제로 트러스트 수용: 안전하고 민첩한 비즈니스 혁신 전략

# AWS 규범적 지침

# AWS 규범적 지침: 제로 트러스트 수용: 안전하고 민첩한 비즈니스 혁신 전략

# Table of Contents

# 제로 트러스트 수용: 안전하고 민첩한 비즈니스 혁신 전략

Greg Gooden, Amazon Web Services(AWS)

2023년 12월(문서 기록)

오늘날 조직은 그 어느 때보다 보안을 최우선 과제로 삼고 있습니다. 이를 통해 고객의 신뢰 유지부터 직원 이동성 향상, 새로운 디지털 비즈니스 기회 창출에 이르기까지 다양한 혜택을 누릴 수 있습니다. 그러면서 '시스템과 데이터에 대한 적절한 수준의 보안과 가용성을 보장하기 위한 최적의 패턴은 무엇인가'라는 오래된 질문을 계속 던집니다. 이 질문에 대한 현대적 해답을 설명하는 데 제로 트러스트라는 용어가 점점 더 많이 사용되고 있습니다.

제로 트러스트 아키텍처(ZTA)는 기존 네트워크 제어나 네트워크 경계에만 전적으로 또는 근본적으로 의존하지 않는 디지털 자산에 대한 보안 제어를 제공하는 데 초점을 맞춘 개념적 모델이자 관련 메커니즘입니다. 대신 네트워크 제어에는 ID, 디바이스, 동작 및 기타 풍부한 컨텍스트와 신호가 추가되어 보다 세분화되고 지능적이며 적응력이 뛰어나고 지속적인 액세스 결정을 내릴 수 있습니다. ZTA 모델을 구현하면 사이버 보안의 지속적인 성숙과 특히 심층적인 방어 개념에서 의미 있는 다음 반복을 달성할 수 있습니다.

## 의사 결정 프로세스

ZTA 전략을 구현하려면 신중한 계획과 의사 결정이 필요합니다. 여기에는 다양한 요인을 평가하고 조직 목표에 맞게 조정하는 작업이 포함됩니다. ZTA 여정을 시작하기 위한 주요 의사 결정 프로세스는 다음과 같습니다.

1. 이해관계자 참여 - 다른 CXO, VP, 고위 관리자를 참여시켜 조직의 보안 태세에 대한 우선순위, 우려 사항, 비전을 이해하는 것이 중요합니다. 처음부터 주요 이해관계자를 참여시킴으로써 ZTA 구현을 전체 전략 목표에 맞추고 필요한 지원과 리소스를 확보할 수 있습니다.
2. 위험 평가 - 포괄적인 위험 평가를 수행하면 문제, 과도한 표면적, 중요 자산을 식별하는 데 도움이 되며, 이를 통해 보안 통제 및 투자에 대한 정보에 입각한 결정을 내리는 데 도움이 됩니다. 조직의 기존 보안 태세를 평가하고, 잠재적 약점을 식별하고, 산업 및 운영 환경별 위험 환경을 기반으로 개선 영역의 우선순위를 정합니다.
3. 기술 평가 - 조직의 기존 기술 환경을 평가하고 격차를 식별하면 ZTA 원칙에 부합하는 적절한 도구와 솔루션을 선택하는 데 도움이 됩니다. 이 평가에는 다음 사항에 대한 철저한 분석이 포함되어야 합니다.
   - 네트워크 아키텍처

- Identity and Access Management 시스템
- 인증 및 권한 부여 메커니즘
- 통합 엔드포인트 관리
- 리소스 소유권 도구 및 프로세스
- 암호화 기술
- 모니터링 및 로깅 기능
- 견고한 ZTA 모델을 구축하려면 올바른 기술 스택을 선택하는 것이 중요합니다.

4. 변경 관리 - ZTA 모델 도입이 문화 및 조직에 미치는 영향을 인식하는 것이 필수적입니다. 변경 관리 관행을 구현하면 조직 전체에서 원활한 전환과 수용을 보장할 수 있습니다. 여기에는 직원을 대상으로 ZTA의 원칙과 이점에 대한 교육을 실시하고, 새로운 보안 관행에 대한 교육을 제공하고, 책임과 지속적인 학습을 장려하는 보안 중시 문화를 조성하는 것이 포함됩니다.

