다.
3. 대시보드 오른쪽 상단에서 피드백을 선택합니다. 그러면 양식이 열립니다. 피드백을 제공한 후 제출을 선택합니다.

조사 결과 필터링

결과 필터를 사용하면 지정한 기준과 일치하는 결과를 보고 일치하지 않는 결과를 필터링할 수 있습니다. Amazon GuardDuty 콘솔을 사용하여 쉽게 찾기 필터를 만들거나 JSON을 사용하여 CreateFilterAPI로 검색 필터를 생성할 수 있습니다. 콘솔에서 필터를 생성하는 방법을 이해하려면 다음 섹션을 검토하세요. 이러한 필터를 사용하여 발생한 결과를 자동으로 보관하려면 억제 규칙 섹션을 참조하세요.

콘솔에서 GuardDuty 필터 생성

검색 필터는 GuardDuty 콘솔을 통해 생성하고 테스트할 수 있습니다. 콘솔을 통해 생성된 필터는 억제 규칙 또는 향후 필터 작업에 사용할 수 있도록 저장할 수 있습니다. 필터는 하나 이상의 필터 기준으로 구성되고, 이 기준은 하나 이상의 값과 쌍을 이루는 하나의 필터 속성으로 구성됩니다.

필터를 생성할 때 다음 사항을 인식합니다.

- 필터에는 와일드카드가 허용되지 않습니다.
- 특정 필터 기준으로 최소 1개부터 최대 50개까지 속성을 지정할 수 있습니다.
- equal to 또는 not equal to 조건을 사용하여 Account ID 같은 속성 값을 필터링하면 최대 50개의 값을 지정할 수 있습니다.
- 각 필터 기준 속성은 AND 연산자로 평가됩니다. 동일한 속성에 대한 여러 개의 값은 AND/OR로 평가됩니다.

결과를 필터링하려면(콘솔)

1. 표시된 GuardDuty 결과 목록 위에 필터 기준 추가를 선택합니다.
2. 속성 목록을 확장한 후 필터링 기준으로 지정할 속성을 선택합니다(예: 계정 ID 또는 작업 유형).

> **Note**
>
> 필터 기준 생성에 사용할 수 있는 속성 목록은 이 페이지에 나와 있는 필터 속성 표를 참조하세요.

3. 표시되는 텍스트 필드에 선택한 속성마다 값을 지정한 후 적용을 선택합니다.

> **Note**
>
> 필터를 적용한 경우 필터 이름 왼쪽의 검은색 점을 선택하여 필터와 일치하는 결과를 제외하도록 필터를 변환할 수 있습니다. 이렇게 하면 선택된 속성에 대한 "not equals" 필터가 효과적으로 생성됩니다.

4. 지정한 속성과 속성 값(필터 기준)을 필터로 저장하려면 저장을 선택합니다. 필터 이름과 설명을 입력하고 완료를 선택합니다.

필터 속성

API 작업을 사용하여 필터를 만들거나 결과를 정렬할 때는 JSON에서 필터 기준을 지정해야 합니다. 이러한 필터 기준은 결과의 세부 정보 JSON과 상관관계가 있습니다. 다음 표에는 필터 속성에 대해 콘솔에 표시되는 이름 및 해당 JSON 필드 이름 목록이 나와 있습니다.

콘솔 필드 이름	JSON 필드 이름
계정 ID	accountId
결과 ID	id
지역	region
심각도	severity API AWS CLI AWS CloudFormation, 또는 `severity` 와 함께 사용하는 경우 숫자 값을 갖게 됩니다. 자세한 내용은 findingCriteria를 참조하세요.
찾기 유형	type

콘솔 필드 이름	JSON 필드 이름
업데이트된 시간	updatedAt
액세스 키 ID	리소스. accessKeyDetails. accessKeyId
보안 주체 ID	의지. accessKeyDetails. 주체 ID
사용자 이름	리소스. accessKeyDetails.사용자명
사용자 유형	리소스. accessKeyDetails. 사용자 유형
IAM 인스턴스 프로파일 ID	리소스. 인스턴스 세부 정보. iamInstanceProfile .id
인스턴스 ID	resource.instanceDetails.instanceId
인스턴스 이미지 ID	resource.instanceDetails.imageId
인스턴스 태그 키	resource.instanceDetails.tags.key
인스턴스 태그 값	resource.instanceDetails.tags.value
IPv6 주소	resource.instanceDetails.networkInterfaces.ip v6Addresses
프라이빗 IPv4 주소	리소스. 인스턴스 세부 정보. 네트워크 인터페이스. privateIpAddresses. privateIpAddress
공개 DNS 이름	리소스. 인스턴스 세부 정보. 네트워크 인터페이스. publicDnsName
퍼블릭 IP	resource.instanceDetails.networkInterfaces.pu blicIp
보안 그룹 ID	resource.instanceDetails.networkInterfaces.se curityGroups.groupId
보안 그룹 이름	resource.instanceDetails.networkInterfaces.se curityGroups.groupName

콘솔 필드 이름	JSON 필드 이름
서브넷 ID	resource.instanceDetails.networkInterfaces.subnetId
VPC ID	resource.instanceDetails.networkInterfaces.vpcId
Outpost ARN	resource.instanceDetails.outpostARN
리소스 유형	resource.resourceType
버킷 권한	리소스.s3BucketDetails. 공개 액세스. 유효 권한
버킷 이름	BucketDetails리소스.s3. 이름
버킷 태그 키	리소스.s3 BucketDetails .tags.key
버킷 태그 값	리소스.s3 BucketDetails .tags.value
버킷 유형	BucketDetails리소스.s3. type
작업 유형	service.action.actionType
API 호출됨	서비스. 액션. awsApiCall액션.api
API 호출자 유형	서비스. 액션. awsApiCall액션. 호출자 유형
API 오류 코드	서비스. 액션. awsApiCall액션. 오류 코드
API 호출자 도시	서비스. 액션. awsApiCall액션. remoteIpDetails. 도시. 도시 이름
API 호출자 국가	서비스. 액션. awsApiCall액션. remoteIpDetails. 국가. 국가 이름
API 호출자 IPv4 주소	서비스. 액션. awsApiCall액션. remoteIpDetails.IP 주소 V4
API 콜러 IPv6 주소	서비스. 액션. awsApiCall액션. remoteIpDetails.IP 주소 V6

콘솔 필드 이름	JSON 필드 이름
API 호출자 ASN ID	서비스. 액션. awsApiCall액션. remoteIpDetails.orgation.asn
API 호출자 ASN 이름	서비스. 액션. awsApiCall액션. remoteIpDetails. 조직. ASNORG
API 호출자 서비스 이름	서비스. 액션. awsApiCall액션. 서비스 이름
DNS 요청 도메인	서비스. 액션. dnsRequestAction.도메인
DNS 요청 도메인 접미사	서비스. 액션. dnsRequestAction. domainWithSuffix
네트워크 연결 차단됨	서비스. 액션. networkConnectionAction. 차단됨
네트워크 연결 방향	서비스. 액션. networkConnectionAction. 연결 방향
네트워크 연결 로컬 포트	서비스. 액션. networkConnectionAction. localPortDetails. 포트
네트워크 연결 프로토콜	서비스. 액션. networkConnectionAction. 프로토콜
네트워크 연결 도시	서비스. 액션. networkConnectionAction. remoteIpDetails.도시. 도시 이름
네트워크 연결 국가	서비스. 액션. networkConnectionAction. remoteIpDetails. 국가. 국가 이름
네트워크 연결 원격 IPv4 주소	서비스. 액션. networkConnectionAction. remoteIpDetails.IP 주소 V4
네트워크 연결, 원격 IPv6 주소	서비스. 액션. networkConnectionAction. remoteIpDetails.IP 주소 V6
네트워크 연결 원격 IP ASN ID	서비스. 액션. networkConnectionAction. remoteIpDetails.orgation.asn

콘솔 필드 이름	JSON 필드 이름
네트워크 연결 원격 IP ASN 이름	서비스. 액션. networkConnectionAction. remoteIpDetails. 조직. ASNORG
네트워크 연결 원격 포트	서비스. 액션. networkConnectionAction. remotePortDetails. 포트
원격 계정 연결	서비스. 액션. awsApiCall액션. remoteAcc ountDetails. 제휴
Kubernetes API 호출자 IPv4 주소	서비스. 액션. kubernetesApiCall액션. remoteIpDetails.IP 주소 V4
쿠버네티스 API 콜러 IPv6 주소	서비스. 액션. kubernetesApiCall액션. remoteIpDetails.IP 주소 V6
Kubernetes 네임스페이스	서비스. 액션. kubernetesApiCall액션. 네임스페이스
Kubernetes API 호출자 ASN ID	서비스. 액션. kubernetesApiCall액션. remoteIpDetails.orgation.asn
Kubernetes API 호출 요청 URI	서비스. 액션. kubernetesApiCall액션. 리퀘스트
Kubernetes API 상태 코드	서비스. 액션. kubernetesApiCall액션. 상태 코드
네트워크 연결 로컬 IPv4 주소	서비스. 액션. networkConnectionAction. localIpDetails.IP 주소 V4
네트워크 연결 로컬 IPv6 주소	서비스. 액션. networkConnectionAction. localIpDetails.IP 주소 V6
프로토콜	서비스. 액션. networkConnectionAction. 프로토콜
API 호출 서비스 이름	서비스. 액션. awsApiCall액션. 서비스 이름
API 호출자 계정 ID	서비스. 액션. awsApiCall액션. remoteAcc ountDetails. 계정 ID

콘솔 필드 이름	JSON 필드 이름
위협 목록 이름	서비스. 추가 정보. threatListName
리소스 역할	service.resourceRole
EKS 클러스터 이름	의지. eksClusterDetails.이름
Kubernetes 워크로드 이름	리소스. 쿠버네티스 세부 정보. kubernetesWorkloadDetails.name
Kubernetes 워크로드 네임스페이스	리소스. 쿠버네티스 세부 정보. kubernetesWorkloadDetails. 네임스페이스
Kubernetes 사용자 이름	리소스. 쿠버네티스 세부 정보. kubernetesUserDetails. 사용자 이름
Kubernetes 컨테이너 이미지	리소스. 쿠버네티스 세부 정보. kubernetesWorkloadDetails. 컨테이너. 이미지
Kubernetes 컨테이너 이미지 접두사	리소스. 쿠버네티스 세부 정보. kubernetesWorkloadDetails. 컨테이너. 이미지 접두사
스캔 ID	서비스. ebsVolumeScan세부 정보. 스캔 ID
EBS 볼륨 스캔 위협 이름	서비스. ebsVolumeScan세부 정보. 탐지 스캔. threatDetectedBy이름. 위협 이름. 이름
위협 심각도	서비스. ebsVolumeScan세부 정보. 탐지 스캔. threatDetectedBy이름. 위협 이름. 심각도
파일 SHA	서비스. ebsVolumeScan세부 정보. 탐지 스캔. threatDetectedBy이름. 위협 이름. 파일 경로. 해시
ECS 클러스터 이름	리소스. ecsClusterDetails.이름
ECS 컨테이너 이미지	리소스. ecsClusterDetails. 작업 세부 정보. 컨테이너. 이미지

콘솔 필드 이름	JSON 필드 이름
ECS 작업 정의 ARN	리소스. ecsClusterDetails. 작업 세부 정보. 정의 ARN
독립형 컨테이너 이미지	resource.containerDetails.image
데이터베이스 인스턴스 ID	리소스. rdsDbInstance세부 정보. dbInstanceIdentifier
데이터베이스 클러스터 ID	의지. rdsDbInstance세부 정보. dbClusterIdentifier
데이터베이스 엔진	의지. rdsDbInstance세부 정보. 엔진
데이터베이스 사용자	리소스. rdsDbUser세부 정보. 사용자
데이터베이스 인스턴스 태그 키	리소스. rdsDbInstance세부 정보. 태그. 키
데이터베이스 인스턴스 태그 값	리소스. rdsDbInstance세부 정보.태그.값
실행 파일 SHA-256	service.runtimeDetails.process.executableSha256
프로세스 이름	service.runtimeDetails.process.name
실행 가능한 경로	service.runtimeDetails.process.executablePath
Lambda 함수 이름	resource.lambdaDetails.functionName
Lambda 함수 ARN	resource.lambdaDetails.functionArn
Lambda 함수 태그 키	resource.lambdaDetails.tags.key
Lambda 함수 태그 값	resource.lambdaDetails.tags.value
DNS 요청 도메인	서비스. 액션. dnsRequestAction. domainWithSuffix

억제 규칙

억제 규칙은 지정된 기준과 일치하는 새 결과를 자동으로 보관하여 결과를 필터링하는 데 사용되는 값과 페어링된 필터 속성으로 구성된 일련의 기준입니다. 억제 규칙을 사용하면 가치가 낮은 결과, 오탐지 결과 또는 조치를 취하지 않으려는 위협을 필터링할 수 있으므로 환경에 가장 큰 영향을 미치는 보안 위협을 보다 쉽게 파악할 수 있습니다.

억제 규칙을 생성한 후, 억제 규칙이 지정되어 있는 동안에는 규칙에 정의된 기준과 일치하는 새 결과가 자동으로 보관됩니다. 기존 필터를 사용하여 억제 규칙을 생성하거나 정의한 새 필터에서 억제 규칙을 생성할 수 있습니다. 억제 규칙을 구성하여 전체 결과 유형을 억제하거나, 보다 세부적인 필터 기준을 정의하여 특정 결과 유형의 특정 인스턴스만 억제할 수 있습니다. 억제 규칙은 언제든지 편집할 수 있습니다.

숨겨진 검색 결과는 Amazon Simple Storage Service AWS Security Hub, Amazon Detective 또는 Amazon으로 전송되지 않으므로 Security Hub, 타사 SIEM 또는 기타 알림 및 티켓 애플리케이션을 통해 결과를 사용할 GuardDuty 경우 검색 결과 노이즈 수준이 낮아집니다. EventBridge 활성화한 경우GuardDuty 멀웨어 보호, 차단된 GuardDuty 발견으로 인해 멀웨어 스캔이 시작되지 않습니다.

GuardDuty 검색 결과가 금지 규칙과 일치하는 경우에도 검색 결과가 계속 생성되지만 해당 결과는 자동으로 보관된 것으로 표시됩니다. 보관된 검색 결과는 90일 동안 저장되며 해당 기간 중 언제든지 볼 수 있습니다. GuardDuty 검색 결과 테이블에서 보관됨을 선택하여 GuardDuty 콘솔에서 숨겨진 검색 결과를 보거나, `findingCriteria` 기준이 true와 같으면 GuardDuty API를 사용하여 API를 통해 숨겨진 검색 결과를 볼 수 있습니다. ListFindings`service.archived`

> **Note**
>
> 다중 계정 환경에서는 GuardDuty 관리자만 금지 규칙을 생성할 수 있습니다.

억제 규칙의 일반 사용 사례 및 예시

다음 결과 유형은 억제 규칙 적용에 대한 일반 사용 사례입니다. 결과 이름을 선택하여 해당 결과에 대해 자세히 알아보거나 정보를 검토하여 콘솔에서 해당 결과에 대한 억제 규칙을 구축하세요.

> **Important**
>
> GuardDuty 반복적으로 오탐이 확인된 결과에 대해서만 사후 대응적으로 금지 규칙을 작성할 것을 권장합니다.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS - VPC 네트워킹이 인터넷 트래픽을 라우팅하도록 구성되어 있고 VPC 인터넷 게이트웨이가 아닌 온프레미스 게이트웨이에서 인터넷 트래픽이 나가는 경우 억제 규칙을 사용하여 생성된 결과를 자동으로 보관합니다.

  이 결과는 네트워킹이 인터넷 트래픽을 라우팅하도록 구성되어 VPC 인터넷 게이트웨이(IGW)가 아닌 온프레미스 게이트웨이에서 나가는 경우에 생성됩니다. AWS Outposts 또는 VPC VPN 연결을 사용하는 것과 같은 일반적인 구성으로 인해 트래픽이 이러한 방식으로 라우팅될 수 있습니다. 예상된 동작인 경우 의 억제 규칙을 사용하고 두 개의 필터 기준으로 구성된 규칙을 만드는 것이 좋습니다. 첫 번째 기준은 결과 유형으로 `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`이어야 합니다. 두 번째 필터 기준은 온프레미스 인터넷 게이트웨이의 IP 주소 또는 CIDR 범위를 포함하는 API 호출자 IPv4 주소입니다. 아래 예시는 API 호출자 IP 주소를 기반으로 이 결과 유형을 억제하는 데 사용할 필터를 나타냅니다.

  ```
  Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
   API caller IPv4 address: 198.51.100.6
  ```

  > **Note**
  >
  > 여러 개의 API 호출자 IP를 포함하려면 각각에 대해 새 API 호출자 IPv4 주소 필터를 추가할 수 있습니다.

- Recon:EC2/Portscan - 취약성 평가 애플리케이션을 사용하는 경우 억제 규칙을 사용하여 자동으로 결과를 보관합니다.

  억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 `Recon:EC2/Portscan` 값을 사용해야 합니다. 두 번째 필터 기준은 이러한 취약성 평가 도구를 호스팅하는 인스턴스와 일치해야 합니다. 이러한 도구를 호스팅하는 인스턴스에서 식별 가능한 기준에 따라 Instance image ID 속성 또는 Tag 값 속성을 사용할 수 있습니다. 아래 예시는 특정 AMI를 기반으로 이 결과 유형을 억제하는 데 사용할 필터를 나타냅니다.

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce - Bastion 인스턴스를 대상으로 하는 경우 억제 규칙을 사용하여 자동으로 결과를 보관합니다.

  무차별 대입 시도의 대상이 배스천 호스트인 경우 이는 사용자 환경에 예상되는 동작일 수 있습니다. AWS 이 경우 이 결과에 대해 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과

UnauthorizedAccess:EC2/SSHBruteForce 값을 사용해야 합니다. 두 번째 필터 기준은 Bastion Host로 사용되는 인스턴스와 일치해야 합니다. 이러한 도구를 호스팅하는 인스턴스에서 식별 가능한 기준에 따라 인스턴스 이미지 ID 속성 또는 태그 값 속성을 사용할 수 있습니다. 아래 예시는 특정 인스턴스 태그 값을 기반으로 이 결과 유형을 억제하는 데 사용할 필터를 나타냅니다.

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- Recon:EC2/PortProbeUnprotectedPort - 의도적으로 노출된 인스턴스를 대상으로 하는 경우 억제 규칙을 사용하여 자동으로 결과를 보관합니다.

  인스턴스가 웹 서버를 호스팅하는 경우와 같이 의도적으로 노출되는 경우가 있을 수 있습니다. 사용자 AWS 환경에서 이런 경우에는 이 검색 결과에 대한 억제 규칙을 설정하는 것이 좋습니다. 억제 규칙은 두 개의 필터 기준으로 구성해야 합니다. 첫 번째 기준에는 Finding type(결과 유형) 속성과 Recon:EC2/PortProbeUnprotectedPort 값을 사용해야 합니다. 두 번째 필터 기준은 Bastion Host로 사용되는 인스턴스와 일치해야 합니다. 이러한 도구를 호스팅하는 인스턴스에서 식별 가능한 기준에 따라 인스턴스 이미지 ID 속성 또는 태그 값 속성을 사용할 수 있습니다. 아래 예시는 콘솔의 특정 인스턴스 태그 키를 기반으로 이 결과 유형을 억제하는 데 사용할 필터를 나타냅니다.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

런타임 모니터링 결과에 대한 권장 금지 규칙

- PrivilegeEscalation:Runtime/DockerSocketAccessed는 컨테이너 내부의 프로세스가 Docker 소켓과 통신할 때 생성됩니다. 환경에 합법적인 이유로 Docker 소켓에 액세스해야 하는 컨테이너가 있을 수 있습니다. 이러한 컨테이너에서 액세스하면 PrivilegeEscalation:Runtime/DockerSocketAccessed 결과가 생성됩니다. 사용자 AWS 환경에서 이런 경우가 발생하는 경우 이 검색 유형에 대한 억제 규칙을 설정하는 것이 좋습니다. 첫 번째 기준에는 값이 PrivilegeEscalation:Runtime/DockerSocketAccessed와 같은 결과 유형 필드를 사용해야 합니다. 두 번째 필터 기준은 생성된 결과에서 프로세스의 executablePath와 값이 동일한 실행 파일 경로 필드입니다. 또는 두 번째 필터 기준에서 생성된 결과에서 프로세스의 executableSha256와 값이 동일한 실행 파일 SHA-256 필드를 사용할 수 있습니다.
- Kubernetes 클러스터는 자체 DNS 서버를 포드로 실행할 수 있습니다(예: coredns). 따라서 포드에서 DNS를 조회할 때마다 두 개의 DNS 이벤트를 GuardDuty 캡처합니다. 하나는 포드에서, 다른 하나는 서버 포드에서 캡처됩니다. 이로 인해 다음과 같은 DNS 결과가 중복될 수 있습니다.
  - Backdoor:Runtime/C&CActivity.B!DNS
  - CryptoCurrency:Runtime/BitcoinTool.B!DNS

- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

중복 결과에는 DNS 서버 포드에 해당하는 포드, 컨테이너 및 프로세스 세부 정보가 포함됩니다. 이러한 필드를 사용하여 이러한 중복 결과를 억제하는 억제 규칙을 설정할 수 있습니다. 첫 번째 필터 기준은 앞서 이 섹션에 제공된 결과 목록의 DNS 결과 유형과 값이 동일한 결과 유형 필드를 사용해야 합니다. 두 번째 필터 기준은 생성된 결과에서 값이 DNS 서버의 `executablePath`와 같은 실행 파일 경로 또는 DNS 서버의 `executableSHA256`과 같은 실행 파일 SHA-256일 수 있습니다. 세 번째 필터 기준은 선택 사항으로 생성된 결과에서 DNS 서버 포드의 컨테이너 이미지와 동일한 값을 갖는 Kubernetes 컨테이너 이미지 필드를 사용할 수 있습니다.

억제 규칙 생성

선호하는 액세스 방법을 선택하여 유형을 GuardDuty 찾기 위한 금지 규칙을 생성하십시오.

Console

콘솔을 사용하여 금지 규칙을 시각화, 생성 및 관리할 수 있습니다. GuardDuty 억제 규칙은 필터와 동일한 방식으로 생성되며, 기존에 저장된 필터를 억제 규칙으로 사용할 수 있습니다. 필터 생성에 대한 자세한 내용은 조사 결과 필터링 섹션을 참조하세요.

콘솔을 사용하여 억제 규칙 생성:

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 결과 페이지에서 결과 표시 안 함을 선택하여 억제 규칙 패널을 엽니다.
3. 필터 기준 메뉴를 열려면 필터 기준 추가에 **`filter criteria`**를 입력합니다. 목록에서 기준을 선택할 수 있습니다. 선택한 기준에 유효한 값을 입력합니다.

> **Note**
>
> 유효한 값을 결정하려면 결과 테이블을 보고 억제하려는 결과를 선택합니다. 결과 패널에서 세부 정보를 검토합니다.

여러 필터 기준을 추가하고 억제하려는 결과만 테이블에 표시되도록 할 수 있습니다.

4. 억제 규칙의 이름과 설명을 입력합니다. 유효한 문자에는 영숫자, 마침표(.), 밑줄(_), 대시(-) 및 공백이 포함됩니다.
5. 저장을 선택합니다.

또한 기존의 저장된 필터에서 억제 규칙을 생성할 수 있습니다. 필터 생성에 대한 자세한 내용은 조사 결과 필터링 섹션을 참조하세요.

저장된 필터에서 금지 규칙 생성:

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 결과 페이지에서 결과 표시 안 함을 선택하여 억제 규칙 패널을 엽니다.
3. 저장된 규칙 드롭다운에서 저장된 필터를 선택합니다.
4. 또한 새 필터 기준을 추가할 수 있습니다. 추가 필터 기준이 필요하지 않은 경우 이 단계를 건너뜁니다.

   필터 기준 메뉴를 열려면 필터 기준 추가에 **`filter criteria`**를 입력합니다. 목록에서 기준을 선택할 수 있습니다. 선택한 기준에 유효한 값을 입력합니다.

> **Note**
>
> 유효한 값을 결정하려면 결과 테이블을 보고 억제하려는 결과를 선택합니다. 결과 패널에서 세부 정보를 검토합니다.

5. 억제 규칙의 이름과 설명을 입력합니다. 유효한 문자에는 영숫자, 마침표(.), 밑줄(_), 대시(-) 및 공백이 포함됩니다.
6. 저장을 선택합니다.

API/CLI

API를 사용하여 억제 규칙 생성:

1. CreateFilter API를 통해 억제 규칙을 생성할 수 있습니다. 이를 위해 아래에 설명하는 예시의 형식을 따라 JSON 파일에 필터 기준을 지정하세요. 아래 예시에서는 test.example.com 도메인에 대한 DNS 요청이 있는 보관되지 않은 낮은 심각도 결과를 모두 표시하지 않습니다. 심각도가 중간인 결과의 경우 입력 목록은 ["4", "5", "7"]입니다. 심각도가 높은 결과의 경우 입력 목록은 ["6", "7", "8"]입니다. 목록에 있는 값 하나를 기준으로 필터링할 수도 있습니다.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

JSON 필드 이름 및 이에 상응하는 콘솔의 목록은 필터 속성 단원을 참조하십시오.

필터 기준을 테스트하려면 ListFindings API에서 동일한 JSON 기준을 사용하고, 올바른 결과가 선택되었는지 확인합니다. 를 사용하여 필터 기준을 테스트하려면 자체 DetectorID와.json 파일을 사용하여 예제를 AWS CLI 따르세요.

계정과 현재 지역에 `detectorId` 맞는 항목을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. CreateFilter API를 사용하거나 자체 탐지기 ID, 억제 규칙의 이름 및 .json 파일을 사용하는 아래 예시에 따라 AWS CLI를 사용하여 억제 규칙으로 사용할 필터를 업로드합니다.

   계정과 현재 지역을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

```
aws guardduty create-filter --action ARCHIVE --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
 file://criteria.json
```

ListFilter API를 사용하여 프로그래밍 방식으로 필터 목록을 볼 수 있습니다. GetFilter API에 필터 이름을 제공하여 개별 필터의 세부 정보를 볼 수 있습니다. UpdateFilter를 사용하여 필터를 업데이트하거나 DeleteFilter API를 사용하여 삭제합니다.

억제 규칙 삭제

선호하는 액세스 방법을 선택하여 유형 GuardDuty 검색에 대한 금지 규칙을 삭제하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 결과 페이지에서 결과 표시 안 함을 선택하여 억제 규칙 패널을 엽니다.
3. 저장된 규칙 드롭다운에서 저장된 필터를 선택합니다.
4. 규칙 삭제를 선택합니다.

API/CLI

DeleteFilter API를 실행합니다. 특정 지역의 필터 이름과 관련 탐지기 ID를 지정합니다.

또는 다음 AWS CLI 예제를 사용하여 *###* 형식의 값을 바꿀 수 있습니다.

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

계정과 현재 지역에 `detectorId` 맞는 값을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

신뢰할 수 있는 IP 목록 및 위협 목록 사용

Amazon은 VPC 흐름 로그, AWS CloudTrail 이벤트 로그 및 DNS 로그를 분석하고 처리하여 AWS 환경의 보안을 GuardDuty 모니터링합니다. 신뢰할 수 있는 IP 목록에서 신뢰할 수 있는 IP에 대한 알림을 중지하고 자체 위협 목록에서 알려진 악성 IP에 대해서는 GuardDuty 경고하도록 구성하여 이 모니터링 범위를 사용자 지정할 수 있습니다.

신뢰할 수 있는 IP 목록과 위협 목록은 공개적으로 라우팅 가능한 IP 주소로 가는 트래픽에만 적용됩니다. 목록의 효과는 모든 VPC 흐름 로그 및 CloudTrail 결과에 적용되지만 DNS 결과에는 적용되지 않습니다.

GuardDuty 다음 유형의 목록을 사용하도록 구성할 수 있습니다.

신뢰할 수 있는 IP 목록

신뢰할 수 있는 IP 목록은 AWS 인프라 및 애플리케이션과의 보안 통신을 위해 신뢰할 수 있는 IP 주소로 구성됩니다. GuardDuty 신뢰할 수 있는 IP 목록의 IP 주소에 대한 VPC 흐름 로그 또는 CloudTrail 검색 결과를 생성하지 않습니다. 신뢰할 수 있는 IP 목록당 최대 2000개의 IP 주소 및 CIDR 범위를 포함할 수 있습니다. 해당 시점에 리전별로 AWS 계정당 신뢰할 수 있는 IP 목록을 하나만 업로드할 수 있습니다.

위협 IP 목록

위협 목록은 알려진 악성 IP 주소로 구성되어 있습니다. 이 목록은 타사 위협 인텔리전스에서 제공하거나 조직에 맞춰 특별히 만들 수 있습니다. 잠재적으로 의심스러운 활동으로 인한 탐지 결과를 생성하는 것 외에도 이러한 위협 목록을 기반으로 조사 결과를 생성합니다. GuardDuty 단일 위협 목록에 최대 250,000개의 IP 주소와 CIDR 범위를 포함할 수 있습니다. GuardDuty 위협 목록의 IP 주소 및 CIDR 범위와 관련된 활동을 기반으로 탐지 결과만 생성합니다. 탐지 결과는 도메인 이름을 기반으로 생성되지 않습니다. 어느 시점에서든 각 AWS 계정 지역당 최대 6개의 위협 목록을 업로드할 수 있습니다.

> **Note**
>
> 신뢰할 수 있는 IP 목록과 위협 목록에 동일한 IP를 포함하면 신뢰할 수 있는 IP 목록에서 해당 IP가 먼저 처리되며 결과가 생성되지 않습니다.

다중 계정 환경에서는 GuardDuty 관리자 계정 계정의 사용자만 신뢰할 수 있는 IP 목록 및 위협 목록을 추가하고 관리할 수 있습니다. 관리자 계정 계정에서 업로드한 신뢰할 수 있는 IP 목록 및 위협 목록은 해당 구성원 계정의 GuardDuty 기능에 적용됩니다. 즉, 구성원 GuardDuty 계정에서는 관리자 계정의 위협 목록에 있는 알려진 악성 IP 주소와 관련된 활동을 기반으로 검색 결과를 생성하며 관리자 계정의 신뢰할 수 있는 IP 목록에 있는 IP 주소와 관련된 활동을 기반으로 검색 결과를 생성하지는 않습니다. 자세한 정보는 Amazon에서 여러 계정 관리 GuardDuty을 참조하세요.

목록 형식

GuardDuty 다음 형식의 목록을 수락합니다.

신뢰할 수 있는 IP 목록 및 위협 IP 목록을 호스팅하는 각 파일의 최대 크기는 35MB입니다. 신뢰할 수 있는 IP 목록 및 위협 IP 목록에서 IP 주소와 CIDR 범위는 줄당 하나씩 표시되어야 합니다. IPv4 주소만 허용됩니다.

- 일반 텍스트(TXT)

  이 형식은 CIDR 블록과 개별 IP 주소를 모두 지원합니다. 다음 샘플 목록은 일반 텍스트(TXT) 형식을 사용합니다.

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- Structured Threat Information Expression(STIX)

  이 형식은 CIDR 블록과 개별 IP 주소를 모두 지원합니다. 다음 샘플 목록은 STIX 형식을 사용합니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
```

```
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
```

```
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- Open Threat Exchange(OTX)™ CSV

  이 형식은 CIDR 블록과 개별 IP 주소를 모두 지원합니다. 다음 샘플 목록은 OTX™ CSV 형식을 사용합니다.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ iSight 위협 인텔리전스 CSV

  이 형식은 CIDR 블록과 개별 IP 주소를 모두 지원합니다. 다음 샘플 목록은 FireEye™ CSV 형식을 사용합니다.

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
```

```
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- Proofpoint™ ET Intelligence Feed CSV

  이 형식은 개별 IP 주소만 지원합니다. 다음 샘플 목록은 `Proofpoint` CSV 형식을 사용합니다. `ports` 파라미터는 선택 항목입니다. 포트를 건너뛰는 경우 끝에 쉼표(,)를 남겨야 합니다.

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVault™ 평판 피드

  이 형식은 개별 IP 주소만 지원합니다. 다음 샘플 목록은 `AlienVault` 형식을 사용합니다.

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

신뢰할 수 있는 IP 목록 및 위협 목록을 업로드하는 데 필요한 권한

다양한 IAM ID에는 신뢰할 수 있는 IP 목록 및 위협 목록을 다루려면 특별한 권한이 필요합니다. GuardDuty AmazonGuardDutyFullAccess 관리형 정책이 연결되어 있는 ID는 업로드된 신뢰할 수 있는 IP 목록과 위협 목록의 이름을 바꾸거나 비활성화하는 것만 가능합니다.

신뢰할 수 있는 IP 목록 및 위협 목록으로 작업할 수 있는 전체 액세스 권한(이름 변경 및 비활성화 외에 추가, 활성화, 삭제, 목록 위치 또는 이름 업데이트까지 포함)을 여러 ID에 부여하려면 IAM 사용자, 그룹, 역할에 연결된 권한 정책에 다음과 같은 작업이 들어 있어야 합니다.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
```

```
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> 이러한 작업은 AmazonGuardDutyFullAccess 관리형 정책에 들어 있지 않습니다.

신뢰할 수 있는 IP 목록 및 위협 목록에 대한 서버 측 암호화 사용

GuardDuty 목록에 다음과 같은 암호화 유형을 지원합니다: SSE-AES256 및 SSE-KMS. SSE-C는 지원되지 않습니다. S3의 암호 유형에 대한 자세한 내용은 서버 측 암호화를 사용하여 데이터 보호를 참조하세요.

목록이 서버측 암호화 GuardDuty SSE-KMS를 사용하여 암호화된 경우 목록을 활성화하려면 서비스 연결 역할에 파일을 해독할 수 있는 AWSServiceRoleForAmazonGuardDuty권한을 부여해야 합니다. KMS 키 정책에 다음 문을 추가하고 계정 ID를 자신의 ID로 바꿉니다.

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

신뢰할 수 있는 IP 목록 또는 위협 IP 목록 추가 및 활성화

다음 액세스 방법 중 하나를 선택하여 신뢰할 수 있는 IP 목록 또는 위협 IP 목록을 추가하고 활성화합니다.

Console

(선택 사항) 1단계: 목록의 위치 URL 가져오기

1. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.

2. 탐색 창에서 버킷을 선택합니다.
3. 추가할 특정 목록이 포함된 Amazon S3 버킷 이름을 선택합니다.
4. 세부 정보를 보려면 객체(목록) 이름을 선택합니다.
5. 속성 탭에서 이 객체의 S3 URI를 복사합니다.

2단계: 신뢰할 수 있는 IP 목록 또는 위협 목록 추가

> **Important**
>
> 기본적으로 어느 시점에서든 신뢰할 수 있는 IP 목록은 하나만 있을 수 있습니다. 마찬가지로 최대 6개의 위협 목록을 보유할 수 있습니다.

1. GuardDuty https://console.aws.amazon.com/guardduty/ 에서 콘솔을 엽니다.
2. 탐색 창에서 목록을 선택합니다.
3. [List management] 페이지에서 [Add a trusted IP list] 또는 [Add a threat list]를 선택합니다.
4. 선택에 따라 대화 상자가 표시됩니다. 다음 단계를 수행합니다.

   a. 목록 이름에 목록의 이름을 입력합니다.

      목록 이름 지정 제약 조건 — 목록 이름에는 소문자, 대문자, 숫자, 대시 (-), 밑줄 (_) 이 포함될 수 있습니다.

   b. 위치에 목록을 업로드한 위치를 입력합니다. 아직 없는 경우 Step 1: Fetching location URL of your list 섹션을 참조하세요.

      위치 URL의 형식

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt
      - s3://bucket.name/file.txt

   c. [I agree] 확인란을 선택합니다.

   d. [Add list]를 선택합니다. 추가된 목록의 상태는 기본적으로 비활성입니다. 목록이 유효하려면 목록을 활성화해야 합니다.

3단계: 신뢰할 수 있는 IP 목록 또는 위협 목록 활성화

1. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 GuardDuty 엽니다.
2. 탐색 창에서 목록을 선택합니다.
3. 목록 관리 페이지에서 활성화할 목록을 선택합니다.
4. 작업을 선택한 후 활성화를 선택합니다. 목록이 유효하려면 최대 15분이 걸릴 수 있습니다.

API/CLI

신뢰할 수 있는 IP 목록

- CreateIPSet를 실행합니다. 이 신뢰할 수 있는 IP 목록을 만들려는 멤버 계정의 `detectorId`를 제공해야 합니다.

  목록 이름 지정 제약 조건 — 목록 이름에는 소문자, 대문자, 숫자, 대시 (-), 밑줄 (_) 이 포함될 수 있습니다.

  - 또는 다음 AWS Command Line Interface 명령을 실행하고 `detector-id`를 신뢰할 수 있는 IP 목록을 업데이트할 멤버 계정의 탐지기 ID로 바꿉니다.

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

위협 목록

- CreateThreatIntelSet를 실행합니다. 이 위협 목록을 만들려는 멤버 계정의 `detectorId`를 제공해야 합니다.
  - 다음 명령을 실행하여 이 작업을 수행할 수도 있습니다. AWS Command Line Interface 위협 목록을 만들려는 멤버 계정의 `detectorId`를 제공해야 합니다.

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

> **Note**
>
> IP 목록을 활성화하거나 업데이트한 후 목록을 동기화하는 데 최대 15분이 GuardDuty 걸릴 수 있습니다.

신뢰할 수 있는 IP 목록 및 위협 목록 업데이트

이미 추가 및 활성화된 목록에 추가된 목록의 이름 또는 IP 주소를 업데이트할 수 있습니다. 목록을 업데이트한 경우 최신 버전의 목록을 GuardDuty 사용하려면 목록을 다시 활성화해야 합니다.

액세스 방법 중 하나를 선택하여 신뢰할 수 있는 IP 또는 위협 목록을 업데이트합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 목록을 선택합니다.
3. 목록 관리 페이지에서 업데이트하고자 하는 신뢰할 수 있는 IP 세트 또는 위협 목록을 선택합니다.
4. 작업을 선택한 후 편집을 선택합니다.
5. 목록 업데이트 대화 상자에서 필요에 따라 정보를 업데이트합니다.

   목록 이름 지정 제약 조건 — 목록 이름에는 소문자, 대문자, 숫자, 대시 (-), 밑줄 (_) 이 포함될 수 있습니다.
6. 동의함 확인란을 선택한 다음 목록 업데이트를 선택합니다. 상태 열의 값이 비활성으로 변경됩니다.
7. 업데이트된 목록 재활성화

   a. 목록 관리 페이지에서 다시 활성화할 목록을 선택합니다.

   b. 작업을 선택한 후 활성화를 선택합니다.

API/CLI

1. UpdateIPSet를 실행하여 신뢰할 수 있는 IP 목록을 업데이트합니다.
   - 또는 다음 AWS CLI 명령을 실행하여 신뢰할 수 있는 IP 목록을 업데이트하고 `detector-id`를 신뢰할 수 있는 IP 목록을 업데이트할 멤버 계정의 탐지기 ID로 바꿉니다.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

2. UpdateThreatIntelSet를 실행하여 위협 목록 업데이트
   - 또는 다음 AWS CLI 명령을 실행하여 위협 목록을 업데이트하고 `detector-id`를 위협 목록을 업데이트할 멤버 계정의 탐지기 ID로 바꿉니다.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

신뢰할 수 있는 IP 목록 또는 위협 목록 비활성화 또는 삭제

액세스 방법 중 하나를 선택하여 신뢰할 수 있는 IP 목록 또는 위협 목록을 삭제(콘솔 사용)하거나 비활성화(API/CLI 사용)합니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 콘솔을 GuardDuty 엽니다.
2. 탐색 창에서 목록을 선택합니다.
3. 목록 관리 페이지에서 삭제할 목록을 선택합니다.
4. 작업을 선택한 후 삭제를 선택합니다.
5. 작업을 확인하고 삭제를 선택합니다. 더 이상 테이블에서 특정 목록을 사용할 수 없습니다.