이 권장 가이드는 CXO, VP, 고위 관리자에게 ZTA 구현을 위한 포괄적인 전략을 제공하는 것을 목표로 합니다. 다음을 포함하여 ZTA의 주요 측면을 자세히 살펴보겠습니다.

- 조직의 준비 상태
- 단계별 도입 접근 방식
- 이해관계자 협업
- 안전하고 민첩한 비즈니스 혁신을 달성하기 위한 모범 사례

이 가이드에 따라 조직은 ZTA 환경을 탐색하고 Amazon Web Services(AWS) 클라우드의 보안 여정에서 성공적인 결과를 얻을 수 있습니다. AWS는 AWS Verified Access, AWS Identity and Access Management(IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway, and Amazon GuardDuty 등 ZTA 구현에 사용할 수 있는 다양한 서비스를 제공합니다. 이러한 서비스를 사용하여 무단 액세스로부터 AWS 리소스를 보호할 수 있습니다.

# 목표 비즈니스 성과

이 섹션에서는 조직 전반에 걸쳐 제로 트러스트 아키텍처를 정의하고 구현하는 것과 관련된 예상 결과를 설명합니다.

## 보안 태세 개선

조직은 제로 트러스트 원칙을 도입하여 보안 태세를 강화하고, 보안 위험을 완화하고, 클라우드 인프라 및 데이터를 보호할 수 있습니다. 필요에 따라 액세스 권한을 부여하는 제로 트러스트의 기본 원칙은 엄격한 통제와 함께 표면적을 크게 줄이고 보안 이벤트의 잠재적 영향을 제한합니다. 이러한 사전 예방적 접근 방식을 통해 조직은 새로운 보안 위험에 대비하고 자산의 기밀성, 무결성 및 가용성을 보장할 수 있습니다.

## 원활한 클라우드 도입

잘 정의된 제로 트러스트 아키텍처(ZTA) 도입 계획을 개발하면 클라우드 환경으로 원활하고 성공적으로 전환하는 데 도움이 될 수 있습니다. ZTA 원칙은 조직이 클라우드 컴퓨팅의 이점을 안전하게 누릴 수 있는 강력한 기반을 제공함으로써 클라우드 보안 모범 사례와 긴밀히 연계되어 있습니다. 처음부터 ZTA 원칙을 통합하면 조직이 보안을 핵심 요소로 하여 클라우드 아키텍처를 설계하는 데 도움이 됩니다.

## 규정 준수 및 규제 조정

ZTA 관행을 구현하면 조직이 산업 및 규제 요구 사항과 표준을 충족하는 데 도움이 될 수 있습니다. ZTA는 기본적으로 최소 권한 원칙을 장려하고 엄격한 액세스 제어를 시행합니다. 액세스 제어는 종종 다음과 같은 규정에 의해 의무화됩니다.

- 연방정부의 위험 및 인증 관리 프로그램(FedRAMP)
- HIPAA(미국 건강 보험 양도 및 책임에 관한 법)
- PCI DSS(지불 카드 산업 데이터 보안 표준)

조직은 제로 트러스트를 도입하여 데이터 보호, 개인정보 보호 및 규제 준수에 대한 노력을 입증하는 동시에 벌금이나 평판 훼손의 가능성을 최소화할 수 있습니다.

# 향상된 데이터 보호

조직은 데이터 암호화, 액세스 제어 및 정기적인 보안 평가를 구현하여 클라우드 도입 프로세스 전반에서 민감한 데이터를 보호할 수 있습니다. 조직은 다음과 같은 구체적인 조치를 취할 수 있습니다:

- 데이터 암호화 - 데이터 암호화 - 데이터 암호화는 데이터를 원래 일반 텍스트 형식으로 다시 복호화하려면 키가 필요한 방식으로 일반 텍스트 데이터를 사이퍼텍스트로 암호화하는 프로세스입니다. 따라서 권한이 없는 개인은 데이터 사본을 얻을 수 있더라도 민감한 데이터에 액세스하는 것이 훨씬 더 어려워집니다.
- 액세스 제어 - 액세스 제어는 민감한 데이터에 액세스할 수 있는 사용자와 해당 데이터로 수행할 수 있는 작업을 제한합니다. 이는 사용자 역할과 권한을 할당하고 다중 인증 또는 기타 방법을 사용하여 사용자 ID를 확인하는 방법으로 수행할 수 있습니다.
- 정기적인 보안 평가 - 정기적인 보안 평가를 통해 조직은 보안 문제를 식별 및 해결하고 사전에 해결할 수 있습니다. 내부 보안 팀이나 외부 보안 회사에서 이러한 평가를 수행할 수 있습니다.