API/CLI

1. 신뢰할 수 있는 IP 목록

   UpdateIPSet를 실행하여 신뢰할 수 있는 IP 목록을 업데이트합니다.
   - 또는 다음 AWS CLI 명령을 실행하여 신뢰할 수 있는 IP 목록을 업데이트하고 `detector-id`를 신뢰할 수 있는 IP 목록을 업데이트할 멤버 계정의 탐지기 ID로 바꿉니다.

     계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
no-activate
```

2. 위협 목록

   UpdateThreatIntelSet를 실행하여 위협 목록 업데이트

   - 또는 다음 AWS CLI 명령을 실행하여 신뢰할 수 있는 IP 목록을 업데이트하고 `detector-id`를 위협 목록을 업데이트할 멤버 계정의 탐지기 ID로 바꿉니다.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --no-activate
```

결과 내보내기

GuardDuty 생성된 결과를 90일 동안 보관합니다. GuardDuty 활성 결과를 Amazon EventBridge (EventBridge) 으로 내보냅니다. 선택적으로 생성된 결과를 Amazon Simple Storage 서비스 (Amazon S3) 버킷으로 내보낼 수 있습니다. 이렇게 하면 계정에서 잠재적으로 의심스러운 활동의 기록 데이터를 추적하고 권장 해결 단계가 성공적이었는지 평가하는 데 도움이 됩니다.

새로 GuardDuty 생성되는 활성 검색 결과는 모두 검색 결과 생성 후 약 5분 이내에 자동으로 내보내집니다. 활성 검색 결과에 대한 업데이트를 내보내는 빈도를 설정할 수 EventBridge 있습니다. 선택한 빈도는 기존 검색 결과를 S3 버킷 (구성된 경우) 및 Detective (통합된 경우) 로 새로 내보내는 데 EventBridge 적용됩니다. 기존 검색 결과의 여러 발생을 GuardDuty 집계하는 방법에 대한 자세한 내용은 을 참조하십시오. GuardDuty 집계 결과 찾기

결과를 Amazon S3 버킷으로 내보내도록 설정을 구성하는 경우, AWS Key Management Service (AWS KMS) 를 GuardDuty 사용하여 S3 버킷의 결과 데이터를 암호화합니다. 이를 위해서는 계정에서 결과를 내보내는 데 사용할 GuardDuty 수 있도록 S3 버킷과 AWS KMS 키에 권한을 추가해야 합니다.

내용

- 4단계 - 결과를 S3 버킷으로 내보내기 (콘솔)
- 5단계 — 업데이트된 활성 결과를 내보내는 빈도 설정

고려 사항

결과를 내보내기 위한 사전 요구 사항 및 단계를 진행하기 전에 다음 주요 개념을 고려하십시오.

- 내보내기 설정은 지역입니다. — 사용하는 각 지역에서 내보내기 옵션을 구성해야 합니다. GuardDuty
- 결과를 다른 AWS 리전 (지역 간) 의 Amazon S3 버킷으로 내보내기 — 다음 내보내기 설정을 GuardDuty 지원합니다.
  - Amazon S3 버킷 또는 객체와 AWS KMS 키는 동일한 객체에 속해야 합니다 AWS 리전.
  - 상업 지역에서 생성된 검색 결과의 경우 해당 결과를 상업 지역의 S3 버킷으로 내보내도록 선택할 수 있습니다. 하지만 옵트인 지역의 S3 버킷으로 이러한 결과를 내보낼 수는 없습니다.
  - 옵트인 지역에서 생성된 결과의 경우, 이러한 결과를 생성된 동일한 옵트인 리전 또는 상업용 리전으로 내보낼 수 있습니다. 하지만 한 옵트인 지역의 결과를 다른 옵트인 지역으로 내보낼 수는 없습니다.
- 검색 결과 내보내기 권한 - 활성 검색 결과를 내보내기 위한 설정을 구성하려면 S3 버킷에 객체 업로드를 허용하는 GuardDuty 권한이 있어야 합니다. 또한 결과를 암호화하는 데 사용할 GuardDuty 수 있는 AWS KMS 키가 있어야 합니다.
- 보관된 검색 결과는 내보내지 않음 - 기본 동작은 숨겨진 검색 결과의 새 인스턴스를 포함하여 보관된 검색 결과를 내보내지 않는 것입니다.

  보관된 결과를 내보내려면 보관을 취소해야 합니다. 그러면 상태가 활성으로 변경됩니다. 내보내기 빈도에 따라 검색 결과가 구성된 S3 버킷으로 내보내집니다.
- GuardDuty 관리자 계정은 관련 멤버 계정에서 생성된 검색 결과를 내보낼 수 있습니다. — 관리자 계정에서 내보내기 결과를 구성하면 동일한 지역에서 생성된 관련 멤버 계정의 모든 검색 결과도 관리자 계정 계정에 대해 구성한 동일한 위치로 내보냅니다. 자세한 정보는 GuardDuty 관리자 계정과 구성원 계정 간의 관계 이해을 참조하세요.

1단계 — 검색 결과를 내보내는 데 필요한 권한

검색 결과 내보내기 설정을 구성할 때는 검색 결과를 저장할 수 있는 Amazon S3 버킷과 데이터 암호화에 사용할 AWS KMS 키를 선택합니다. 결과를 내보내는 설정을 성공적으로 구성하려면 GuardDuty 작업에 대한 권한 외에도 다음 작업에 대한 권한도 있어야 합니다.

- s3: GetBucketLocation
- s3: PutObject

2단계 — KMS 키에 정책 연결

GuardDuty 를 사용하여 버킷의 검색 결과 데이터를 암호화합니다. AWS Key Management Service설정을 성공적으로 구성하려면 먼저 KMS 키 사용 GuardDuty 권한을 부여해야 합니다. KMS 키에 정책을 연결하여 권한을 부여할 수 있습니다.

다른 계정의 KMS 키를 사용하는 경우 키를 AWS 계정 소유한 사람에게 로그인하여 키 정책을 적용해야 합니다. 결과를 내보내도록 설정을 구성할 때는 키를 소유한 계정의 키 ARN도 필요합니다.

내보낸 결과를 암호화하도록 KMS 키 정책을 GuardDuty 수정하려면

1. https://console.aws.amazon.com/kms 에서 AWS KMS 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. 기존 KMS 키를 선택하거나 AWS Key Management Service 개발자 가이드에서 내보낸 결과를 암호화하는 데 사용할 새 키를 만드는 단계를 수행하십시오.

   > **Note**
   >
   > KMS 키와 Amazon S3 버킷의 키는 동일해야 합니다. AWS 리전
   >
   > 동일한 S3 버킷과 KMS 키 페어를 사용하여 적용 가능한 모든 지역에서 결과를 내보낼 수 있습니다. 자세한 고려 사항 내용은 지역 간 결과 내보내기를 참조하십시오.

4. Key policy(키 정책) 섹션에서 Edit(편집)를 선택합니다.

   정책 보기로 전환이 표시되면 이를 선택하여 키 정책을 표시한 다음 편집을 선택합니다.

5. 다음 정책 블록을 KMS 키 정책에 복사하여 키 사용 GuardDuty 권한을 부여합니다.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
```

```
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. 정책 예제에서 *###* 서식이 지정된 다음 값을 대체하여 정책을 편집하십시오.

   1. *KMS # ARN#* KMS 키의 아마존 리소스 이름 (ARN) 으로 대체합니다. 키 ARN을 찾으려면 개발자 안내서의 키 ID 및 ARN 찾기를 참조하십시오.AWS Key Management Service
   2. *123456789012#* 결과를 내보내는 계정을 소유한 AWS 계정 ID로 바꾸십시오. GuardDuty
   3. *## 2# ## ### ### ###* 바꾸십시오. AWS 리전 GuardDuty
   4. *SourceDetectorID#* 조사 결과가 `detectorID` 생성된 특정 지역의 GuardDuty 계정 이름으로 바꾸십시오.

      계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

   > **Note**
   >
   > 옵트인 GuardDuty 지역에서 사용하는 경우 “서비스” 값을 해당 지역의 지역 엔드포인트로 바꾸십시오. 예를 들어 중동 (바레인) (me-south-1) GuardDuty 지역에서 사용하는 경우 로 바꾸십시오. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` 각 옵트인 지역의 엔드포인트에 대한 자세한 내용은 엔드포인트 및 할당량을 참조하십시오. GuardDuty

7. 최종 성명서 앞에 정책 설명을 추가한 경우 이 설명을 추가하기 전에 쉼표를 추가하세요. KMS 키 정책의 JSON 구문이 유효한지 확인하세요.

   저장을 선택합니다.

8. (선택 사항) 이후 단계에서 사용할 수 있도록 키 ARN을 메모장에 복사합니다.

3단계 — Amazon S3 버킷에 정책 연결

이 S3 버킷에 객체를 업로드할 GuardDuty 수 있도록 결과를 내보낼 Amazon S3 버킷에 권한을 추가합니다. 사용자 계정이나 다른 AWS 계정계정에 속한 Amazon S3 버킷을 사용하는 것과 별개로 이러한 권한을 추가해야 합니다.

어느 시점에서든 다른 S3 버킷으로 결과를 내보내려는 경우, 검색 결과를 계속 내보내려면 해당 S3 버킷에 권한을 추가하고 검색 결과 내보내기 설정을 다시 구성해야 합니다.

이러한 결과를 내보낼 Amazon S3 버킷이 아직 없는 경우 Amazon S3 사용 설명서의 버킷 생성을 참조하십시오.

S3 버킷 정책에 권한을 추가하려면

1. Amazon S3 사용 설명서의 버킷 정책 생성 또는 편집하기에서 버킷 정책 편집 페이지가 나타날 때까지 아래의 단계를 수행하십시오.
2. 예제 정책은 Amazon S3 버킷으로 결과를 내보낼 GuardDuty 권한을 부여하는 방법을 보여줍니다. 내보내기 결과를 구성한 후 경로를 변경하는 경우 새 위치에 권한을 부여하도록 정책을 수정해야 합니다.

   다음 예제 정책을 복사하여 버킷 정책 편집기에 붙여넣습니다.

   최종 명령문 앞에 정책 설명을 추가한 경우 이 설명을 추가하기 전에 쉼표를 추가하세요. KMS 키 정책의 JSON 구문이 유효한지 확인하세요.

   S3 버킷 예시 정책

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
```

```
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
```

```
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. 정책 예제에서 *###* 서식이 지정된 다음 값을 대체하여 정책을 편집하십시오.

   1. *Amazon S3 ## ARN#* Amazon S3 버킷의 Amazon 리소스 이름 (ARN) 으로 교체합니다. 버킷 ARN은 https://console.aws.amazon.com/s3/ 콘솔의 버킷 정책 편집 페이지에서 찾을 수 있습니다.
   2. *123456789012#* 결과를 내보내는 계정을 소유한 AWS 계정 ID로 바꾸십시오. GuardDuty
   3. *## 2# ## ### ### ###* 바꾸십시오. AWS 리전 GuardDuty
   4. *SourceDetectorID#* 조사 결과가 `detectorID` 생성된 특정 지역의 GuardDuty 계정 이름으로 바꾸십시오.

      계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.
   5. *S3 ## ARN/ [### ###] ## ### ## [### ###]* 부분을 결과를 내보낼 선택적 폴더 위치로 바꿉니다. 접두사 사용에 대한 자세한 내용은 Amazon S3 사용 설명서의 접두사를 사용한 객체 구성을 참조하십시오.

아직 존재하지 않는 선택적 폴더 위치를 GuardDuty 제공하면 S3 버킷과 연결된 계정이 결과를 내보내는 계정과 동일한 경우에만 해당 위치가 생성됩니다. 다른 계정에 속한 S3 버킷으로 결과를 내보내는 경우 폴더 위치가 이미 있어야 합니다.

6. *KMS # ARN#* S3 버킷으로 내보낸 결과의 암호화와 관련된 KMS 키의 Amazon 리소스 이름 (ARN) 으로 대체합니다. 키 ARN을 찾으려면 개발자 안내서의 키 ID 및 ARN 찾기를 참조하십시오.AWS Key Management Service

> **Note**
>
> 옵트인 GuardDuty 지역에서 사용하는 경우 “서비스”의 값을 해당 지역의 지역 엔드포인트로 바꾸십시오. 예를 들어 중동 (바레인) (me-south-1) GuardDuty 지역에서 사용하는 경우 로 바꾸십시오. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` 각 옵트인 지역의 엔드포인트에 대한 자세한 내용은 엔드포인트 및 할당량을 참조하십시오. GuardDuty

4. 저장을 선택합니다.

4단계 - 결과를 S3 버킷으로 내보내기 (콘솔)

GuardDuty 결과를 다른 AWS 계정버킷의 기존 버킷으로 내보낼 수 있습니다.

새 S3 버킷을 만들거나 계정에서 기존 버킷을 선택할 때 선택적 접두사를 추가할 수 있습니다. 내보내기 결과를 구성할 때 S3 버킷에 결과를 저장할 새 폴더를 GuardDuty 생성합니다. 생성된 기본 폴더 구조에 접두사가 추가됩니다. GuardDuty 선택적 접두사의 형식을 예로 들 수 있습니다. `/AWSLogs/123456789012/GuardDuty/Region`

S3 객체의 전체 경로는 입니다. *DOC-EXAMPLE-BUCKET*`/`*prefix-name*`/UUID.`*jsonl.gz* UUID는 무작위로 생성되며 탐지기 ID 또는 검색 ID를 나타내지 않습니다.

> **Important**
>
> KMS 키와 S3 버킷이 동일한 리전에 있어야 합니다.

이 단계를 완료하기 전에 KMS 키와 기존 S3 버킷에 해당 정책을 연결했는지 확인하세요.

내보내기 결과를 구성하려면

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 설정 페이지의 검색 결과 내보내기 옵션에서 S3 버킷에 대해 지금 구성 (또는 필요에 따라 편집)을 선택합니다.
4. S3 버킷 ARN의 경우 를 입력합니다. **`bucket ARN`** 버킷 ARN을 찾으려면 Amazon S3 사용 설명서의 S3 버킷의 속성 보기를 참조하십시오. https://console.aws.amazon.com/guardduty/ 콘솔의 관련 버킷 속성 페이지에 있는 권한 탭에서
5. KMS 키 ARN의 경우 를 입력합니다. **`key ARN`** 키 ARN을 찾으려면 개발자 안내서의 키 ID 및 ARN 찾기를 참조하십시오.AWS Key Management Service
6. 정책 첨부

   - 단계를 수행하여 S3 버킷 정책을 연결합니다. 자세한 정보는 3단계 — Amazon S3 버킷에 정책 연결을 참조하세요.

   - KMS 키 정책을 연결하는 단계를 수행하십시오. 자세한 정보는 2단계 — KMS 키에 정책 연결을 참조하세요.
7. 저장(Save)을 선택합니다.

5단계 — 업데이트된 활성 결과를 내보내는 빈도 설정

업데이트된 활성 결과를 내보내는 빈도를 환경에 맞게 구성하십시오. 기본적으로 업데이트된 결과는 6시간마다 내보내집니다. 즉, 가장 최근 내보내기 이후에 업데이트된 모든 결과가 새 내보내기에 포함됩니다. 업데이트된 결과를 6시간마다 내보내고 내보내기가 12:00에 발생하는 경우 12:00 이후에 업데이트한 결과는 18:00에 내보냅니다.

빈도를 설정하려면

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 결과 내보내기 옵션 섹션에서 결과 업데이트 빈도를 선택합니다. 이렇게 하면 업데이트된 활성 검색 결과를 Amazon EventBridge S3와 Amazon S3로 내보내는 빈도가 설정됩니다. 사용자는 다음 중에서 선택할 수 있습니다.

   - 15분마다 EventBridge S3와 S3를 업데이트합니다.

- 1시간마다 EventBridge S3와 S3를 업데이트합니다.
- Update CWE and S3 every 6 hours (default)(6시간마다 CWE 및 S3 업데이트(기본값))

4. 변경 사항 저장를 선택합니다.

Amazon CloudWatch Events를 사용하여 GuardDuty 결과에 대한 사용자 지정 응답 생성

GuardDuty 결과가 변경되면 Amazon CloudWatch Events에 대한 이벤트를 생성합니다. CloudWatch 이벤트를 생성하는 변경 사항 검색에는 새로 생성된 결과 또는 새로 집계된 결과가 포함됩니다. 이벤트는 최선의 작업을 기반으로 발생됩니다.

모든 GuardDuty 검색 결과에는 검색 결과 ID가 할당됩니다. GuardDuty 고유한 찾기 ID를 사용하여 모든 검색 결과에 대해 CloudWatch 이벤트를 생성합니다. 기존 결과의 후속 발생은 모두 원래 결과에 집계됩니다. 자세한 설명은 GuardDuty 집계 결과 찾기 섹션을 참조하세요.

> **Note**
>
> 계정이 GuardDuty 위임된 관리자인 경우 CloudWatch 이벤트는 사용자 계정뿐만 아니라 검색 결과가 생성된 회원 계정에도 게시됩니다.

에서 CloudWatch 이벤트를 사용하면 GuardDuty GuardDuty 조사 결과로 밝혀진 보안 문제에 대응하는 데 도움이 되는 작업을 자동화할 수 있습니다.

이벤트 기반 GuardDuty 결과에 대한 알림을 받으려면 CloudWatch CloudWatch 이벤트 규칙과 대상을 만들어야 GuardDuty 합니다. 이 규칙을 사용하면 GuardDuty 생성된 결과에 대한 알림을 규칙에 지정된 대상에 CloudWatch 보낼 수 있습니다. 자세한 설명은 GuardDuty (CLI) 에 대한 CloudWatch 이벤트 규칙 및 대상 생성 섹션을 참조하세요.

주제

- CloudWatch 이벤트 알림 빈도: GuardDuty
- CloudWatch 이벤트 형식: GuardDuty
- GuardDuty 결과를 알려주는 CloudWatch 이벤트 규칙 만들기 (콘솔)
- GuardDuty (CLI) 에 대한 CloudWatch 이벤트 규칙 및 대상 생성
- CloudWatch GuardDuty 다중 계정 환경을 위한 이벤트

CloudWatch 이벤트 알림 빈도: GuardDuty

고유한 결과 ID가 있는 새로 생성된 결과 알림

GuardDuty 발견 후 5분 이내에 CloudWatch 이벤트를 기반으로 알림을 보냅니다. 이 이벤트(및 알림)는 또한 고유한 ID를 포함한 이 결과가 생성된 이후 5분마다 발생하는 이 결과의 모든 후속 발생을 포함합니다.

> **Note**
>
> 새로 생성된 결과에 대한 알림의 기본 빈도는 5분입니다. 이 빈도는 업데이트할 수 없습니다.

후속 결과 발생에 대한 알림

기본적으로 고유한 검색 결과 ID를 가진 모든 검색 결과에 대해 6시간 간격 내에 발생하는 특정 검색 결과 유형의 모든 후속 항목을 단일 이벤트로 GuardDuty 집계합니다. GuardDuty 그러면 이 이벤트를 기반으로 이러한 후속 발생에 대한 알림을 보냅니다. 기본적으로 기존 검색 결과가 이후에 발생하는 경우 CloudWatch 이벤트를 기반으로 GuardDuty 6시간마다 알림을 보냅니다.

관리자 계정 계정만 후속 이벤트 발생 발견에 대해 전송되는 알림의 기본 빈도를 사용자 지정할 수 있습니다. CloudWatch 멤버 계정의 사용자는 이 빈도 값을 사용자 지정할 수 없습니다. 관리자 계정 계정이 자체 계정에 설정한 빈도 값은 모든 구성원 계정의 GuardDuty 기능에 적용됩니다. 관리자 계정 사용자가 이 빈도 값을 1시간으로 설정하면 모든 구성원 계정에서 1시간 간격으로 다음 검색 결과 발생 빈도에 대한 알림을 받게 됩니다. 자세한 설명은 Amazon에서 여러 계정 관리 GuardDuty 섹션을 참조하세요.

> **Note**
>
> 관리자 계정은 후속 검색 결과 발생에 대한 기본 알림 빈도를 사용자 지정할 수 있습니다. 가능한 값은 15분, 1시간 또는 기본값 6시간입니다. 이러한 알림의 빈도 설정에 대한 자세한 내용은 5단계 — 업데이트된 활성 결과를 내보내는 빈도 설정 섹션을 참조하세요.

이벤트를 사용하여 보관된 결과를 GuardDuty 모니터링합니다. CloudWatch

수동으로 보관된 검색 결과의 경우 이러한 검색 결과의 초기 및 이후에 발생하는 모든 결과 (보관이 완료된 후 생성됨) 는 위에서 설명한 빈도에 따라 CloudWatch 이벤트로 전송됩니다.

자동 보관된 검색 결과의 경우 이러한 검색 결과가 처음 발생하거나 이후에 발생하는 모든 결과 (보관이 완료된 후 생성됨) 는 Events로 전송되지 않습니다. CloudWatch

CloudWatch 이벤트 형식: GuardDuty

의 CloudWatch 이벤트 GuardDuty 형식은 다음과 같습니다.

```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

> **Note**
>
> 세부 정보 값은 단일 결과에 대한 JSON 세부 정보를 객체로 반환하지만, 배열 내에서 여러 결과를 지원할 수 있는 "결과" 값을 반환합니다.

GUARDDUTY_FINDING_JSON_OBJECT에 포함된 모든 파라미터의 전체 목록은 GetFindings 단원을 참조하십시오. GUARDDUTY_FINDING_JSON_OBJECT에 보이는id 파라미터가 이전에 설명한 결과 ID입니다.

GuardDuty 결과를 알려주는 CloudWatch 이벤트 규칙 만들기 (콘솔)

Events with GuardDuty 를 사용하면 찾기 CloudWatch 이벤트를 메시징 허브로 전송하여 GuardDuty 검색 GuardDuty 결과의 가시성을 높이는 데 도움이 되도록 자동 찾기 알림을 설정할 수 있습니다. 이 주제에서는 SNS 주제를 설정한 다음 해당 주제를 Events 이벤트 규칙에 연결하여 결과 알림을 이메일, Slack 또는 Amazon Chime으로 CloudWatch 보내는 방법을 보여줍니다.

Amazon SNS 주제 및 엔드포인트 설정

시작하려면 먼저 Amazon Simple Notification Service에서 주제를 설정하고 엔드포인트를 추가해야 합니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 시작하기를 참조하세요.

이 절차를 통해 검색 결과 데이터를 전송할 GuardDuty 위치를 설정합니다. 이벤트 규칙 생성 중 또는 생성 후에 CloudWatch 이벤트 이벤트 규칙에 SNS 주제를 추가할 수 있습니다.

Email setup

SNS 주제 생성

1. Amazon SNS 콘솔(https://console.aws.amazon.com/sns/v3/home)에 로그인합니다.
2. 탐색 창에서 주제를 선택한 다음 주제 생성을 선택합니다.
3. 주제 생성 섹션에서 표준을 선택합니다. 다음으로 주제 이름을 입력합니다(예: **`GuardDuty_to_Email`**). 기타 세부 정보는 선택 사항입니다.
4. 주제 생성을 선택합니다. 새로운 주제에 대한 주제 세부 정보가 열립니다.
5. 구독 섹션에서 구독 생성을 선택합니다.
6. a. 프로토콜 메뉴에서 이메일을 선택합니다.
   b. 엔드포인트 필드에서 알림을 받을 이메일 주소를 추가합니다.

   > **Note**
   > 구독을 생성한 후 이메일 클라이언트를 통해 구독을 확인해야 합니다.

   c. 구독 생성을 선택합니다.
7. 받은 편지함에서 구독 메시지를 확인하고 구독 확인을 선택합니다.

Slack setup

SNS 주제 생성

1. Amazon SNS 콘솔(https://console.aws.amazon.com/sns/v3/home)에 로그인합니다.
2. 탐색 창에서 주제를 선택한 다음 주제 생성을 선택합니다.
3. 주제 생성 섹션에서 표준을 선택합니다. 다음으로 주제 이름을 입력합니다(예: **`GuardDuty_to_Slack`**). 기타 세부 정보는 선택 사항입니다. 주제 생성을 선택하여 마무리합니다.

AWS Chatbot 클라이언트 구성

1. AWS Chatbot 콘솔로 이동
2. 구성된 클라이언트 패널에서 새 클라이언트 구성을 선택합니다.
3. Slack을 선택하고 '구성'을 선택하여 확인합니다.

> **Note**
>
> Slack을 선택할 때는 '허용'을 선택하여 AWS Chatbot의 채널 액세스 권한을 확인해야 합니다.

4. 새 채널 구성을 선택하여 구성 세부 정보 창을 엽니다.
   a. 채널 이름을 입력합니다.
   b. Slack 채널의 경우 사용할 채널을 선택합니다. AWS Chatbot에서 프라이빗 Slack 채널을 사용하려면 프라이빗 채널을 선택합니다.
   c. Slack에서 채널 이름을 마우스 오른쪽 버튼으로 클릭하고 링크 복사를 선택하여 프라이빗 채널의 채널 ID를 복사합니다.
   d. AWS 관리 콘솔의 AWS Chatbot 창에서 Slack에서 복사한 ID를 프라이빗 채널 ID 필드에 붙여넣습니다.
   e. 권한에서 아직 역할이 없는 경우 템플릿을 사용하여 IAM 역할을 생성하도록 선택합니다.
   f. 정책 템플릿에서 Notification permissions를 선택합니다. 이는 AWS Chatbot에 대한 IAM 정책 템플릿입니다. CloudWatch 경보, 이벤트, 로그, Amazon SNS 주제에 필요한 읽기 및 목록 권한을 제공합니다.
   g. 이전에 SNS 주제를 만든 리전을 선택한 다음 생성한 Amazon SNS 주제를 선택하여 Slack 채널에 알림을 전송합니다.
5. 구성을 선택합니다.

Chime setup

SNS 주제 생성

1. Amazon SNS 콘솔(https://console.aws.amazon.com/sns/v3/home)에 로그인합니다.
2. 탐색 창에서 주제를 선택한 다음 주제 생성을 선택합니다.

3. 주제 생성 섹션에서 표준을 선택합니다. 다음으로 주제 이름을 입력합니다(예: **`GuardDuty_to_Chime`**). 기타 세부 정보는 선택 사항입니다. 주제 생성을 선택하여 마무리합니다.

AWS Chatbot 클라이언트 구성

1. AWS Chatbot 콘솔로 이동
2. 구성된 클라이언트 패널에서 새 클라이언트 구성을 선택합니다.
3. Chime을 선택하고 '구성'을 선택하여 확인합니다.
4. 구성 세부 정보 창에서 채널 이름을 입력합니다.
5. Chime에서 원하는 채팅룸을 엽니다.
   a. 오른쪽 상단 모서리에 있는 기어 모양 아이콘을 선택하고 Manage webhooks(Webhook 관리)를 선택합니다.
   b. URL 복사를 선택하여 웹후크 URL을 클립보드에 복사합니다.
6. AWS 관리 콘솔의 AWS Chatbot 창에서 웹후크 URL 필드에 복사한 URL을 붙여넣습니다.
7. 권한에서 아직 역할이 없는 경우 템플릿을 사용하여 IAM 역할을 생성하도록 선택합니다.
8. 정책 템플릿에서 Notification permissions를 선택합니다. 이는 AWS Chatbot에 대한 IAM 정책 템플릿입니다. CloudWatch 경보, 이벤트, 로그, Amazon SNS 주제에 필요한 읽기 및 목록 권한을 제공합니다.
9. 이전에 SNS 주제를 만든 리전을 선택한 다음 생성한 Amazon SNS 주제를 선택하여 Chime 룸에 알림을 전송합니다.
10. 구성을 선택합니다.

결과를 위한 CloudWatch GuardDuty 이벤트 설정

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택한 다음 규칙 생성을 선택합니다.
3. 서비스 이름 메뉴에서 선택합니다 GuardDuty.
4. [이벤트 유형] 메뉴에서 [GuardDuty찾기] 를 선택합니다.
5. 이벤트 패턴 미리 보기에서 편집을 선택합니다.
6. 아래 JSON 코드를 이벤트 패턴 미리보기에 붙여넣고 저장을 선택합니다.

```
{
```

```
"source": [
  "aws.guardduty"
],
"detail-type": [
  "GuardDuty Finding"
],
"detail": {
  "severity": [
    4,
    4.0,
    4.1,
    4.2,
    4.3,
    4.4,
    4.5,
    4.6,
    4.7,
    4.8,
    4.9,
    5,
    5.0,
    5.1,
    5.2,
    5.3,
    5.4,
    5.5,
    5.6,
    5.7,
    5.8,
    5.9,
    6,
    6.0,
    6.1,
    6.2,
    6.3,
    6.4,
    6.5,
    6.6,
    6.7,
    6.8,
    6.9,
    7,
    7.0,
    7.1,
```