제로 트러스트 아키텍처는 다양한 보안 조치를 구현하여 데이터 보호에 대한 포괄적인 접근 방식을 취합니다. 이러한 조치에는 강력한 인증, 데이터 암호화, 세분화된 액세스 제어가 포함됩니다. 이 접근 방식은 데이터 관련 보안 이벤트의 위험을 최소화하고 무단 액세스로부터 민감한 정보를 보호합니다.

# 효율적인 인시던트 대응

조직은 클라우드 환경에서 모니터링 및 인시던트 대응 프레임워크를 구축하여 보안 이벤트를 보다 빠르고 효과적으로 탐지하고 대응할 수 있습니다. 제로 트러스트 아키텍처는 지속적인 모니터링, 위협 인텔리전스 통합, 사용자 활동, 네트워크 트래픽 및 시스템 동작에 대한 실시간 가시성을 강조합니다. 그러면 보안 팀이 보안 이벤트를 사전에 식별하고 완화할 수 있습니다. 이 접근 방식은 잠재적 문제를 탐지하고, 대응하는 시간을 줄이고, 비즈니스 운영에 미치는 영향을 최소화합니다. 핵심 사항은 다음과 같습니다.

- 테스트 - 조직이 따르는 인시던트 대응 프레임워크 또는 방법론에 관계없이 인시던트 대응 계획을 정기적으로 테스트해야 합니다. 테이블탑 연습, 시뮬레이션 및 팀 구성을 통해 실제 환경에서 인시던트 대응을 연습하고, 도구 및 기능 격차를 발견하고, 인시던트 대응 담당자의 경험과 자신감을 쌓을 수 있습니다.
- 모니터링 - 클라우드 환경을 지속적으로 모니터링하여 비정상적인 활동의 징후가 있는지 확인합니다. 로그 분석, 네트워크 모니터링, 취약성 검사와 같은 다양한 도구 및 기법을 사용하여 이를 수행할 수 있습니다.

- 위협 인텔리전스 통합 - 모니터링 및 인시던트 대응 프레임워크에 위협 인텔리전스를 통합합니다. 이를 통해 조직은 더 빠르고 효과적으로 위협을 식별하고 이에 대응할 수 있습니다.
- 실시간 가시성 - 보안 인시던트를 신속하게 식별하고 이에 대응하려면 조직에 사용자 활동, 네트워크 트래픽 및 시스템 동작에 대한 실시간 가시성이 필요합니다.
- 사전 식별 및 완화 - 조직은 보안 이벤트를 사전에 식별하고 완화하여 잠재적 위협을 탐지하고 이에 대응하는 시간을 줄이고 비즈니스 운영에 미치는 영향을 최소화할 수 있습니다.

## 직원 생산성 향상

현대의 인력은 점점 더 많은 장소, 디바이스 및 시간에서 작업을 수행할 수 있는 유연성을 필요로 합니다. ZTA를 구현하면 조직의 보안 태세를 유지하거나 개선하는 동시에 이러한 요구 사항을 지원하고 직원 이동성, 생산성 및 만족도를 개선할 수 있습니다.

## 디지털 트랜스포메이션 활성화

디지털 트랜스포메이션의 일환으로 기존 네트워크 경계 외부의 디바이스, 기계, 시설, 인프라 및 프로세스의 상호 연결을 추구하는 조직이 점점 더 많아지고 있습니다. 사물 인터넷(IoT) 및 운영 기술(OT, 산업용 사물 인터넷 또는 IIoT라고도 함) 디바이스는 종종 텔레메트리 및 예측 유지 보수 정보를 클라우드로 직접 전송합니다. 워크로드를 보호하려면 기존의 경계 접근 방식을 넘어서는 보안 제어를 적용해야 합니다.

## 섹션 요약

조직은 이러한 목표 비즈니스 성과에 집중하여 ZTA의 잠재력을 최대한 실현하고 클라우드에서 보안 태세를 강화할 수 있습니다. 이러한 결과를 특정 조직 목표에 맞추고, 고유한 비즈니스 요구 사항에 맞게 조정하고, 정기적으로 효율성을 평가하여 지속적인 개선을 추진하는 것이 중요합니다.

# 제로 트러스트 원칙 이해

제로 트러스트 아키텍처(ZTA)는 보안 모델의 기초를 형성하는 일련의 핵심 원칙을 기반으로 합니다. 이러한 원칙을 이해하는 것은 ZTA 전략을 효과적으로 도입하고자 하는 조직에 필수적입니다. 이 섹션에서는 ZTA의 핵심 원칙을 다룹니다.

## 확인 및 인증

확인 및 인증 원칙은 사용자, 시스템, 디바이스를 포함한 모든 유형의 보안 주체에 대한 강력한 식별 및 인증의 중요성을 강조합니다. ZTA는 세션 전반에 걸쳐, 이상적으로는 각 요청에 대해 지속적인 ID 및 인증 상태 확인을 요구하며, 기존 네트워크 위치나 제어에만 의존하지는 않습니다. 여기에는 현대의 강력한 다중 인증(MFA) 구현과 인증 프로세스 중 추가적인 환경 및 컨텍스트 신호 평가가 포함됩니다. 조직은 이 원칙을 도입하여 리소스 권한 부여 결정에 가능한 최상의 ID 입력을 보장할 수 있습니다.

## 최소 권한 액세스

최소 권한 원칙에는 보안 주체에게 작업을 수행하는 데 필요한 최소한의 액세스 수준 부여가 포함됩니다. 최소 권한 액세스 원칙을 도입함으로써 조직은 세분화된 액세스 제어를 시행하여 보안 주체가 자신의 역할과 책임을 수행하는 데 필요한 리소스에만 액세스하도록 할 수 있습니다. 여기에는 노출 영역과 무단 액세스의 위험을 최소화하기 위한 적시 액세스 프로비저닝, 역할 기반 액세스 제어(RBAC) 및 정기적인 액세스 검토 구현이 포함됩니다.

## 마이크로 분할

마이크로 분할은 네트워크를 더 작고 격리된 세그먼트로 나누어 특정 트래픽 흐름을 승인하는 네트워크 보안 전략입니다. 워크로드 경계를 만들고 서로 다른 세그먼트 간에 엄격한 액세스 제어를 적용하여 마이크로 분할을 수행할 수 있습니다.

마이크로 분할은 네트워크 가상화, 소프트웨어 정의 네트워킹(SDN), 호스트 기반 방화벽, 네트워크 액세스 제어 목록(NACL) 및 Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹 또는 AWS PrivateLink 등의 AWS 고유 기능을 통해 구현할 수 있습니다. 분할 게이트웨이는 세그먼트 간 트래픽을 제어하여 액세스를 명시적으로 승인합니다. 마이크로 분할 및 분할 게이트웨이는 조직이 네트워크를 통한 불필요한 경로, 특히 중요한 시스템 및 데이터로 이어지는 경로를 제한하는 데 도움이 됩니다.

# 지속적인 모니터링 및 분석

지속적인 모니터링 및 분석에는 조직 환경 전반에서 보안 관련 이벤트 및 데이터 수집, 분석, 상관관계 파악이 포함됩니다. 조직은 강력한 모니터링 및 분석 도구를 구현하여 보안 데이터와 텔레메트리를 융합된 방식으로 평가할 수 있습니다.

이 원칙은 이상과 잠재적 보안 이벤트를 식별하기 위해 사용자 동작, 네트워크 트래픽 및 시스템 활동에 대한 가시성의 중요성을 강조합니다. 보안 정보 및 이벤트 관리(SIEM), 사용자 및 엔터티 행동 분석(UEBA), 위협 인텔리전스 플랫폼과 같은 고급 기술은 지속적인 모니터링과 사전 위협 탐지를 달성하는 데 중요한 역할을 합니다.