```
        7.2,
        7.3,
        7.4,
        7.5,
        7.6,
        7.7,
        7.8,
        7.9,
        8,
        8.0,
        8.1,
        8.2,
        8.3,
        8.4,
        8.5,
        8.6,
        8.7,
        8.8,
        8.9
      ]
    }
}
```

> **Note**
>
> 위의 코드는 중간에서 높음에 이르는 결과에 대해 알립니다.

7. 대상 섹션에서 대상 추가를 클릭합니다.
8. 대상 선택 메뉴에서 SNS 주제를 선택합니다.
9. 주제 선택에서 1단계에서 생성한 SNS 주제의 이름을 선택합니다.
10. 이벤트에 대한 입력을 구성합니다.

    - Chime 또는 Slack에 대한 알림을 설정하고 11단계로 건너뛴 경우 입력 유형의 기본값은 일치하는 이벤트로 설정됩니다.
    - SNS를 통한 이메일 알림을 설정하는 경우 아래 단계에 따라 받은 편지함으로 전송되는 메시지를 사용자 지정합니다.

    a. 입력 구성을 확장한 후 입력 변환기를 선택합니다.

    b. 다음 코드를 복사하여 입력 경로 필드에 붙여넣습니다.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

c. 다음 코드를 복사하고 입력 템플릿 필드에 붙여넣어 이메일의 형식을 지정합니다.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. 세부 정보 구성을 클릭합니다.
12. 규칙 세부 정보 구성 페이지에서 해당 규칙의 이름과 설명을 입력한 후 규칙 생성을 선택합니다.

GuardDuty (CLI) 에 대한 CloudWatch 이벤트 규칙 및 대상 생성

다음 절차는 AWS CLI 명령을 사용하여 CloudWatch 이벤트 규칙 및 대상을 만드는 방법을 보여줍니다. GuardDuty 특히, 이 프로시저는 함수를 GuardDuty 생성하는 모든 검색 결과에 대해 이벤트를 전송하고 규칙을 위한 대상으로 AWS Lambda 함수를 추가할 수 있는 규칙을 만드는 방법을 보여줍니다. CloudWatch

> **Note**
>
> Lambda 함수 외에도 Amazon EC2 인스턴스 GuardDuty , CloudWatch Amazon Kinesis 스트림, Amazon AWS Step Functions ECS 작업, 상태 run 머신, 명령, 내장 대상 등의 대상 유형을 지원합니다.

이벤트 콘솔을 통해 CloudWatch 이벤트 규칙 및 대상을 생성할 수도 있습니다. GuardDuty CloudWatch 자세한 내용과 자세한 단계는 이벤트를 트리거하는 CloudWatch 이벤트 규칙 만들기를 참조하십시오. 이벤트 소스 섹션에서 서비스 이름은 **GuardDuty**, 이벤트 유형은 **GuardDuty Finding**을 선택합니다.

규칙 및 대상을 만들려면

1. 생성되는 모든 검색 결과에 대해 이벤트를 전송할 수 CloudWatch 있는 규칙을 GuardDuty 생성하려면 다음 CloudWatch CLI 명령을 실행합니다.

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > 생성된 검색 결과의 하위 집합에 대해서만 이벤트를 CloudWatch 전송하도록 지시하도록 규칙을 추가로 사용자 지정할 수 있습니다. GuardDuty 이 하위 집합은 규칙에서 지정되는 결과 속성 또는 속성을 기반으로 합니다. 예를 들어, 다음 CLI 명령을 사용하여 심각도가 5 또는 8인 GuardDuty 검색 결과에 대한 이벤트만 전송할 수 있는 규칙을 생성합니다.
   > CloudWatch
   > ```
   > AWS events put-rule --name Test --event-pattern "{\"source\":
   > [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],
   > \"detail\":{\"severity\":[5,8]}}"
   > ```
   > 이를 위해 JSON에 있는 모든 속성 값을 검색 결과에 사용할 수 있습니다. GuardDuty

2. Lambda 함수를 1단계에서 생성한 규칙의 대상으로 연결하려면 다음 CloudWatch CLI 명령을 실행합니다.

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > <your_function>위 명령을 이벤트의 실제 Lambda 함수로 바꿔야 합니다. GuardDuty

3. 대상을 간접적으로 호출하는 데 필요한 권한을 추가하려면 다음 Lambda CLI 명령을 실행합니다.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

> **Note**
>
> <your_function>위 명령을 이벤트의 실제 Lambda 함수로 바꿔야 합니다. GuardDuty

> **Note**
>
> 위 절차에서는 Lambda 함수를 이벤트를 트리거하는 규칙의 대상으로 사용하고 있습니다. CloudWatch 다른 AWS 리소스를 이벤트를 트리거하는 대상으로 구성할 수도 있습니다. CloudWatch 자세한 설명은 PutTargets 섹션을 참조하세요.

CloudWatch GuardDuty 다중 계정 환경을 위한 이벤트

GuardDuty 관리자의 경우 계정 내 CloudWatch 이벤트 규칙은 회원 계정에서 발생한 해당 결과에 따라 트리거됩니다. 즉, 이전 섹션에 설명된 대로 관리자 계정의 CloudWatch 이벤트를 통해 검색 결과 알림을 설정하면 사용자 계정 외에도 회원 계정에서 생성되는 심각도가 높거나 중간 정도인 결과에 대한 알림을 받게 됩니다.

검색 결과의 JSON 세부 정보 `accountId` 필드를 사용하여 GuardDuty 검색 결과가 나온 회원 계정을 식별할 수 있습니다.

콘솔에서 환경의 특정 멤버 계정에 대한 사용자 지정 이벤트 규칙을 작성하려면 새 규칙을 생성하고 다음 템플릿을 이벤트 패턴 미리 보기에 붙여넣고 이벤트를 트리거하려는 멤버 계정의 계정 ID를 추가합니다.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> 이 예시에서는 나열된 계정 ID의 모든 결과에 대해 트리거됩니다. JSON 구문에 따라 여러 ID를 쉼표로 구분하여 추가할 수 있습니다.

멀웨어 보호 검사 중 리소스를 건너뛰는 이유와 CloudWatch 로그 이해

GuardDuty 멀웨어 보호는 Amazon CloudWatch 로그 그룹 malware-scan-events/aws/guardduty/에 이벤트를 게시합니다. 맬웨어 스캔과 관련된 각 이벤트에 대해 영향을 받는 리소스의 상태 및 스캔 결과를 모니터링할 수 있습니다. 맬웨어 보호 스캔 중에 특정 Amazon EC2 리소스 및 Amazon EBS 볼륨을 건너뛰었을 수 있습니다.

멀웨어 CloudWatch 보호의 감사 로그 GuardDuty

malware-scan-events CloudWatch /aws/guardduty/ 로그 그룹에서는 세 가지 유형의 스캔 이벤트가 지원됩니다.

맬웨어 보호 스캔 이벤트 이름	설명
`EC2_SCAN_STARTED`	GuardDuty 멀웨어 보호가 악성코드 검사 프로세스 (예: EBS 볼륨의 스냅샷 생성 준비) 를 시작할 때 생성됩니다.
`EC2_SCAN_COMPLETED`	영향을 받는 리소스의 EBS 볼륨 중 하나 이상에 대한 GuardDuty 멀웨어 보호 검사가 완료될 때 생성됩니다. 이 이벤트에는 스캔한 EBS 볼륨에 속하는 `snapshotId` 도 포함됩니다. 스캔 완료 후에는 스캔 결과가 `CLEAN`, `THREATS_FOUND` 또는 `NOT_SCANNED` 입니다.
`EC2_SCAN_SKIPPED`	GuardDuty 멀웨어 방지 스캔이 영향을 받는 리소스의 모든 EBS 볼륨을 건너뛸 때 생성됩니다. 건너뛴 이유를 식별하려면 해당 이벤트를 선택하고 세부 정보를 확인합니다. 건너뛴 이유에 대

맬웨어 보호 스캔 이벤트 이름	설명
	한 자세한 내용은 아래의 맬웨어 스캔 중에 리소스를 건너뛴 이유 섹션을 참조하세요.

> **Note**
>
> 를 사용하는 경우 AWS Organizations Organizations의 멤버 계정의 CloudWatch 로그 이벤트가 관리자 계정과 멤버 계정의 로그 그룹 모두에 게시됩니다.

원하는 액세스 방법을 선택하여 CloudWatch 이벤트를 보고 쿼리하세요.

Console

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 왼쪽 탐색 창의 [로그(Logs)]에서 [로그 그룹(Log groups)]을 선택합니다. /aws/guardduty/malware-scan-events log 그룹을 선택하여 멀웨어 방지에 대한 검사 이벤트를 확인하십시오. GuardDuty

   쿼리를 실행하려면 Log Insights를 선택합니다.

   쿼리 실행에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 CloudWatch Logs Insights를 사용한 로그 데이터 분석을 참조하십시오.
3. 스캔 ID를 선택하여 영향을 받는 리소스 및 맬웨어 결과의 세부 정보를 모니터링합니다. 예를 들어, 다음 쿼리를 실행하여 를 사용하여 CloudWatch 로그 이벤트를 필터링할 수 `scanId` 있습니다. 유효한 *`scan-id`*를 사용해야 합니다.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- 로그 그룹을 사용하려면 Amazon 사용 CloudWatch 설명서의 AWS CLI를 사용하여 로그 항목 검색을 참조하십시오.

멀웨어 방지에 대한 스캔 이벤트를 보려면 /aws/guardduty/ malware-scan-events 로그 그룹을 선택하십시오. GuardDuty

- 로그 이벤트를 보고 필터링하려면 Amazon CloudWatch API 참조의 GetLogEvents 및 FilterLogEvents를 각각 참조하십시오.

GuardDuty 멀웨어 보호 로그 보존

/aws/guardduty/ 로그 그룹의 기본 로그 보존 기간은 90일이며, 이 기간이 지나면 malware-scan-events 로그 이벤트가 자동으로 삭제됩니다. 로그 그룹의 로그 보존 정책을 변경하려면 로그 또는 로그에서 CloudWatch 로그 데이터 보존 변경을 참조하십시오. CloudWatch PutRetentionPolicy

맬웨어 스캔 중에 리소스를 건너뛴 이유

맬웨어 스캔과 관련된 이벤트에서 특정 EC2 리소스 및 EBS 볼륨이 검사 프로세스 중에 건너뛰기되었을 수 있습니다. 다음 표에는 GuardDuty 멀웨어 보호가 리소스를 스캔하지 못할 수 있는 이유가 나와 있습니다. 해당하는 경우 제안된 단계를 사용하여 이러한 문제를 해결하고 다음에 Malware Protection에서 GuardDuty 맬웨어 검사를 시작할 때 해당 리소스를 검사하십시오. 다른 문제는 이벤트 진행 상황을 알려주는 데 사용되며 조치를 취할 수 없습니다.

건너뛰는 이유	설명	제안 단계	
`RESOURCE_NOT_FOUND`	온디맨드 맬웨어 검사를 시작하기 위해 `resourceArn` 제공된 내용을 사용자 환경에서 찾을 수 없습니다. AWS	Amazon EC2 인스턴스 또는 컨테이너 워크로드의 `resourceArn` 을 검증하고 다시 시도합니다.	
`ACCOUNT_INELIGIBLE`	온디맨드 멀웨어 검사를 시작하려고 시도한 AWS 계정 ID가 활성화되지 않았습니다. GuardDuty	이 AWS 계정에 GuardDuty 활성화되어 있는지 확인하세요. 새 AWS 리전 계정을 GuardDuty 활성화하면 동기화하는 데 최대	

건너뛰는 이유	설명	제안 단계	
		20분이 걸릴 수 있습니다.	
UNSUPPORTED_KEY_ENCRYPTION	GuardDuty 멀웨어 보호는 암호화되지 않은 볼륨과 고객 관리 키로 암호화된 볼륨을 모두 지원합니다. Amazon EBS 암호화를 사용하여 암호화된 EBS 볼륨의 스캔은 지원하지 않습니다. 현재 이러한 건너뛰기 사유가 적용되지 않는 지역적 차이가 있습니다. 이에 대한 자세한 내용은 AWS 리전을 참조하십시오. 리전별 기능 가용성	암호화 키를 고객 관리 키로 교체하세요. GuardDuty 지원되는 암호화 유형에 대한 자세한 내용은 을 참조하십시오멀웨어 스캔을 지원하는 Amazon EBS 볼륨.	

건너뛰는 이유	설명	제안 단계	
EXCLUDED_BY_SCAN_SETTINGS	EC2 인스턴스 또는 EBS 볼륨이 맬웨어 스캔 도중 제외되었습니다. 태그가 포함 목록에 추가되었지만 리소스가 이 태그와 연결되지 않았거나, 태그가 제외 목록에 추가되었고 리소스가 이 태그와 연결되어 있거나, GuardDuty Excluded 태그가 이 리소스에 대해 true로 설정되었을 가능성이 있습니다.	스캔 옵션이나 Amazon EC2 리소스에 연결된 태그를 업데이트하세요. 자세한 정보는 사용자 정의 태그를 사용하는 스캔 옵션을 참조하세요.	
UNSUPPORTED_VOLUME_SIZE	볼륨이 2048GB를 초과합니다.	실행 불가.	
NO_VOLUMES_ATTACHED	GuardDuty Malware Protection이 사용자 계정에서 인스턴스를 찾았지만 스캔을 진행하기 위한 EBS 볼륨이 이 인스턴스에 연결되어 있지 않았습니다.	실행 불가.	
UNABLE_TO_SCAN	내부 서비스 오류입니다.	실행 불가.	

건너뛰는 이유	설명	제안 단계	
SNAPSHOT_NOT_FOUND	EBS 볼륨에서 생성되어 서비스 계정과 공유된 스냅샷을 찾을 수 없었고 GuardDuty Malware Protection에서 검사를 진행할 수 없었습니다.	스냅샷이 의도적으로 제거되지 않았는지 확인하십시오 CloudTrail .	
SNAPSHOT_QUOTA_REACHED	각 리전의 스냅샷에 허용되는 최대 볼륨에 도달했습니다. 이로 인해 스냅샷 보존뿐 아니라 새 스냅샷 생성도 불가능합니다.	기존 스냅샷을 제거하거나 할당량 증가를 요청할 수 있습니다. 리전별 스냅샷의 기본 한도와 할당량 증가를 요청하는 방법은AWS 일반 참조 가이드의 Service quotas에서 찾아볼 수 있습니다.	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	11개 이상의 EBS 볼륨이 EC2 인스턴스에 연결되었습니다. GuardDuty 멀웨어 보호 기능은 알파벳순으로 정렬하여 처음 11개의 EBS 볼륨을 스캔했습니다. deviceName	실행 불가.	

건너뛰는 이유	설명	제안 단계	
UNSUPPORTED_PRODUCT_CODE_TYPE	GuardDuty as가 포함된 인스턴스의 스캔은 지원하지 않습니다. `productCode` `marketplace` 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 유료 AMI를 참조하세요. `productCode` 에 대한 자세한 내용은 Amazon EC2 API 참조의 ProductCode 섹션을 참조하세요.	실행 불가.	

GuardDuty 맬웨어 보호에서 오탐지 보고

GuardDuty 맬웨어 보호는 Amazon EC2 인스턴스 또는 컨테이너 워크로드에서 무해한 파일을 악성이거나 유해한 것으로 식별할 수 있습니다. 맬웨어 보호 및 GuardDuty 서비스 경험을 개선하기 위해 스캔 중에 악성 또는 유해한 것으로 식별된 파일에 실제로 맬웨어가 포함되어 있지 않다고 생각되는 경우 오탐지 결과를 보고할 수 있습니다.

오탐지 파일 제출

1. https://console.aws.amazon.com/guardduty/ 콘솔에 로그인합니다.
2. 오탐지 결과인 것으로 파악되면 AWS Support에 문의하여 오탐지 파일 제출 과정을 시작합니다.
3. 맬웨어 스캔을 선택합니다.
4. 스캔을 선택하여 결과 ID를 봅니다.
5. 결과 ID를 제공합니다. 파일의 SHA-256 해시도 제공해야 합니다. 이는 GuardDuty 맬웨어 보호에서 올바른 파일을 수신했는지 확인하는 데 필요합니다.
6. AWS Support 팀에서 파일 및 SHA-256 해시를 업로드하는 데 사용할 수 있는 Amazon Simple Storage Service(S3) URL을 제공합니다. 파일을 업로드한 후 AWS Support 팀에 알립니다.

> **Warning**
>
> 파일이나 SHA-256 해시를 AWS Support에 직접 제공하지 마세요. 제공된 URL을 통해 Amazon S3에 파일과 해시를 업로드해야만 합니다. URL 수신 후 7일 이내에 파일 및 해시를 업로드하지 않으면 URL은 무효화됩니다. URL이 무효화되면 AWS Support에 문의하여 새 URL을 받아야 합니다.

GuardDuty는 30일을 초과하여 파일을 보관하지 않습니다. GuardDuty 팀 멤버은 제출된 사항을 분석하고 적절한 조치를 취하여 맬웨어 보호 및 GuardDuty 서비스 경험을 개선합니다.

에서 발견한 보안 문제 해결 GuardDuty

Amazon은 잠재적 보안 문제를 나타내는 결과를 GuardDuty 생성합니다. 이번 릴리스의 GuardDuty 잠재적 보안 문제는 EC2 인스턴스 또는 컨테이너 워크로드가 손상되었거나 사용자 환경의 자격 증명 세트가 손상되었음을 나타냅니다. AWS 다음 섹션에서는 이러한 시나리오에 대한 권장 해결 단계를 설명합니다. 다른 수정 시나리오가 있는 경우 해당 특정 결과 유형에 대한 항목에서 시나리오가 설명됩니다. 활성 결과 유형 표에서 선택하여 결과 유형에 대한 전체 정보에 액세스할 수 있습니다.

내용

잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결

다음 권장 단계에 따라 사용자 환경에서 잠재적으로 손상된 EC2 인스턴스를 수정하십시오. AWS

1. 잠재적으로 손상된 Amazon EC2 인스턴스를 식별합니다.

   잠재적으로 손상된 인스턴스에 맬웨어가 있는지 조사하고, 맬웨어가 발견되면 모두 제거합니다. 온디맨드 맬웨어 스캔 사용을 통해 잠재적으로 손상된 EC2 인스턴스에서 맬웨어를 식별하거나, AWS Marketplace에서 맬웨어를 식별 및 제거하는 데 유용한 파트너 제품이 있는지 확인할 수 있습니다.
2. 잠재적으로 손상된 Amazon EC2 인스턴스를 격리합니다.

   가능하면 다음 단계를 사용하여 잠재적으로 손상된 인스턴스를 격리하십시오.

   1. 전용 격리 보안 그룹을 만드세요.
   2. 아웃바운드 규칙의 모든 트래픽에 `0.0.0.0/0 (0-65535)` 대한 단일 규칙을 생성합니다.

이 규칙이 적용되면 기존 (및 신규) 아웃바운드 트래픽을 모두 추적되지 않은 트래픽으로 전환하여 설정된 모든 아웃바운드 세션을 차단합니다. 자세한 내용은 추적되지 않은 연결을 참조하십시오.

3. 잠재적으로 손상된 인스턴스에서 현재 보안 그룹 연결을 모두 제거합니다.
4. 격리 보안 그룹을 이 인스턴스에 연결합니다.

   연결한 후에는 격리 보안 그룹의 아웃바운드 규칙에서 모든 트래픽에 `0.0.0.0/0` (`0-65535`) 대한 규칙을 삭제하십시오.

3. 의심스러운 활동의 출처 식별

   맬웨어가 탐지되면 계정의 결과 유형에 따라 EC2 인스턴스에서 잠재적으로 승인되지 않은 활동을 식별하고 중지합니다. 이를 위해 열려 있는 포트를 닫고, 액세스 정책을 변경하고, 취약성을 수정하기 위해 애플리케이션을 업그레이드하는 등의 조치가 필요할 수 있습니다.

   잠재적으로 손상된 EC2 인스턴스의 무단 활동을 식별하여 중지할 수 없는 경우 손상된 EC2 인스턴스를 종료하고 필요에 따라 새 인스턴스로 교체하는 것이 좋습니다. 다음은 EC2 인스턴스의 보안 유지를 위한 추가 리소스입니다.

   - Amazon EC2 모범 사례의 보안 및 네트워크 섹션
   - Linux 인스턴스용 Amazon EC2 Amazon 보안 그룹과 Windows 인스턴스용 Amazon EC2 보안 그룹
   - Amazon EC2의 보안
   - EC2 인스턴스의 보안을 유지하기 위한 팁(Linux)
   - AWS 보안 모범 사례
   - 다음과 같은 인프라 도메인 인시던트 AWS

4. 찾아보기 AWS re:Post

   추가 AWS re:Post지원이 필요하면 찾아보십시오.

5. 기술 지원 요청 제출

   Premium Support 패키지를 구독하는 경우 기술 지원 요청을 제출할 수 있습니다.

잠재적으로 손상된 S3 버킷 수정

다음 권장 단계에 따라 사용자 환경에서 잠재적으로 손상된 Amazon S3 버킷을 수정하십시오. AWS

1. 잠재적으로 손상된 S3 리소스를 식별하십시오.

   S3에 대한 GuardDuty 검색 결과에는 관련 S3 버킷, Amazon 리소스 이름 (ARN) 및 해당 소유자가 검색 결과 세부 정보에 나열됩니다.

2. 의심스러운 활동과 사용된 API 직접 호출의 소스를 식별합니다.

   사용된 API 호출은 결과 세부 정보에 API로 나열됩니다. 소스는 IAM 보안 주체(IAM 역할, 사용자 또는 계정)이며 식별 세부 정보는 결과에 나열됩니다. 소스 유형에 따라 원격 IP 주소 또는 소스 도메인 정보가 제공되며 소스가 승인되었는지 여부를 평가하는 데 도움이 될 수 있습니다. 검색 결과에 Amazon EC2 인스턴스의 자격 증명이 포함된 경우 해당 리소스에 대한 세부 정보도 포함됩니다.

3. 직접 호출 소스가 식별된 리소스에 액세스할 권한이 있는지 확인합니다.

   예를 들어 다음을 고려합니다.

   - IAM 사용자가 관여했다면 자격 증명이 잠재적으로 손상되었을 가능성이 있습니까? 자세한 정보는 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS을 참조하세요.
   - 이전에 이러한 유형의 API를 간접적으로 호출한 기록이 없는 보안 주체가 API를 간접적으로 호출한 경우 이 소스에 이 작업에 대한 액세스 권한이 필요합니까? 버킷 권한이 추가로 제한될 수 있나요?
   - 사용자 유형이 AWSAccount인 사용자 이름 ANONYMOUS_PRINCIPAL의 액세스가 확인된 경우 이는 버킷이 퍼블릭 상태이고 액세스되었음을 나타냅니다. 이 버킷이 퍼블릭 상태여야 하나요? 그렇지 않은 경우 아래 보안 권장 사항에서 S3 리소스 공유를 위한 대체 솔루션을 검토하세요.
   - 사용자 유형이 AWSAccount인 사용자 이름 ANONYMOUS_PRINCIPAL로부터의 성공적인 PreflightRequest 직접 호출을 통해 액세스가 이루어졌다면 이는 버킷에 교차 오리진 리소스 공유(CORS) 정책이 설정되어 있음을 나타냅니다. 이 버킷에 CORS 정책이 있어야 합니까? 그렇지 않은 경우 버킷이 실수로 인해 퍼블릭 상태가 되지 않도록 하고 아래 보안 권장 사항에서 S3 리소스 공유를 위한 대체 솔루션을 검토하세요. CORS에 대한 자세한 내용은 S3 사용 설명서의 교차 오리진 리소스 공유(CORS) 사용을 참조하세요.

4. S3 버킷에 민감한 데이터가 포함되어 있는지 확인합니다.

   Amazon Macie를 사용하여 S3 버킷에 개인 식별 정보(PII), 금융 데이터 또는 보안 인증 정보와 같은 민감한 데이터가 포함되어 있는지 확인합니다. Macie 계정에서 민감한 데이터 자동 검색이 활성화된 경우 S3 버킷의 세부 정보를 검토하여 S3 버킷의 콘텐츠에 관한 내용을 자세히 살펴보세요. Macie 계정에서 이 기능이 비활성화된 경우 평가를 신속하게 진행하기 위해 이 기능을 켜는 것이 좋습니다. 아니면 민감한 데이터 검색 작업을 생성하고 실행하여 S3 버킷의 객체에서 민감한 데이터를 검사할 수 있습니다. 자세한 내용은 Discovering sensitive data with Macie를 참조하세요.

액세스가 승인되었다면 결과를 무시할 수 있습니다. https://console.aws.amazon.com/guardduty/ 콘솔에서 더 이상 표시되지 않도록 개별 결과를 완전히 차단하는 규칙을 설정할 수 있습니다. 자세한 정보는 억제 규칙을 참조하세요.

S3 데이터가 무단으로 노출되거나 액세스된 것으로 확인되면 다음 S3 보안 권장 사항을 검토하여 권한을 강화하고 액세스를 제한하십시오. 적절한 해결 솔루션은 특정 환경의 요구 사항에 따라 달라집니다.

특정 S3 버킷 액세스 요구 사항에 기반한 권장 사항

다음 목록은 특정 Amazon S3 버킷 액세스 요구 사항에 따른 권장 사항을 제공합니다.

- S3 데이터 사용에 대한 퍼블릭 액세스를 제한하는 중앙 집중식 방법을 위해 S3는 퍼블릭 액세스를 차단합니다. 액세스 세분성을 제어하는 4가지 설정을 통해 액세스 포인트, 버킷 및 AWS 계정에 대한 퍼블릭 액세스 차단 설정을 활성화할 수 있습니다. 자세한 내용은 S3 퍼블릭 액세스 차단 설정을 참조하세요.
- AWS 액세스 정책을 사용하여 IAM 사용자가 리소스에 액세스하는 방법이나 버킷에 액세스하는 방법을 제어할 수 있습니다. 자세한 내용은 버킷 정책 및 사용자 정책 사용을 참조하세요.

  또한 S3 버킷 정책에 Virtual Private Cloud(VPC) 엔드포인트를 사용하여 특정 VPC 엔드포인트에 대한 액세스를 제한할 수 있습니다. 자세한 내용은 Amazon S3의 VPC 엔드포인트에 대한 버킷 정책 예시를 참조하세요.
- 계정 외부의 신뢰할 수 있는 엔터티에 대한 S3 객체 액세스를 일시적으로 허용하려면 S3를 통해 미리 서명된 URL을 생성하면 됩니다. 이 액세스는 계정 보안 인증 정보를 사용하여 생성되고 사용되는 보안 인증 정보에 따라 6시간에서 7일까지 지속될 수 있습니다. 자세한 내용은 S3를 사용하여 미리 서명된 URL 생성을 참조하세요.
- 서로 다른 소스 간에 S3 객체를 공유해야 하는 사용 사례의 경우 S3 액세스 포인트를 사용하여 프라이빗 네트워크 내에 있는 사용자에게만 액세스를 제한하는 권한 세트를 생성할 수 있습니다. 자세한 내용은 Amazon S3 액세스 포인트를 사용한 데이터 액세스 관리를 참조하세요.
- 액세스 제어 목록 (ACL) 을 사용하여 S3 리소스에 대한 액세스 권한을 다른 AWS 계정에 안전하게 부여할 수 있습니다. 자세한 내용은 ACL을 통한 S3 액세스 관리를 참조하십시오.

S3 보안 옵션에 대한 자세한 내용은 S3 보안 모범 사례를 참조하십시오.

잠재적으로 손상된 ECS 클러스터의 문제 해결

다음 권장 단계에 따라 사용자 환경에서 잠재적으로 손상된 Amazon ECS 클러스터를 수정하십시오. AWS

1. 잠재적으로 손상된 ECS 클러스터를 식별하십시오.

   ECS의 GuardDuty 멀웨어 보호 검색 결과는 검색 결과의 세부 정보 패널에 ECS 클러스터 세부 정보를 제공합니다.

2. 맬웨어의 소스 평가

   탐지된 맬웨어가 컨테이너 이미지에 있었는지 평가합니다. 이미지에 맬웨어가 있었다면 이 이미지를 사용하여 실행하는 다른 모든 작업을 식별합니다. 작업 실행에 대한 자세한 내용은 을 참조하십시오. ListTasks

3. 영향을 받을 수 있는 작업을 분리하세요.

   작업에 대한 모든 수신 및 송신 트래픽을 거부하여 영향을 받는 작업을 격리합니다. 모든 트래픽 거부 규칙은 작업에 대한 모든 연결을 끊어 이미 진행 중인 공격을 중지하는 데 도움이 될 수 있습니다.

액세스가 승인되었다면 결과를 무시할 수 있습니다. https://console.aws.amazon.com/guardduty/ 콘솔에서 더 이상 표시되지 않도록 개별 결과를 완전히 차단하는 규칙을 설정할 수 있습니다. 자세한 정보는 억제 규칙을 참조하세요.

잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS

사용자 환경에서 잠재적으로 손상되었을 수 있는 자격 증명을 수정하려면 다음 권장 단계를 따르십시오. AWS

1. 잠재적으로 침해된 IAM 엔티티와 사용된 API 호출을 식별하십시오.

   사용된 API 호출은 결과 세부 정보에 API로 나열됩니다. IAM 개체 (IAM 역할 또는 사용자) 와 해당 식별 정보는 검색 결과 세부 정보의 리소스 섹션에 나열됩니다. 관련된 IAM 엔터티의 유형은 User Type(사용자 유형) 필드에 의해 결정될 수 있으며 IAM 엔터티의 이름은 User name(사용자 이름) 필드에 표시됩니다. 결과에 관여한 IAM 엔터티의 유형은 사용된 Access key ID(Access 키 ID)에 의해 결정될 수도 있습니다.

`AKIA`로 시작하는 키의 경우:

이 유형의 키는 IAM 사용자 또는 AWS 계정 루트 사용자와 연결된 장기 고객 관리형 보안 인증 정보입니다. IAM 사용자의 액세스 키 관리에 대한 자세한 내용은 IAM 사용자의 액세스 키 관리를 참조하세요.

`ASIA`로 시작하는 키의 경우:

이 유형의 키는 AWS Security Token Service에서 생성되는 단기 임시 자격 증명입니다. 이러한 키는 잠시 동안만 존재하며 AWS 관리 콘솔에서 보거나 관리할 수 없습니다. IAM 역할은 항상 AWS STS 자격 증명을 사용하지만 IAM 사용자에 대해 생성할 수도 있습니다. 자세한 내용은 IAM: 임시 보안 자격 증명을 AWS STS 참조하십시오.

역할을 사용한 경우 사용자 이름 필드에는 사용된 역할의 이름이 표시됩니다. CloudTrail 로그 항목의 `sessionIssuer` 요소를 AWS CloudTrail 검사하여 키가 요청된 방식을 확인할 수 있습니다. 자세한 내용은 IAM 및 정보를 참조하십시오. AWS STS CloudTrail

2. IAM 엔터티에 대한 권한을 검토합니다.

   IAM 콘솔(IAM console)을 엽니다. 사용된 엔티티의 유형에 따라 사용자 또는 역할 탭을 선택하고 식별된 이름을 검색 필드에 입력하여 영향을 받는 엔티티를 찾습니다. Permission(권한) 및 Access Advisor(액세스 관리자) 탭을 사용하여 해당 엔터티에 대한 유효한 권한을 검토합니다.

3. IAM 엔터티 자격 증명이 합법적으로 사용되었는지 여부를 확인합니다.

   자격 증명 사용자에게 연락하여 활동이 의도적이었는지 여부를 확인합니다.

   예를 들어, 사용자가 다음을 수행했는지 확인합니다.

   - 검색 결과에 나열된 API 작업을 호출했습니다. GuardDuty
   - 검색 결과에 나열된 시간에 API 작업을 호출했습니다. GuardDuty
   - 검색 결과에 나열된 IP 주소에서 API 작업을 호출했습니다. GuardDuty

이 활동이 AWS 자격 증명을 합법적으로 사용하는 경우 결과를 무시해도 됩니다 GuardDuty . https://console.aws.amazon.com/guardduty/ 콘솔에서 더 이상 표시되지 않도록 개별 결과를 완전히 차단하는 규칙을 설정할 수 있습니다. 자세한 정보는 억제 규칙을 참조하세요.

이 활동이 합법적인 사용인지 확인할 수 없다면 특정 액세스 키, 즉 IAM 사용자의 로그인 자격 증명 또는 전체가 손상되었기 때문일 수 있습니다. AWS 계정자격 증명이 침해된 것으로 의심되는 경우 내 정보가 침해될 AWS 계정 수 있음 문서의 정보를 검토하여 이 문제를 해결하십시오.

잠재적으로 손상되었을 수 있는 독립형 컨테이너의 문제 해결

1. 잠재적으로 손상되었을 수 있는 컨테이너를 격리하십시오.

   다음 단계는 잠재적으로 악의적인 컨테이너 워크로드를 식별하는 데 도움이 됩니다.

   - https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
   - 검색결과 페이지에서 해당하는 검색결과를 선택하여 검색결과 패널을 확인합니다.
   - 결과 패널의 영향을 받는 리소스 섹션에서 컨테이너의 ID와 이름을 볼 수 있습니다.

   이 컨테이너를 다른 컨테이너 워크로드로부터 격리합니다.
2. 컨테이너 일시 중지

   컨테이너의 모든 프로세스를 일시 중단합니다.

   컨테이너 동결에 대한 자세한 내용은 컨테이너 일시 중지를 참조하십시오.

   컨테이너 중지

   위 단계에 실패하고 컨테이너가 일시 중지되지 않으면 컨테이너 실행을 중지하세요. 이 스냅샷 보존 기능을 활성화한 경우 멀웨어가 포함된 EBS 볼륨의 스냅샷이 GuardDuty 보존됩니다.

   컨테이너 중지에 대한 자세한 내용은 컨테이너 중지를 참조하십시오.
3. 맬웨어의 존재 여부 평가

   맬웨어가 컨테이너 이미지에 있었는지 평가합니다.

액세스가 승인되었다면 결과를 무시할 수 있습니다. https://console.aws.amazon.com/guardduty/ 콘솔에서 더 이상 표시되지 않도록 개별 결과를 완전히 차단하는 규칙을 설정할 수 있습니다. GuardDuty 콘솔에서는 개별 결과를 완전히 숨겨 더 이상 나타나지 않도록 규칙을 설정할 수 있습니다. 자세한 내용은 억제 규칙을(를) 참조하세요.

EKS 감사 로그 모니터링 결과 해결

Amazon은 계정에 대해 EKS 감사 로그 모니터링이 활성화된 경우 잠재적인 Kubernetes 보안 문제를 나타내는 결과를 GuardDuty 생성합니다. 자세한 설명은 EKS 감사 로그 모니터링 섹션을 참조하세요. 다음 섹션에서는 이러한 시나리오에 대한 권장 해결 단계를 설명합니다. 특정 문제 해결 조치는 해당 결과 유형의 항목에 설명되어 있습니다. 활성 결과 유형 표에서 선택하여 결과 유형에 대한 전체 정보에 액세스할 수 있습니다.

EKS 감사 로그 모니터링 결과 유형이 예상대로 생성된 경우 억제 규칙 추가를 통해 향후 알림을 방지하는 것을 고려할 수 있습니다.

다양한 유형의 공격과 구성 문제가 Kubernetes 탐지 결과를 유발할 수 있습니다. GuardDuty 이 가이드는 클러스터에 대한 GuardDuty 발견의 근본 원인을 식별하고 적절한 수정 지침을 설명하는 데 도움이 됩니다. GuardDuty 쿠버네티스 발견으로 이어지는 주요 근본 원인은 다음과 같습니다.

- 잠재적 구성 문제
- 잠재적으로 침해된 Kubernetes 사용자 문제 해결
- 잠재적으로 손상될 수 있는 Kubernetes 포드 수정
- 잠재적으로 손상될 수 있는 Kubernetes 노드의 문제 해결
- 잠재적으로 손상되었을 수 있는 컨테이너 이미지 수정

> **Note**
>
> 쿠버네티스 버전 1.14 이전에는 `system:unauthenticated` 그룹이 기본적으로 연결되어 있었습니다. `system:discovery` `system:basic-user` ClusterRoles 이로 인해 익명 사용자의 의도하지 않은 액세스가 허용될 수 있습니다. 클러스터 업데이트는 이러한 권한을 철회하지 않으므로 클러스터를 버전 1.14 이상으로 업데이트한 경우에도 이러한 권한이 계속 유지될 수 있습니다. `system:unauthenticated` 그룹에서 이러한 권한을 분리하는 것이 좋습니다. 이러한 권한을 제거하는 방법에 대한 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS의 보안 모범 사례를 참조하십시오.

잠재적 구성 문제

결과에 구성 문제가 있는 경우 해당 결과의 해결 섹션에서 특정 문제를 해결하는 방법에 대한 지침을 참조하세요. 자세한 내용은 구성 문제를 나타내는 다음 결과 유형을 참조하세요.

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- 다음으로 끝나는 모든 결과 SuccessfulAnonymousAccess

잠재적으로 침해된 Kubernetes 사용자 문제 해결

GuardDuty 탐지 결과에서 식별된 사용자가 예상치 못한 API 작업을 수행한 경우 탐지 결과는 Kubernetes 사용자가 침해되었음을 의미할 수 있습니다. 콘솔의 결과 세부 정보에 있는 Kubernetes 사용자 세부 정보 섹션 또는 결과 JSON의 `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails`에서 사용자를 식별할 수 있습니다. 이러한 사용자 세부 정보에는 `user name`, `uid` 및 사용자가 속한 Kubernetes 그룹이 포함됩니다.

사용자가 IAM 엔터티를 사용하여 워크로드에 액세스하는 경우 `Access Key details` 섹션을 사용하여 IAM 역할 또는 사용자의 세부 정보를 식별할 수 있습니다. 다음 사용자 유형 및 해결 지침을 참조하세요.

> **Note**
>
> Amazon Detective를 사용하여 결과에서 식별된 IAM 역할 또는 사용자를 추가로 조사할 수 있습니다. GuardDuty 콘솔에서 검색 결과 세부 정보를 보는 동안 Detective에서 조사를 선택합니다. 그런 다음 나열된 항목에서 AWS 사용자 또는 역할을 선택하여 Detective에서 조사하십시오.

기본 제공 Kubernetes 관리자 - Amazon EKS에서 클러스터를 생성한 IAM ID에 할당한 기본 사용자입니다. 이 사용자 유형은 사용자 이름 `kubernetes-admin`으로 식별됩니다.

기본 제공 Kubernetes 관리자의 액세스 권한 철회:

- `Access Key details` 섹션에서 `userType`을 찾습니다.
  - `userType`이 역할이고 역할이 EC2 인스턴스 역할에 속하는 경우:
    - 해당 인스턴스를 식별한 다음 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결의 지침을 따릅니다.
  - `userType`이 사용자이거나 사용자가 맡은 역할인 경우:
    1. 해당 사용자의 액세스 키를 교체합니다.
    2. 사용자가 액세스할 수 있었던 모든 보안 암호를 교체합니다.
    3. 자세한 내용은 내 AWS 계정이 침해될 수 있는 정보를 검토하십시오.

OIDC 인증 사용자 - OIDC 공급자를 통해 액세스 권한이 부여된 사용자입니다. 일반적으로 OIDC 사용자는 이메일 주소를 사용자 이름으로 사용합니다. `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`* 명령으로 클러스터가 OIDC를 사용하는지 확인할 수 있습니다.

OIDC 인증 사용자의 액세스 철회:

1. OIDC 공급자에서 해당 사용자의 보안 인증 정보를 교체합니다.
2. 사용자가 액세스할 수 있었던 모든 보안 암호를 교체합니다.

AWS-인증 ConfigMap 정의 사용자 — -auth를 통해 액세스 권한을 부여받은 IAM 사용자입니다. AWSConfigMap 자세한 내용은 EKS 사용 설명서의 클러스터의 사용자 또는 IAM 역할 관리를 참조하세요. 다음 `kubectl edit configmaps aws-auth --namespace kube-system` 명령을 사용하여 권한을 검토할 수 있습니다.

사용자 액세스 취소하기: AWS ConfigMap

1. 다음 명령을 사용하여 를 엽니다. ConfigMap

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. 검색 결과의 Kubernetes 사용자 세부 정보 섹션에 보고된 것과 동일한 사용자 이름을 사용하여 MapRoles 또는 MapUsers 섹션에서 역할 또는 사용자 항목을 식별하십시오. GuardDuty 다음 예시에서는 관리자가 결과에서 식별되었습니다.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. 에서 해당 사용자를 제거하세요. ConfigMap 다음 예시에서는 관리자가 결과에서 제거되었습니다.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. `userType`이 사용자이거나 사용자가 맡은 역할인 경우:
   a. 해당 사용자의 액세스 키를 교체합니다.
   b. 사용자가 액세스할 수 있었던 모든 보안 암호를 교체합니다.
   c. 자세한 내용은 내 AWS 계정의 정보가 유출될 수 있다는 정보를 검토하십시오.

결과에 `resource.accessKeyDetails` 섹션이 없는 경우 사용자는 Kubernetes 서비스 계정입니다.

서비스 계정 - 서비스 계정은 포드의 ID를 제공하고 `system:serviceaccount:`*`namespace`*`:`*`service_account_name`* 형식의 사용자 이름으로 식별할 수 있습니다.

서비스 계정에 대한 액세스 권한 철회:

1. 서비스 계정 보안 인증 정보를 교체합니다.
2. 다음 섹션의 포드 손상 안내를 검토합니다.

잠재적으로 손상될 수 있는 Kubernetes 포드 수정

`resource.kubernetesDetails.kubernetesWorkloadDetails`섹션 내 포드 또는 워크로드 리소스의 세부 정보를 GuardDuty 지정할 때 해당 포드 또는 워크로드 리소스가 잠재적으로 손상되었을 수 있습니다. GuardDuty 검색 결과는 단일 포드가 손상되었거나 상위 수준 리소스를 통해 여러 포드가

손상되었음을 나타낼 수 있습니다. 손상된 포드를 식별하는 방법에 대한 지침은 다음 보안 침해 시나리오를 참조하세요.

단일 포드 손상

`resource.kubernetesDetails.kubernetesWorkloadDetails` 섹션 내 `type` 필드가 포드인 경우 결과에서 단일 포드가 식별됩니다. 이름 필드는 포드의 `name`이고 `namespace` 필드는 네임스페이스입니다.

포드를 실행하는 워커 노드를 식별하는 방법에 대한 자세한 내용은 문제가 되는 포드 및 작업자 노드 식별을 참조하십시오.

워크로드 리소스를 통해 포드가 손상됨

`resource.kubernetesDetails.kubernetesWorkloadDetails` 섹션 내 `type` 필드에서 워크로드 리소스(예: `Deployment`)가 식별되면 해당 워크로드 리소스 내의 모든 포드가 손상되었을 수 있습니다.

워크로드 리소스의 모든 포드와 해당 포드가 실행 중인 노드를 식별하는 방법에 대한 자세한 내용은 워크로드 이름을 사용하여 문제가 되는 포드 및 작업자 노드 식별을 참조하십시오.

서비스 계정을 통해 포드가 손상됨

GuardDuty 검색 결과 `resource.kubernetesDetails.kubernetesUserDetails` 섹션에서 서비스 계정이 식별되면 식별된 서비스 계정을 사용하는 포드가 손상될 가능성이 높습니다. 형식이 `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*인 경우 결과에 보고된 사용자 이름은 서비스 계정입니다.

서비스 계정을 사용하여 모든 포드와 해당 포드가 실행 중인 노드를 식별하는 방법에 대한 자세한 내용은 서비스 계정 이름을 사용하여 문제가 되는 포드 및 워커 노드 식별을 참조하십시오.

손상된 파드와 파드가 실행 중인 노드를 모두 식별한 후에는 Amazon EKS 모범 사례 가이드를 참조하여 파드를 분리하고, 자격 증명을 교체하고, 포렌식 분석을 위한 데이터를 수집하십시오.

잠재적으로 손상되었을 수 있는 파드를 해결하려면:

1. 포드를 손상시킨 취약성을 식별합니다.
2. 해당 취약성에 대한 수정 사항을 구현하고 새 대체 포드를 시작합니다.
3. 취약한 포드를 삭제합니다.

   자세한 내용은 손상된 포드 또는 워크로드 리소스 재배포를 참조하십시오.

작업자 노드에 파드가 다른 AWS 리소스에 액세스할 수 있도록 허용하는 IAM 역할을 할당받은 경우, 해당 역할을 인스턴스에서 제거하여 공격으로 인한 추가 피해를 방지하세요. 마찬가지로 포드에 IAM 역할이 할당된 경우 다른 워크로드에 영향을 미치지 않으면서 역할에서 IAM 정책을 안전하게 제거할 수 있는지 평가합니다.

잠재적으로 손상되었을 수 있는 컨테이너 이미지 수정

파드 GuardDuty 손상이 발견된 경우 파드를 시작하는 데 사용된 이미지는 잠재적으로 악의적이거나 손상된 것일 수 있습니다. GuardDuty 조사 결과는 `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` 필드 내 컨테이너 이미지를 식별합니다. 맬웨어를 스캔하여 이미지가 악성인지 확인할 수 있습니다.

잠재적으로 손상되었을 수 있는 컨테이너 이미지를 수정하려면:

1. 이미지 사용을 즉시 중지하고 이미지 리포지토리에서 이미지를 제거합니다.
2. 손상 가능성이 있는 이미지를 사용하여 모든 포드를 식별하십시오.

   자세한 내용은 잠재적으로 취약하거나 손상된 컨테이너 이미지와 워커 노드가 있는 포드 식별을 참조하십시오.
3. 잠재적으로 손상될 수 있는 파드를 분리하고, 자격 증명을 교체하고, 분석을 위한 데이터를 수집하세요. 자세한 내용은 Amazon EKS 모범 사례 가이드를 참조하십시오.
4. 손상 가능성이 있는 이미지를 사용하는 모든 포드를 삭제하십시오.

잠재적으로 손상될 수 있는 Kubernetes 노드의 문제 해결

GuardDuty 검색 결과에서 식별된 사용자가 노드 ID를 나타내거나 검색 결과가 권한 있는 컨테이너의 사용을 나타내는 경우, 검색 결과는 노드 손상을 의미할 수 있습니다.

사용자 이름 필드에 `system:node:node name` 형식이 있는 경우 사용자 ID는 워커 노드입니다. 예를 들어 `system:node:ip-192-168-3-201.ec2.internal`입니다. 이는 공격자가 노드에 대한 액세스 권한을 얻었고 노드의 보안 인증 정보를 사용하여 Kubernetes API 엔드포인트와 통신하고 있음을 나타냅니다.

결과에 나열된 하나 이상의 컨테이너에 `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` 결과 필드가 `True`로 설정된 경우 결과에서 권한이 있는 컨테이너의 사용을 나타냅니다.

잠재적으로 손상된 노드를 수정하려면:

1. 포드를 격리하고, 자격 증명을 교체하고, 포렌식 분석을 위한 데이터를 수집하십시오.

   자세한 내용은 Amazon EKS 모범 사례 가이드를 참조하십시오.
2. 잠재적으로 손상된 노드에서 실행되는 모든 포드가 사용하는 서비스 계정을 식별하십시오. 권한을 검토하고 필요한 경우 서비스 계정을 교체합니다.
3. 잠재적으로 손상된 노드를 종료합니다.

런타임 모니터링 결과 수정

계정에 대해 런타임 모니터링을 활성화하면 Amazon에서 사용자 AWS 환경의 잠재적 보안 문제를 런타임 모니터링 검색 유형 나타내는 런타임 모니터링을 생성할 GuardDuty 수 있습니다. 잠재적인 보안 문제는 사용자 환경의 Amazon EC2 인스턴스, 컨테이너 워크로드, Amazon EKS 클러스터 또는 일련의 자격 증명이 손상되었음을 나타냅니다. AWS 보안 에이전트는 여러 리소스 유형의 런타임 이벤트를 모니터링합니다. 잠재적으로 손상된 리소스를 식별하려면 GuardDuty 콘솔에서 생성된 검색 결과 세부 정보에서 리소스 유형을 확인하십시오. 다음 섹션에서는 각 리소스 유형에 대한 권장 해결 단계를 설명합니다.

Instance

결과 세부 정보의 리소스 유형이 인스턴스인 경우 EC2 인스턴스 또는 EKS 노드가 손상되었을 수 있음을 나타냅니다.

- 손상된 EKS 노드 문제를 해결하려면 잠재적으로 손상될 수 있는 Kubernetes 노드의 문제 해결 섹션을 참조하세요.
- 손상된 EC2 인스턴스 문제를 해결하려면 잠재적으로 손상된 Amazon EC2 인스턴스의 문제 해결 섹션을 참조하세요.

EKSCluster

결과 세부 정보의 리소스 유형이 EKSCluster인 경우 EKS 클러스터 내부의 포드 또는 컨테이너가 손상되었을 수 있음을 나타냅니다.

- 손상된 포드 문제를 해결하려면 잠재적으로 손상될 수 있는 Kubernetes 포드 수정 섹션을 참조하세요.
- 손상된 컨테이너 이미지 문제를 해결하려면 잠재적으로 손상되었을 수 있는 컨테이너 이미지 수정 섹션을 참조하세요.

ECSCluster

검색 결과 세부 정보의 리소스 유형이 ECSCluster인 경우 ECS 작업이나 ECS 작업 내의 컨테이너가 잠재적으로 손상되었을 수 있음을 나타냅니다.

1. 영향을 받는 ECS 클러스터를 식별하십시오.

   GuardDuty 런타임 모니터링 검색 결과는 검색 결과의 세부 정보 패널 또는 검색 결과 JSON의 `resource.ecsClusterDetails` 섹션에 ECS 클러스터 세부 정보를 제공합니다.

2. 영향을 받는 ECS 작업을 식별하십시오.

   GuardDuty 런타임 모니터링 검색 결과는 검색 결과의 세부 정보 패널 또는 검색 결과 JSON의 `resource.ecsClusterDetails.taskDetails` 섹션에 ECS 작업 세부 정보를 제공합니다.

3. 영향을 받는 작업을 분리하세요.

   작업에 대한 모든 수신 및 송신 트래픽을 거부하여 영향을 받는 작업을 격리합니다. 모든 트래픽 거부 규칙은 작업에 대한 모든 연결을 끊어 이미 진행 중인 공격을 중단하는 데 도움이 될 수 있습니다.

4. 손상된 작업을 수정하세요.

   a. 작업을 손상시킨 취약성을 식별하십시오.

   b. 해당 취약성에 대한 수정 사항을 구현하고 새로운 대체 작업을 시작하십시오.

   c. 취약한 작업을 중지하세요.

Container

결과 세부 정보의 리소스 유형이 컨테이너인 경우 독립형 컨테이너가 손상되었을 수 있음을 나타냅니다.

- 문제를 해결하려면 잠재적으로 손상되었을 수 있는 독립형 컨테이너의 문제 해결 섹션을 참조하세요.
- 동일한 컨테이너 이미지를 사용하여 여러 컨테이너에서 결과가 생성되는 경우 잠재적으로 손상되었을 수 있는 컨테이너 이미지 수정 섹션을 참조하세요.
- 컨테이너가 기본 EC2 호스트에 액세스한 경우 관련 인스턴스 보안 인증 정보가 손상되었을 수 있습니다. 자세한 정보는 잠재적으로 손상되었을 수 있는 자격 증명 수정 AWS을 참조하세요.
- 잠재적으로 악의적인 작업자가 기본 EKS 노드 또는 EC2 인스턴스에 액세스한 경우 EKSCluster 및 인스턴스 탭의 권장 문제 해결을 참조하세요.

손상된 컨테이너 이미지 문제 해결

GuardDuty 검색 결과 작업 손상이 확인되면 작업을 시작하는 데 사용된 이미지가 악의적이거나 손상된 것일 수 있습니다. GuardDuty 조사 결과는 `resource.ecsClusterDetails.taskDetails.containers.image` 필드 내의 컨테이너 이미지를 식별합니다. 멀웨어를 검사하여 이미지가 악성인지 여부를 확인할 수 있습니다.

손상된 컨테이너 이미지를 치료하려면

1. 이미지 사용을 즉시 중지하고 이미지 리포지토리에서 이미지를 제거합니다.
2. 이 이미지를 사용하는 모든 작업을 식별하십시오.
3. 손상된 이미지를 사용하는 모든 작업을 중지하세요. 손상된 이미지 사용을 중단하도록 작업 정의를 업데이트하세요.

잠재적으로 손상되었을 수 있는 데이터베이스 수정

GuardDuty 활성화한 이후에 발생할 수 있는 의심스럽고 비정상적인 로그인 동작을 나타내는 메시지가 생성됩니다RDS 보호 결과 유형. 지원되는 데이터베이스 GuardDuty RDS 프로텍션 RDS 로그인 활동을 사용하여 로그인 시도의 특이한 패턴을 식별하여 위협을 GuardDuty 분석하고 프로파일링합니다.

> **Note**
>
> 결과 테이블에서 선택하여 결과 유형에 대한 전체 정보에 액세스할 수 있습니다.

다음 권장 단계에 따라 사용자 환경에서 잠재적으로 손상된 Amazon Aurora 데이터베이스를 수정하십시오. AWS

주제

- 성공적인 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결
- 실패한 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결
- 손상되었을 수 있는 보안 인증 정보 문제 해결
- 네트워크 액세스 제한

성공적인 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결

다음 권장 단계는 성공적인 로그인 이벤트와 관련하여 비정상적인 동작을 보이는 잠재적으로 손상된 Aurora 데이터베이스를 해결하는 데 도움이 될 수 있습니다.

1. 영향을 받는 데이터베이스와 사용자를 식별합니다.

   생성된 GuardDuty 검색 결과는 영향을 받는 데이터베이스의 이름과 해당 사용자 세부 정보를 제공합니다. 자세한 설명은 조사 결과 세부 정보 섹션을 참조하세요.
2. 이 동작이 예상된 것인지 여부를 확인합니다.

   다음 목록은 검색 결과 생성으로 GuardDuty 인해 발생할 수 있는 잠재적 시나리오를 설명합니다.

   - 오랜 시간이 지난 후 데이터베이스에 로그인하는 사용자.
   - 가끔 데이터베이스에 로그인하는 사용자(예: 분기마다 로그인하는 재무 분석가).
   - 데이터베이스를 손상시킬 수 있는 성공적인 로그인 시도에 관여한 잠재적으로 의심스러운 작업자.
3. 예상치 않은 동작이 발생한 경우 이 단계를 시작합니다.

   1. 데이터베이스 액세스 제한

      의심되는 계정 및 이 로그인 활동의 출처에 대한 데이터베이스 액세스를 제한합니다. 자세한 내용은 손상되었을 수 있는 보안 인증 정보 문제 해결 및 네트워크 액세스 제한 섹션을 참조하세요.
   2. 영향을 평가하고 어떤 정보가 액세스되었는지 확인합니다.
      - 가능한 경우 감사 로그를 검토하여 액세스되었을 수 있는 정보를 식별합니다. 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora DB 클러스터에서 이벤트, 로그 및 스트림 모니터링을 참조하세요.
      - 민감하거나 보호되는 정보가 액세스 또는 수정되었는지 확인합니다.

실패한 로그인 이벤트를 통해 손상되었을 수 있는 데이터베이스 문제 해결

다음 권장 단계는 실패한 로그인 이벤트와 관련하여 비정상적인 동작을 보이는 잠재적으로 손상된 Aurora 데이터베이스를 해결하는 데 도움이 될 수 있습니다.

1. 영향을 받는 데이터베이스와 사용자를 식별합니다.

생성된 GuardDuty 검색 결과는 영향을 받는 데이터베이스의 이름과 해당 사용자 세부 정보를 제공합니다. 자세한 설명은 조사 결과 세부 정보 섹션을 참조하세요.

2. 실패한 로그인 시도의 출처를 식별합니다.

   생성된 GuardDuty 검색 결과는 검색 결과 패널의 Actor 섹션 아래에 IP 주소 및 ASN 조직 (공용 연결인 경우) 을 제공합니다.

   Autonomous System(AS)은 명확하게 정의된 단일 라우팅 정책을 유지하는 하나 이상의 네트워크 운영자가 실행하는 하나 이상의 IP 접두사 그룹입니다(네트워크에서 액세스할 수 있는 IP 주소 목록). 네트워크 운영자가 네트워크 내 라우팅을 제어하고 다른 인터넷 서비스 제공업체(ISP)와 라우팅 정보를 교환하려면 Autonomous System Number(ASN)가 필요합니다.

3. 이 동작이 예상치 않은 것인지 확인합니다.

   다음과 같이 이 활동이 데이터베이스에 대한 추가 무단 액세스 권한을 얻으려는 시도를 나타내는지 검사합니다.

   - 내부 소스인 경우 애플리케이션이 잘못 구성되어 있고 연결을 반복해서 시도하고 있지 않은지 검사합니다.
   - 외부 작업자인 경우 해당 데이터베이스가 공개되어 있거나 잘못 구성되어 있어 잠재적인 악성 공격자가 일반적인 사용자 이름을 무차별 대입할 수 있는지 확인합니다.

4. 예상치 않은 동작이 발생한 경우 이 단계를 시작합니다.

   1. 데이터베이스 액세스 제한

      의심되는 계정 및 이 로그인 활동의 출처에 대한 데이터베이스 액세스를 제한합니다. 자세한 내용은 손상되었을 수 있는 보안 인증 정보 문제 해결 및 네트워크 액세스 제한 섹션을 참조하세요.

   2. 근본 원인 분석을 수행하고 이러한 활동의 원인이 될 수 있었던 단계를 파악합니다.

      활동으로 인해 네트워킹 정책이 수정되어 안전하지 않은 상태가 발생할 경우 알림을 받도록 설정합니다. 자세한 내용은AWS Network Firewall 개발자 안내서의 Firewall policies in AWS Network Firewall을 참조하세요.

손상되었을 수 있는 보안 인증 정보 문제 해결

GuardDuty 검색 결과에 따르면 검색 결과에서 식별된 사용자가 예상치 못한 데이터베이스 작업을 수행했을 때 영향을 받는 데이터베이스의 사용자 자격 증명이 손상되었음을 나타낼

수 있습니다. 콘솔의 결과 패널에 있는 RDS DB 사용자 세부 정보 섹션 또는 결과 JSON의 `resource.rdsDbUserDetails`에서 사용자를 식별할 수 있습니다. 이러한 사용자 세부 정보에는 사용자 이름, 사용된 애플리케이션, 액세스한 데이터베이스, SSL 버전 및 인증 방법이 포함됩니다.

- 결과와 관련된 특정 사용자의 액세스 권한을 철회하거나 암호를 교체하려면 Amazon Aurora 사용 설명서의 Amazon Aurora MySQL를 사용한 보안 또는 Amazon Aurora PostgreSQL를 사용한 보안을 참조하세요.
- Amazon RDS (관계형 데이터베이스 서비스) 데이터베이스의 보안 정보를 안전하게 저장하고 자동으로 교체하는 AWS Secrets Manager 데 사용합니다. 자세한 내용은AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 자습서를 참조하세요.
- IAM 데이터베이스 인증을 사용하여 암호 없이도 데이터베이스 사용자의 액세스를 관리합니다. 자세한 내용은 Amazon Aurora 사용 설명서의 IAM 데이터베이스 인증을 참조하세요.

  자세한 내용은 Amazon RDS 사용 설명서의 Security best practices for Amazon Relational Database Service를 참조하세요.

네트워크 액세스 제한

GuardDuty 검색 결과는 애플리케이션 또는 VPC (Virtual Private Cloud) 를 넘어서 데이터베이스에 액세스할 수 있음을 나타낼 수 있습니다. 결과의 원격 IP 주소가 예상치 못한 연결 소스인 경우 보안 그룹을 감사합니다. 데이터베이스에 연결된 보안 그룹 목록은 https://console.aws.amazon.com/rds/ 콘솔의 보안 그룹 또는 결과 JSON의 `resource.rdsDbInstanceDetails.dbSecurityGroups`에서 확인할 수 있습니다. 보안 그룹 구성에 대한 자세한 내용은 Amazon RDS 사용 설명서의 보안 그룹을 통한 액세스 제어를 참조하세요.

방화벽을 사용하는 경우 네트워크 액세스 제어 목록(NACL)을 재구성하여 데이터베이스에 대한 네트워크 액세스를 제한합니다. 자세한 내용은AWS Network Firewall 개발자 안내서의 Firewalls in AWS Network Firewall을 참조하세요.

잠재적으로 손상된 Lambda 함수 수정

Lambda 보호 검색 결과를 GuardDuty 생성할 때 활동이 예상치 못한 경우 Lambda 함수가 손상될 수 있습니다. 손상된 Lambda 함수 문제를 해결하려면 다음 단계를 완료하는 것이 좋습니다.

Lambda 보호 결과 해결

1. 잠재적으로 손상된 Lambda 함수 버전을 식별합니다.

Lambda 보호 GuardDuty 검색 결과는 결과 세부 정보에 나열된 Lambda 함수와 관련된 이름, Amazon 리소스 이름 (ARN), 함수 버전 및 수정 ID를 제공합니다.

2. 잠재적으로 의심스러운 활동의 출처를 식별하십시오.

   a. 결과와 관련된 Lambda 함수 버전과 관련된 코드를 검토합니다.

   b. 결과와 관련된 Lambda 함수 버전의 가져온 라이브러리 및 계층을 검토합니다.

   c. Amazon Inspector에서 스캔 AWS Lambda 기능을 활성화한 경우 검색과 관련된 Lambda 함수와 관련된 Amazon Inspector 검색 결과를 검토하십시오.

   d. AWS CloudTrail 로그를 검토하여 함수 업데이트를 일으킨 보안 주체를 식별하고 활동이 승인되었거나 예상되었는지 확인하십시오.

3. 잠재적으로 손상된 Lambda 함수를 수정하십시오.

   a. 결과와 관련된 Lambda 함수의 실행 트리거를 비활성화합니다. 자세한 내용은 을 참조하십시오. DeleteFunctionEventInvokeConfig

   b. Lambda 코드를 검토하고 라이브러리 가져오기 및 Lambda 함수 계층을 업데이트하여 잠재적으로 의심스러운 라이브러리와 계층을 제거합니다.

   c. 결과와 관련된 Lambda 함수와 관련이 있는 Amazon Inspector 결과를 완화하세요.

Amazon에서 여러 계정 관리 GuardDuty

AWS 환경에 계정이 여러 개 있는 경우 한 계정을 관리자 계정으로 지정하여 AWS 계정을 관리할 수 있습니다. 그런 다음 다른 AWS 계정을 이 관리자 계정과 구성원 계정으로 연결할 수 있습니다. 이 지정된 GuardDuty 관리자 계정은 보호 계획을 구성할 수 있습니다. 계정을 관리자 계정과 연결하는 방법에는 두 가지가 있습니다. 관리자 AWS Organizations 계정과 하나 이상의 구성원 계정이 이 조직에 속해 있는 계정을 사용하여 조직을 만들거나 를 통해 AWS 계정으로 초대를 보내는 방법이 GuardDuty 있습니다. GuardDuty

GuardDuty AWS Organizations 방법 사용을 권장합니다. 조직 설정에 대한 자세한 내용은AWS Organizations 사용 설명서에서 조직 생성을 참조하세요.

다음과 같은 방법으로 여러 계정을 관리합니다. AWS Organizations

GuardDuty 관리자 계정으로 지정하려는 계정이 에 AWS Organizations있는 조직의 일부인 경우 해당 계정을 조직의 위임 관리자로 지정할 수 있습니다. GuardDuty 위임된 관리자로 등록된 계정은 자동으로 관리자 계정이 됩니다. GuardDuty

이 관리자 계정을 구성원 계정으로 추가하면 조직 AWS 계정 내 모든 GuardDuty 사용자를 활성화하고 관리할 수 있습니다.

초대를 통해 이미 GuardDuty 관리자 계정과 연결된 구성원 계정이 있는 경우 해당 계정을 기관의 GuardDuty 위임 관리자로 등록할 수 있습니다. 이렇게 하면 현재 연결된 모든 구성원 계정이 구성원으로 남아 있으므로 GuardDuty 계정을 관리하는 추가 기능을 최대한 활용할 수 있습니다. AWS Organizations

조직을 GuardDuty 통해 여러 계정을 지원하는 방법에 대한 자세한 내용은 을 참조하십시오를 통한 GuardDuty 계정 관리 AWS Organizations.

초대를 통한 다중 계정 관리

연결하려는 계정이 조직의 일부가 아닌 경우 관리자 계정을 지정한 다음 관리자 계정을 사용하여 다른 사용자를 구성원 계정으로 AWS 계정 초대할 수 있습니다. GuardDuty 초대된 계정이 초대를 수락하면 해당 계정은 관리자 계정과 연결된 GuardDuty 구성원 계정이 됩니다.

초대를 통해 여러 계정을 지원하는 방법에 대한 GuardDuty 자세한 내용은 을 참조하십시오초대를 통한 GuardDuty 계정 관리.

GuardDuty 관리자 계정과 구성원 계정 간의 관계 이해

다중 계정 GuardDuty 환경에서 사용하는 경우 관리자 계정이 구성원 계정을 GuardDuty 대신하여 특정 측면을 관리할 수 있습니다. 관리자 계정이 수행할 수 있는 기본 기능은 다음과 같습니다.

- 연결된 멤버 계정을 추가 및 제거할 수 있습니다. 이러한 작업이 수행되는 프로세스는 계정이 조직을 통해 연결되었는지 또는 초대를 통해 연결되었는지에 따라 다릅니다.
- 활성화 및 일시 중지를 포함하여 연결된 구성원 계정 GuardDuty 내의 상태를 관리합니다. GuardDuty

  > **Note**
  >
  > 구성원으로 추가된 GuardDuty 계정에서 AWS Organizations 자동으로 활성화되도록 관리되는 위임 관리자 계정.

- 억제 규칙, 신뢰할 수 있는 IP 목록 및 위협 목록을 만들고 관리하여 GuardDuty 네트워크 내 탐지 결과를 사용자 지정합니다. 멤버 계정은 여러 계정 환경에서 이러한 기능에 액세스할 수 없습니다.

다음 표에는 GuardDuty 관리자 계정과 구성원 계정 간의 관계가 자세히 설명되어 있습니다.

이 표에서

- Self - 계정은 자신의 계정에 대해서만 나열된 작업을 수행할 수 있습니다.
- 임의 — 계정은 모든 관련 계정에 대해 나열된 작업을 수행할 수 있습니다.
- 모두 — 계정은 나열된 작업을 수행할 수 있으며 이는 모든 관련 계정에 적용됩니다. 일반적으로 이 작업을 수행하는 계정은 지정된 GuardDuty 관리자 계정입니다.

대시 (-) 가 있는 표 셀은 해당 계정이 나열된 작업을 수행할 수 없음을 나타냅니다.

작업	를 통해 AWS Organizations		초대장별	
	위임된 GuardDuty 관리자 계정	관련 회원 계정	위임된 GuardDuty 관리자 계정	관련 회원 계정
Enable GuardDuty	Any	–	Self	Self

Enable GuardDuty automatically for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–
View all Organizations member accounts regardless of GuardDuty status	Any	–	–	–
Generate sample findings	Self	Self	Self	Self
View all GuardDuty findings	Any	Self	Any	Self
Archive GuardDuty findings	Any	–	Any	–
Apply suppression rules	All	–	All	–
Create trusted IP list or threat lists	All	–	All	–
Update trusted IP list or threat lists	All	–	All	–

Delete trusted IP list or threat lists	All	–	All	–
Set EventBridge notification frequency	All	–	All	Self
Set Amazon S3 location for exporting findings	All	–	All	Self
Enable one or more optional protection plans for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–
Enable any GuardDuty protection plan for individual accounts	Any	–	Any	Self
Disassociate a member account	Any	–	Any	–
Disassociate from an administrator account account	–	Self[#]	–	Self
Delete a disassociated member account	Any	–	Any	–

Suspend GuardDuty	Any*	–	Any*	–
Disable GuardDuty	Any*	–	Any*	–

- # 위임된 GuardDuty 관리자 계정이 기관 구성원에 대한 자동 활성화 기본 설정을 지정하지 않은 경우에만 계정에서 이 작업을 수행할 수 있음을 나타냅니다. ALL
- * 이 계정을 사용하기 전에 모든 관련 계정에 대해 이 작업을 수행해야 함을 나타냅니다. 이러한 계정을 분리한 후에는 해당 계정을 삭제해야 합니다. 조직에서 이러한 작업을 수행하는 방법에 대한 자세한 내용은 을 참조하십시오조직 내에서 조직 유지 GuardDuty.

를 통한 GuardDuty 계정 관리 AWS Organizations

조직에서 사용하는 GuardDuty 경우 해당 AWS 조직의 관리 계정은 조직 내 모든 계정을 GuardDuty 위임된 관리자 계정으로 지정할 수 있습니다. 이 관리자 계정의 경우 지정된 계정에서만 자동으로 GuardDuty 활성화됩니다. AWS 리전또한 이 계정에는 해당 지역 내 조직의 모든 계정을 활성화하고 관리할 GuardDuty 수 있는 권한이 있습니다. 관리자 계정은 이 AWS 기관의 구성원을 보고 구성원을 추가할 수 있습니다.

초대를 통해 연결된 구성원 계정이 있는 GuardDuty 관리자 계정을 이미 설정했고 구성원 계정이 같은 조직에 속해 있는 경우, 조직에 위임된 GuardDuty 관리자 계정을 설정하면 계정 유형이 초대의에서 Via Organizations로 변경됩니다. 위임된 GuardDuty 관리자 계정이 이전에 초대를 통해 동일한 조직에 속하지 않은 구성원을 추가한 경우, 해당 유형은 초대를 통해 유지됩니다. 두 경우 모두 이전에 추가된 계정은 조직의 위임된 GuardDuty 관리자 계정과 연결된 구성원 계정입니다.

조직 외부에 있는 경우에도 계정을 계속 멤버로 추가할 수 있습니다. 자세한 내용은 초대를 통한 계정 추가 및 관리 또는 콘솔을 사용하여 위임된 GuardDuty 관리자 계정을 지정하고 구성원을 관리합니다. GuardDuty 을 참조하세요.

내용

- GuardDuty 위임된 관리자 계정을 지정할 때의 고려 사항 및 권장 사항
- 위임된 GuardDuty 관리자 계정을 지정하는 데 필요한 권한
- 콘솔을 사용하여 위임된 GuardDuty 관리자 계정을 지정하고 구성원을 관리합니다. GuardDuty
- API를 사용하여 GuardDuty 위임된 GuardDuty 관리자 계정을 지정하고 구성원을 관리합니다.

- 조직 내에서 조직 유지 GuardDuty
- 위임된 GuardDuty 관리자 계정 변경

GuardDuty 위임된 관리자 계정을 지정할 때의 고려 사항 및 권장 사항

다음 고려 사항 및 권장 사항은 위임된 GuardDuty 관리자 계정이 어떻게 운영되는지 이해하는 데 도움이 될 수 있습니다. GuardDuty

위임된 GuardDuty 관리자 계정은 최대 50,000명의 구성원을 관리할 수 있습니다.

위임된 GuardDuty 관리자 계정당 회원 계정은 50,000개로 제한됩니다. 여기에는 통해 추가된 구성원 계정 AWS Organizations 또는 GuardDuty 관리자 계정의 기관 가입 초대를 수락한 사용자가 포함됩니다. 하지만 AWS 조직에 50,000개 이상의 계정이 있을 수 있습니다.

50,000개의 멤버 계정 한도를 초과하는 경우 지정된 위임된 GuardDuty 관리자 계정으로부터 CloudWatch 알림 및 이메일을 받게 됩니다. AWS Health Dashboard

위임된 GuardDuty 관리자 계정은 지역별 계정입니다.

반면 AWS Organizations, GuardDuty 은 지역 서비스입니다. 위임된 GuardDuty 관리자 계정과 해당 구성원 계정을 GuardDuty 활성화한 각 원하는 지역을 통해 AWS Organizations 추가해야 합니다. 조직 관리 계정이 미국 동부 (버지니아 북부) 에서만 위임된 GuardDuty 관리자 계정을 지정하는 경우 위임된 GuardDuty 관리자 계정은 해당 지역의 조직에 추가된 구성원 계정만 관리합니다. 사용 가능한 지역의 기능 패리티에 대한 자세한 내용은 을 참조하십시오. GuardDuty 리전 및 엔드포인트

옵트인 지역의 특수 사례

- 위임된 GuardDuty 관리자 계정이 옵트인 지역에서 옵트아웃하는 경우, 조직의 GuardDuty 자동 활성화 구성이 새 멤버 계정만 (NEW) 또는 모든 멤버 계정 () 으로 설정되어 있더라도 조직의 현재 비활성화된 멤버 계정에 대해서는 GuardDuty 활성화할 수 없습니다. ALL GuardDuty 멤버 계정 구성에 대한 자세한 내용을 보려면 GuardDuty 콘솔 탐색 창에서 계정을 열거나 API를 사용하십시오. ListMembers
- GuardDuty 자동 활성화 구성을 로 NEW 설정한 상태에서 작업할 때는 다음 순서가 충족되는지 확인하십시오.

  1. 멤버 계정은 옵트인 지역을 선택합니다.
  2. 에서 회원 계정을 조직에 추가합니다. AWS Organizations

  이러한 단계의 순서를 변경하면 특정 옵트인 지역에서 GuardDuty 자동 활성화 설정이 작동하지 않습니다. 이는 해당 구성원 계정이 조직에 더 이상 처음 추가되지 않기 때문입니다. NEW GuardDuty 두 가지 대체 솔루션을 제공합니다.

- GuardDuty 자동 활성화 구성을 신규 및 기존 회원 계정을 포함하는 로 ALL 설정합니다. 이 경우 이러한 단계의 순서는 중요하지 않습니다.
- 구성원 계정이 이미 조직에 속해 있는 경우 GuardDuty 콘솔 또는 API를 사용하여 특정 옵트인 지역에서 이 계정의 GuardDuty 구성을 개별적으로 관리하십시오.

모든 AWS 조직에서 동일한 위임 GuardDuty 관리자 계정을 사용하는 것이 좋습니다. AWS 리전

활성화한 모든 AWS 리전 위치에서 조직에 동일한 위임 GuardDuty 관리자 계정을 지정하는 것이 좋습니다. GuardDuty 한 지역에서 계정을 위임된 GuardDuty 관리자 계정으로 지정하는 경우 다른 모든 지역의 위임된 GuardDuty 관리자 계정과 동일한 계정을 사용하는 것이 좋습니다.

언제든지 새 위임된 GuardDuty 관리자 계정을 지정할 수 있습니다. 기존의 위임된 GuardDuty 관리자 계정을 제거하는 방법에 대한 자세한 내용은 을 참조하십시오. 위임된 GuardDuty 관리자 계정 변경

조직의 관리 계정을 위임된 GuardDuty 관리자 계정으로 설정하는 것은 권장되지 않습니다.

조직의 관리 계정은 위임된 GuardDuty 관리자 계정일 수 있습니다. 하지만 AWS 보안 모범 사례는 최소 권한 원칙을 따르므로 이 구성을 권장하지 않습니다.

위임된 GuardDuty 관리자 계정을 변경해도 구성원 계정은 GuardDuty 비활성화되지 않습니다.

위임된 GuardDuty 관리자 계정을 제거하면 이 GuardDuty 위임된 관리자 계정과 연결된 모든 구성원 계정이 GuardDuty 제거됩니다. GuardDuty 이 모든 회원 계정에는 여전히 활성화되어 있습니다.

위임된 GuardDuty 관리자 계정을 지정하는 데 필요한 권한

위임된 GuardDuty 관리자 계정을 위임할 때는 특정 API GuardDuty 작업뿐만 아니라 활성화할 수 있는 권한이 있어야 합니다. AWS Organizations 기존 IAM 정책의 끝에 다음 문을 추가하여 이러한 권한을 부여할 수 있습니다.

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

또한 AWS Organizations 관리 계정을 GuardDuty 위임된 GuardDuty 관리자 계정으로 지정하려면 해당 엔티티가 초기화할 수 있는 권한이 필요합니다. `CreateServiceLinkedRole` GuardDuty 이렇게 하려면 IAM 정책에 다음 명령문을 추가하고 *111122223333#* 조직의 관리 계정 ID로 바꾸십시오. AWS 계정

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

콘솔을 사용하여 위임된 GuardDuty 관리자 계정을 지정하고 구성원을 관리합니다. GuardDuty

내용

1단계 — 조직의 위임된 GuardDuty 관리자 계정 지정

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

로그인하려면 AWS Organizations 조직의 관리 계정 보안 인증 정보를 사용합니다.

2. 관리 계정을 이미 GuardDuty 활성화한 경우 이 단계를 건너뛰고 다음 단계를 따르세요.

   GuardDuty 아직 활성화하지 않았다면 시작하기를 선택한 다음 시작 페이지에서 위임된 GuardDuty 관리자 계정을 지정하십시오. GuardDuty

   > **Note**
   >
   > 위임된 GuardDuty 관리자 계정이 해당 계정에서 활성화하고 관리할 수 있으려면 관리 계정에 GuardDuty 서비스 연결 역할 (SLR) 이 있어야 합니다. GuardDuty 지역에서 관리 계정을 GuardDuty 활성화하면 이 SLR이 자동으로 생성됩니다.

3. 관리 계정을 GuardDuty 활성화한 후 이 단계를 수행하십시오. GuardDuty 콘솔의 탐색 창에서 설정을 선택합니다. 설정 페이지에서 조직의 위임된 GuardDuty 관리자 계정으로 지정하려는 계정의 12자리 AWS 계정 ID를 입력합니다.

   새로 지정된 위임된 GuardDuty 관리자 계정을 GuardDuty 활성화해야 합니다. 그렇지 않으면 아무 조치도 취할 수 없습니다.

4. 위임을 선택합니다.

5. (권장) 이전 단계를 반복하여 활성화한 각 AWS 리전 위치에서 위임된 GuardDuty 관리자 계정을 지정하세요. GuardDuty

2단계 — 조직의 자동 활성화 기본 설정 구성

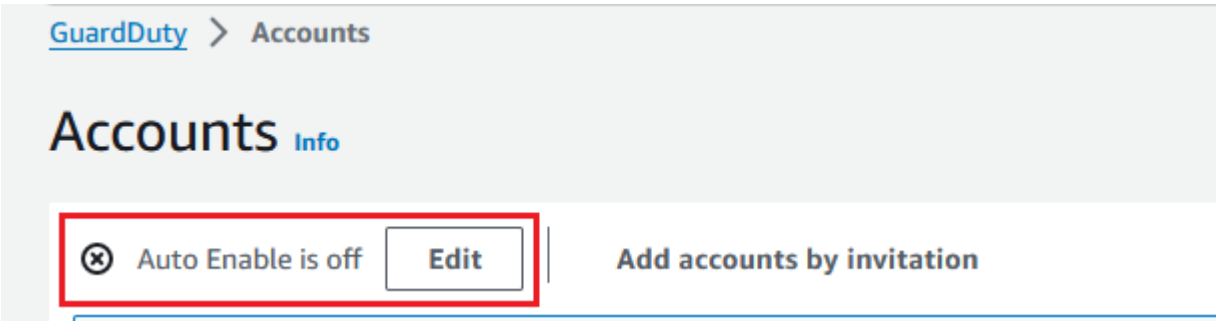
1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   로그인하려면 GuardDuty 관리자 계정 자격 증명을 사용하십시오.

2. 탐색 창에서 Accounts(계정)를 선택합니다.

   계정 페이지에서는 자동 활성화할 수 있는 GuardDuty 관리자 계정의 구성 GuardDuty 옵션과 조직에 속한 구성원 계정을 위한 선택적 보호 플랜을 제공합니다.

3. 기존 자동 활성화 설정을 업데이트하려면 편집을 선택합니다.



이 지원은 사용자 내에서 구성할 수 GuardDuty 있으며 지원되는 모든 선택적 보호 플랜을 구성할 수 있습니다. AWS 리전회원 계정을 GuardDuty 대신하여 다음 구성 옵션 중 하나를 선택할 수 있습니다.

- 모든 계정에 대해 활성화 (**ALL**) - 조직의 모든 계정에 대해 해당 옵션을 활성화하려면 선택합니다. 여기에는 조직에 가입하는 새 계정과 조직에서 일시 중지되거나 제거되었을 수 있는 계정이 포함됩니다. 여기에는 위임된 GuardDuty 관리자 계정도 포함됩니다.

  > **Note**
  >
  > 모든 회원 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

- 새 계정 자동 활성화 (**NEW**) - 선택하면 새 멤버 계정만 조직에 가입할 때 자동으로 GuardDuty 활성화하거나 선택적 보호 플랜이 활성화됩니다.
- 활성화 안 **NONE** 함 () - 조직의 새 계정에 해당 옵션이 활성화되지 않도록 하려면 이 옵션을 선택합니다. 이 경우 GuardDuty 관리자 계정이 각 계정을 개별적으로 관리합니다.

  자동 활성화 설정을 ALL 또는 NEW 에서 업데이트해도 기존 계정의 해당 옵션이 비활성화되지 않습니다. NONE 이 구성은 조직에 가입하는 새 계정에 적용됩니다. 자동 활성화 설정을 업데이트한 후에는 새 계정에서 해당 옵션이 활성화되지 않습니다.

> **Note**
>
> 위임된 GuardDuty 관리자 계정이 옵트인 지역에서 옵트아웃하는 경우, 조직의 GuardDuty 자동 활성화 구성이 새 멤버 계정만 (NEW) 또는 모든 멤버 계정 () 으로 설정되어 있더라도 조직의 현재 비활성화된 멤버 계정에 대해서는 GuardDuty 활성화할 수 없습니다. ALL GuardDuty 멤버 계정 구성에 대한 자세한 내용을 보려면 GuardDuty 콘솔 탐색 창에서 계정을 열거나 API를 사용하십시오. ListMembers

4. 변경 사항 저장를 선택합니다.
5. (선택 사항) 각 지역에서 동일한 환경설정을 사용하려면 지원되는 각 지역의 환경설정을 개별적으로 업데이트하십시오.

   일부 선택적 보호 GuardDuty 플랜은 가능한 모든 지역에서 사용 가능하지 않을 수도 있습니다. AWS 리전 자세한 정보는 리전 및 엔드포인트을 참조하세요.

3단계 - 조직에 멤버로 계정 추가

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   로그인하려면 위임된 GuardDuty 관리자 계정 자격 증명을 사용하십시오.
2. 탐색 창에서 Accounts(계정)를 선택합니다.

   계정 테이블에는 조직을 통해(AWS Organizations) 또는 초대 기준으로 추가된 모든 계정이 표시됩니다. 구성원 계정이 조직의 GuardDuty 관리자 계정과 연결되어 있지 않은 경우 이 구성원 계정의 상태는 비구성원으로 표시됩니다.
3. 멤버로 추가할 계정 ID를 하나 또는 여러 개 선택합니다. 이러한 계정 ID의 유형은 조직을 통해여야 합니다.

   초대를 통해 추가된 계정은 조직에 속하지 않습니다. 이러한 계정을 개별적으로 관리할 수 있습니다. 자세한 정보는 초대를 통한 계정 관리을 참조하세요.
4. 작업 드롭다운을 선택하고 멤버 추가를 선택합니다. 이 계정을 구성원으로 추가하면 자동 활성화 GuardDuty 구성이 적용됩니다. 의 the section called “1단계 — 조직의 위임된 GuardDuty 관리자 계정 지정” 설정에 따라 이러한 계정의 GuardDuty 구성이 변경될 수 있습니다.
5. 상태 열의 아래쪽 화살표를 선택하여 회원이 아님 상태별로 계정을 정렬한 다음 현재 지역에서 GuardDuty 활성화되지 않은 각 계정을 선택할 수 있습니다.

   계정 테이블에 나열된 계정 중 아직 구성원으로 추가된 계정이 없는 경우 현재 지역에서 모든 조직 계정을 GuardDuty 활성화할 수 있습니다. 페이지 상단의 배너에서 활성화를 선택합니다. 이 작업을 수행하면 자동 활성화 GuardDuty 구성이 자동으로 활성화되어 조직에 가입하는 모든 새 계정에 대해 GuardDuty 활성화됩니다.
6. 확인을 선택하여 계정을 멤버로 추가합니다. 또한 이 작업을 수행하면 선택한 모든 계정에 GuardDuty 사용할 수 있습니다. 초대된 계정의 상태가 활성화됨으로 변경됩니다.
7. (권장) 각 단계에서 이 단계를 반복하세요 AWS 리전. 이렇게 하면 위임된 GuardDuty 관리자 계정으로 GuardDuty 활성화한 모든 지역의 구성원 계정에 대한 검색 결과 및 기타 구성을 관리할 수 있습니다.

자동 활성화 기능은 향후 조직의 모든 구성원이 GuardDuty 사용할 수 있습니다. 이렇게 하면 위임된 GuardDuty 관리자 계정으로 조직 내에서 생성되거나 조직에 추가되는 모든 새 구성원을 관리할 수 있습니다. 회원 계정 수가 50,000개 한도에 도달하면 자동 활성화 기능이 자동으로 꺼집니다. 회원 계정을 제거한 후 총 회원 수가 50,000명 미만으로 줄어들면 자동 활성화 기능이 다시 켜집니다.

(선택 사항) 4단계 — 개별 계정에 대한 보호 계획 구성

계정 페이지를 통해 개별 계정의 보호 플랜을 구성할 수 있습니다.

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   위임된 GuardDuty 관리자 계정 자격 증명을 사용하십시오.
2. 탐색 창에서 Accounts(계정)를 선택합니다.
3. 보호 플랜을 구성할 하나 이상의 계정을 선택합니다. 구성할 각 보호 플랜에 대해 다음 단계를 반복합니다.

   a. 보호 계획 편집을 선택합니다.

   b. 보호 플랜 목록에서 구성할 보호 플랜 하나를 선택합니다.

   c. 이 보호 플랜에 대해 수행할 작업 중 하나를 선택한 다음 확인을 선택합니다.

   d. 선택한 계정에서 구성된 보호 플랜에 해당하는 열에 업데이트된 구성이 활성화됨 또는 활성화되지 않음으로 표시됩니다.

API를 사용하여 GuardDuty 위임된 GuardDuty 관리자 계정을 지정하고 구성원을 관리합니다.

내용

1단계 — 조직의 위임된 GuardDuty 관리자 계정 지정 AWS

1. 조직 관리 계정의 자격 AWS 계정 증명을 enableOrganizationAdminAccount사용하여 실행합니다.

- 를 AWS Command Line Interface 사용하여 이 작업을 수행할 수도 있습니다. 다음 AWS CLI 명령은 현재 지역에만 위임된 GuardDuty 관리자 계정을 지정합니다. 다음 AWS CLI 명령을 실행하고 *111111111#* 위임된 관리자 계정으로 지정하려는 계정의 AWS 계정 ID로 바꿔야 합니다. GuardDuty

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

다른 지역의 위임된 GuardDuty 관리자 계정을 지정하려면 명령에서 지역을 지정합니다. AWS CLI 다음 예시는 미국 서부 (오레곤) 에서 위임된 GuardDuty 관리자 계정을 활성화하는 방법을 보여줍니다. *us-west-2#* 위임된 관리자 계정을 할당하려는 지역으로 바꿔야 합니다. GuardDuty GuardDuty

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
 --region us-west-2
```

사용 AWS 리전 가능한 위치에 대한 자세한 내용은 을 참조하십시오 GuardDuty . 리전 및 엔드포인트

위임된 GuardDuty 관리자 계정에 이 (GuardDuty 가) 활성화되어 있지 않으면 아무 조치도 취할 수 없습니다. 아직 활성화하지 않았다면 새로 지정된 위임된 GuardDuty 관리자 계정을 GuardDuty 활성화하세요.

2. (권장) 이전 단계를 반복하여 활성화한 각 AWS 리전 위치에서 위임된 GuardDuty 관리자 계정을 지정하십시오. GuardDuty

2단계 - 조직의 자동 활성화 기본 설정 구성

1. 1. 위임된 GuardDuty 관리자 계정의 자격 증명을 사용하여 실행하면 UpdateOrganizationConfiguration해당 지역에서 조직에 맞는 보호 계획을 자동으로 GuardDuty 구성하고 선택적 보호 계획을 구성할 수 있습니다.

   계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

> **Note**
>
> 다양한 자동 활성화 구성에 대한 자세한 내용은 autoEnableOrganization멤버를 참조하십시오.

2. 해당 리전에서 지원되는 선택적 보호 플랜에 대한 자동 활성화 기본 설정을 지정하려면 각 보호 플랜의 해당 설명서 섹션에 제공된 단계를 따르세요.
3. 현재 리전에서 조직의 기본 설정을 검증할 수 있습니다. describeOrganizationConfiguration를 실행합니다. 위임된 GuardDuty 관리자 계정의 탐지기 ID를 지정해야 합니다.

> **Note**
>
> 모든 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.

- 1. 또는 다음 AWS CLI 명령을 실행하여 해당 GuardDuty 지역에서 조직에 가입하는 새 계정 (NEW), 모든 계정 () 또는 조직 내 모든 계정 (ALL) 에 대해 자동으로 활성화하거나 비활성화하도록 기본 설정을 지정합니다. NONE 자세한 내용은 autoEnableOrganization구성원을 참조하십시오. 기본 설정에 따라 NEW를 ALL 또는 NONE으로 바꿔야 할 수 있습니다. 로 ALL 보호 계획을 구성하면 위임된 GuardDuty 관리자 계정에 대해서도 보호 계획이 활성화됩니다. 조직 구성을 관리하는 위임된 GuardDuty 관리자 계정의 탐지기 ID를 지정해야 합니다.

  계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
  ```

  2. 현재 리전에서 조직의 기본 설정을 검증할 수 있습니다. 위임된 GuardDuty 관리자 계정의 탐지기 ID를 사용하여 다음 AWS CLI 명령을 실행합니다.

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0
  ```

2. (권장) 위임된 GuardDuty 관리자 계정 탐지기 ID를 사용하여 각 지역에서 이전 단계를 반복하세요.

> **Note**
>
> 위임된 GuardDuty 관리자 계정이 옵트인 지역에서 옵트아웃하는 경우, 조직의 GuardDuty 자동 활성화 구성이 새 멤버 계정만 (NEW) 또는 모든 멤버 계정 () 으로 설정되어 있더라도 조직의 현재 비활성화된 멤버 계정에 대해서는 GuardDuty 활성화할 수 없습니다. ALL GuardDuty 멤버 계정 구성에 대한 자세한 내용을 보려면 GuardDuty 콘솔 탐색 창에서 계정을 열거나 API를 사용하십시오. ListMembers

3단계 - 조직에 멤버로 계정 추가

- 이전 단계에서 지정한 위임된 GuardDuty 관리자 계정의 자격 증명을 사용하여 실행합니다 CreateMembers.

  위임된 GuardDuty 관리자 계정의 지역 탐지기 ID와 구성원으로 GuardDuty 추가하려는 계정의 계정 세부 정보 (AWS 계정 ID 및 해당 이메일 주소) 를 지정해야 합니다. 이 API 작업을 이용해 한 명 이상의 멤버를 만들 수 있습니다.