# 자동화 및 오케스트레이션

자동화 및 오케스트레이션을 통해 조직은 보안 프로세스를 간소화하고, 수동 개입을 줄이고, 응답 시간을 개선할 수 있습니다. 조직은 일상적인 보안 작업을 자동화하고 오케스트레이션 기능을 사용하여 일관된 보안 정책을 적용하고 보안 이벤트에 신속하게 대응할 수 있습니다. 이 원칙에는 사용자 권한을 시기적절하고 정확하게 관리할 수 있도록 액세스 프로비저닝 및 프로비저닝 해제 프로세스를 자동화하는 것도 포함됩니다. 자동화와 오케스트레이션을 도입함으로써 조직은 운영 효율성을 높이고 인적 오류를 줄이고 리소스를 보다 전략적인 보안 이니셔티브에 집중할 수 있습니다.

# 권한 부여

ZTA에서는 리소스에 액세스하려는 각 요청이 게이트 시행 지점에 의해 명시적으로 승인되어야 합니다. 인증 정책은 인증된 ID 외에도 디바이스 상태 및 상태, 동작 패턴, 리소스 분류, 네트워크 요인과 같은 추가 컨텍스트를 고려해야 합니다. 권한 부여 프로세스는 액세스 중인 리소스와 관련된 해당 액세스 정책을 기준으로 이 통합 컨텍스트를 평가해야 합니다. 기계 학습 모델은 선언적 정책을 동적으로 보완할 수 있는 최적의 모델입니다. 이러한 모델을 활용할 때는 추가 제한에만 초점을 맞춰야 하며, 명시적으로 지정되지 않은 액세스 권한을 부여해서는 안 됩니다.

# 섹션 요약

조직은 ZTA의 이러한 핵심 원칙을 준수하여 현대 기업 환경의 다양성에 부합하는 강력한 보안 모델을 구축할 수 있습니다. 이러한 원칙을 구현하려면 기술, 프로세스, 사람을 결합하여 제로 트러스트 사고방식을 계발하고 탄력적인 보안 태세를 구축하는 포괄적인 접근 방식이 필요합니다.

# 제로 트러스트 아키텍처의 주요 구성 요소

제로 트러스트 아키텍처(ZTA) 전략을 효과적으로 구현하려면 조직에서 ZTA를 구성하는 주요 구성 요소를 이해해야 합니다. 이러한 구성 요소가 함께 작용하여 제로 트러스트 원칙에 부합하는 포괄적인 보안 모델을 바탕으로 지속적으로 개선합니다. 이 섹션에서는 ZTA의 주요 구성 요소를 다룹니다.

## 자격 증명 및 액세스 관리

ID 및 액세스 관리는 강력한 사용자 인증과 대략적인 액세스 제어 메커니즘을 제공하여 ZTA의 기반을 형성합니다. 여기에는 Single Sign-On(SSO), 다중 인증(MFA), ID 거버넌스 및 관리 솔루션과 같은 기술이 포함됩니다. ID 및 액세스 관리는 제로 트러스트 권한 부여 결정을 내리는 데 필수적인 높은 수준의 인증 보장과 중요한 컨텍스트를 제공합니다. 동시에 ZTA는 사용자별, 디바이스별, 세션별로 애플리케이션 및 리소스에 대한 액세스 권한을 부여하는 보안 모델입니다. 이를 통해 사용자의 보안 인증이 침해되더라도 조직을 무단 액세스로부터 보호할 수 있습니다.

## Secure Access Service Edge

SASE(Secure Access Service Edge)는 네트워킹 및 보안 기능을 단일 클라우드 기반 서비스로 가상화, 결합 및 배포하는 네트워크 보안에 대한 새로운 접근 방식입니다. SASE는 사용자의 위치와 관계없이 애플리케이션 및 리소스에 대한 보안 액세스를 제공할 수 있습니다.

SASE에는 보안 웹 게이트웨이, 서비스형 방화벽, 제로 트러스트 네트워크 액세스(ZTNA)와 같은 다양한 보안 기능이 포함되어 있습니다. 이러한 기능이 함께 작동하여 멀웨어, 피싱, 랜섬웨어를 비롯한 광범위한 위협으로부터 조직을 보호합니다.

## 데이터 손실 방지

데이터 손실 방지(DLP) 기술은 조직이 민감한 데이터가 무단으로 공개되지 않도록 보호하는 데 도움이 될 수 있습니다. DLP 솔루션은 이동 중인 데이터와 저장 데이터를 모니터링하고 제어합니다. 이를 통해 조직은 데이터 관련 보안 이벤트를 방지하는 정책을 정의하고 시행하여 네트워크 전체에서 민감한 정보를 계속 보호할 수 있습니다.

## 보안 정보 및 이벤트 관리

보안 정보 및 이벤트 관리(SIEM) 솔루션은 조직 인프라 전반의 다양한 소스에서 보안 이벤트 로그를 수집, 집계 및 분석합니다. 이 데이터를 사용하여 보안 인시던트를 탐지하고, 인시던트 대응을 촉진하고, 잠재적 위협 및 취약성에 대한 인사이트를 제공할 수 있습니다.

특히 ZTA의 경우, 비정상 패턴의 탐지 및 대응을 개선하기 위해서는 다양한 보안 시스템의 관련 텔레메트리를 상호 연관시키고 이해하는 SIEM 솔루션의 기능이 매우 중요합니다.

## 엔터프라이즈 리소스 소유권 카탈로그

기업 리소스에 대한 액세스 권한을 올바르게 부여하려면 조직은 이러한 리소스를 분류하는 신뢰할 수 있는 시스템을 갖추고 있어야 하며, 중요한 것은 누가 해당 리소스를 소유하고 있는지 파악하는 것입니다. 이러한 정보 소스는 액세스 요청, 관련 승인 결정 및 이에 대한 정기적인 증명을 용이하게 하는 워크플로를 제공해야 합니다. 시간이 지나면 이 정보 소스에는 조직 내에서 '누가 무엇에 액세스할 수 있는가?'에 대한 답이 포함될 것입니다. 권한 부여, 감사 및 규정 준수에 대한 답변을 모두 사용할 수 있습니다.

## 통합 엔드포인트 관리

ZTA는 사용자를 강력하게 인증하는 것 외에도 사용자 디바이스의 상태와 태세를 고려하여 기업 데이터 및 리소스 액세스가 안전한지 평가해야 합니다. 통합 엔드포인트 관리(UEM) 플랫폼은 다음과 같은 기능을 제공합니다.

- 디바이스 프로비저닝
- 지속적인 구성 및 패치 관리
- 보안 기준 설정
- 텔레메트리 보고
- 디바이스 정리 및 사용 중지

## 정책 기반 시행 지점

ZTA에서는 각 리소스에 대한 액세스가 게이트 정책 기반 시행 지점에 의해 명시적으로 승인되어야 합니다. 처음에 이러한 시행 지점은 기존 네트워크 및 ID 시스템의 기존 시행 지점을 기반으로 할 수 있습니다. ZTA가 제공하는 다양한 상황과 신호를 고려하면 시행 지점의 역량을 점차 강화할 수 있습니다. 장기적으로는 통합 컨텍스트에서 운영되는 ZTA 전용 시행 지점을 구현하고, 신호 제공업체를 일관되게 통합하고, 포괄적인 정책 세트를 유지하고, 결합된 텔레메트리를 통해 수집한 인텔리전스를 통해 강화되는 ZTA 전용 시행 지점을 구현해야 합니다.

# 섹션 요약

ZTA 도입을 계획하는 조직에서는 이러한 주요 구성 요소를 이해하는 것이 필수적입니다. 이러한 구성 요소를 구현하고 보안 모델에 통합하여 조직은 제로 트러스트 원칙에 따라 강력한 보안 태세를 구축할 수 있습니다. 다음 섹션에서는 조직 내에서 ZTA를 성공적으로 구현하는 데 도움이 되는 조직의 준비 상태, 단계별 도입 접근 방식, 모범 사례를 살펴봅니다.

# 제로 트러스트 도입을 위한 조직의 준비 상태 평가

새로운 아키텍처 전략 도입은 조직적 요소를 신중하게 계획하고 고려해야 하는 중요한 작업입니다. 이 섹션에서는 전사적 제로 트러스트 도입을 위한 조직의 주요 준비 상태 고려 사항을 중점적으로 다룹니다. 이러한 고려 사항을 해결함으로써 조직은 보다 강력하고 성공적인 보안 태세를 위한 기반을 마련할 수 있습니다.