  CreateMembers조직에서 계정을 실행하면 새 구성원 계정이 기관에 가입할 때 새 구성원에 대한 자동 활성화 기본 설정이 적용됩니다. 기존 구성원 CreateMembers 계정으로 실행하는 경우 조직 구성이 기존 구성원에게도 적용됩니다. 이로 인해 기존 구성원 계정의 현재 구성이 변경될 수 있습니다.

  AWS Organizations API ListAccountsReference에서 실행하면 AWS 조직의 모든 계정을 볼 수 있습니다.

  > **Important**
  >
  > 계정을 GuardDuty 구성원으로 추가하면 해당 지역에서 계정이 자동으로 GuardDuty 활성화됩니다. 조직 관리 계정에는 예외가 있습니다. 관리 계정 계정을 GuardDuty 구성원으로 추가하려면 먼저 GuardDuty 활성화해야 합니다.

- 또는 사용할 수도 있습니다 AWS Command Line Interface. 다음 AWS CLI 명령을 실행하고 유효한 탐지기 ID, AWS 계정 ID 및 계정 ID와 연결된 이메일 주소를 사용해야 합니다.

  계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-details AccountId=111122223333,Email=guardduty-member-name@amazon.com
```

다음 AWS CLI 명령어를 실행하여 모든 기관 구성원의 목록을 볼 수 있습니다.

```
aws organizations list-accounts
```

이 계정을 구성원으로 추가하면 자동 활성화 GuardDuty 구성이 적용됩니다.

조직 내에서 조직 유지 GuardDuty

위임된 GuardDuty 관리자 계정은 지원되는 각 계정의 조직 내 모든 계정에 대한 구성 GuardDuty 및 선택적 보호 계획을 유지 관리할 책임이 있습니다. AWS 리전다음 섹션에서는 구성 상태 GuardDuty 또는 선택적 보호 계획을 유지 관리하는 방법에 대한 옵션을 제공합니다.

각 지역에서 전체 조직의 구성 상태를 유지하려면

- GuardDuty 콘솔을 사용하여 기관 전체에 대한 자동 활성화 환경설정 지정 - 기관의 모든 구성원 또는 기관에 가입한 새 (ALLNEW) 구성원에 대해 GuardDuty 자동으로 활성화하거나, 기관의 모든 구성원이 자동으로 활성화하지 않도록 (NONE) 선택할 수 있습니다.

  또한 내의 모든 보호 계획에 대해 동일하거나 다른 설정을 구성할 수 있습니다. GuardDuty

  조직 내 모든 구성원 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다.
- API — 실행을 UpdateOrganizationConfiguration사용하여 자동 활성화 기본 설정을 GuardDuty 업데이트하고 조직에 대한 선택적 보호 계획을 자동으로 구성합니다. 를 CreateMembers실행하여 조직에 새 구성원 계정을 추가하면 구성된 설정이 자동으로 적용됩니다. 기존 구성원 CreateMembers 계정으로 실행하는 경우 조직 구성이 기존 구성원에게도 적용됩니다. 이로 인해 기존 구성원 계정의 현재 구성이 변경될 수 있습니다.

  조직의 모든 계정을 보려면 AWS Organizations API ListAccountsReference에서 실행하세요.

각 지역의 멤버 계정에 대한 구성 상태를 개별적으로 유지하려면

- 조직의 모든 계정을 보려면 AWS Organizations API ListAccountsReference에서 실행하세요.

- 선택적 구성원 계정의 구성 상태를 다르게 하려면 각 구성원 계정에 UpdateMemberDetectors대해 개별적으로 실행하십시오.

  GuardDuty 콘솔을 사용하여 콘솔의 계정 페이지로 이동하여 동일한 작업을 수행할 수 있습니다. GuardDuty

  콘솔 또는 API를 사용하여 개별 계정의 보호 계획을 활성화하는 방법에 대한 자세한 내용은 해당 보호 계획의 구성 페이지를 참조하십시오.

위임된 GuardDuty 관리자 계정 변경

각 지역에서 조직의 위임된 GuardDuty 관리자 계정을 변경한 다음 각 지역의 새 관리자를 위임할 수 있습니다. 지역 내 조직 구성원 계정의 보안 태세를 유지하려면 해당 지역에 위임된 GuardDuty 관리자 계정이 있어야 합니다.

기존의 위임된 관리자 계정 GuardDuty 제거

1단계 - 각 지역의 기존 위임된 GuardDuty 관리자 계정을 제거하려면

1. 기존의 위임된 GuardDuty 관리자 계정으로서 관리자 계정과 연결된 모든 구성원 계정을 나열하십시오. ListMembers로 실행합니다. `OnlyAssociated=false`
2. 자동 활성화 기본 설정 GuardDuty 또는 선택적 보호 계획이 로 설정된 경우 를 UpdateOrganizationConfiguration실행하여 `ALL` 조직 구성을 `NEW` 또는 `NONE` 로 업데이트하십시오. 이렇게 하면 다음 단계에서 모든 구성원 계정의 연결을 끊을 때 오류가 발생하지 않도록 할 수 있습니다.
3. DisassociateMembers를 실행하여 관리자 계정과 연결된 모든 구성원 계정의 연결을 해제합니다.
4. DeleteMembers를 실행하여 관리자 계정과 구성원 계정 간의 연결을 삭제합니다.
5. 조직 관리 계정으로 DisableOrganizationAdminAccount를 실행하여 기존의 위임된 GuardDuty 관리자 계정을 제거합니다.
6. 이 위임된 GuardDuty 관리자 계정이 AWS 리전 있는 각 위치에서 이 단계를 반복합니다.

2단계 - 기존의 위임된 GuardDuty 관리자 계정을 등록 취소하려면 AWS Organizations (일회성 글로벌 작업)

- AWS Organizations API DeregisterDelegatedAdministratorReference에서 실행하여 기존의 GuardDuty 위임된 관리자 계정을 등록 취소합니다. AWS Organizations

또는 다음 AWS CLI 명령을 실행할 수 있습니다.

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --
service-principal guardduty.amazonaws.com
```

111122223333# 기존의 위임된 관리자 계정으로 바꿔야 합니다. GuardDuty

이전의 위임된 GuardDuty 관리자 계정을 등록 취소한 후 이 계정을 새 위임된 관리자 계정에 구성원 계정으로 추가할 수 있습니다. GuardDuty

각 지역의 새로운 위임된 관리자 계정 GuardDuty 지정

1. 다음 액세스 방법 중 하나를 사용하여 각 지역에 새로운 위임된 GuardDuty 관리자 계정을 지정하십시오.
   - GuardDuty 콘솔 사용 —. 1단계 — 조직의 위임된 GuardDuty 관리자 계정 지정
   - GuardDuty API 사용 —1단계 — 조직의 위임된 GuardDuty 관리자 계정 지정 AWS.
2. 을 (를) DescribeOrganizationConfiguration실행하여 조직의 현재 자동 활성화 구성을 확인합니다.

> **Important**
>
> 새 위임된 GuardDuty 관리자 계정에 구성원을 추가하기 전에 조직의 자동 활성화 구성을 확인해야 합니다. 이 구성은 새로 위임된 GuardDuty 관리자 계정 및 선택한 지역에만 적용되며 관련되지 않습니다. AWS Organizations새 위임된 관리자 계정으로 (새 또는 기존) 조직 구성원 계정을 추가하면 새 위임된 GuardDuty 관리자 계정의 자동 활성화 구성이 사용 설정 시점 GuardDuty 또는 선택적 보호 플랜 사용 시점에 적용됩니다. GuardDuty

새 위임된 GuardDuty 관리자 계정의 이 조직 구성을 변경하려면 다음 액세스 방법 중 하나를 사용하십시오.

- GuardDuty 콘솔 사용 —2단계 — 조직의 자동 활성화 기본 설정 구성.
- GuardDuty API 사용 —2단계 - 조직의 자동 활성화 기본 설정 구성.

초대를 통한 GuardDuty 계정 관리

조직 외부의 계정을 관리하려면 레거시 초대 방법을 사용할 수 있습니다. 이 방법을 사용할 경우, 다른 계정이 멤버 계정 가입 초대를 수락하면 본인의 계정이 관리자 계정으로 지정됩니다.

계정이 관리자 계정이 아닌 경우 다른 계정의 초대를 수락할 수 있습니다. 수락하면 이 계정은 멤버 계정이 됩니다. AWS 계정은 GuardDuty 관리자 계정과 멤버 계정을 동시에 사용할 수 없습니다.

한 계정의 초대를 수락하면 다른 계정의 초대는 수락할 수 없습니다. 다른 계정의 초대를 수락하려면 먼저 기존 관리자 계정에서 계정 연결을 끊어야 합니다. 또는 관리자 계정에서 사용자 계정을 분리하고 조직에서 계정을 제거할 수도 있습니다.

에 설명된 대로 초대를 통해 연결된 계정은 연결된 계정과 동일한 전체 관리자 account-to-member 관계를 갖습니다. AWS Organizations GuardDuty 관리자 계정과 구성원 계정 간의 관계 이해 하지만 초대 관리자 계정 사용자는 연결된 구성원 계정을 GuardDuty 대신하여 활성화하거나 AWS Organizations 조직 내 다른 비구성원 계정을 볼 수 없습니다.

> **Important**
>
> 이 방법을 사용하여 구성원 계정을 GuardDuty 생성할 경우 지역 간 데이터 전송이 발생할 수 있습니다. 회원 계정의 이메일 주소를 확인하기 위해 미국 동부 (버지니아 북부) 지역에서만 운영되는 이메일 확인 서비스를 GuardDuty 사용합니다.

초대를 통한 계정 추가 및 관리

액세스 방법 중 하나를 선택하여 계정을 추가하고 GuardDuty 관리자 계정으로 가입할 계정을 GuardDuty 회원 계정으로 초대하십시오.

Console

1단계 - 계정 추가

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.
3. 상단 패널에서 초대 기준으로 계정 추가를 선택합니다.
4. 구성원 계정 추가 페이지의 계정 세부 정보 입력에 추가하려는 계정과 연결된 AWS 계정 ID와 이메일 주소를 입력합니다.

5. 다른 행을 추가하여 계정 세부 정보를 한 번에 하나씩 입력하려면 다른 계정 추가를 선택합니다. 계정 세부 정보가 포함된.csv 파일 업로드를 선택하여 계정을 대량으로 추가할 수도 있습니다.

> **Important**
>
> .csv 파일의 첫 줄에는 다음 예시에 표시된 것처럼 `Account ID,Email` 헤더가 포함되어 있어야 합니다. 이어지는 각 줄에는 유효한 AWS 계정 ID 하나와 관련 이메일 주소가 포함되어야 합니다. 행 형식은 AWS 계정 ID가 하나이고 관련 이메일 주소를 쉼표로 구분한 경우에만 유효합니다.
>
> ```
> Account ID,Email
> 555555555555,user@example.com
> ```

6. 모든 계정 세부 정보를 추가한 후 다음을 선택합니다. 계정 테이블에서 새로 추가된 계정을 볼 수 있습니다. 이러한 계정의 상태는 초대를 전송하지 않음으로 표시됩니다. 추가된 하나 이상의 계정에 초대를 보내는 방법에 대한 자세한 내용은 Step 2 - Invite an account 섹션을 참조하세요.

2단계 - 계정 초대

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.
3. Amazon에 초대하려는 계정을 하나 이상 선택합니다 GuardDuty.
4. 작업 드롭다운 메뉴를 선택한 다음 초대를 선택합니다.
5. 초대 대상 GuardDuty 대화 상자에 초대 메시지 (선택 사항) 를 입력합니다.

   초대된 계정이 이메일에 액세스할 수 없는 경우 초대 대상자의 AWS 계정 계정에 있는 루트 사용자에게 이메일 알림 전송과 초대 대상자의 AWS Health Dashboard에서 알림 생성 확인란을 선택합니다.
6. [Send invitation]을 선택합니다. 초대받은 사람이 지정된 이메일 주소에 액세스할 수 있는 경우 https://console.aws.amazon.com/guardduty/ GuardDuty 콘솔을 열어 초대를 볼 수 있습니다.
7. 초대 대상자가 초대를 수락하면 상태 열 값이 초대됨으로 변경됩니다. 초대 수락에 대한 자세한 내용은 Step 3 - Accept an invitation 섹션을 참조하세요.

3단계 - 초대 수락

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   > **Important**
   >
   > 멤버십 초대를 보거나 수락하려면 GuardDuty 먼저 활성화해야 합니다.

2. GuardDuty 아직 활성화하지 않은 경우에만 다음 단계를 수행하십시오. 그렇지 않으면 이 단계를 건너뛰고 다음 단계를 계속할 수 있습니다.

   아직 GuardDuty 활성화하지 않은 경우 Amazon GuardDuty 페이지에서 시작하기를 선택하십시오.

   시작 GuardDuty 페이지에서 활성화를 선택합니다 GuardDuty.

3. 계정을 GuardDuty 활성화한 후 다음 단계에 따라 멤버십 초대를 수락하십시오.

   a. 탐색 창에서 설정을 선택합니다.

   b. 계정을 선택합니다.

   c. 계정에서 초대를 수락한 계정의 소유자를 확인해야 합니다. 수락을 켜서 멤버십 초대를 수락합니다.

4. 초대를 수락하면 계정이 GuardDuty 회원 계정이 됩니다. 소유자가 초대를 보낸 계정이 GuardDuty 관리자 계정이 됩니다. 관리자 계정은 초대를 수락했음을 알 수 있습니다. 해당 계정의 계정 테이블이 업데이트됩니다. GuardDuty 회원 계정 ID에 해당하는 상태 열의 값이 활성화됨으로 변경됩니다. 이제 관리자 계정 소유자는 계정을 GuardDuty 대신하여 보호 계획 구성을 보고 관리할 수 있습니다. 또한 관리자 계정은 구성원 계정에 대해 생성된 GuardDuty 결과를 보고 관리할 수 있습니다.

API/CLI

GuardDuty 관리자 계정을 지정하고 API 작업을 통해 초대를 통해 GuardDuty 구성원 계정을 만들거나 추가할 수 있습니다. 에서 관리자 계정과 멤버 계정을 지정하려면 다음 GuardDuty API 작업을 실행합니다. GuardDuty

GuardDuty 관리자 계정으로 지정하려는 사용자의 자격 증명을 사용하여 다음 절차를 완료하십시오. AWS 계정

멤버 계정 생성 또는 추가

1. GuardDuty 활성화한 AWS 계정의 자격 증명을 사용하여 CreateMembersAPI 작업을 실행합니다. 이 계정은 관리자 계정 계정으로 사용하려는 GuardDuty 계정입니다.

   현재 AWS 계정의 탐지기 ID와 GuardDuty 회원이 되려는 계정의 계정 ID 및 이메일 주소를 지정해야 합니다. 이 API 작업을 이용해 한 명 이상의 멤버를 만들 수 있습니다.

   AWS 명령줄 도구를 사용하여 다음 CLI 명령을 실행하여 관리자 계정을 지정할 수도 있습니다. 유효한 감지기 ID, 계정 ID 및 이메일을 사용해야 합니다.

   계정 및 현재 지역의 계정을 `detectorId` 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. InviteMembers GuardDuty 활성화한 AWS 계정의 자격 증명을 사용하여 실행하십시오. 이 계정은 관리자 계정 계정으로 사용하려는 GuardDuty 계정입니다.

   현재 AWS 계정의 탐지기 ID와 GuardDuty 구성원이 되려는 계정의 계정 ID를 지정해야 합니다. 이 API 작업을 이용해 한 명 이상의 멤버를 초대할 수 있습니다.

   > **Note**
   >
   > `message` 요청 파라미터를 사용하여 초대 메시지를 지정할 수도 있습니다.

   다음 명령을 AWS Command Line Interface 실행하여 멤버 계정을 지정하는 데 사용할 수도 있습니다. 초대하려는 계정에 대해 본인의 유효한 감지기 ID 및 유효한 계정 ID를 사용해야 합니다.

   계정과 현재 지역에 `detectorId` 맞는 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

   ```
   aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-ids 111122223333
   ```

초대 수락

GuardDuty 회원 계정으로 지정하려는 각 AWS 계정의 자격 증명을 사용하여 다음 절차를 완료하십시오.

1. GuardDuty 구성원 AWS 계정으로 초대되었고 초대를 수락하려는 각 계정에 대해 CreateDetectorAPI 작업을 실행합니다.

   GuardDuty서비스를 사용하여 탐지기 리소스를 활성화할지 여부를 지정해야 합니다. 작동하려면 탐지기를 만들고 활성화해야 합니다. GuardDuty 초대를 수락하려면 GuardDuty 먼저 활성화해야 합니다.

   다음 CLI AWS 명령을 사용하여 명령줄 도구를 사용하여 이 작업을 수행할 수도 있습니다.

   ```
   aws guardduty create-detector --enable
   ```

2. 멤버십 초대를 수락하려는 각 AWS 계정에 대해 해당 계정의 자격 증명을 사용하여 AcceptAdministratorInvitationAPI 작업을 실행합니다.

   멤버 AWS 계정의 이 계정의 감지기 ID, 초대를 보낸 관리자 계정의 계정 ID, 수락하려는 초대의 초대 ID를 지정해야 합니다. 관리자 계정의 계정 ID는 초대 이메일에서 확인하거나 API의 ListInvitations 작업을 사용하여 찾을 수 있습니다.

   AWS 명령줄 도구를 사용하여 다음 CLI 명령을 실행하여 초대를 수락할 수도 있습니다. 유효한 탐지기 ID, 관리자 계정 ID 및 초대 ID를 사용해야 합니다.

   계정과 현재 지역의 계정을 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오. `detectorId`

   ```
   aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --administrator-id 444455556666 --invitation-
   id 84b097800250d17d1872b34c4daadcf5
   ```

GuardDuty 관리자 계정을 단일 조직 위임 GuardDuty 관리자 계정으로 통합

GuardDuty 연결을 통해 위임된 GuardDuty 관리자 계정으로 구성원 계정을 관리할 AWS Organizations 것을 권장합니다. 아래에 설명된 예제 프로세스를 사용하여 관리자 계정과 조직의 초대를 통해 연결된 구성원을 하나의 GuardDuty GuardDuty 위임된 관리자 계정으로 통합할 수 있습니다.

> **Note**
>
> 위임된 관리자 계정으로 이미 관리하고 있는 계정이나 위임된 GuardDuty 관리자 계정과 연결된 활성 구성원 계정을 다른 위임된 GuardDuty 관리자 계정에 추가할 수 없습니다. GuardDuty 각 조직은 지역당 하나의 위임된 GuardDuty 관리자 계정만 가질 수 있으며, 각 구성원 계정에는 위임된 관리자 계정을 하나만 가질 수 있습니다. GuardDuty

접근 방법 중 하나를 선택하여 GuardDuty 관리자 계정을 단일 GuardDuty 위임된 관리자 계정으로 통합하십시오.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   로그인하려면 조직의 관리 계정 보안 인증 정보를 사용합니다.
2. 관리하려는 모든 계정은 조직의 GuardDuty 일부여야 합니다. 조직에 계정을 추가하는 방법에 대한 자세한 내용은 조직에 AWS 계정 가입하도록 초대하기를 참조하십시오.
3. 모든 구성원 계정이 단일 위임 GuardDuty 관리자 계정으로 지정하려는 계정과 연결되어 있는지 확인하십시오. 기존 관리자 계정과 아직 연결되어 있는 모든 멤버 계정의 연결을 해제합니다.

   다음 단계는 기존 관리자 계정에서 회원 계정을 분리하는 데 도움이 됩니다.

   a. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
   b. 로그인하려면 기존 관리자 계정의 보안 인증 정보를 사용합니다.
   c. 탐색 창에서 Accounts(계정)를 선택합니다.
   d. 계정 페이지에서 관리자 계정과 연결을 해제할 계정을 하나 이상 선택합니다.
   e. 작업을 선택한 다음 계정 연결 해제를 선택합니다.
   f. 확인 선택하여 단계를 완료합니다.
4. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

   로그인하려면 관리 계정 보안 인증 정보를 사용합니다.
5. 탐색 창에서 설정을 선택합니다. 설정 페이지에서 조직의 위임된 GuardDuty 관리자 계정을 지정합니다.
6. 지정된 위임된 GuardDuty 관리자 계정으로 로그인합니다.

7. 조직에서 멤버를 추가합니다. 자세한 정보는 를 통한 GuardDuty 계정 관리 AWS Organizations을 참조하세요.

API/CLI

1. 관리하려는 모든 계정은 조직의 GuardDuty 일부여야 합니다. 조직에 계정을 추가하는 방법에 대한 자세한 내용은 조직에 AWS 계정 가입하도록 초대하기를 참조하십시오.
2. 모든 구성원 계정이 단일 위임 GuardDuty 관리자 계정으로 지정하려는 계정과 연결되어 있는지 확인하십시오.

   a. 기존 관리자 계정과 아직 연결되어 있는 모든 구성원 계정의 연결을 DisassociateMembers끊으려면 실행하십시오.

   b. 또는 다음 명령을 AWS Command Line Interface 실행하여 *777777777777#* 구성원 계정 연결을 끊으려는 기존 관리자 계정의 탐지기 ID로 바꿀 수 있습니다. *666666666666*을 연결 해제하려는 멤버 계정의 AWS 계정 ID로 바꿉니다.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-
   ids 666666666666
   ```

3. 를 EnableOrganizationAdminAccount실행하여 위임된 관리자 계정으로 를 위임합니다. AWS 계정 GuardDuty

   또는 다음 명령을 AWS Command Line Interface 실행하여 위임된 관리자 계정을 위임할 수 있습니다. GuardDuty

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. 조직에서 멤버를 추가합니다. 자세한 정보는 Create or add member member accounts using API을 참조하세요.

> **Important**
>
> 지역 서비스의 GuardDuty 효율성을 극대화하려면 위임된 GuardDuty 관리자 계정을 지정하고 모든 지역에 모든 구성원 계정을 추가하는 것이 좋습니다.

여러 GuardDuty 계정에서 동시에 활성화할 수 있습니다.

다음 방법을 사용하여 여러 GuardDuty 계정에서 동시에 활성화할 수 있습니다.

Python 스크립트를 사용하여 여러 GuardDuty 계정에서 동시에 활성화하세요

Amazon GuardDuty 다중 계정 스크립트의 샘플 리포지토리에 GuardDuty 있는 스크립트를 사용하여 여러 계정의 활성화 또는 비활성화를 자동화할 수 있습니다. 이 섹션의 프로세스를 사용하여 Amazon EC2를 사용하는 회원 계정 목록을 활성화할 수 GuardDuty 있습니다. 비활성화 스크립트를 사용하거나 로컬에서 스크립트를 설정하는 방법에 대한 자세한 내용은 공유 링크의 지침을 참조하십시오.

`enableguardduty.py`스크립트는 관리자 계정에서 초대를 활성화하고 GuardDuty, 초대를 보내고, 모든 구성원 계정에서 초대를 수락합니다. 그 결과 모든 구성원 GuardDuty 계정에 대한 모든 보안 탐지 결과를 포함하는 관리자 계정이 생성됩니다. 지역별로 GuardDuty 분리되어 있기 때문에 각 구성원 계정의 검색 결과는 관리자 계정의 해당 지역으로 롤업됩니다. 예를 들어 GuardDuty 관리자 계정의 us-east-1 지역에는 모든 관련 구성원 계정의 모든 us-east-1 검색 결과에 대한 보안 조사 결과가 포함됩니다.

이러한 스크립트는 AWS 관리형 정책: AmazonGuardDutyFullAccess 관리형 정책이 포함된 공유 IAM 역할에 종속되어 있습니다. 이 정책은 엔티티가 관리자 계정 GuardDuty 및 활성화하려는 각 계정에 대한 액세스 권한을 제공하며 해당 계정에 존재해야 합니다. GuardDuty

다음 프로세스는 기본적으로 사용 가능한 모든 GuardDuty 지역에서 활성화됩니다. 선택적 `--enabled_regions` 인수를 사용하고 쉼표로 구분된 지역 목록을 제공하여 지정된 GuardDuty 지역에서만 활성화할 수 있습니다. 또한 선택적으로 `enableguardduty.py`를 열고 `gd_invite_message` 문자열을 편집하여 멤버 계정으로 전송되는 초대 메시지를 사용자 지정할 수 있습니다.

1. GuardDuty 관리자 계정에서 IAM 역할을 생성하고 활성화할 정책을 연결합니다. AWS 관리형 정책: AmazonGuardDutyFullAccess GuardDuty
2. GuardDuty 관리자 계정으로 관리하려는 각 구성원 계정에 IAM 역할을 생성합니다. 이 역할은 1단계에서 만든 역할과 이름이 같아야 하고, 관리자 계정을 신뢰할 수 있는 주체로 허용해야 하며, 앞서 설명한 것과 동일한 AmazonGuardDutyFullAccess 관리형 정책을 가져야 합니다.
3. 인스턴스가 서비스 역할을 수임할 수 있도록 다음과 같은 신뢰 관계를 가지고 있는 연결된 역할로 새 Amazon Linux 인스턴스를 시작합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 새 인스턴스에 로그인하고 다음 명령을 실행하여 설정합니다.

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. 2단계에서 역할을 추가한 멤버 계정의 계정 ID 및 이메일 목록이 포함된 CSV 파일을 만듭니다. 계정은 다음 예시와 같이 한 줄에 하나씩 표시해야 하며, 계정 ID와 이메일 주소는 쉼표로 구분해야 합니다.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> CSV 파일은 enableguardduty.py 스크립트와 동일한 위치에 있어야 합니다. 다음과 같은 방법을 사용하여 기존 CSV 파일을 Amazon S3에서 현재 디렉터리로 복사할 수 있습니다.
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Python 스크립트를 실행합니다. GuardDuty 관리자 계정 ID, 첫 단계에서 만든 역할 이름, CSV 파일 이름을 인수로 제공해야 합니다.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

비용 추정 GuardDuty

GuardDuty 콘솔 또는 API 작업을 사용하여 의 일일 평균 사용 비용을 GuardDuty 추정할 수 있습니다. 30일 무료 평가판 기간 도중 비용 추정을 통해 평가판 기간 이후의 예상 비용을 예상합니다. 다중 계정 환경에서 운영하는 경우 GuardDuty 관리자 계정으로 모든 구성원 계정의 비용 지표를 모니터링할 수 있습니다.

다음 지표를 기반으로 비용 예상을 확인할 수 있습니다.

- 계정 ID — 사용자 계정 또는 GuardDuty 관리자 계정으로 운영하는 경우 회원 계정의 예상 비용을 나열합니다.
- 데이터 원본 - VPC 흐름 로그, CloudTrail 관리 로그, 데이터 이벤트 또는 DNS 로그와 같은 GuardDuty 데이터 원본 유형에 대한 지정된 CloudTrail 데이터 원본의 예상 비용을 나열합니다.
- 기능 — S3에 대한 데이터 이벤트, EKS 감사 로그 모니터링, EBS 볼륨 CloudTrail 데이터, RDS 로그인 활동, EKS 런타임 모니터링, Fargate 런타임 모니터링, EC2 런타임 모니터링 또는 Lambda 네트워크 활동 모니터링과 같은 GuardDuty 기능에 대한 지정된 데이터 소스의 예상 비용을 나열합니다.
- S3 버킷 - 지정된 버킷의 S3 데이터 이벤트에 대한 추정 비용 또는 환경의 계정에서 가장 비용이 많이 드는 버킷이 나열됩니다.

> **Note**
>
> S3 버킷 통계는 계정에서 S3 보호가 활성화된 경우에만 제공됩니다. 자세한 정보는 아마존에서의 아마존 S3 보호 GuardDuty을 참조하세요.

GuardDuty 사용 비용 계산 방법에 대한 이해

콘솔에 표시되는 예상치는 GuardDuty 콘솔에 표시된 예상 값과 약간 다를 수 있습니다 AWS Billing and Cost Management . 다음 목록은 사용 비용을 GuardDuty 추정하는 방법을 설명합니다.

- 예상 GuardDuty 사용량은 현재 지역에만 해당됩니다.
- GuardDuty 사용 비용은 지난 30일간의 사용량을 기준으로 합니다.
- 평가판 사용 비용 추정치에는 현재 평가판 기간이 진행 중인 기본 데이터 소스 및 기능에 대한 비용 추정치가 포함됩니다. 각 기능 및 데이터 GuardDuty 원본에는 자체 평가 기간이 있지만 동시에 활성화된 다른 기능 GuardDuty 또는 평가판 기간과 겹칠 수 있습니다.

- 예상 GuardDuty 사용량에는 Amazon GuardDuty Pricing 페이지에 자세히 설명된 대로 지역별 GuardDuty 대량 구매 요금 할인이 포함되지만 대량 구매 요금 티어를 충족하는 개별 계정에만 해당됩니다. 대량 요금 할인은 조직 내 계정 간 총 사용량에 대한 추정치에 포함되지 않습니다. 통합 사용량 대량 할인 요금에 대한 자세한 내용은 AWS 빌링: 대량 구매 할인을 참조하세요.
- 조직 AWS 계정 내 각 사용 비용의 합계가 선택한 데이터 원본의 최근 30일 예상 비용과 항상 같지는 않을 수 있습니다. 더 많은 이벤트 또는 데이터를 GuardDuty 처리함에 따라 가격 책정 계층이 변경될 수 있습니다. 자세한 내용은 AWS Billing 사용 설명서의 가격 책정 등급을 참조하십시오.

런타임 모니터링 — EC2 인스턴스의 VPC 흐름 로그가 사용 비용에 미치는 영향

EC2 인스턴스용 EKS 런타임 모니터링 또는 런타임 모니터링에서 보안 에이전트를 관리 (수동 또는 통해 GuardDuty) 하고 GuardDuty 현재 Amazon EC2 인스턴스에 배포되어 있고 이 수집된 런타임 이벤트 유형 인스턴스로부터 수신한 경우, 이 Amazon EC2 인스턴스의 VPC 흐름 로그 분석에 GuardDuty 대해서는 요금이 부과되지 않습니다. AWS 계정 이렇게 하면 계정에서 이중 사용 비용이 발생하는 GuardDuty 것을 방지할 수 있습니다.

CloudTrail 이벤트 사용 비용을 GuardDuty 추정하는 방법

GuardDuty활성화하면 선택한 계정에 기록된 AWS CloudTrail 이벤트 로그가 자동으로 소비되기 시작합니다 AWS 리전. GuardDuty 글로벌 서비스 이벤트 로그를 복제하고 GuardDuty 활성화한 각 지역에서 이러한 이벤트를 독립적으로 처리합니다. 이렇게 하면 각 지역의 사용자 및 역할 프로필을 GuardDuty 유지 관리하여 이상 현상을 식별하는 데 도움이 됩니다.

CloudTrail 구성은 GuardDuty 사용 비용이나 이벤트 로그 GuardDuty 처리 방식에 영향을 주지 않습니다. GuardDuty 사용 비용은 로그인한 AWS CloudTrail API 사용에 영향을 받습니다. 자세한 정보는 AWS CloudTrail 이벤트 로그을 참조하세요.

사용 통계 검토 GuardDuty

선호하는 액세스 방법을 선택하여 GuardDuty 계정의 사용 통계를 검토하세요. GuardDuty 관리자 계정인 경우 다음 방법을 사용하여 모든 구성원의 사용 통계를 검토할 수 있습니다.

Console

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.

GuardDuty 관리자 계정 계정을 사용해야 합니다.

2. 탐색 창에서 사용량을 선택합니다.
3. 사용 페이지에서 구성원 계정이 있는 GuardDuty 관리자 계정은 지난 30일간의 예상 조직 비용을 볼 수 있습니다. 이는 조직의 예상 총 사용 비용입니다.
4. GuardDuty 구성원이 있는 관리자 계정은 데이터 원본 또는 계정별 사용 비용 내역을 볼 수 있습니다. 개인 또는 독립형 계정은 데이터 소스별 내역을 볼 수 있습니다.

   멤버 계정이 있는 경우 계정 테이블에서 해당 계정을 선택하여 개별 계정의 통계를 볼 수 있습니다.

   데이터 원본별 탭에서 사용 비용이 관련된 데이터 원본을 선택할 때 계정 수준의 해당 비용 분석 합계가 항상 같지는 않을 수 있습니다.

API/CLI

GuardDuty 관리자 계정 계정의 자격 증명을 사용하여 GetUsageStatisticsAPI 작업을 실행합니다. 다음 정보를 제공하여 명령을 실행합니다.

- (필수) 통계를 검색하려는 계정의 지역 GuardDuty 탐지기 ID를 제공하십시오.
- (필수) 검색할 통계 유형 중 하나 제공: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

  현재 사용 통계 `RDS_LOGIN_EVENTS` 검색은 지원되지 `TOP_ACCOUNTS_BY_FEATURE` 않습니다.
- (필수) 사용 통계를 쿼리할 데이터 소스 또는 기능을 하나 이상 제공하십시오.
- (선택) 사용량 통계를 검색하려는 계정 ID 목록을 제공합니다.

AWS Command Line Interface도 사용할 수 있습니다. 다음 명령은 계정별로 계산된 모든 데이터 원본 및 기능에 대한 사용 통계를 검색하는 방법에 대한 예제입니다. `detector-id`를 유효한 자체 탐지기 ID로 바꿔야 합니다. 독립 실행형 계정의 경우 이 명령은 계정에 대한 지난 30일 동안의 사용량 비용만 반환합니다. 구성원 계정이 있는 GuardDuty 관리자 계정인 경우 모든 구성원의 비용이 계정별로 나열되어 있습니다.

계정 및 현재 지역에 `detectorId` 대한 정보를 찾으려면 https://console.aws.amazon.com/guardduty/ 콘솔의 설정 페이지를 참조하십시오.

사용 통계를 계산하려는 유형으로 `SUM_BY_ACCOUNT` 바꾸십시오.

데이터 소스의 비용만 모니터링하기 위함입니다.

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

기능 비용 모니터링하기

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Amazon GuardDuty의 보안

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 매우 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 AWS 규정 준수 프로그램의 일부분으로 보안 효과를 정기적으로 테스트하고 검증합니다. GuardDuty에 적용되는 규정 준수 프로그램에 대한 자세한 내용을 알아보려면 규정 준수 프로그램 제공 AWS 범위 내 서비스를 참조하세요.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스로 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 GuardDuty 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 보안 및 규정 준수 목표에 맞게 GuardDuty를 구성하는 방법을 보여줍니다. 또한 GuardDuty 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

목차

아마존에서의 데이터 보호 GuardDuty

AWS 공동 책임 모델 Amazon의 데이터 보호에 적용됩니다 GuardDuty. 이 모델에 설명된 대로 AWS은 (는) 모두를 실행하는 글로벌 인프라를 보호할 책임이 AWS 클라우드있습니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터

프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API GuardDuty 또는 AWS 서비스 SDK를 사용하거나 다른 방법으로 작업하는 경우가 포함됩니다. AWS CLI AWS 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

모든 GuardDuty 고객 데이터는 AWS 암호화 솔루션을 사용하여 유휴 상태에서 암호화됩니다.

GuardDuty 조사 결과와 같은 데이터는 고객 AWS 소유의 관리 키를 사용하여 AWS Key Management Service (AWS KMS) 를 사용하여 저장 중에 암호화됩니다.

전송 중 암호화

GuardDuty 다른 서비스의 로그 데이터를 분석합니다. HTTPS 및 KMS를 사용하는 이러한 서비스에서 전송 중에 모든 데이터를 암호화합니다. 로그에서 필요한 정보를 GuardDuty 추출한 후에는 삭제됩니다. 다른 서비스의 정보를 GuardDuty 사용하는 방법에 대한 자세한 내용은 GuardDuty 데이터 원본을 참조하십시오.

GuardDuty 서비스 간 전송 시 데이터가 암호화됩니다.

서비스 개선을 위한 데이터 사용 거부

옵트아웃 정책을 사용하여 자신의 데이터가 개발 및 개선 GuardDuty 및 기타 AWS 보안 서비스에 사용되지 않도록 선택할 수 있습니다. AWS Organizations 현재 그러한 데이터를 수집하지 GuardDuty 않더라도 옵트아웃을 선택할 수 있습니다. 옵트아웃 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AI 서비스 옵트아웃 정책을 참조하십시오.

> **Note**
>
> 옵트아웃 정책을 사용하려면 AWS 계정을 중앙에서 AWS Organizations관리해야 합니다. AWS 계정에 사용할 조직을 아직 만들지 않은 경우 AWS Organizations 사용 설명서의 조직 만들기 및 관리를 참조하십시오.

옵트아웃은 다음과 같은 효과가 있습니다.

- GuardDuty 서비스 개선을 위해 수집 및 저장한 데이터를 옵트아웃 (있는 경우) 하기 전에 삭제합니다.
- 옵트아웃한 후에는 더 이상 서비스 개선 목적으로 이 데이터를 수집하거나 저장하지 않습니다. GuardDuty

다음 항목에서는 서비스 개선을 위해 내 각 기능이 데이터를 GuardDuty 잠재적으로 처리하는 방법을 설명합니다.

내용

GuardDuty 런타임 모니터링

GuardDuty 런타임 모니터링은 사용자 환경의 Amazon Elastic Kubernetes Service (Amazon EKS) 클러스터 AWS Fargate (Fargate) , Amazon Elastic Container Service (Amazon ECS) 전용 및 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스에 대한 런타임 위협 탐지 기능을 제공합니다. AWS 런타임 모니터링을 활성화하고 리소스용 GuardDuty 보안 에이전트를 배포하면 리소스와 관련된 런타임 이벤트를 모니터링하고 분석하기 GuardDuty 시작합니다. 이러한 런타임 이벤트 유형에는 프로세스

이벤트, 컨테이너 이벤트, DNS 이벤트 등이 포함됩니다. 자세한 정보는 를 사용하는 수집된 런타임 이벤트 유형 GuardDuty 을 참조하세요.

GuardDuty Now는 워크로드에 전달할 수 있는 명령줄 인수를 수집하지만 현재는 서비스 개선 목적으로 이러한 인수를 사용하지 않습니다 (향후 사용할 수 있음). 새로운 위협 탐지 규칙 및 조사 결과가 곧 발표될 것으로 예상하여 명령줄 인수 수집을 시작했습니다. 사용자의 신뢰, 프라이버시 및 콘텐츠 보안을 최우선으로 생각하며, 약속한 대로 데이터를 사용하도록 할 것입니다. 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

GuardDuty 멀웨어 보호

GuardDuty 멀웨어 보호는 잠재적으로 손상된 Amazon EC2 인스턴스 및 컨테이너 워크로드에 연결된 EBS 볼륨에 포함된 멀웨어를 검사하고 탐지합니다. GuardDuty 멀웨어 보호 기능이 EBS 볼륨 파일을 악성이거나 유해한 것으로 식별하면 GuardDuty 멀웨어 보호 기능은 이 파일을 수집 및 저장하여 멀웨어 탐지 및 서비스를 개발하고 개선합니다. GuardDuty 이 파일은 다른 AWS 보안 서비스를 개발하고 개선하는 데에도 사용될 수 있습니다. 사용자의 신뢰, 프라이버시 및 콘텐츠 보안을 최우선으로 생각하며, 약속한 대로 데이터를 사용하도록 할 것입니다. 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

를 GuardDuty 사용하여 Amazon API 호출을 로깅합니다. AWS CloudTrail

GuardDuty Amazon은 사용자AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되어 GuardDuty 있습니다. CloudTrail GuardDuty 콘솔에서의 호출 및 API로의 코드 호출을 포함하여 GuardDuty as 이벤트에 대한 모든 API 호출을 캡처합니다 GuardDuty . 트레일을 생성하면 Amazon Simple Storage Service (Amazon S3) 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 있습니다. 여기에는 에 대한 이벤트가 포함됩니다. GuardDuty 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 GuardDuty, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 활성화 방법을 CloudTrail 비롯한 자세한 내용은 사용 AWS CloudTrail설명서를 참조하십시오.

GuardDuty 자세한 내용은 CloudTrail

CloudTrail 계정을 만들 때 AWS 계정에서 활성화됩니다. 에서 GuardDuty 지원되는 이벤트 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다.

AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

에 대한 이벤트를 포함하여 AWS 계정에서 진행 중인 이벤트의 기록을 보려면 GuardDuty 트레일을 생성하세요. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 이벤트 또는 로그 항목에는 요청을 생성한 사용자의 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청에서 루트 사용자 또는 IAM 사용자의 로그인 보안 인증 정보를 사용했는지 여부
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청했는지 여부

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

GuardDuty 의 컨트롤 플레인 이벤트 CloudTrail

기본적으로 Amazon API 참조에 제공된 모든 GuardDuty GuardDuty API 작업을 CloudTrail 파일에 이벤트로 CloudTrail 기록합니다.

GuardDuty 의 데이터 이벤트 CloudTrail

GuardDuty 런타임 모니터링는 Amazon Elastic Kubernetes Service (Amazon EKS) 클러스터, Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 및 (Amazon Elastic AWS Fargate Container Service (Amazon ECS) 전용) 작업에 배포된 GuardDuty 보안 에이전트를 사용하여 워크로드를 수집한 다음 위협 탐지 및 분석을 위해 보내는 `aws-guardduty-agent` 애드온 () 수집된 런타임 이벤트 유형 을 수집합니다. AWS GuardDuty

데이터 이벤트 로깅 및 모니터링

선택적으로 보안 에이전트에 대한 데이터 이벤트를 볼 수 있도록 AWS CloudTrail 로그를 구성할 수 있습니다. GuardDuty

생성 및 구성하려면 CloudTrail 사용 AWS CloudTrail설명서의 데이터 이벤트를 참조하고 의 고급 이벤트 선택기로 데이터 이벤트 로깅에 대한 지침을 따르십시오. AWS Management Console 트레일을 로깅하는 동안 다음을 변경해야 합니다.

- 데이터 이벤트 유형으로는 GuardDuty detector를 선택하세요.
- 로그 선택기 템플릿에서 모든 이벤트 로그를 선택합니다.
- 구성을 위해 JSON 보기를 확장합니다. 다음 JSON과 유사합니다.

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

트레일 셀렉터를 활성화한 후 https://console.aws.amazon.com/s3/ 에서 Amazon S3 콘솔로 이동합니다. CloudTrail 로그를 구성할 때 선택한 S3 버킷에서 데이터 이벤트를 다운로드할 수 있습니다.

예: GuardDuty 로그 파일 항목

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며

요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 데이터 플레인 이벤트를 보여주는 CloudTrail 로그 항목을 보여줍니다.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
```

```
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

다음 예제는 CreateIPThreatIntelSet 작업 (컨트롤 플레인 이벤트) 을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


위 이벤트 정보에서 GuardDuty에서 위협 목록 `Example`을 생성하는 요청인 것을 알 수 있습니다. 또한 Alice라는 이름의 사용자가 2018년 6월 14일에 요청을 생성한 것도 확인할 수 있습니다.

Amazon용 ID 및 Access Management GuardDuty

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. GuardDuty IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- Amazon GuardDuty 자격 증명 및 액세스 문제 해결

고객

사용하는 방식 AWS Identity and Access Management (IAM) 은 수행하는 작업에 따라 다릅니다. GuardDuty

서비스 사용자 - GuardDuty 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 GuardDuty 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. 에서 GuardDuty 기능에 액세스할 수 없는 경우 을 참조하십시오Amazon GuardDuty 자격 증명 및 액세스 문제 해결.

서비스 관리자 — 회사에서 GuardDuty 리소스를 담당하고 있다면 전체 액세스 권한이 있을 것입니다 GuardDuty. 서비스 사용자가 액세스해야 하는 GuardDuty 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해합니다. 회사에서 IAM을 어떻게 사용할 수 있는지 자세히 GuardDuty 알아보려면 을 참조하십시오아마존이 IAM과 협력하는 GuardDuty 방식.

IAM 관리자 — IAM 관리자라면 액세스 관리를 위한 정책을 작성하는 방법에 대해 자세히 알고 싶을 것입니다. GuardDuty IAM에서 사용할 수 있는 GuardDuty ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon의 ID 기반 정책 예제 GuardDuty

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용

하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용

자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 아이덴티티에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접 호출을 수행하면 일반적으로 해당 서비스는 EC2에서 애플리케이션을 실행하거나 Amazon S3에 개체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을

수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요를 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

아마존이 IAM과 협력하는 GuardDuty 방식

IAM을 사용하여 액세스를 GuardDuty 관리하기 전에 어떤 IAM 기능을 사용할 수 있는지 알아보십시오. GuardDuty

Amazon에서 사용할 수 있는 IAM 기능 GuardDuty

IAM 특성	GuardDuty 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	예
서비스 연결 역할	예

GuardDuty 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

ID 기반 정책은 다음과 같습니다. GuardDuty

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

다음에 대한 ID 기반 정책 예제 GuardDuty

GuardDuty ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon의 ID 기반 정책 예제 GuardDuty

내 리소스 기반 정책 GuardDuty

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

에 대한 정책 조치 GuardDuty

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는

권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

GuardDuty 조치 목록을 보려면 서비스 승인 GuardDuty 참조에서 Amazon이 정의한 작업을 참조하십시오.

정책 조치 중 조치 앞에 다음 접두사를 GuardDuty 사용합니다.