## 리더십 정비 및 커뮤니케이션

제로 트러스트를 성공적으로 구현하려면 리더십 정비와 커뮤니케이션이 필수적입니다. 리더십은 제로 트러스트의 이점과 필요한 리소스를 파악해야 합니다. 또한 리더는 조직의 문화와 프로세스를 바꿀 의지가 있어야 합니다. 신뢰와 지지를 얻으려면 직원과의 커뮤니케이션이 필요합니다. 직원들은 조직이 제로 트러스트를 구현하는 이유, 제로 트러스트가 자신에게 어떤 의미가 있는지, 어떻게 도울 수 있는지 이해해야 합니다. 커뮤니케이션은 개방적이고 투명하고 지속적이어야 합니다.

리더십 지원 및 동의

성공적인 제로 트러스트 아키텍처(ZTA) 구현을 위해서는 아키텍처의 목표, 이점 및 성공 척도에 대해 주요 이해관계자와 경영진을 조율하는 것이 중요합니다. 기존의 경계 기반 보안에서 벗어나 사용자 중심의 보다 세분화된 접근 방식으로 보안을 강화하고 비즈니스 민첩성을 지원하는 데 있어 제로 트러스트 원칙의 중요성을 공유합니다. 이 접근 방식으로 전환하면 조직이 변화와 위협에 더 빠르게 적응할 수 있습니다. 경영진 조율은 조직의 분위기를 조성하고 변화에 대한 잠재적 저항을 극복하는 데 도움이 됩니다.

투명한 커뮤니케이션

제로 트러스트 구현 프로세스 전반에 걸쳐 직원들과 개방적이고 투명한 커뮤니케이션을 유지합니다. 도입의 근거, 이점 및 예상 결과를 설명하고 우려 사항을 즉시 해결합니다. 구현 진행 상황에 대한 정기적인 업데이트를 제공합니다. 이를 통해 지지를 늘리고 저항을 줄이고 신뢰를 구축할 수 있습니다.

## 기술 개발 및 교육

리더십이 정비되고 열린 커뮤니케이션이 이루어진 후에는 제로 트러스트를 구현할 직원의 기술과 지식을 개발하는 것이 중요합니다. 여기에는 제로 트러스트 원칙의 이해, 업무에서 이를 이행하는 방법, 보안 이벤트에 대응하는 방법이 포함됩니다. 직원들이 이러한 기술을 습득할 수 있도록 교육 및 개발 기회를 제공합니다.

클라우드 지식 및 기술

클라우드 기술 및 제로 트러스트 원칙에 대한 조직의 기술 및 지식 격차를 평가합니다. 직원의 기술을 향상시키고 클라우드 중심 및 제로 트러스트 환경에서 효과적으로 작업하는 데 필요한 전문 지식을 갖추도록 교육 및 개발 프로그램을 제공합니다. 진화하는 기술 및 보안 관행과 보조를 맞추기 위한 지속적인 학습 문화를 조성합니다.

보안 문화 및 인식

조직의 보안 문화를 평가합니다. 직원들의 보안 인식 수준, 보안 모범 사례에 대한 이해, 정책 및 절차 준수 여부를 평가합니다. 보안 지식의 격차를 파악합니다. 직원들에게 제로 트러스트의 중요성과 보안 환경 유지에 있어 직원의 역할을 교육하는 보안 인식 교육 프로그램을 실시하는 것을 고려해 봅니다.

## 조직 구조 및 역할

제로 트러스트를 성공적으로 구현하려면 효과적인 조직 구조와 역할을 정립합니다. 여기에는 클라우드 혁신 센터(CCoE) 설립, 보안 운영 검토 및 수정, 취약성 관리, 인시던트 대응, 보안 모니터링을 위한 역할 및 책임 할당이 포함됩니다.