```
guardduty
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

GuardDuty ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon의 ID 기반 정책 예제 GuardDuty

에 대한 정책 리소스 GuardDuty

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

GuardDuty 리소스 유형 및 해당 ARN 목록을 보려면 서비스 인증 참조의 GuardDuty Amazon이 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 Amazon에서 정의한 작업을 참조하십시오. GuardDuty

GuardDuty ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon의 ID 기반 정책 예제 GuardDuty

에 대한 정책 조건 키 GuardDuty

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition`요소를 지정하거나 단일 `Condition`요소에서 여러 키를 지정하는 경우 AWS 는 논리적 `AND`태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

GuardDuty 조건 키 목록을 보려면 서비스 인증 GuardDuty 참조의 Amazon용 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 Amazon에서 정의한 작업을 참조하십시오 GuardDuty.

GuardDuty ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon의 ID 기반 정책 예제 GuardDuty

GuardDuty의 ACL(액세스 제어 목록)

ACL 지원	아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC (속성 기반 액세스 제어) 를 통한 GuardDuty

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

임시 자격 증명 사용: GuardDuty

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

서비스 간 사용자 권한: GuardDuty

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

GuardDuty의 서비스 역할

서비스 역할 지원	예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할의 권한을 변경하면 GuardDuty 기능이 중단될 수 있습니다. 서비스 역할을 편집하기 위한 지침이 GuardDuty 제공되는 경우에만 서비스 역할을 편집하십시오.

서비스 연결 역할은 다음과 같습니다. GuardDuty

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해

당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

GuardDuty 서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. Amazon의 서비스 연결 역할 사용 GuardDuty

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스 단원을 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Amazon의 ID 기반 정책 예제 GuardDuty

기본적으로 사용자와 역할에는 리소스를 생성하거나 수정할 GuardDuty 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형의 ARN 형식을 비롯하여 GuardDuty 에서 정의한 GuardDuty 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조의 Amazon용 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- GuardDuty 콘솔 사용
- GuardDuty를 활성화하는 데 필요한 권한
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 읽기 전용 액세스 권한을 부여하는 사용자 지정 IAM 정책 GuardDuty
- 조사 결과에 대한 액세스 거부 GuardDuty
- 사용자 지정 IAM 정책을 사용하여 리소스에 대한 액세스를 제한하기 GuardDuty

정책 모범 사례

ID 기반 정책은 누군가가 계정에서 GuardDuty 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

GuardDuty 콘솔 사용

Amazon GuardDuty 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 GuardDuty 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 GuardDuty 콘솔을 계속 사용할 수 있도록 하려면 엔티티에 GuardDuty `ConsoleAccess` 또는 `ReadOnly` AWS 관리형 정책도 연결하세요. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

GuardDuty를 활성화하는 데 필요한 권한

다양한 IAM ID (사용자, 그룹, 역할) 가 가져야 하는 권한을 부여하려면 필요한 AWS 관리형 정책: AmazonGuardDutyFullAccess 정책을 추가하여 활성화하십시오. GuardDuty

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

읽기 전용 액세스 권한을 부여하는 사용자 지정 IAM 정책 GuardDuty

읽기 전용 액세스 권한을 GuardDuty 부여하려면 관리형 정책을 사용할 수 있습니다. `AmazonGuardDutyReadOnlyAccess`

IAM 역할, 사용자 또는 그룹에 읽기 전용 액세스 권한을 부여하는 사용자 지정 정책을 만들려면 다음 GuardDuty 명령문을 사용할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

조사 결과에 대한 액세스 거부 GuardDuty

다음 정책을 사용하여 결과에 대한 IAM 역할, 사용자 또는 그룹 액세스를 거부할 수 있습니다. GuardDuty 사용자는 조사 결과나 조사 결과에 대한 세부 정보를 볼 수 없지만 다른 GuardDuty 모든 작업에는 액세스할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
```

```
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

사용자 지정 IAM 정책을 사용하여 리소스에 대한 액세스를 제한하기 GuardDuty

탐지기 ID를 GuardDuty 기반으로 사용자 액세스를 정의하려면 다음 작업을 제외하고 사용자 지정 IAM 정책의 모든 GuardDutyAPI 작업을 사용할 수 있습니다.

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

IAM 정책에서 다음 작업을 사용하여 IPSet ID 및 ID를 GuardDuty 기반으로 사용자 액세스를 정의하십시오. ThreatIntelSet

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

다음 예제에서는 앞의 작업 몇 가지를 사용하여 정책을 생성하는 방법을 보여줍니다.

- 이 정책에서는 사용자가 us-east-1 리전의 탐지기 ID 1234567을 사용하여 `guardduty:UpdateDetector` 작업을 실행할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- 이 정책에서는 사용자가 us-east-1 리전의 탐지기 ID 1234567 및 IPSet ID 000000을 사용하여 `guardduty:UpdateIPSet` 작업을 실행할 수 있습니다.

> **Note**
>
> 사용자가 에서 신뢰할 수 있는 IP 목록 및 위협 목록에 액세스하는 데 필요한 권한을 가지고 있는지 확인하십시오. GuardDuty 자세한 정보는 신뢰할 수 있는 IP 목록 및 위협 목록을 업로드하는 데 필요한 권한을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- 이 정책에서는 사용자가 us-east-1 리전의 모든 탐지기 ID 및 IPSet ID 000000을 사용하여 `guardduty:UpdateIPSet` 작업을 실행할 수 있습니다.

> **Note**
>
> 사용자가 에서 신뢰할 수 있는 IP 목록 및 위협 목록에 액세스하는 데 필요한 권한을 가지고 있는지 확인하십시오 GuardDuty. 자세한 정보는 신뢰할 수 있는 IP 목록 및 위협 목록을 업로드하는 데 필요한 권한을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- 이 정책에서는 사용자가 us-east-1 리전의 탐지기 ID 및 모든 IPSet ID를 사용하여 `guardduty:UpdateIPSet` 작업을 실행할 수 있습니다.

> **Note**
>
> 사용자가 에서 신뢰할 수 있는 IP 목록 및 위협 목록에 액세스하는 데 필요한 권한을 가지고 있는지 확인하십시오 GuardDuty. 자세한 정보는 신뢰할 수 있는 IP 목록 및 위협 목록을 업로드하는 데 필요한 권한을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Amazon의 서비스 연결 역할 사용 GuardDuty

GuardDuty Amazon은 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할 (SLR) 은 직접 연결되는 고유한 유형의 IAM 역할입니다. GuardDuty 서비스 연결 역할은 에 의해 GuardDuty 사전 정의되며 사용자를 대신하여 다른 서비스를 호출하는 데 GuardDuty 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 GuardDuty 추가하지 않고도 설정할 수 있습니다. GuardDuty 서비스 연결 역할의 권한을 정의하며, 권한이 달리 정의되지 않는 한 역할만 역할을 GuardDuty 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

GuardDuty 사용 가능한 모든 지역에서 서비스 연결 역할을 사용할 수 있도록 지원합니다. GuardDuty 자세한 정보는 리전 및 엔드포인트을 참조하세요.

GuardDuty 서비스 연결 역할은 활성화된 모든 GuardDuty 지역에서 먼저 비활성화한 후에만 삭제할 수 있습니다. 이렇게 하면 액세스 권한을 실수로 제거할 수 없으므로 GuardDuty 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM 사용 설명서에서 AWS IAM으로 작업하는 서비스를 살펴보고 서비스 연결 역할 열이 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

에 대한 서비스 연결 역할 권한 GuardDuty

GuardDuty 라는 이름의 서비스 연결 역할 (SLR) 을 사용합니다. `AWSServiceRoleForAmazonGuardDuty` GuardDuty SLR을 사용하면 다음 작업을 수행할 수 있습니다. 또한 EC2 인스턴스에 속하는 검색된 메타데이터를 잠재적 위협에 대해 GuardDuty 생성될 수 있는 조사 결과에 포함할 수 있습니다. GuardDuty `AWSServiceRoleForAmazonGuardDuty` 서비스 연결 역할은 역할을 수임하기 위해 `guardduty.amazonaws.com` 서비스를 신뢰합니다.

권한 정책은 다음 GuardDuty 작업을 수행하는 데 도움이 됩니다.

- Amazon EC2 작업을 사용하여 EC2 인스턴스, 이미지 및 네트워킹 구성 요소 (예: VPC, 서브넷, 전송 게이트웨이) 에 대한 정보를 관리하고 검색할 수 있습니다.
- Amazon EC2용 자동 에이전트로 런타임 모니터링을 GuardDuty 활성화하면 Amazon EC2 인스턴스에서 SSM 연결을 관리하는 AWS Systems Manager 작업을 사용하십시오. GuardDuty 자동 에이전트 구성을 비활성화하면 포함 태그 (:) 가 있는 EC2 인스턴스만 GuardDuty 고려합니다. `GuardDutyManaged true`
- AWS Organizations 작업을 사용하여 관련 계정 및 조직 ID를 설명하십시오.
- Amazon S3 작업을 사용하여 S3 버킷 및 객체에 대한 정보를 검색할 수 있습니다.
- AWS Lambda 작업을 사용하여 Lambda 함수 및 태그에 대한 정보를 검색할 수 있습니다.
- Amazon EKS 작업을 사용하여 EKS 클러스터에 대한 정보를 관리 및 검색하고, EKS 클러스터의 Amazon EKS 추가 기능을 관리합니다. EKS 작업은 연결된 태그에 대한 정보도 검색합니다. GuardDuty
- IAM을 사용하여 맬웨어 보호가 활성화된 후 맬웨어 보호에 대한 서비스 연결 역할 권한을 생성합니다.
- Amazon ECS 작업을 사용하여 Amazon ECS 클러스터에 대한 정보를 관리 및 검색하고, Amazon ECS 계정 설정을 관리할 수 있습니다. `guarddutyActivate` Amazon ECS와 관련된 작업은 연결된 태그에 대한 정보도 검색합니다. GuardDuty

역할은 다음 AWS 관리형 정책인 `AmazonGuardDutyServiceRolePolicy`를 통해 구성됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
```

```
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:security-group/*",
```

```
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
            }
```

```
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
```

```
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
```

```
            ],
            "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
}
```

다음은 AWSServiceRoleForAmazonGuardDuty 서비스 연결 역할에 연결된 신뢰 정책입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AmazonGuardDutyServiceRolePolicy 정책의 업데이트에 대한 자세한 정보는 GuardDuty 관리형 정책 업데이트 AWS 섹션을 참조하세요. 이 정책의 변경 사항에 대한 자동 알림을 받으려면 페이지의 RSS 피드를 구독하십시오. 사용 설명서 기록

에 대한 서비스 연결 역할 생성 GuardDuty

AWSServiceRoleForAmazonGuardDuty서비스 연결 역할은 처음으로 활성화하거나 이전에 GuardDuty 활성화하지 않은 지원 GuardDuty 지역에서 활성화하면 자동으로 생성됩니다. IAM 콘솔, 또는 IAM API를 사용하여 서비스 연결 역할을 수동으로 생성할 수도 있습니다. AWS CLI

> **Important**
>
> GuardDuty 위임된 관리자 계정에 대해 생성된 서비스 연결 역할은 구성원 계정에는 적용되지 않습니다. GuardDuty

IAM 보안 주체(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성해야 합니다. AWSServiceRoleForAmazonGuardDuty서비스 연결 역할을 성공적으로 생성하려면 GuardDuty 함께 사용하는 IAM 보안 주체에 필요한 권한이 있어야 합니다. 필수 권한을 부여하려면 다음 정책을 이 사용자, 그룹 또는 역할에 연결하십시오.

> **Note**
>
> 다음 예제의 샘플 *## ID#* 실제 AWS 계정 ID로 바꾸십시오.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

수동 서비스 역할 생성에 대한 자세한 내용은 IAM 사용 설명서의 서비스에 대한 역할 만들기를 참조하십시오.

에 대한 서비스 연결 역할 편집 GuardDuty

GuardDuty AWSServiceRoleForAmazonGuardDuty서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

에 대한 서비스 연결 역할 삭제 GuardDuty

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔티티가 없도록 합니다.

> **Important**
>
> 맬웨어 보호를 활성화한 경우 AWSServiceRoleForAmazonGuardDuty를 삭제해도 자동으로 AWSServiceRoleForAmazonGuardDutyMalwareProtection이 삭제되지 않습니다. AWSServiceRoleForAmazonGuardDutyMalwareProtection을 삭제하려면 맬웨어 보호에 대한 서비스 연결 역할 삭제를 참조하세요.

를 삭제하려면 먼저 활성화된 모든 GuardDuty 지역에서 비활성화해야 합니다. AWSServiceRoleForAmazonGuardDuty GuardDuty 서비스에 연결된 역할을 삭제하려고 할 때 서비스가 비활성화되지 않으면 삭제에 실패합니다. 자세한 정보는 일시 중지 또는 비활성화 GuardDuty을 참조하세요.

GuardDuty비활성화하면 이 자동으로 AWSServiceRoleForAmazonGuardDuty 삭제되지 않습니다. GuardDuty 다시 활성화하면 기존 기능을 사용하기 시작합니다AWSServiceRoleForAmazonGuardDuty.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 IAM API를 사용하여 AWSServiceRoleForAmazonGuardDuty 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

지원됨 AWS 리전

Amazon은 가능한 모든 AWS 리전 곳에서 AWSServiceRoleForAmazonGuardDuty GuardDuty 서비스 연결 역할을 사용할 수 있도록 GuardDuty 지원합니다. 현재 사용 가능한 GuardDuty 지역 목록은 의 Amazon GuardDuty 엔드포인트 및 할당량을 참조하십시오. Amazon Web Services 일반 참조

맬웨어 보호에 대한 서비스 연결 역할 권한

맬웨어 보호는 AWSServiceRoleForAmazonGuardDutyMalwareProtection이라는 서비스 연결 역할(SLR)을 사용합니다. 이 SLR을 사용하면 멀웨어 보호 기능이 에이전트 없이 스캔을 수행하여 계정에서 멀웨어를 탐지할 수 있습니다. GuardDuty GuardDuty 이를 통해 계정에서 EBS 볼륨 스냅샷을 생성하고 해당 스냅샷을 서비스 계정과 공유할 수 있습니다. GuardDuty 스냅샷을 GuardDuty 평가

한 후에는 검색된 EC2 인스턴스 및 컨테이너 워크로드 메타데이터가 멀웨어 보호 결과에 포함됩니다. AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할은 역할을 수임하기 위해 malware-protection.guardduty.amazonaws.com 서비스를 신뢰합니다.

이 역할에 대한 권한 정책은 멀웨어 보호가 다음 작업을 수행하는 데 도움이 됩니다.

- Amazon Elastic Compute Cloud (Amazon EC2) 작업을 사용하여 Amazon EC2 인스턴스, 볼륨 및 스냅샷에 대한 정보를 검색할 수 있습니다. 맬웨어 보호는 또한 Amazon EKS 및 Amazon ECS 클러스터 메타데이터에 액세스할 수 있는 권한을 제공합니다.
- GuardDutyExcluded 태그가 true로 설정되지 않은 EBS 볼륨의 스냅샷을 생성합니다. 기본적으로 스냅샷은 GuardDutyScanId 태그로 생성됩니다. 이 태그를 제거하면 안 됩니다. 제거하면 맬웨어 보호에서 스냅샷에 액세스할 수 없습니다.

  > **Important**
  >
  > GuardDutyExcluded로 true 설정하면 GuardDuty 서비스가 향후 이러한 스냅샷에 액세스할 수 없게 됩니다. 이는 이 서비스 연결 역할의 다른 명령문이 GuardDuty 로 설정된 스냅샷에 대해 어떤 작업도 수행하지 못하도록 하기 때문입니다. GuardDutyExcluded true

- GuardDutyScanId 태그가 존재하고 GuardDutyExcluded 태그가 true로 설정되지 않은 경우에만 스냅샷 공유 및 삭제를 허용합니다.

  > **Note**
  >
  > 맬웨어 보호에서 스냅샷 공개를 허용하지 않습니다.

- GuardDutyExcluded태그가 로 설정된 키를 제외한 고객 관리 키에 액세스하여 CreateGrant 호출하여 true 서비스 계정과 공유되는 암호화된 스냅샷에서 암호화된 EBS 볼륨을 생성하고 액세스할 수 있습니다. GuardDuty 각 지역의 GuardDuty 서비스 계정 목록은 을 참조하십시오GuardDuty 서비스 계정 기준 AWS 리전.
- 고객의 CloudWatch 로그에 액세스하여 멀웨어 보호 로그 그룹을 생성하고 멀웨어 스캔 이벤트 로그를 /aws/guardduty/malware-scan-events 로그 그룹 아래에 배치합니다.
- 고객이 맬웨어가 탐지된 스냅샷을 계정에 보관할지 여부를 결정하도록 허용합니다. 검사 결과 멀웨어가 탐지되면 서비스 연결 역할을 통해 스냅샷에 두 개의 태그 (및) GuardDuty 를 추가할 수 있습니다. GuardDutyFindingDetected GuardDutyExcluded

> **Note**
>
> `GuardDutyFindingDetected` 태그는 스냅샷에 맬웨어가 포함되어 있음을 나타냅니다.

- 볼륨이 EBS 관리 키로 암호화되었는지 확인하십시오. GuardDuty 계정의 EBS 관리 키를 확인하는 `DescribeKey` 작업을 수행합니다. `key Id`
- 에서 AWS 관리형 키, 를 사용하여 암호화된 EBS 볼륨의 스냅샷을 가져와서 에 복사합니다 AWS 계정 . GuardDuty 서비스 계정 이를 위해 권한 `GetSnapshotBlock` 및 을 사용합니다. `ListSnapshotBlocks` GuardDuty 그런 다음 서비스 계정의 스냅샷을 스캔합니다. 암호화된 EBS 볼륨 스캔을 위한 멀웨어 방지 지원은 현재 일부 버전에서 제공되지 AWS 관리형 키 않을 수 있습니다. AWS 리전자세한 정보는 리전별 기능 가용성을 참조하세요.
- Amazon EC2가 멀웨어 보호를 AWS KMS 대신하여 고객 관리 키에 대해 여러 암호화 작업을 수행하도록 요청하도록 허용합니다. 고객 관리 키로 암호화된 스냅샷을 공유하려면 `kms:ReEncryptTo` 및 `kms:ReEncryptFrom` 등의 작업이 필요합니다. `GuardDutyExcluded` 태그가 `true`로 설정되지 않은 키에만 액세스할 수 있습니다.

역할은 다음 AWS 관리형 정책인 `AmazonGuardDutyMalwareProtectionServiceRolePolicy`를 통해 구성됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
```

```
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
```

```
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "PreventPublicAccessToSnapshotPermission",
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Add/group": "all"
                }
            }
        },
        {
            "Sid": "CreateGrantPermission",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*"
```

```
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "ShareSnapshotKMSPermission",
            "Effect": "Allow",
            "Action": [
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "ec2.*.amazonaws.com"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "GuardDutyLogGroupPermission",
            "Effect": "Allow",
            "Action": [
```

```
                "logs:DescribeLogGroups",
                "logs:CreateLogGroup",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
        },
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

다음은 AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할에 연결된 신뢰 정책입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

맬웨어 보호에 대한 서비스 연결 역할 생성

AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할은 처음으로 맬웨어 보호를 활성화하거나 이전에 활성화하지 않은 지원 리전에서 맬웨어 보호를 활성화할 때 자동으로 생성됩니다. 또한 IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할을 수동으로 생성할 수 있습니다.

> **Note**
>
> GuardDutyAmazon을 처음 사용하는 경우 기본적으로 멀웨어 방지가 자동으로 활성화됩니다.

> **Important**
>
> 위임된 GuardDuty 관리자 계정에 대해 생성된 서비스 연결 역할은 구성원 계정에는 적용되지 않습니다. GuardDuty

IAM 보안 주체(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성해야 합니다. AWSServiceRoleForAmazonGuardDutyMalwareProtection서비스 연결 역할을 성공적으로 생성하려면 사용하는 GuardDuty IAM ID에 필요한 권한이 있어야 합니다. 필수 권한을 부여하려면 다음 정책을 이 사용자, 그룹 또는 역할에 연결하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

수동 서비스 역할 생성에 대한 자세한 내용은 IAM 사용 설명서의 서비스에 대한 역할 만들기를 참조하세요.

맬웨어 보호에 대한 서비스 연결 역할 편집

맬웨어 보호에서는 AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할 편집을 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

맬웨어 보호에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔티티가 없도록 합니다.

> **Important**
>
> AWSServiceRoleForAmazonGuardDutyMalwareProtection 삭제를 위해 활성화된 모든 리전에서 맬웨어 보호를 비활성화해야 합니다.
> 서비스 연결 역할을 삭제하려고 할 때 맬웨어 보호가 비활성화되지 않는 경우 삭제에 실패합니다. 자세한 정보는 GuardDuty시작된 멀웨어 검사를 활성화 또는 비활성화하려면을 참조하세요.

비활성화를 선택하여 맬웨어 보호 서비스를 중지하면 AWSServiceRoleForAmazonGuardDutyMalwareProtection이 자동으로 삭제되지 않습니다. 그런 다음 활성화를 선택하여 멀웨어 보호 서비스를 다시 시작하면 기존 서비스를 사용하기 시작합니다. GuardDuty AWSServiceRoleForAmazonGuardDutyMalwareProtection

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔, AWS CLI 또는 IAM API를 사용하여 서비스 연결 역할을 삭제합니다AWSServiceRoleForAmazonGuardDutyMalwareProtection. 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

지원됨 AWS 리전

GuardDuty Amazon은 멀웨어 AWS 리전 방지가 제공되는 모든 지역에서 AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할을 사용할 수 있도록 지원합니다.

현재 사용 가능한 GuardDuty 지역 목록은 의 Amazon GuardDuty 엔드포인트 및 할당량을 참조하십시오. Amazon Web Services 일반 참조

> **Note**
>
> 멀웨어 방지는 현재 AWS GovCloud (미국 동부) 및 (미국 서부) 에서 사용할 수 없습니다. AWS GovCloud

AWS 아마존 관리형 정책 GuardDuty

사용자, 그룹, 역할에 권한을 추가하려면 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의AWS 관리형 정책을 참조하십시오.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스가 새 기능을 지원하기 위해 AWS 관리형 정책에 권한을 추가하는 경우가 있습니다. 이 타입의 업데이트는 정책이 연결된 모든 보안 인증(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새 기능이 출시되거나 새 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonGuardDutyFullAccess

`AmazonGuardDutyFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 사용자에게 모든 GuardDuty 작업에 대한 전체 액세스를 허용하는 관리자 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `GuardDuty`— 사용자에게 모든 GuardDuty 작업에 대한 전체 액세스를 허용합니다.
- `IAM`— 사용자가 GuardDuty 서비스 연결 역할을 생성할 수 있습니다. 이를 통해 GuardDuty 관리자는 구성원 계정을 활성화할 수 있습니다 GuardDuty .
- `Organizations`— 사용자가 조직의 위임된 관리자를 지정하고 구성원을 관리할 수 있습니다 GuardDuty .

AWSServiceRoleForAmazonGuardDutyMalwareProtection에서 iam:GetRole 작업을 수행하는 권한은 맬웨어 보호에 대한 서비스 연결 역할(SLR)이 계정에 있는지 여부를 설정합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
```

```
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

AWS 관리형 정책: AmazonGuardDutyReadOnlyAccess

`AmazonGuardDutyReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 사용자에게 GuardDuty 조직의 GuardDuty 조사 결과 및 세부 정보를 볼 수 있는 읽기 전용 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `GuardDuty`— 사용자가 GuardDuty 결과를 보고 `GetList`, 또는 `Describe` 로 시작하는 API 작업을 수행할 수 있습니다.
- `Organizations`— 사용자가 위임된 관리자 계정의 세부 정보를 포함하여 GuardDuty 조직 구성에 대한 정보를 검색할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AmazonGuardDutyServiceRolePolicy

`AmazonGuardDutyServiceRolePolicy`를 IAM 엔터티에 연결할 수 없습니다. 이 AWS 관리형 정책은 사용자를 GuardDuty 대신하여 작업을 수행할 수 있는 서비스 연결 역할에 연결됩니다. 자세한 정보는 에 대한 서비스 연결 역할 권한 GuardDuty을 참조하세요.

GuardDuty 관리형 정책 업데이트 AWS

이 서비스가 이러한 변경 사항을 추적하기 시작한 GuardDuty 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 GuardDuty 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AmazonGuardDutyServiceRolePolicy - 기존 정책에 대한 업데이트	Amazon EC2용 자동 에이전트로 런타임 모니터링을 GuardDuty 활성화하면 Amazon EC2 인스턴스에서 SSM 연결을 관리하는 AWS Systems Manager 작업을 사용하십시오. GuardDuty 자동 에이전트 구성을 비활성화하면 포함 태그 (:) 가 있는 EC2 인스턴스만 GuardDuty 고려합니다. `GuardDutyManaged true`	2024년 3월 26일

변경 사항	설명	날짜
AmazonGuardDutyServiceRolePolicy - 기존 정책에 대한 업데이트	GuardDuty 공유 Amazon VPC 계정의 조직 ID를 검색하고 조직 ID를 `organization:DescribeOrganization` 사용하여 Amazon VPC 엔드포인트 정책을 설정할 수 있는 새 권한을 추가했습니다.	2024년 2월 9일
AmazonGuardDutyMalwareProtectionServiceRolePolicy - 기존 정책에 대한 업데이트	멀웨어 보호 기능은 두 가지 `GetSnapshotBlock` 권한을 추가했습니다. 하나는 악성코드 스캔을 시작하기 전에 사용자로부터 EBS 볼륨의 스냅샷 (을 사용하여 AWS 관리형 키암호화됨) 을 AWS 계정 가져와 GuardDuty 서비스 계정에 복사하는 것입니다. `ListSnapshotBlocks`	2024년 1월 25일
AmazonGuardDutyServiceRolePolicy-기존 정책 업데이트	`guardduty Activate` Amazon ECS 계정 설정을 추가하고 Amazon ECS 클러스터에서 목록 작성 및 설명 작업을 수행할 수 있는 새 권한이 추가되었습니다. GuardDuty	2023년 11월 26일
AmazonGuardDutyReadOnlyAccess-기존 정책 업데이트	GuardDuty `organizations` 에 `ListAccounts` 대한 새 정책이 추가되었습니다.	2023년 11월 16일
AmazonGuardDutyFullAccess-기존 정책 업데이트	GuardDuty to에 새 정책을 추가했습니다`ListAccounts` . `organizations`	2023년 11월 16일

변경 사항	설명	날짜
AmazonGuardDutyServiceRolePolicy-기존 정책 업데이트	GuardDuty 곧 출시될 GuardDuty EKS 런타임 모니터링 기능을 지원하는 새 권한이 추가되었습니다.	2023년 3월 8일
AmazonGuardDutyServiceRolePolicy-기존 정책 업데이트	GuardDuty 멀웨어 방지를 위한 서비스 연결 역할을 생성할 수 GuardDuty 있는 새 권한이 추가되었습니다. 이렇게 하면 멀웨어 보호를 활성화하는 프로세스를 GuardDuty 간소화하는 데 도움이 됩니다. GuardDuty 이제 다음과 같은 IAM 작업을 수행할 수 있습니다. `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	2023년 2월 21일

변경 사항	설명	날짜
AmazonGuardDutyFullAccess- 기존 정책 업데이트	GuardDuty 에 대한 `iam:GetRole` ARN이 업데이트되었습니다. `*AWSServiceRoleForAmazonGuardDutyMalwareProtection`	2022년 7월 26일
AmazonGuardDutyFullAccess- 기존 정책 업데이트	GuardDuty GuardDuty 멀웨어 보호 서비스를 사용하여 `iam:CreateServiceLinkedRole` 서비스 연결 역할을 생성할 수 있는 새로운 `AWSServiceName` 기능이 추가되었습니다. GuardDuty 이제 정보를 얻기 위한 `iam:GetRole` 작업을 수행할 수 있습니다. `AWSServiceRole`	2022년 7월 26일

변경 사항	설명	날짜
AmazonGuardDutyServiceRolePolicy-기존 정책 업데이트	GuardDuty Amazon EC2 네트워킹 작업을 GuardDuty 사용하여 결과를 개선할 수 있는 새로운 권한이 추가되었습니다. GuardDuty 이제 다음 EC2 작업을 수행하여 EC2 인스턴스가 통신하는 방식에 대한 정보를 얻을 수 있습니다. 이 정보는 결과 정확도 개선에 사용됩니다. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	2021년 8월 3일
GuardDuty 변경 사항 추적을 시작했습니다.	GuardDuty AWS 관리형 정책의 변경 사항 추적을 시작했습니다.	2021년 8월 3일

Amazon GuardDuty 자격 증명 및 액세스 문제 해결

다음 정보를 사용하면 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 GuardDuty 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 다음과 같은 작업을 수행할 권한이 없습니다. GuardDuty
- 저는 PassRole iam:을 수행할 권한이 없습니다.
- 외부 사용자가 내 GuardDuty 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

저는 다음과 같은 작업을 수행할 권한이 없습니다. GuardDuty

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojacksonIAM 사용자가 콘솔을 사용하여 가상 *my-example-widget*리소스에 대한 세부 정보를 보려고 하지만 가상 guardduty:*GetWidget*권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

이 경우 guardduty:*GetWidget*작업을 사용하여 *my-example-widget*리소스에 액세스할 수 있도록 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 PassRole iam:을 수행할 권한이 없습니다.

작업을 수행할 권한이 없다는 오류가 발생하는 경우 역할을 넘길 수 있도록 정책을 업데이트해야 합니다. iam:PassRole GuardDuty

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 이라는 IAM 사용자가 콘솔을 사용하여 작업을 marymajor 수행하려고 할 때 발생합니다. GuardDuty 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 GuardDuty 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 이러한 기능의 GuardDuty 지원 여부를 알아보려면 을 참조하십시오아마존이 IAM과 협력하는 GuardDuty 방식.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

Amazon에 대한 규정 준수 검증 GuardDuty

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Amazon GuardDuty의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

Amazon GuardDuty의 인프라 보안

관리형 서비스인 Amazon GuardDuty는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 호출을 사용하여 네트워크를 통해 GuardDuty에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

GuardDuty와의 AWS 서비스 통합

GuardDuty는 다른 AWS 보안 서비스와 통합할 수 있습니다. 이러한 서비스를 통해 GuardDuty에서 데이터를 수집하여 새로운 방식으로 결과를 확인할 수 있습니다. GuardDuty에서 사용하도록 각 서비스를 설정하는 방식에 대해 자세히 알아보려면 다음 통합 옵션을 검토하세요.

AWS Security Hub와의 GuardDuty 통합

AWS Security Hub는 AWS 계정, 서비스 및 지원되는 타사 파트너 제품에서 보안 데이터를 수집하여 업계 표준 및 모범 사례에 따라 환경의 보안 상태를 평가합니다. 보안 태세 평가 외에도 Security Hub는 모든 통합 AWS 서비스 및 AWS 파트너 제품에 대한 결과를 중앙에서 확인할 수 있는 위치를 생성합니다. GuardDuty에서 Security Hub를 활성화하면 GuardDuty 결과 데이터를 Security Hub에서 자동으로 수집할 수 있습니다.

GuardDuty에서의 Security Hub 사용에 대한 자세한 내용은 와의 통합 AWS Security Hub 섹션을 참조하세요.

Amazon Detective와의 GuardDuty 통합

Amazon Detective는 AWS 계정의 로그 데이터를 사용하여 환경과 상호 작용하는 리소스 및 IP 주소에 대한 데이터 시각화를 생성합니다. Detective의 시각화를 통해 보안 문제를 빠르고 쉽게 조사할 수 있습니다. 두 서비스가 모두 활성화되면 GuardDuty 결과 세부 정보를 Detective 콘솔의 정보로 피벗할 수 있습니다.

GuardDuty에서의 Detective 사용에 대한 자세한 내용은 Amazon Detective와 통합 섹션을 참조하세요.

와의 통합 AWS Security Hub

AWS Security Hub에서는 AWS 에서 보안 상태를 포괄적으로 파악할 수 있으며 보안 업계 표준 및 모범 사례와 비교하여 환경을 확인할 수 있습니다. Security Hub는 AWS 계정, 서비스 및 지원되는 타사 파트너 제품 전반에서 보안 데이터를 수집하여 보안 동향을 분석하고 가장 우선순위가 높은 보안 문제를 식별할 수 있도록 지원합니다.

Amazon과 Security Hub의 GuardDuty 통합을 통해 보안 허브에서 GuardDuty 조사 결과를 전송할 수 있습니다. 그러면 Security Hub의 보안 태세 분석에 이러한 결과가 포함됩니다.

목차

Amazon에서 조사 결과를 GuardDuty 다음 주소로 보내는 방법 AWS Security Hub

AWS Security Hub에서는 보안 문제가 발견으로 추적됩니다. 일부 결과는 다른 AWS 서비스나 타사 파트너가 감지한 문제에서 비롯됩니다. Security Hub에는 보안 문제를 감지하고 조사 결과를 생성하는 데 사용하는 규칙 집합도 있습니다.

Security Hub는 이러한 모든 출처를 총망라하여 조사 결과를 관리할 도구를 제공합니다. 사용자는 조사 결과 목록을 조회하고 필터링할 수 있으며 주어진 조사 결과의 세부 정보를 조회할 수도 있습니다. 자세한 내용은 AWS Security Hub User Guide의 Viewing findings를 참조하세요. 또한 주어진 결과에 대한 조사 상태를 추적할 수도 있습니다. 자세한 내용은 AWS Security Hub User Guide의 Taking action on findings를 참조하세요.

Security Hub의 모든 검색 결과는 AWS 보안 검색 결과 형식 (ASFF) 이라는 표준 JSON 형식을 사용합니다. ASFF에는 문제의 출처, 영향을 받은 리소스와 결과의 현재 상태 등에 관한 세부 정보가 포함됩니다. AWS Security Hub 사용 설명서에서 AWS Security Finding 형식(ASFF)을 참조하세요.

GuardDuty Amazon은 조사 결과를 Security Hub로 보내는 AWS 서비스 중 하나입니다.

Security Hub로 GuardDuty 보내는 검색 결과 유형

동일한 계정 내에서 Security Hub를 GuardDuty 활성화하고 나면 생성된 모든 검색 결과를 Security Hub로 보내기 GuardDuty 시작합니다. AWS 리전이러한 검색 결과는 보안 검색 결과 형식 (ASFF) 을 사용하여AWS Security Hub에 전송됩니다. ASFF의 경우, `Types` 필드가 결과 유형을 제공합니다.

새 검색 결과 전송 지연 시간

새 검색 결과가 GuardDuty 생성되면 일반적으로 5분 이내에 Security Hub로 전송됩니다.

Security Hub를 사용할 수 없을 때 다시 시도

Security Hub를 사용할 수 없는 경우 결과를 수신할 때까지 전송을 GuardDuty 재시도합니다.

Security Hub에서 기존 조사 결과 업데이트

검색 결과를 Security Hub로 보낸 후 검색 결과 활동에 대한 추가 관찰 내용을 반영하는 업데이트를 Security Hub에 GuardDuty 보냅니다. 이러한 결과에 대한 새로운 관찰 결과는 사용자의 5단계 — 업데이트 빈도 내보내기 설정에 따라 Security Hub로 전송됩니다 AWS 계정.

검색 결과를 보관하거나 보관 취소하는 경우 Security Hub에 해당 검색 결과를 보내지 GuardDuty 않습니다. 수동으로 보관하지 않은 검색 결과가 나중에 활성화되면 Security GuardDuty Hub로 전송되지 않습니다.

에서 결과 보기 GuardDuty AWS Security Hub

Security Hub에서 GuardDuty 조사 결과를 보려면 요약 페이지에서 GuardDutyAmazon의 조사 결과 보기를 선택하십시오. 또는 탐색 패널에서 검색 결과를 선택하고 값이 인 제품 이름: 필드를 선택하여 GuardDuty 검색 결과만 표시하도록 검색 결과를 필터링할 수 `GuardDuty` 있습니다.

에서 GuardDuty 찾은 이름 해석 AWS Security Hub

GuardDuty ASFF (보안 검색 결과 형식) 를 사용하여 검색 결과를AWS Security Hub에 보냅니다. ASFF의 경우, `Types` 필드가 결과 유형을 제공합니다. ASFF 유형은 유형과는 다른 이름 지정 체계를 사용합니다. GuardDuty 아래 표에는 Security Hub에 나타나는 ASFF와 관련된 모든 GuardDuty 검색 결과 유형이 자세히 설명되어 있습니다.

> **Note**
>
> 일부 GuardDuty 검색 유형의 경우 Security Hub는 검색 결과 세부 정보의 리소스 역할이 ACTOR 또는 TARGET인지에 따라 다른 ASFF 검색 결과 이름을 할당합니다. 자세한 내용은 결과 세부 정보단원을 참조하세요.

GuardDuty 검색 유형	ASFF 결과 유형
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B

GuardDuty 검색 유형	ASFF 결과 유형
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS

GuardDuty 검색 유형	ASFF 결과 유형
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion검색 유형 ----sep----:IAM 사용자/ AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
검색: IAM 사용자/ AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked

GuardDuty 검색 유형	ASFF 결과 유형
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile

GuardDuty 검색 유형	ASFF 결과 유형
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation

GuardDuty 검색 유형	ASFF 결과 유형
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
영향: IAM 사용자/ AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual

GuardDuty 검색 유형	ASFF 결과 유형
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess영향: IAM 사용자/ ----9월 ----: IAM 사용자/ AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
지속성: IAM 사용자/ AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted

GuardDuty 검색 유형	ASFF 결과 유형
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation지속성: 아이엠유저/ ----셉----:아이엠유저/ AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort

GuardDuty 검색 유형	ASFF 결과 유형
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic

GuardDuty 검색 유형	ASFF 결과 유형
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS

GuardDuty 검색 유형	ASFF 결과 유형
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B

GuardDuty 검색 유형	ASFF 결과 유형
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom

GuardDuty 검색 유형	ASFF 결과 유형
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

GuardDuty의 일반적 결과

GuardDuty ASFF (보안 검색 결과 형식) 를 사용하여AWS Security Hub에 검색 결과를 보냅니다.

다음은 에서 GuardDuty 찾은 일반적인 결과의 예입니다.


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
```

```
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
```

```
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


통합 활성화 및 구성

와의 AWS Security Hub통합을 사용하려면 Security Hub를 활성화해야 합니다. Security Hub를 활성화하는 방법에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 Security Hub 설정을 참조하세요.

Security GuardDuty Hub와 둘 다 활성화하면 통합이 자동으로 활성화됩니다. GuardDuty검색 결과를 Security Hub에 즉시 보내기 시작합니다.

Security Hub로의 결과 게시 중지

Security Hub로 결과를 전송하는 작업을 중지하려면 Security Hub 콘솔 또는 API를 사용하면 됩니다.

사용 설명서의 통합 결과 흐름 비활성화 및 활성화 (콘솔) 또는 통합 결과 흐름 비활성화 (Security Hub API, AWS CLI) 를 참조하십시오.AWS Security Hub

Amazon Detective와 통합

Amazon Detective는 시간 경과에 따른 리소스 동작 및 상호 작용을 나타내는 데이터 시각화를 생성하여 하나 이상의 AWS 계정에서 발생하는 보안 이벤트를 신속하게 분석하고 조사하는 데 도움을 줍니다. Detective는 GuardDuty 결과의 시각화를 생성합니다.

Detective는 모든 결과 유형에 대해 결과 세부 정보를 수집하고, 엔터티 프로파일에 대한 액세스를 제공하여 결과와 관련된 다양한 엔터티를 조사합니다. 엔터티는 AWS 계정, 계정 내 AWS 리소스 또는 리소스와 상호 작용한 외부 IP 주소일 수 있습니다. GuardDuty 콘솔은 결과 유형에 따라 AWS 계정, IAM 역할, 사용자 또는 역할 세션, 사용자 에이전트, 페더레이션 사용자, Amazon EC2 인스턴스 또는 IP 주소 등 엔터티에서 Amazon Detective로의 피벗을 지원합니다.

목차

통합 활성화

GuardDuty에서 Amazon Detective를 사용하려면 먼저 Amazon Detective를 활성화해야 합니다. Detective를 활성화하는 방법에 대한 자세한 내용은 Amazon Detective 관리 안내서의 Setting up Amazon Detective를 참조하세요.

GuardDuty와 Detective를 모두 활성화하면 통합이 자동으로 활성화됩니다. 활성화되면 Detective는 GuardDuty 결과 데이터를 즉시 수집합니다.

> **Note**
>
> GuardDuty는 GuardDuty 결과 내보내기 빈도에 따라 결과를 Detective로 보냅니다. 기본적으로 기존 결과 업데이트의 내보내기 빈도는 6시간입니다. Detective가 결과에 대한 최신 업데이트를 받을 수 있도록 하려면 GuardDuty에서 Detective를 사용하는 각 리전의 내보내기 빈도를 15분으로 변경하는 것이 좋습니다. 자세한 내용은 5단계 — 업데이트된 활성 결과를 내보내는 빈도 설정 단원을 참조하세요.

GuardDuty 결과에서 Amazon Detective로 피벗

1. https://console.aws.amazon.com/guardduty/ 콘솔에 로그인합니다.
2. 결과 표에서 단일 결과를 선택합니다.
3. 결과 세부 정보 창에서 Detective를 통해 조사를 선택합니다.
4. Amazon Detective를 통해 조사할 결과의 부분을 선택합니다. 그러면 해당 결과 또는 엔터티에 대한 Detective 콘솔이 열립니다.

피벗이 예상대로 작동하지 않는 경우 Amazon Detective 사용 설명서의 피벗 문제 해결을 참조하세요.

> **Note**
>
> Detective 콘솔에 GuardDuty 결과를 보관하는 경우 해당 결과는 GuardDuty 콘솔에도 보관됩니다.

GuardDuty 다중 계정 환경과의 통합 사용

GuardDuty에서 다중 계정 환경을 관리하는 경우 Amazon Detective에 멤버 계정을 추가해야 해당 계정의 결과 및 엔터티에 대한 Detective 데이터 시각화를 볼 수 있습니다.

Detective의 관리자 계정과 동일한 GuardDuty 관리자 계정을 사용하는 것이 좋습니다. Detective에서 멤버 계정을 추가하는 방법에 대한 자세한 내용은 멤버 계정 초대를 참조하세요.

> **Note**
>
> Detective는 리전 서비스이므로 Detective를 활성화하고 통합을 사용하려는 각 리전에 멤버 계정을 추가해야 합니다.

일시 중지 또는 비활성화 GuardDuty

GuardDuty 콘솔을 사용하여 GuardDuty 서비스를 일시 중지하거나 비활성화할 수 있습니다. 서비스가 일시 중지된 GuardDuty 경우에는 사용 요금이 부과되지 않습니다.

- 일시 중지하거나 비활성화하려면 먼저 모든 회원 계정을 연결 GuardDuty 해제하거나 삭제해야 합니다.
- 일시 GuardDuty 중지하면 더 이상 AWS 환경의 보안을 모니터링하거나 새로운 검색 결과를 생성하지 않습니다. 기존 조사 결과는 그대로 유지되며 GuardDuty 일시 중단의 영향을 받지 않습니다. 나중에 다시 GuardDuty 활성화하도록 선택할 수 있습니다.
- GuardDuty 계정에서 비활성화하면 현재 선택한 AWS 리전계정에서만 비활성화됩니다. 완전히 GuardDuty 비활성화하려면 활성화된 각 지역에서 비활성화해야 합니다.
- GuardDuty비활성화하면 기존 검색 결과 및 GuardDuty 구성이 손실되고 복구할 수 없습니다. 기존 검색 결과를 저장하려면 비활성화를 확인하기 전에 기존 검색 결과를 내보내야 GuardDuty 합니다. 결과를 내보내는 방법에 대한 자세한 내용은 결과 내보내기 섹션을 참조하세요.

일시 중지 또는 비활성화하기 GuardDuty

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 일시 중지 GuardDuty 섹션에서 일시 중지 GuardDuty 또는 비활성화를 GuardDuty 선택한 다음 작업을 확인합니다.

일시 중지 GuardDuty 후 다시 활성화하려면

1. https://console.aws.amazon.com/guardduty/ 에서 GuardDuty 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. [다시 활성화 GuardDuty] 를 선택합니다.

Amazon SNS GuardDuty 공지 구독하기

이 섹션에서는 새로 릴리스된 검색 결과 유형에 대한 알림 수신, 기존 검색 결과 유형에 대한 업데이트 및 기타 기능 변경 GuardDuty 사항에 대한 알림을 받기 위한 Amazon SNS (Simple Notification Service) 구독에 대한 정보를 제공합니다. 알림은 Amazon SNS에서 지원하는 모든 형식으로 사용할 수 있습니다.

GuardDuty SNS는 구독한 모든 계정을 통해 GuardDuty 서비스 업데이트에 대한 AWS 공지를 전송합니다. 계정 내 결과에 대한 알림을 받으려면 Amazon CloudWatch Events를 사용하여 GuardDuty 결과에 대한 사용자 지정 응답 생성 섹션을 참조하세요.

> **Note**
>
> IAM 사용자에 `sns::subscribe` 권한이 있어야 SNS 구독이 가능합니다.

알림 주제에 대해 Amazon SQS 대기열을 구독할 수 있지만 동일한 리전에 있는 주제 ARN을 사용해야 합니다. 자세한 내용은 Amazon Simple Queue Service 개발자 안내서에서 자습서: Subscribing an Amazon SQS queue to an Amazon SNS topic 섹션을 참조하세요.

알림이 수신되면 AWS Lambda 함수를 사용하여 이벤트를 트리거할 수도 있습니다. 자세한 내용은 Amazon Simple Queue Service 개발자 안내서에서 Invoking Lambda functions using Amazon SNS notifications 섹션을 참조하세요.

각 리전에 대한 Amazon SNS 주제 ARN은 다음과 같습니다.

AWS 지역	Amazon SNS 주제 ARN
us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements
us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements

AWS 지역	Amazon SNS 주제 ARN
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements

AWS 지역	Amazon SNS 주제 ARN
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements

AWS 지역	Amazon SNS 주제 ARN
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements

AWS 지역	Amazon SNS 주제 ARN
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements

AWS 지역	Amazon SNS 주제 ARN
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

GuardDuty 업데이트 알림 이메일을 구독하려면 AWS Management Console

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 리전 목록에서 구독할 주제 ARN과 동일한 리전을 선택합니다. 이 예에서는 us-west-2 리전을 사용합니다.
3. 왼쪽 탐색 창에서 구독과 구독 생성을 선택합니다.
4. 구독 생성 대화 상자의 주제 ARN에 업데이트 주제 ARN: arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements를 붙여 넣습니다.
5. 프로토콜에서 이메일을 선택합니다. 엔드포인트에서 알림을 받는 데 사용할 수 있는 이메일 주소를 입력합니다.
6. 구독 생성을 선택합니다.
7. 이메일 애플리케이션에서 AWS 알림의 메시지를 열고 링크를 열어 구독을 확인합니다.

   웹 브라우저에 Amazon SNS의 확인 응답이 표시됩니다.

다음을 포함하는 GuardDuty 업데이트 알림 이메일을 구독하려면 AWS CLI

1. AWS CLI와 함께 다음 명령을 실행합니다.

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. 이메일 애플리케이션에서 AWS 알림의 메시지를 열고 링크를 열어 구독을 확인합니다.

웹 브라우저에 Amazon SNS의 확인 응답이 표시됩니다.

Amazon SNS 메시지 형식

새로운 결과에 대한 GuardDuty 업데이트 알림 메시지의 예는 다음과 같습니다.

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

구문 분석 메시지 값(이스케이프된 따옴표 제거)은 다음과 같습니다.

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
```

```
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

GuardDuty 기능 GuardDuty 업데이트에 대한 업데이트 알림 메시지의 예는 다음과 같습니다.

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_cloudtrail\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

구문 분석 메시지 값(이스케이프된 따옴표 제거)은 다음과 같습니다.

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_cloudtrail"
    }]
}
```

업데이트된 결과에 대한 GuardDuty 업데이트 알림 메시지의 예는 다음과 같습니다.

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

구문 분석 메시지 값(이스케이프된 따옴표 제거)은 다음과 같습니다.

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
```

```
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

아마존 할당량 GuardDuty

AWS 계정에는 각 서비스에 대한 기본 할당량 (이전에는 한도라고 함) 이 있습니다. AWS 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

에 대한 GuardDuty 할당량을 보려면 Service Quotas 콘솔을 엽니다. 탐색 창에서 AWS 서비스를 선택하고 Amazon을 선택합니다 GuardDuty.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

AWS 계정에는 GuardDuty 지역별 Amazon 할당량이 다음과 같습니다.

> **Note**
>
> GuardDuty 멀웨어 방지와 관련된 할당량은 을 참조하십시오. 맬웨어 보호 할당량

Resource	기본값	설명
탐지기	1	리전별로 AWS 계정당 생성할 수 있는 탐지기 리소스의 최대 수입니다. 할당량 증가를 요청할 수 없습니다.
필터	100	지역별 AWS 계정당 저장된 필터의 최대 수. 할당량 증가를 요청할 수 없습니다.
결과 보존 기간	90일	결과가 보관되는 최대 일수입니다.

Resource	기본값	설명
		할당량 증가를 요청할 수 없습니다.
신뢰할 수 있는 IP 목록당 IP 주소 및 CIDR 범위	2,000	하나의 신뢰할 수 있는 IP 목록에 포함할 수 있는 최대 IP 주소 수와 CIDR 범위입니다. 할당량 증가를 요청할 수 없습니다.
위협 목록당 IP 주소 및 CIDR 범위	250,000	하나의 위협 목록에 포함할 수 있는 최대 IP 주소 수와 CIDR 범위입니다. 할당량 증가를 요청할 수 없습니다.
최대 파일 크기	35MB	신뢰할 수 있는 IP 목록 또는 위협 목록에 포함할 IP 주소 목록 또는 CIDR 범위를 업로드하는 데 사용된 파일의 최대 크기입니다. 할당량 증가를 요청할 수 없습니다.
멤버 계정(초대장 이용)	5000	관리자 계정 계정과 연결된 최대 구성원 계정 수. 할당량 증가를 요청할 수 없습니다.

Resource	기본값	설명
멤버 계정	50,000	관리자 계정 계정과 연결된 최대 구성원 계정 수입니다 AWS Organizations. 여기에는 초대를 통해 조직에 추가된 멤버 계정이 포함됩니다. 이 기본값은 의 멤버 계정에 대한 현재 할당량에 따라 달라집니다 AWS Organizations. 추가된 구성원 계정의 수는 조직의 구성원 계정 수를 AWS Organizations 초과할 수 없습니다. GuardDuty 조직의 수에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AWS 계정 최대값 및 최소값을 참조하십시오.
위협 인텔리전스 세트	6	리전별로 AWS 계정당 추가할 수 있는 위협 인텔리전스 세트의 최대 수입니다. 할당량 증가를 요청할 수 없습니다.

Resource	기본값	설명
신뢰할 수 있는 IP 세트	1	지역별 AWS 계정당 업로드 및 활성화할 수 있는 신뢰할 수 있는 IP 세트의 최대 수. 할당량 증가를 요청할 수 없습니다.

아마존 문제 해결 GuardDuty

특정 작업 수행과 관련된 문제가 발생하면 이 섹션의 주제를 참조하십시오. GuardDuty

주제

의 일반 문제 GuardDuty

GuardDuty 결과를 내보내는 중 액세스 오류가 발생합니다. 이 문제를 해결하려면 어떻게 해야 하나요?

검색 결과를 내보내도록 설정을 구성한 후 검색 결과를 내보낼 수 없는 경우 GuardDuty GuardDuty 콘솔의 설정 페이지에 오류 메시지가 표시됩니다. Amazon S3 버킷이 삭제되었거나 버킷에 액세스할 GuardDuty 수 있는 권한이 수정된 경우와 같이 대상 리소스에 더 이상 액세스할 수 없을 때 이 문제가 발생할 수 있습니다. Amazon S3 버킷의 데이터를 암호화하는 데 사용된 AWS KMS 키에 더 이상 액세스할 GuardDuty 수 없는 경우에도 이러한 문제가 발생할 수 있습니다. 내보낼 수 없는 경우 GuardDuty 계정과 연결된 이메일로 알림을 보내 이 문제에 대한 정보를 제공합니다.

문제를 해결하려면 해당 리소스가 존재하고 GuardDuty 필요한 리소스에 액세스할 수 있는 권한이 있는지 확인하십시오. 90일의 검색 결과 보존 기간이 완료되기 전에 문제를 해결하지 않으면 결과를 GuardDuty 내보낼 수 없습니다. GuardDuty 특정 지역에서 이 계정에 대한 내보내기 설정을 찾을 수 없게 됩니다. 이 보존 날짜 이후에도 구성 설정을 업데이트하여 특정 지역에서 검색 결과 내보내기를 다시 시작할 수 있습니다.

자세한 정보는 결과 내보내기을 참조하세요.

멀웨어 보호 문제

온디맨드 맬웨어 스캔을 시작하려고 하는 데 필요한 권한이 없다는 오류가 발생합니다.

Amazon EC2 인스턴스에서 온디맨드 맬웨어 스캔을 시작하는 데 필요한 권한이 없다는 오류 메시지가 표시되는 경우 AWS 관리형 정책: AmazonGuardDutyFullAccess 정책을 IAM 역할에 연결했는지 확인하세요.

AWS 조직의 구성원인데도 여전히 같은 오류가 발생하는 경우 관리 계정으로 연결하세요. 자세한 정보는 AWS Organizations SCP — 액세스 거부을 참조하세요.

맬웨어 보호 사용 중 **`iam:GetRole`** 오류 메시지가 표시됩니다.

`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`—라는 오류가 GuardDuty 표시되면 시작 맬웨어 검사를 활성화하거나 온디맨드 맬웨어 검사를 사용할 수 있는 권한을 놓친 것입니다. AWS 관리형 정책: AmazonGuardDutyFullAccess 정책을 IAM 역할에 연결했는지 확인합니다.

저는 GuardDuty 관리자 계정으로 악성 프로그램 GuardDuty 시작 검사를 활성화해야 하지만 관리형 정책을 사용하여 AWS 관리하지는 않습니다. AmazonGuardDutyFullAccess GuardDuty

- 함께 GuardDuty 사용하는 IAM 역할에 악성코드 검사를 시작하는 데 필요한 권한을 갖도록 구성하십시오 GuardDuty. 필요한 권한에 대한 자세한 내용은 맬웨어 보호에 대한 서비스 연결 역할 생성을 참조하세요.
- AWS 관리형 정책: AmazonGuardDutyFullAccess를 IAM 역할에 연결합니다. 이렇게 하면 멤버 계정에 대한 악성코드 GuardDuty 시작 스캔을 활성화하는 데 도움이 됩니다.

런타임 모니터링 문제

AWS Step Functions 워크플로가 예기치 않게 실패합니다.

GuardDuty 컨테이너가 워크플로 실패에 기여한 경우 을 참조하십시오. 적용 범위 문제 해결 문제가 지속되면 GuardDuty 컨테이너로 인한 워크플로 실패를 방지하려면 다음 단계 중 하나를 수행하십시오.

- 연결된 Amazon ECS 클러스터에`GuardDutyManaged: false` 태그를 추가합니다.
- 계정 수준에서 AWS Fargate (ECS만 해당) 의 자동 에이전트 구성을 비활성화합니다. GuardDuty 자동 에이전트로 계속 모니터링하려는 관련 Amazon ECS 클러스터에 포함 태그`GuardDutyManaged: true` 를 추가합니다.

런타임 모니터링의 메모리 부족 오류 문제 해결 (Amazon EC2 지원만 해당)

이 섹션에서는 GuardDuty 보안 에이전트를 수동으로 CPU 및 메모리 제한 배포하는 방법에 따라 메모리 부족 오류가 발생할 때의 문제 해결 단계를 제공합니다.

`out-of-memory`문제로 인해 GuardDuty 에이전트가 `systemd` 종료되고 GuardDuty 에이전트에 메모리를 더 제공하는 것이 합리적이라고 판단되면 제한을 업데이트할 수 있습니다.

1. 루트 권한으로 엽니다`/lib/systemd/system/amazon-guardduty-agent.service`.
2. 두 값을 모두 `MemoryLimit` 찾아 `MemoryMax` 업데이트하십시오.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. 값을 업데이트한 후 다음 명령을 사용하여 GuardDuty 에이전트를 다시 시작합니다.

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. 다음 명령을 실행하여 상태를 확인합니다.

```
sudo systemctl status amazon-guardduty-agent
```

예상 출력에는 새 메모리 제한이 표시됩니다.

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

복수 계정 문제 관리

여러 계정을 관리하고 싶은데 필수 AWS Organizations 관리 권한이 없습니다.

이 오류가 표시되면 조직의 `The request failed because you do not have required AWS Organization master permission.` 여러 계정에 대해 GuardDuty 시작 멀웨어 검사를 활성화할 수 있는 권한을 놓친 것입니다. 관리 계정에 권한을 제공하는 방법에 대한 자세한 내용은 을 참조하십시오. 신뢰할 수 있는 액세스를 설정하여 악성코드 검사를 시작할 수 있도록 합니다 GuardDuty.

기타 문제 해결

문제에 적합한 시나리오를 찾지 못한 경우 다음 문제 해결 옵션을 확인하세요.

- https://console.aws.amazon.com/guardduty/ 액세스 시의 일반적인 IAM 문제는 Amazon GuardDuty 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.
- 액세스 AWS AWS Console Home시 인증 및 권한 부여 문제에 대해서는 IAM 문제 해결을 참조하십시오.

리전 및 엔드포인트

GuardDuty Amazon을 이용할 수 AWS 리전 있는 지역을 보려면 의 Amazon Web Services 일반 참조Amazon GuardDuty 엔드포인트를 참조하십시오.

지원되는 AWS 리전모든 GuardDuty 항목에서 활성화하는 것이 좋습니다. 이렇게 하면 GuardDuty 활발히 사용하지 않는 지역에서도 무단 또는 비정상적 활동에 대한 결과를 얻을 수 있습니다. 또한 지원 AWS 리전대상자의 AWS CloudTrail 이벤트를 GuardDuty 모니터링할 수 있으므로 글로벌 서비스와 관련된 활동을 탐지하는 기능이 저하됩니다.

리전별 기능 가용성

GuardDuty 기능 가용성을 지정하는 지역별 차이 목록.

ListFindings 및 GetFindingsStatistics API

GetFindingsStatistics및 ListFindingsAPI에는 임시 `consoleOnly` 플래그가 있습니다. 이러한 API 중 하나 또는 둘 다를 사용하는 경우 `consoleOnly` 플래그는 API가 결과를 최대 1,000개까지 가져올 수 있음을 의미합니다.

GuardDuty 지역 차이가 있는 기능

GuardDuty 멀웨어 보호

GuardDuty AWS 전용 Local Zone에서 멀웨어 방지 기능을 지원합니다.

Amazon GuardDuty API Reference의 다음 API는 이전에 지정한 데이터 소스 또는 기능 중 일부를 사용할 수 없기 때문에 지역별로 차이가 있을 수 있습니다. AWS 리전

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors
- DescribeOrganizationConfiguration

Amazon EC2 결과 유형 - DefenseEvasion:EC2/UnusualDoHActivity 및 DefenseEvasion:EC2/UnusualDoTActivity

다음 표에는 사용 가능한 AWS 리전 위치가 GuardDuty 나와 있지만 이 두 가지 Amazon EC2 검색 유형은 아직 지원되지 않습니다.

AWS 리전	리전 코드
아시아 태평양(서울)	ap-northeast-2
아시아 태평양(오사카)	ap-northeast-3
아시아 태평양(자카르타)	ap-southeast-3

AWS GovCloud (US) 지역

최신 정보는 AWS GovCloud (US) 사용 설명서의 GuardDutyAmazon을 참조하십시오.

중국 지역

최신 정보는 기능 가용성 및 구현 차이를 참조하세요.

GuardDuty 레거시 동작 및 매개변수

GuardDuty Amazon은 일부 API 작업 및 파라미터를 지원 중단했지만 여전히 지원합니다. 모범 사례는 기존 옵션을 대체하는 새 API 작업과 파라미터를 사용하는 것입니다. 다음 표에서는 기존 작업과 새 작업 및 파라미터를 비교합니다.

레거시 작업/파라미터	새 작업/파라미터	비교
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	두 작업 모두 동일하게 구현되었으므로 에서 이 용어를 GuardDuty `Administrator` 사용합니다. `DisassociateFromAdministratorAccount`
`autoEnable` 매개 변수 입력 DescribeOrganizationConfiguration및 UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	를 사용하면 `autoEnableOrganizationMembers` GuardDuty 관리자 계정이 모든 멤버 계정을 감사하고 두 값 중 하나에 GuardDuty 대해 적용할 수 있습니다. API를 사용하면 모든 멤버 계정의 구성을 업데이트하는 데 최대 24시간이 걸릴 수 있습니다. `autoEnableOrganizationMembers` 필드의 가능한 값에 대한 자세한 내용은 구성원을 참조하십시오autoEnableOrganization.
API의 `dataSources` 파라미터는 GuardDuty 2023년 3월 API 변경에 나열되어 있습니다.	`features`	2023년 3월부터 를 사용하여 새 GuardDuty 보호 계획을 Amazon의 멀웨어 보호 GuardDuty 구성하고 구성할 수 `features` 있습니다. 맬웨어 보호를 포함하여 2023년 3월 이전에 출시된 보호 플랜은 여전히 `dataSources` 사용 구성을 지원합니다. API를 사용하여 보호 플랜을 구성하는 경우 각 API 요청에는 `dataSources` 또

레거시 작업/파라미터	새 작업/파라미터	비교
		는 features가 포함되지만 둘 다 포함되지는 않습니다.

아마존의 문서 기록 GuardDuty

다음 표에는 Amazon GuardDuty User Guide의 마지막 릴리스 이후 문서에 대한 중요한 변경 사항이 설명되어 있습니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
GuardDuty 런타임 모니터링 - Fargate의 업데이트된 기능 (Amazon ECS만 해당)	런타임 모니터링은 AWS Fargate (Amazon ECS만 해당) 리소스용 새 에이전트 버전 1.2.0을 출시했습니다. 릴리스 노트에 대한 자세한 내용은 Fargate-ECS용 GuardDuty 보안 에이전트를 참조하십시오.	2024년 5월 31일
GuardDuty 멀웨어 방지의 업데이트된 기능	Amazon EC2 인스턴스 및 컨테이너 워크로드에 GuardDuty 연결된 각 Amazon EBS 볼륨에 대해 멀웨어 보호 기능은 스캔하는 EBS 볼륨의 크기를 최대 2048GB까지 늘렸습니다. 인스턴스에 연결된 Amazon EBS 볼륨 검사에 대한 자세한 내용은 GuardDuty 멀웨어 보호를 참조하십시오.	2024년 5월 29일
런타임 모니터링의 업데이트된 기능	Amazon ECS-Fargate 리소스의 런타임 모니터링은 이제 에서 시작한 작업에 대한 잠재적 위협 탐지를 지원합니다. AWS Batch자세한 내용은 Fargate에서의 런타임 모니터링 작동 방식 (Amazon ECS만 해당) 을 참조하십시오.	2024년 5월 28일
런타임 모니터링 기능 업데이트	런타임 모니터링은 Amazon EKS 리소스용 새 에이전트 버	2024년 5월 14일

	전 1.6.1을 출시했습니다. 릴리스 노트에 대한 자세한 내용은 EKS 애드온 에이전트 릴리스 기록을 참조하십시오.	
런타임 모니터링에 대한 지역 지원 확대	GuardDuty 런타임 모니터링 지원을 캐나다 서부 (캘거리) 지역으로 확대합니다. 런타임 모니터링을 시작하는 방법에 대한 자세한 내용은 런타임 모니터링 활성화를 참조하십시오.	2024년 5월 7일
RDS 보호를 위한 확장된 지역 지원	GuardDuty RDS 보호 지원을 다음과 같이 확장합니다. AWS 리전 • 캐나다 서부(캘거리) • 아시아 태평양(하이데라바드) • 유럽(스페인) • 유럽(취리히) • 중동(UAE) • 이스라엘(텔아비브) • 아시아 태평양(멜버른) 이 기능을 활성화하는 방법에 대한 자세한 내용은 RDS 보호를 참조하십시오.	2024년 5월 3일
런타임 모니터링의 업데이트된 기능	런타임 모니터링은 AWS Fargate (Amazon ECS만 해당) 리소스용 새 에이전트 버전 1.1.0을 출시했습니다. 릴리스 노트에 대한 자세한 내용은 Fargate-ECS용 GuardDuty 보안 에이전트를 참조하십시오.	2024년 5월 1일

런타임 모니터링의 업데이트된 기능	런타임 모니터링은 Amazon EKS 리소스용 새 에이전트 버전 1.6.0을 출시했습니다. 릴리스 노트에 대한 자세한 내용은 EKS 애드온 에이전트 릴리스 기록을 참조하십시오.	2024년 4월 29일
IP 주소 지원 (V6)	GuardDuty 로컬 및 원격 IP 세부 정보 모두에 대한 IPAddresv6 지원이 추가되었습니다. 관련 필터 속성을 사용하여 GuardDuty 결과를 필터링하거나 금지 규칙을 만들 수 있습니다.	2024년 4월 18일
검색 결과 내보내기를 구성하도록 콘솔 환경을 업데이트했습니다.	GuardDuty 에서 생성된 결과를 Amazon S3 버킷으로 내보내도록 콘솔 환경을 업데이트했습니다. AWS 계정자세한 내용은 GuardDuty 결과 내보내기를 참조하십시오.	2024년 4월 1일
런타임 모니터링의 업데이트된 기능	런타임 모니터링은 Amazon EC2 리소스용 새 보안 에이전트 버전 1.1.0을 출시했습니다. 이 버전은 Amazon EC2 인스턴스의 런타임 모니터링에서 GuardDuty 자동 에이전트 구성을 지원합니다. 릴리스 노트에 대한 자세한 내용은 Amazon EC2 인스턴스용 GuardDuty 보안 에이전트를 참조하십시오.	2024년 3월 28일

Amazon EC2 인스턴스에 대한 런타임 모니터링의 일반 가용성	GuardDuty Amazon EC2 인스턴스에 대한 런타임 모니터링의 일반 가용성 (GA) 을 발표합니다. 이제 Amazon EC2 인스턴스용 보안 에이전트를 사용자 대신 설치하고 관리할 수 있는 자동 에이전트 구성을 GuardDuty 활성화할 수 있는 옵션이 있습니다. GuardDuty 자동 에이전트를 사용하면 포함 또는 제외 태그를 사용하여 선택한 Amazon EC2 인스턴스에만 보안 에이전트를 설치하고 GuardDuty 관리하도록 알릴 수 있습니다. 자세한 내용은 How Runtime Monitoring works with Amazon EC2 instances를 참조하세요. 이 GA와 함께 출시된 새로운 검색 결과 유형 목록 • 실행: 런타임/ SuspiciousTool • 실행: 런타임/ SuspiciousCommand • DefenseEvasion실행: 런타임/ ----SEP----:런타임/ SuspiciousCommand • DefenseEvasion:런타임/ ----SEP----:런타임/ PtraceAntiDebugging • 실행: 런타임/ MaliciousFileExecuted	2024년 3월 28일

GuardDuty Amazon은 서비스 연결 역할 (SLR) 을 업데이트했습니다.	Amazon EC2용 자동 에이전트로 런타임 모니터링을 GuardDuty 활성화하면 Amazon EC2 인스턴스에서 SSM 연결을 관리하는 AWS Systems Manager 작업을 사용하십시오. GuardDuty 자동 에이전트 구성을 비활성화하면 포함 태그 (:) 가 있는 EC2 인스턴스만 GuardDuty 고려합니다. `GuardDutyManaged true` • 다음 목록은 새 권한을 보여줍니다. `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	2024년 3월 26일

런타임 모니터링의 기능이 업데이트되었습니다.	Amazon EKS용 최신 GuardDuty 보안 에이전트 (애드온) v1.5.0 릴리스를 통해 런타임 모니터링은 이제 CPU 및 메모리 설정, `PriorityClass` 설정, DNS 정책 설정과 같은 GuardDuty 보안 에이전트의 특정 파라미터 구성을 지원합니다. 자세한 내용은 GuardDuty보안 에이전트 (EKS 애드온) 매개 변수 구성을 참조하십시오.	2024년 3월 7일
런타임 모니터링의 업데이트된 기능	런타임 모니터링은 Amazon EKS 리소스용 새 에이전트 버전 1.5.0을 출시했습니다. 릴리스 노트에 대한 자세한 내용은 EKS 애드온 에이전트 릴리스 기록을 참조하십시오.	2024년 3월 7일
캐나다 서부 (캘거리) 지원	GuardDuty Amazon은 이제 캐나다 서부 (캘거리) 지역에서 사용할 수 있습니다. 이 지역의 일부 보호 플랜은 이 지역에서 제공되지 GuardDuty 않을 수 있습니다. 최신 정보는 지역 및 엔드포인트를 참조하십시오.	2024년 3월 6일
런타임 모니터링의 업데이트된 기능	Amazon EKS 클러스터용 GuardDuty 보안 에이전트 버전 1.0.0 및 1.1.0은 2024년 5월 14일부터 더 이상 지원되지 않습니다. 표준 지원이 종료되기 전에 취할 수 있는 조치에 대한 자세한 내용은 Amazon EKS 클러스터용 GuardDuty 보안 에이전트를 참조하십시오.	2024년 2월 16일

런타임 모니터링의 기능이 업데이트되었습니다.	런타임 모니터링은 기존 보안 에이전트 버전 1.4.1과 함께 최신 Kubernetes 버전 1.29를 지원합니다. 이 쿠버네티스 버전이 출시된 이후 지원이 제공되었습니다. 지원되는 쿠버네티스 버전에 대한 자세한 내용은 보안 에이전트가 지원하는 쿠버네티스 버전을 참조하십시오. GuardDuty	2024년 2월 16일
런타임 모니터링의 업데이트된 기능 - 지역별 가용성	GuardDuty 런타임 모니터링은 이제 동일한 기능 내에서 공유 Amazon VPC를 지원합니다. AWS OrganizationsGuardDuty 서비스 연결 역할 (SLR) 에는 공유 Amazon VPC 계정의 조직 ID를 검색하여 엔드포인트 정책을 설정하는 데 도움이 `organizations:DescribeOrganization` 되는 새로운 권한이 있습니다. 런타임 모니터링에서 공유 Amazon VPC 엔드포인트를 사용하기 위한 사전 요구 사항에 대한 자세한 내용은 공유 Amazon VPC 지원을 참조하십시오. 이 기능은 런타임 모니터링을 지원하는 모든 지역에서 GuardDuty 사용할 수 있습니다.	2024년 2월 12일

런타임 모니터링의 업데이트된 기능 - 지역별 가용성	GuardDuty 런타임 모니터링은 이제 동일한 기능 내에서 공유 Amazon VPC를 지원합니다. AWS OrganizationsGuardDuty 서비스 연결 역할 (SLR) 에는 공유 Amazon VPC 계정의 조직 ID를 검색하여 엔드포인트 정책을 설정하는 데 도움이 `organizations:DescribeOrganization` 되는 새로운 권한이 있습니다. 런타임 모니터링에서 공유 Amazon VPC 엔드포인트를 사용하기 위한 사전 요구 사항에 대한 자세한 내용은 공유 Amazon VPC 지원을 참조하십시오. 현재 이 기능은 일부 지역에서 사용할 수 있습니다. AWS 리전자세한 내용은 리전 및 엔드포인트 섹션을 참조하십시오.	2024년 2월 9일
새로운 기능을 지원하여 기능이 업데이트되었습니다. AWS 리전 — 멀웨어 방지	멀웨어 보호 기능은 이제 미국 서부 (오레곤) AWS 관리형 키 지역에서 암호화된 EBS 볼륨 검사를 지원합니다.	2024년 2월 6일

새로운 기능을 지원하는 업데이트된 기능 AWS 리전 — 멀웨어 방지	멀웨어 보호 기능은 이제 다음과 같이 AWS 리전 암호화된 EBS 볼륨 스캔을 지원합니다. AWS 관리형 키 • 아시아 태평양(싱가포르) (ap-southeast-1) • EU (프랑크푸르트)(eu-central-1) • 아시아 태평양(오사카)(ap-northeast-3) • 미국 동부 (오하이오)(us-east-2) • EU(밀라노)(eu-south-1) • 아시아 태평양(도쿄) (ap-northeast-1) • 아시아 태평양(서울) (ap-northeast-2) • 캐나다(중부) (ca-central-1) • EU (아일랜드)(eu-west-1) • 미국 동부 (버지니아 북부) (us-east-1)	2024년 2월 5일

런타임 모니터링 기능 업데이트	GuardDuty 런타임 모니터링은 Amazon EC2 인스턴스용 새 GuardDuty 보안 에이전트 버전 (v1.0.2) 을 출시했습니다. 이 에이전트 버전에는 최신 Amazon ECS AMI에 대한 지원이 포함되어 있습니다. 에이전트 릴리스 기록에 대한 자세한 내용은 Amazon EC2 인스턴스용 GuardDuty 보안 에이전트를 참조하십시오.	2024년 2월 2일

새로운 기능을 지원하여 기능이 업데이트되었습니다. AWS 리전 — 멀웨어 방지	멀웨어 보호는 이제 다음과 같이 AWS 리전 암호화된 Amazon EBS 볼륨 스캔을 지원합니다. AWS 관리형 키 • EU(런던)(eu-west-2) • EU(스톡홀름)(eu-north-1) • 아시아 태평양(홍콩)ap-east-1 • 아프리카(케이프타운)(af-south-1) • 중동(바레인)(me-south-1) • 아시아 태평양(하이데라바드)(ap-south-2) • 유럽(스페인)(eu-south-2) • 아시아 태평양(멜버른) (ap-southeast-4) • 아시아 태평양(시드니) (ap-southeast-2) • 이스라엘(텔아비브)(il-central-1)	2024년 1월 31일
계정 관리를 다음과 같이 업데이트했습니다. AWS Organizations	계정 관리에서 콘텐츠를 재구성했습니다. AWS Organizations위임된 GuardDuty 관리자 계정을 변경하는 단계를 추가하고 관리자 계정과 구성원 계정 간의 GuardDuty 관계에 대한 이해를 업데이트했습니다.	2024년 1월 30일

새 기능을 지원하여 기능이 업데이트되었습니다. AWS 리전	멀웨어 보호는 이제 다음과 같이 AWS 리전 암호화된 EBS 볼륨 스캔을 지원합니다. AWS 관리형 키 • 아시아 태평양(자카르타) (ap-southeast-3) • 미국 서부(캘리포니아 북부) (us-west-1) • 중동(UAE)(me-central-1) • 유럽(취리히)(eu-central-2) • 아시아 태평양(뭄바이) (ap-south-1) • 남아메리카(상파울루)(sa-east-1)	2024년 1월 29일

멀웨어 방지 기능이 업데이트되었습니다.	멀웨어 보호는 이제 를 사용하여 AWS 관리형 키암호화된 EBS 볼륨 검사를 지원합니다. 멀웨어 보호 서비스 연결 역할 (SLR) 에는 두 개의 새로운 권한 (및) 이 추가되었습니다. `GetSnapshotBlock` `ListSnapshotBlocks` 이러한 권한은 GuardDuty 악성코드 검사를 시작하기 전에 사용자로부터 EBS 볼륨의 스냅샷 (을 사용하여 AWS 관리형 키암호화됨) 을 AWS 계정 가져와 GuardDuty 서비스 계정에 복사하는 데 도움이 됩니다. 현재 이 기능은 유럽 (파리) (`eu-west-3`) 에서만 사용할 수 있습니다. 자세한 내용은 멀웨어 검사 지원 볼륨을 참조하십시오.	2024년 1월 25일
런타임 모니터링의 업데이트된 기능	GuardDuty 런타임 모니터링은 일반적인 성능 조정 및 개선 사항이 포함된 새 GuardDuty 보안 에이전트 버전 (v1.0.1) 을 출시했습니다. 에이전트 릴리스 기록에 대한 자세한 내용은 Amazon EC2 인스턴스용 GuardDuty 보안 에이전트를 참조하십시오.	2024년 1월 23일
런타임 모니터링의 기능이 업데이트되었습니다.	런타임 모니터링은 Amazon EKS 리소스용 새 에이전트 버전 1.4.1을 출시했습니다. 자세한 내용은 EKS add-on agent release history를 참조하세요.	2024년 1월 16일

런타임 모니터링에서 Amazon EKS 리소스용 새 에이전트 v1.4.0을 출시했습니다.	런타임 모니터링은 Amazon EKS 리소스용 새 에이전트 버전 1.4.0을 출시했습니다. 자세한 내용은 EKS add-on agent release history를 참조하세요.	2023년 12월 21일

유럽 (취리히), 유럽 (스페인), 아시아 태평양 (하이데라바드), 아시아 태평양 (멜버른), 이스라엘 (텔아비브) 에 S3 및 AWS CloudTrail 기계 학습 (ML) 기반 검색 결과 유형을 추가했습니다.	이제 유럽 (취리히), 유럽 (스페인), 아시아 태평양 (하이데라바드), 아시아 태평양 (멜버른), 이스라엘 (텔아비브) 지역에서 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델을 사용하여 이상 행동을 식별하는 다음 S3와 CloudTrail 결과를 이용할 수 있습니다. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior	2023년 12월 21일

	• Discovery:IAMUser/AnomalousBehavior	
GuardDuty 를 통해 50,000개의 회원 계정 지원 AWS Organizations	위임된 GuardDuty 관리자는 이제 를 통해 AWS Organizations 최대 50,000개의 회원 계정을 관리할 수 있습니다. 여기에는 초대를 통해 GuardDuty 관리자 계정과 연결된 최대 5000개의 회원 계정도 포함됩니다.	2023년 12월 20일
GuardDuty 런타임 모니터링 지원이 19개로 확대되었습니다. AWS 리전	런타임 모니터링은 이제 아시아 태평양 (자카르타), 유럽 (파리), 아시아 태평양 (오사카), 아시아 태평양 (서울), 중동 (바레인), 유럽 (스페인), 아시아 태평양 (하이데라바드), 아시아 태평양 (멜버른), 이스라엘 (텔아비브), 미국 서부 (캘리포니아 북부), 유럽 (런던), 아시아 태평양 (홍콩), 유럽 (밀라노), 중동 (UAE) 에서 사용할 수 있습니다.), 남미 (상파울루), 아시아 태평양 (뭄바이), 캐나다 (중부), 아프리카 (케이프타운), 유럽 (취리히).	2023년 12월 6일

GuardDuty 런타임 모니터링 기능 확장	Amazon EKS 클러스터에 대한 위협을 탐지하는 것 외에도 Amazon ECS 워크로드에 대한 위협을 탐지하기 위한 런타임 모니터링의 일반 가용성과 Amazon EC2 인스턴스에 대한 위협을 탐지하기 위한 프리뷰 릴리스를 GuardDuty 발표합니다. AWS 리전 현재 런타임 모니터링을 지원하는 항목에 대한 자세한 내용은 지역 및 엔드포인트를 참조하십시오.	2023년 11월 26일
GuardDuty Amazon은 서비스 연결 역할 (SLR) 을 업데이트했습니다.	GuardDuty Amazon ECS 작업을 사용하여 Amazon ECS 클러스터에 대한 정보를 관리 및 검색하고 Amazon ECS 계정 설정을 관리할 수 있는 새로운 권한이 추가되었습니다. `guarddutyActivate` Amazon ECS와 관련된 작업은 연결된 태그에 대한 정보도 검색합니다. GuardDuty • 런타임 모니터링 기능 GuardDuty 확장의 일환으로 다음과 같은 권한이 추가되었습니다. `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	2023년 11월 26일

AWS 관리형 정책을 업데이트했습니다.	GuardDuty AmazonGuardDutyFullAccessPolicy 및에 새 권한을 추가했습니다 AmazonGuardDutyReadOnlyAccess. `organizations:ListAccounts`	2023년 11월 16일

GuardDuty EKS 감사 로그 모니터링을 사용하는 새로운 검색 결과 유형을 출시했습니다.	EKS 감사 로그 모니터링은 이제 아시아 태평양 (멜버른) 에서 다음과 같은 검색 결과 유형을 지원합니다 (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	2023년 11월 11일

GuardDuty EKS 감사 로그 모니터링을 사용하는 새로운 검색 결과 유형이 출시되었습니다.	EKS 감사 로그 모니터링은 이제 아시아 태평양 (하이데라바드) (), 유럽 (취리히) (`ap-south-2`) 및 유럽 (스페인) (`eu-central-2`) 지역에서 다음과 같은 검색 결과 유형을 지원합니다. `eu-south-2` • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	2023년 11월 10일

GuardDuty EKS 감사 로그 모니터링을 사용하는 새로운 검색 결과 유형을 출시했습니다.	EKS 감사 로그 모니터링은 이제 다음 검색 결과 유형을 지원합니다. 아시아 태평양 (하이데라바드) (), 유럽 (취리히) (ap-south-2), 유럽 (스페인) () 및 아시아 태평양 (eu-central-2 멜버른) (eu-south-2) 지역에서는 이러한 검색 유형을 아직 사용할 수 없습니다. ap-southeast-4 • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	2023년 11월 8일

	• Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKS 런타임 모니터링의 새 에이전트 v1.3.1 릴리스	EKS 런타임 모니터링은 중요한 보안 패치 및 업데이트가 포함된 새 에이전트 버전 1.3.1을 출시했습니다.	2023년 10월 23일
결과에 대한 새 필터 속성	GuardDuty 생성된 결과를 필터링하기 위한 새 기준을 추가했습니다. DNS 요청 도메인 접미사는 검색 결과 생성을 요청한 활동과 관련된 두 번째 및 최상위 도메인을 제공합니다. GuardDuty	2023년 10월 17일
EKS 런타임 모니터링에서 Kubernetes 버전 1.28을 지원하는 새 에이전트 v1.3.0 릴리스	EKS 런타임 모니터링은 쿠버네티스 버전 1.28을 지원하는 새 에이전트 버전 1.3.0을 출시했습니다. Ubuntu 지원을 추가했습니다. 자세한 내용은 EKS add-on agent release history를 참조하세요.	2023년 10월 5일

아시아 태평양 (자카르타) 및 중동 (UAE) 지역에 S3 및 AWS CloudTrail 기계 학습 (ML) 기반 검색 결과 유형을 추가했습니다.	이제 아시아 태평양 (자카르타) 및 중동 (UAE) 지역에서 GuardDuty 의 이상 탐지 기계 학습 (ML) 모델을 사용하여 이상 행동을 식별하는 다음 S3 및 CloudTrail 결과를 사용할 수 있습니다. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	2023년 9월 20일

GuardDuty EKS 런타임 모니터링은 클러스터 수준에서 보안 에이전트를 관리하는 방법을 소개합니다. GuardDuty	EKS Runtime Monitoring은 개별 EKS 클러스터의 GuardDuty 보안 에이전트를 관리하여 이러한 선택적 클러스터의 런타임 이벤트만 모니터링하는 지원을 추가합니다. EKS 런타임 모니터링은 태그 지원을 통해 이 기능을 확장합니다.	2023년 9월 13일
GuardDuty 멀웨어 방지는 지원을 더 확대합니다. AWS 리전	이제 아시아 태평양(하이데라바드), 아시아 태평양(멜버른), 유럽(취리히) 및 유럽(스페인) 리전에서 맬웨어 보호를 사용할 수 있습니다.	2023년 9월 11일
GuardDuty 이제 이스라엘 (텔아비브) 지역에서도 사용할 수 있습니다.	현재 이용 가능한 지역 목록에 이스라엘 (텔아비브) 지역을 추가했습니다. AWS 리전 GuardDuty 다음 보호 플랜을 이스라엘(텔아비브) 리전에서도 사용할 수 있습니다. • GuardDuty EKS 보호에는 EKS 감사 로그 모니터링 및 EKS 런타임 모니터링이 포함됩니다. • GuardDuty 람다 프로텍션. • GuardDuty 멀웨어 보호. • GuardDuty S3 보호. 이스라엘(텔아비브) 리전의 보호 플랜 가용성에 대한 자세한 내용은 리전 및 엔드포인트 섹션을 참조하세요.	2023년 8월 24일

GuardDuty 보호 계획 수준에서 조직에 대한 자동 활성화 구성을 추가했습니다.	해당 리전의 보호 플랜에 대한 조직 구성을 업데이트하세요. 가능한 구성 옵션은 모든 계정에 대해 활성화, 새 계정에 대해 자동 활성화, 조직의 모든 계정에 대해 자동 활성화하지 않음입니다.	2023년 8월 16일
GuardDuty의 이상 탐지 기계 학습 (ML) 모델을 사용하여 이상 행동을 식별하는 S3 검색 유형을 이제 아시아 태평양 (오사카) 에서 사용할 수 있습니다.	이제 아시아 태평양(오사카) 리전에서 다음 결과 유형이 제공됩니다. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	2023년 8월 10일
이제 아시아 태평양(멜버른) 리전에서 EKS 런타임 모니터링 사용 가능	EKS 보호 내의 GuardDuty EKS 런타임 모니터링은 환경 내 Amazon EKS 클러스터에 대한 런타임 위협 탐지를 제공합니다. AWS 이제 아시아 태평양(멜버른) 리전에서 지원됩니다.	2023년 8월 8일
시작된 멀웨어 스캔을 GuardDuty 호출하는 GuardDuty 결과 목록을 업데이트했습니다.	이제 특정 EKS 런타임 모니터링 검색 결과 유형이 사용자 내에서 시작된 멀웨어 검사를 GuardDuty 호출할 수 있습니다. AWS 계정	2023년 7월 19일

GuardDuty 를 통해 10,000개의 회원 계정을 지원합니다. AWS Organizations	GuardDuty 관리자 계정은 이제 를 통해 최대 10,000개의 회원 계정을 관리할 수 AWS Organizations있습니다. 여기에는 초대를 통해 GuardDuty 관리자 계정과 연결된 최대 5000개의 회원 계정도 포함됩니다.	2023년 6월 29일
EKS 런타임 모니터링에서 세 가지 새로운 결과 유형을 발표합니다.	EKS 런타임 모니터링은 프로세스 주입 기법을 기반으로 하는 세 가지의 새로운 결과 유형을 지원합니다. 새 검색 유형은 DefenseEvasion 런타임/.Proc, :런타임/.Ptrace, :런타임/입니다. ProcessInjection DefenseEvasion ProcessInjection DefenseEvasion ProcessInjection VirtualMemoryWrite.	2023년 6월 22일
EKS 런타임 모니터링에서 Kubernetes 버전 1.27을 지원하는 새 에이전트 v1.2.0 릴리스	EKS 런타임 모니터링은 ARM64 기반 인스턴스도 지원하는 새 에이전트 버전 1.2.0을 출시했습니다. Bottlerocket에 대한 지원이 추가되었습니다. 자세한 내용은 EKS add-on agent release history를 참조하세요.	2023년 6월 16일

GuardDuty 콘솔은 결과를 요약하여 보여줍니다.	GuardDuty 콘솔의 요약 대시보드는 결과를 집계하여 GuardDuty 보여줍니다. 현재 대시보드에는 현재 지역의 사용자 계정 (또는 GuardDuty 관리자 계정인 경우 멤버 계정) 에 대해 생성된 최근 10,000개의 검색 결과에 대한 데이터가 다양한 위젯을 통해 표시됩니다.	2023년 6월 12일
이제 아시아 태평양(하이데라바드), 아시아 태평양(멜버른), 유럽(취리히) 및 유럽(스페인) 리전에서 EKS 감사 로그 모니터링 사용 가능	계정의 EKS 감사 로그 모니터링 (EKS Protection에서) 을 활성화하면 Amazon EKS 클러스터의 EKS 감사 로그를 모니터링하고 잠재적으로 악의적이고 의심스러운 활동이 있는지 분석할 수 있습니다.	2023년 6월 1일
이제 중동(UAE)에서 EKS 감사 로그 모니터링 사용 가능	이제 중동 (UAE) 에서 EKS 감사 로그 모니터링을 사용할 수 있습니다. 계정에 대한 EKS 감사 로그 모니터링을 활성화하여 Amazon EKS 클러스터의 EKS 감사 로그를 모니터링하고 잠재적으로 악의적이고 의심스러운 활동이 있는지 분석할 수 있습니다.	2023년 5월 3일

GuardDuty 멀웨어 보호, 온디맨드 멀웨어 검사 발표	맬웨어 보호를 사용하면 Amazon EC2 인스턴스와 컨테이너 워크로드에 연결된 Amazon EBS 볼륨의 잠재적 맬웨어의 존재를 탐지할 수 있습니다. 이제 GuardDuty 초기 검사와 온디맨드 검사의 두 가지 유형을 제공합니다. GuardDuty-시작된 멀웨어 스캔은 -시작된 멀웨어 스캔을 호출하는 결과 중 하나를 GuardDuty 생성할 때만 Amazon EBS 볼륨에서 에이전트 없는 스캔을 자동으로 시작합니다. GuardDuty Amazon EC2 인스턴스와 연결된 Amazon 리소스 이름(ARN)을 제공하여 계정의 Amazon EC2 인스턴스에 대해 온디맨드 맬웨어 스캔을 시작할 수 있습니다. 두 스캔 유형이 무엇이 다른지에 대한 자세한 내용은 맬웨어 보호를 참조하세요. • GuardDuty-시작된 멀웨어 스캔 • 온디맨드 맬웨어 스캔	2023년 4월 27일
GuardDuty 람다 프로텍션 발표	Lambda 보호를 사용하면 AWS Lambda 함수에서 잠재적인 보안 위협을 식별할 수 있습니다. • Lambda 보호 결과 유형 • 잠재적으로 손상된 Lambda 함수 수정	2023년 4월 20일

GuardDuty 이제 아시아 태평양 (멜버른) 지역에서 사용할 수 있습니다.	이용 가능 지역 목록에 아시아 태평양 (멜버른) 을 추가했습니다. AWS 리전 GuardDuty 이 리전에서 사용할 수 있는 기능에 대한 자세한 내용은 Regions and endpoints를 참조하세요.	2023년 4월 19일
GuardDuty 세 가지 새로운 EC2 검색 결과 유형이 추가되었습니다.	GuardDuty 외부 DNS 확인자 및 암호화된 DNS 기술의 사용을 탐지하기 위한 새로운 검색 유형을 소개합니다. 이러한 검색 유형이 지원되는 AWS 리전 위치에 대한 자세한 내용은 지역 및 엔드포인트를 참조하십시오. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	2023년 4월 5일

GuardDuty EKS 보호의 EKS 런타임 모니터링을 발표합니다.	EKS 보호 내의 EKS 런타임 모니터링은 환경 내 Amazon EKS 클러스터에 대한 런타임 위협 탐지를 제공합니다. AWS EKS 워크로드에서 런타임 이벤트를 수집하는 Amazon EKS 추가 기능 에이전트(`aws-guardduty-agent`)를 사용합니다. 이러한 런타임 이벤트를 GuardDuty 수신한 후 이를 모니터링하고 분석하여 의심스러운 잠재적 보안 위협을 식별합니다. 자세한 내용은 결과 세부 정보 및 EKS Runtime Mornitoring 결과 유형을 참조하세요.	2023년 3월 30일

GuardDuty 새 기능 추가 — autoEnableOrganizationMembers	Amazon은 GuardDuty 관리자 계정을 감사하고 조직 구성원이 사용할 수 있도록 (필요한 경우) 적용하는 데 도움이 되는 GuardDuty 새로운 조직 구성 옵션을 GuardDuty 추가합니다. ALL 이제 모범 사례는 autoEnable 대신 autoEnableOrganizationMembers 를 사용하는 것입니다. autoEnable 은 사용이 중단되었지만 여전히 지원됩니다. 이 새 기능의 영향을 받는 API는 다음과 같습니다. • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	2023년 3월 23일
GuardDuty Amazon의 RDS 보호 기능을 이제 정식 버전으로 사용할 수 있습니다.	GuardDuty RDS Protection은 RDS 로그인 활동을 모니터링하고 프로파일링하여 Amazon Aurora 데이터베이스 인스턴스에서 의심스러운 로그인 동작을 식별합니다. RDS 보호를 지원하는 AWS 리전 에 대한 자세한 내용은 리전 및 엔드포인트를 참조하세요.	2023년 3월 16일

GuardDuty 기능 활성화를 발표합니다.	과거에는 GuardDuty API를 통해 기능과 데이터 소스를 모두 구성할 수 있었지만 이제는 모든 새로운 GuardDuty 보호 유형이 데이터 소스가 아닌 기능으로 구성됩니다. GuardDuty API를 통해 데이터 소스를 계속 지원하지만 새 API를 추가하지는 않을 예정입니다. 기능 활성화는 활성화에 사용되는 API의 동작 GuardDuty 또는 보호 유형에 영향을 줍니다. GuardDuty API, SDK 또는 CFN 템플릿을 통해 GuardDuty 계정을 관리하는 경우 2023년 3월의 GuardDuty API 변경 사항을 참조하십시오.	2023년 3월 16일
GuardDuty 이제 중동 (UAE) 지역에서 멀웨어 보호를 사용할 수 있습니다.	의 멀웨어 보호 기능은 중동 (UAE) 지역에서 지원됩니다. GuardDuty 자세한 내용은 리전 및 엔드포인트 섹션을 참조하십시오.	2023년 3월 13일

GuardDuty Amazon은 서비스 연결 역할 (SLR) 을 업데이트했습니다.	GuardDuty 곧 출시될 GuardDuty EKS 런타임 모니터링 기능을 지원하기 위해 다음과 같은 새 권한을 추가했습니다. • Amazon EKS 작업을 사용하여 EKS 클러스터에 대한 정보를 관리 및 검색하고, EKS 클러스터의 EKS 추가 기능을 관리할 수 있습니다. EKS 작업은 관련된 태그에 대한 정보도 검색합니다. GuardDuty `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	2023년 3월 8일
GuardDuty Amazon은 서비스 연결 역할 (SLR) 을 업데이트했습니다.	멀웨어 보호가 활성화된 후 멀웨어 보호 SLR을 생성할 수 있도록 SLR이 업데이트되었습니다. GuardDuty	2023년 2월 21일
GuardDuty TLS v1.2 이상이 필요합니다.	AWS 리소스와 통신하려면 TLS GuardDuty v1.2 이상이 필요하고 이를 지원합니다. 자세한 내용은 데이터 보호 및 인프라 보안을 참조하세요.	2023년 2월 14일

GuardDuty 이제 아시아 태평양 (하이데라바드) 지역에서 사용할 수 있습니다.	사용 가능한 지역 목록에 아시아 태평양 (하이데라바드) 지역을 추가했습니다. AWS 리전 GuardDuty 자세한 내용은 리전 및 엔드포인트 섹션을 참조하십시오.	2023년 2월 14일
Amazon GuardDuty 사용 설명서는 IAM 모범 사례와 일치합니다.	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 내용은 IAM의 보안 모범 사례를 참조하십시오.	2023년 2월 10일
GuardDuty 이제 유럽 (스페인) 지역에서 사용할 수 있습니다.	사용 가능 지역 목록에 유럽 (스페인) 을 추가했습니다. AWS 리전 GuardDuty 자세한 내용은 리전 및 엔드포인트 섹션을 참조하십시오.	2023년 2월 8일
GuardDuty 이제 유럽 (취리히) 지역에서 사용할 수 있습니다.	이용 가능 지역 목록에 유럽 (취리히) AWS 리전 을 GuardDuty 추가했습니다. 자세한 내용은 리전 및 엔드포인트 섹션을 참조하십시오.	2022년 12월 12일
새 기능인 GuardDuty RDS 프로텍션의 프리뷰 릴리스	GuardDuty RDS Protection은 RDS 로그인 활동을 모니터링하고 프로파일링하여 Amazon Aurora 데이터베이스 인스턴스에서 의심스러운 로그인 동작을 식별합니다. 현재는 5개 AWS 리전에서 미리 보기 릴리스로 제공됩니다. 자세한 내용은 리전 및 엔드포인트 섹션을 참조하십시오.	2022년 11월 30일

GuardDuty 이제 중동 (UAE) 지역에서 사용할 수 있습니다.	이용 가능 지역 목록에 중동 (UAE) 을 추가했습니다. AWS 리전 GuardDuty 자세한 내용은 리전 및 엔드포인트 섹션을 참조하십시오.	2022년 10월 6일

새 기능인 GuardDuty 멀웨어 방지에 대한 콘텐츠 추가	GuardDuty 멀웨어 방지는 GuardDuty Amazon의 선택적 개선 사항입니다. 멀웨어 프로텍션은 위험에 처한 리소스를 GuardDuty 식별하는 동시에 손상의 원인이 될 수 있는 멀웨어를 탐지합니다. 멀웨어 보호를 활성화하면 멀웨어를 나타내는 Amazon EC2 인스턴스 또는 컨테이너 워크로드에서 의심스러운 동작을 GuardDuty 감지할 때마다 멀웨어 GuardDuty 보호가 영향을 받는 EC2 인스턴스 또는 컨테이너 워크로드에 연결된 EBS 볼륨을 에이전트 없이 스캔하여 멀웨어의 존재를 탐지합니다. 멀웨어 보호의 작동 방식 및 이 기능의 구성에 대한 자세한 내용은 멀웨어 보호를 참조하십시오. GuardDuty • 맬웨어 보호 결과에 대한 자세한 내용은 결과 세부 정보를 참조하세요. • 손상된 EC2 인스턴스 및 독립형 컨테이너를 수정하는 방법에 대한 자세한 내용은 에서 발견한 보안 문제 해결을 참조하십시오. GuardDuty • 멀웨어 스캔 CloudWatch 로그 감사 및 멀웨어 스캔 중에 리소스를 건너뛰는 이유에 대한 자세한 내용은 로그 이해 및 건너뛰기 이유를 참조하십시오. CloudWatch	2022년 7월 26일

	• 오탐지 위협 탐지에 대한 자세한 내용은 멀웨어 방지의 오탐지 보고를 참조하십시오. GuardDuty	
사용 중지된 결과 유형	Exfiltration:S3/ObjectRead.Unusual은 사용 중지되었습니다.	2022년 7월 5일
GuardDuty의 이상 탐지 기계 학습 (ML) 모델을 사용하여 이상 행동을 식별하는 새로운 S3 검색 유형이 추가되었습니다.	다음과 같은 새로운 S3 결과 유형이 추가되었습니다. 이러한 결과 유형은 API 요청이 변칙적인 방식으로 IAM 엔터티를 간접 호출했는지 여부를 식별합니다. ML 모델은 계정에 대한 모든 API 요청을 평가하고 공격자가 사용한 기법과 관련된 변칙 이벤트를 식별합니다. 새로운 결과 각각에 대한 자세한 내용은 S3 결과 유형을 참조하세요. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	2022년 7월 5일

에 대한 EKS 보호 콘텐츠가 추가되었습니다. GuardDuty GuardDuty	GuardDuty 이제 EKS 감사 로그의 모니터링을 통해 Amazon EKS 리소스에 대한 결과를 생성할 수 있습니다. 이 기능을 구성하는 방법을 알아보려면 GuardDutyAmazon의 EKS 보호를 참조하십시오. Amazon EKS 리소스에 대해 생성할 GuardDuty 수 있는 검색 결과 목록은 Kubernetes 검색 결과를 참조하십시오. Kubernetes 결과 해결 가이드에 이러한 결과의 해결을 지원하는 새로운 해결 지침이 추가되었습니다.	2022년 1월 25일
새로운 결과 1개 추가	새 결과 UnauthorizedAccess :IAMUser/InstanceCredential Exfiltration.InsideAWS가 추가되었습니다. 이 검색 결과는 환경 외부의 계정이 인스턴스 자격 증명에 액세스하는 시점을 AWS 알려줍니다. AWS	2022년 1월 20일
log4j 관련 문제 식별에 도움이 되도록 결과 유형 업데이트	GuardDuty Amazon은 CVE-2021-44228 및 CVE-2021-45046 관련 문제를 식별하고 우선 순위를 정하는 데 도움이 되도록 다음과 같은 검색 결과 유형을 업데이트했습니다. 백도어:EC2/C&CActivity.B; 백도어:EC2/C&CActivity.B! NetworkPortUnusualDNS; 동작: EC2/.	2022년 12월 22일

결과 변경	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration이 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS로 변경되었습니다. 이 개선된 버전의 결과는 보안 인증 정보가 사용되는 일반적인 위치를 학습하여 온프레미스 네트워크를 통해 라우팅되는 트래픽에서 결과를 줄입니다. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	2021년 9월 7일
GuardDuty SLR로 업데이트	검색 GuardDuty 정확도를 높이기 위한 새로운 동작으로 SLR이 업데이트되었습니다.	2021년 8월 3일
각 결과 유형에 대한 데이터 소스 정보가 추가되었습니다.	이제 검색 결과 설명에는 해당 검색 결과를 생성하는 데 GuardDuty 사용되는 데이터 소스에 대한 정보가 포함됩니다.	2021년 5월 10일

13개의 결과 유형이 사용 중지되었습니다.	13개의 검색 결과가 삭제되어 새 AnomalousBehavoir 검색 결과로 대체되었습니다. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissionsPersistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResourcesStealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.UnusualImpact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	2021년 3월 12일

이상 동작에 대한 8개의 새로운 결과 유형이 추가되었습니다.	IAM 보안 주체의 이상 동작을 기반으로 하는 8개의 새로운 IAMUser 결과 유형이 추가되었습니다. 해당 결과 유형: CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	2021년 3월 12일
도메인 평판을 기반으로 한 EC2 결과가 추가되었습니다.	도메인 평판을 기반으로 하는 4개의 새로운 영향 결과 유형이 추가되었습니다. 해당 결과 유형: Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. 또한 C&CActivity에 대한 새로운 EC2 결과가 추가되었습니다. 해당 결과: Impact:EC2/SuspiciousDomainRequest.Reputation	2021년 1월 27일

4개의 새로운 결과 유형이 추가되었습니다.	3개의 새로운 S3 MaliciousIPCaller 결과가 추가되었습니다. 해당 결과: 해당 결과 유형: Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. 또한 C&CActivity에 대한 새로운 EC2 결과가 추가되었습니다. 해당 결과: Backdoor:EC2/C&CActivity.B	2020년 12월 21일
UnauthorizedAccess:EC2/TorIPCaller 결과 유형이 사용 중지되었습니다.	UnauthorizedAccess:EC2/TorIPCaller검색 유형은 이제 더 이상 사용되지 않습니다. GuardDuty 자세히 알아보기	2020년 10월 1일
Impact:EC2/WinRmBruteForce 결과 유형이 추가되었습니다.	새로운 Impact 결과인 Impact:EC2/WinRmBruteForce이 추가되었습니다. 자세히 알아보기	2020년 9월 17일
Impact:EC2/PortSweep 결과 유형이 추가되었습니다.	새로운 Impact 결과인 Impact:EC2/PortSweep이 추가되었습니다. 자세히 알아보기	2020년 9월 17일
GuardDuty 이제 아프리카 (케이프타운) 및 유럽 (밀라노) 지역에서 사용할 수 있습니다.	사용 가능한 AWS 지역 목록에 아프리카 (케이프타운) 및 유럽 (밀라노) 을 추가했습니다. GuardDuty 자세히 알아보기	2020년 7월 31일

GuardDuty 비용 모니터링을 위한 새로운 사용 세부 정보가 추가되었습니다.	이제 새 지표를 사용하여 관리하는 계정 및 계정의 GuardDuty 사용 비용 데이터를 쿼리할 수 있습니다. 사용 비용에 대한 새로운 개요는 콘솔(https://console.aws.amazon.com/guardduty/)에서 제공됩니다. API를 통해 더 자세한 정보에 액세스할 수 있습니다.	2020년 7월 31일
에서 S3 데이터 이벤트 모니터링을 통해 S3 보호를 다루는 콘텐츠를 추가했습니다 GuardDuty.	GuardDuty 이제 S3 데이터 플레인 이벤트를 새 데이터 소스로 모니터링하여 S3 보호를 사용할 수 있습니다. 새 계정에서는 이 기능이 자동으로 활성화됩니다. 이미 사용하고 GuardDuty 있는 경우 본인 또는 회원 계정에 대해 새 데이터 소스를 활성화할 수 있습니다.	2020년 7월 31일
14개의 새로운 S3 결과가 추가되었습니다.	S3 컨트롤 플레인 및 데이터 플레인 소스에 대해 14개의 새로운 S3 결과 유형이 추가되었습니다.	2020년 7월 31일

S3 결과에 대한 지원이 추가되었고 기존 결과 유형 이름 2개가 변경되었습니다.	GuardDuty 이제 검색 결과에 S3 버킷과 관련된 결과에 대한 자세한 내용이 포함됩니다. S3 활동과 관련된 기존 결과 유형의 이름 변경: Policy:IAMUser/S3BlockPublicAccessDisabled가 Policy:S3/BucketBlockPublicAccessDisabled로 변경되었습니다. Stealth:IAMUser/S3ServerAccessLoggingDisabled는 Stealth:S3/ServerAccessLoggingDisabled로 변경되었습니다.	2020년 5월 28일
AWS Organizations 통합을 위한 콘텐츠가 추가되었습니다.	GuardDuty 이제 AWS Organizations 위임된 관리자와 통합되어 조직 내 GuardDuty 계정을 관리할 수 있습니다. 위임된 관리자를 관리자 계정으로 설정하면 위임된 GuardDuty 관리자 계정으로 모든 조직 구성원을 관리할 수 있도록 자동으로 GuardDuty 활성화할 수 있습니다. 새 AWS Organizations 구성원 계정을 자동으로 GuardDuty 활성화할 수도 있습니다. 자세히 알아보기	2020년 4월 20일
결과 내보내기 기능에 대한 콘텐츠가 추가되었습니다.	의 조사 결과 내보내기 기능을 설명하는 콘텐츠가 추가되었습니다 GuardDuty.	2019년 11월 14일

UnauthorizedAccess:EC2/MetadataDNSRebind 결과 유형이 추가되었습니다.	새로운 Unauthorized 결과가 추가되었습니다. UnauthorizedAccess:EC2/MetadataDNSRebind. 자세히 알아보기	2019년 10월 10일
Stealth:IAMUser/S3ServerAccessLoggingDisabled 결과 유형이 추가되었습니다.	새로운 Stealth 결과가 추가되었습니다. Stealth:IAMUser/S3ServerAccessLoggingDisabled. 자세히 알아보기	2019년 10월 10일
Policy:IAMUser/S3BlockPublicAccessDisabled 결과 유형이 추가되었습니다.	새로운 Policy 결과가 추가되었습니다. Policy:IAMUser/S3BlockPublicAccessDisabled. 자세히 알아보기	2019년 10월 10일
Backdoor:EC2/XORDDOS 결과 유형이 사용 중지되었습니다.	Backdoor:EC2/XORDDOS검색 유형은 이제 더 이상 사용되지 않습니다. GuardDuty 자세히 알아보기	2019년 6월 12일
PrivilegeEscalation 결과 유형이 추가되었습니다.	PrivilegeEscalation 결과 유형은 사용자가 에스컬레이션되고 보다 허용적인 권한을 본인 계정에 할당하려는 시도를 탐지합니다. 자세히 알아보기	2019년 5월 14일
GuardDuty 이제 유럽 (스톡홀름) 지역에서 사용할 수 있습니다.	사용 가능한 AWS 지역 목록에 유럽 (스톡홀름) 을 추가했습니다. GuardDuty 자세히 알아보기	2019년 5월 9일
새로운 결과 유형이 추가되었습니다. Recon:EC2/PortProbeEMRUnprotectedPort.	이 조사 결과는 EC2 인스턴스의 EMR과 관련된 민감한 포트가 차단되지 않은 상태에서 적극적으로 탐색되고 있음을 알려 줍니다. 자세히 알아보기	2019년 5월 8일

EC2 인스턴스가 서비스 거부(DoS) 공격에 사용될 수 있음을 탐지하는 5개의 새로운 결과 유형이 추가되었습니다.	이러한 조사 결과는 해당 환경에서 DoS(Denial of Service) 공격에 사용 중이라고 볼 수 있는 방식으로 동작하고 있는 EC2 인스턴스를 알려줍니다. 자세히 알아보기	2019년 3월 8일
새로운 결과 유형 추가: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsage유형을 찾으면 해당 루트 사용자 로그인 자격 증명이 프로그래밍 방식으로 서비스를 AWS 계정 요청하는 데 사용되고 있음을 알려줍니다. AWS 자세히 알아보기	2019년 1월 24일
UnauthorizedAccess:IAMUser/UnusualASNCaller 결과 유형 사용 중지	UnauthorizedAccess:IAMUser/UnusualASNCaller 결과 유형이 사용 중지되었습니다. 이제 다른 활성 검색 유형을 통해 특이한 네트워크에서 호출된 활동에 대한 알림을 받게 됩니다. GuardDuty 생성된 결과 유형은 비정상적인 네트워크에서 호출된 API 범주를 기반으로 합니다. 자세히 알아보기	2018년 12월 21일

2개의 새로운 결과 유형 추가: PenTest:IAMUser/ParrotLinux 및 PenTest:IAMUser/PentooLinux	PenTest:IAMUser/ParrotLinux 결과 유형은 Parrot Security Linux를 실행하는 컴퓨터가 AWS 계정에 속한 보안 인증 정보를 사용하여 API 호출을 수행함을 알려줍니다. PenTest:IAMUser/PentooLinux 결과 유형은 Pentoo Linux를 실행하는 컴퓨터가 AWS 계정에 속한 보안 인증 정보를 사용하여 API 호출을 수행함을 알려줍니다. 자세히 알아보기	2018년 12월 21일
Amazon GuardDuty 공지 SNS 주제에 대한 지원이 추가되었습니다.	이제 GuardDuty 공지 SNS 주제를 구독하여 새로 출시된 검색 결과 유형, 기존 검색 결과 유형에 대한 업데이트 및 기타 기능 변경 사항에 대한 알림을 받을 수 있습니다. 알림은 Amazon SNS에서 지원하는 모든 형식으로 사용할 수 있습니다. 자세히 알아보기	2018년 11월 21일
2개의 새로운 결과 유형 추가: UnauthorizedAccess:EC2/TorClient 및 UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClient검색 유형은 사용자 AWS 환경의 EC2 인스턴스가 Tor Guard 또는 Authority 노드에 연결되고 있음을 알려줍니다. UnauthorizedAccess:EC2/TorRelay유형을 찾으면 사용자 AWS 환경의 EC2 인스턴스가 Tor 릴레이 역할을 하는 것처럼 Tor 네트워크에 연결하고 있음을 알 수 있습니다. 자세히 알아보기	2018년 11월 16일

새로운 결과 유형 추가: CryptoCurrency:EC2/BitcoinTool.B	이 발견은 사용자 AWS 환경의 EC2 인스턴스가 비트코인 또는 기타 암호화폐 관련 활동과 관련된 도메인 이름을 쿼리하고 있음을 알려줍니다. 자세히 알아보기	2018년 11월 9일
이벤트에 전송되는 알림의 빈도를 업데이트하기 위한 지원이 추가되었습니다. CloudWatch	이제 CloudWatch 이벤트에 전송되는 알림의 빈도를 업데이트하여 기존 검색 결과가 이후에 발생할 수 있습니다. 가능한 값은 15분, 1시간 또는 기본값 6시간입니다. 자세히 알아보기	2018년 10월 9일
리전 지원 추가	AWS GovCloud (미국 서부) 에 대한 지역 지원 추가 자세히 알아보기	2018년 7월 25일
in에 대한 AWS CloudFormation StackSets 지원 추가 GuardDuty	Enable Amazon GuardDuty 템플릿을 사용하여 여러 계정에서 GuardDuty 동시에 활성화할 수 있습니다. 자세히 알아보기	2018년 6월 25일
GuardDuty 자동 보관 규칙에 대한 지원 추가	고객은 이제 자동 아카이브 규칙을 세분화하여 빌드함으로써 결과의 범위를 제한할 수 있습니다. 자동 보관 규칙과 일치하는 검색 결과의 경우 GuardDuty 자동으로 보관된 것으로 표시합니다. 이를 통해 고객은 현재 결과 테이블에 관련 결과만 GuardDuty 포함되도록 추가로 조정할 수 있습니다. 자세히 알아보기	2018년 5월 4일

GuardDuty 유럽 (파리) 지역에서 사용할 수 있습니다.	GuardDuty 이제 유럽 (파리) 에서 사용할 수 있으므로 이 지역에서 지속적인 보안 모니터링 및 위협 탐지를 확장할 수 있습니다. 자세히 알아보기	2018년 3월 29일
이제 GuardDuty 관리자 계정 및 멤버 계정 AWS CloudFormation 생성이 지원됩니다.	자세한 내용은 `AWS::GuardDuty::master` 및 `AWS::GuardDuty::member` 섹션을 참조하세요.	2018년 3월 6일
9개의 새로운 CloudTrail 기반 이상 탐지가 추가되었습니다.	이러한 새로운 검색 유형은 지원되는 모든 GuardDuty 지역에서 자동으로 활성화됩니다. 자세히 알아보기	2018년 2월 28일
3개의 새로운 위협 인텔리전스 탐지(결과 유형)가 추가되었습니다.	이러한 새로운 검색 유형은 지원되는 모든 GuardDuty 지역에서 자동으로 활성화됩니다. 자세히 알아보기	2018년 2월 5일
GuardDuty 회원 계정의 한도 증가.	이번 릴리스에서는 계정당 AWS 최대 1,000개의 GuardDuty 멤버 계정을 추가할 수 있습니다 (GuardDuty 관리자 계정). 자세히 알아보기	2018년 1월 25일

GuardDuty 관리자 계정 및 구성원 계정의 신뢰할 수 있는 IP 목록 및 위협 목록에 대한 업로드 및 추가 관리 변경	이번 릴리스에서는 관리자 계정 GuardDuty 계정의 사용자가 신뢰할 수 있는 IP 목록 및 위협 목록을 업로드하고 관리할 수 있습니다. 회원 GuardDuty 계정의 사용자는 목록을 업로드하고 관리할 수 없습니다. 관리자 계정 계정에서 업로드한 신뢰할 수 있는 IP 목록 및 위협 목록은 해당 구성원 계정의 GuardDuty 기능에 적용됩니다. 자세히 알아보기	2018년 1월 25일

이전 업데이트

변경 사항	설명	날짜
최초 게시	Amazon GuardDuty 사용 설명서의 최초 출판.	2017년 11월 28일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.