클라우드 혁신 센터

클라우드 운영 지침, 모범 사례 및 감독을 제공하기 위한 CCoE를 설립합니다. CCoE는 클라우드 관련 모범 사례, 지침 및 거버넌스 정책을 만들고 구현하는 일을 담당하는 팀 또는 개인 그룹입니다. CCoE에는 협업과 조율을 보장하기 위해 다양한 사업부와 IT 팀의 담당자가 포함되어야 합니다. CCoE는 클라우드 호스팅 워크로드에 제로 트러스트 원칙을 도입하는 데 중요한 역할을 합니다. 또한 CCoE는 조직 전반에 걸친 지식 공유를 용이하게 합니다.

보안 운영

제로 트러스트 환경의 요구 사항을 충족하려면 현재 보안 운영 조직을 검토하고 수정합니다. 모니터링, 인시던트 대응 및 위협 인텔리전스 기능을 개선하려면 보안 운영 센터(SOC) 또는 관리형 보안 서비스 제공업체(MSSP) 구현을 고려합니다. 취약성 관리, 인시던트 대응 및 보안 모니터링에 대한 역할과 책임을 정립합니다. 잘 작동하는 인시던트 대응 프로세스는 사소한 보안 이벤트를 신속하게 탐지하고 해결하여 이벤트 순서를 중단하는 데 매우 중요합니다. 이를 통해 사소한 이벤트가 더 큰 영향을 미치는 이벤트로 발전하는 것을 막을 수 있습니다.

## IT 인프라 및 아키텍처

회사의 IT 아키텍처와 인프라를 검토하여 제로 트러스트 접근 방식 도입에 영향을 미칠 수 있는 제약이나 종속성을 찾습니다. 현재 애플리케이션 및 시스템이 필요한 제로 트러스트 아키텍처 구성 요소와 호

환되는지 확인합니다. 제로 트러스트 원칙의 성공적인 배포를 지원하기 위해 인프라 개선 또는 조정이 필요한지 분석합니다. 각 애플리케이션이나 시스템에 대해 제로 트러스트가 현재 구현되는 것이 가장 좋은지 아니면 대규모 현대화 노력을 통해 구현되는 것이 가장 좋은지 검토합니다.

# 위험 관리, 거버넌스 및 변경 제어

제로 트러스트를 성공적으로 구현하려면 효과적인 위험 관리, 거버넌스 및 변경 제어 프로세스를 수립합니다. 여기에는 제로 트러스트 원칙에 따른 위험 관리 조정, 인시던트 대응 계획 개발, 법률 및 규정 준수 부서와의 협력, 변경 관리 프로세스 수립 등이 포함됩니다.

위험 관리

회사에서 시행 중인 리스크 관리 전략을 점검하고 제로 트러스트 원칙을 얼마나 잘 준수하는지 확인합니다. 현재 인시던트 대응 시스템, 보안 조치 및 위험 평가 절차의 효율성을 분석합니다. 제로 트러스트 전략을 준수하기 위해 개선이 필요한 영역을 결정합니다. 자동화된 인시던트 대응 시스템 또는 지속적인 모니터링 및 분석 프레임워크 개발을 시작하여 해결 속도를 높입니다.

제어 프로세스 변경

모든 클라우드 관련 수정 사항이 보안 및 규정 준수 요구 사항을 준수하도록 하려면 효과적인 변경 관리 방법을 확립합니다. 보안 구성 분석, 위험 평가, 승인 및 문서화를 포함하는 체계적인 변경 관리 절차를 수립합니다. 제로 트러스트 아키텍처의 무결성을 보존하기 위해 업데이트를 자주 검토하고 감사합니다.

# 모니터링 및 평가

제로 트러스트를 성공적으로 구현하려면 조직에서 보안 상태를 지속적으로 모니터링하고 평가해야 합니다. 여기에는 핵심 성과 지표(KPI) 수립, KPI 모니터링 및 평가, 지속적인 개선 문화 조성 등이 포함됩니다. 이러한 단계를 수행함으로써 조직은 제로 트러스트 구현이 성공적으로 이루어졌는지, 그리고 보안을 개선하기 위해 항상 노력하고 있는지 확인할 수 있습니다.

핵심 성과 지표

제로 트러스트 배포의 성공과 효과를 측정할 수 있는 관련 핵심 성과 지표(KPI)를 설정합니다. 이러한 KPI는 사용자 만족도, 장비 및 롤아웃 진행 상황, 비용 절감, 규정 준수 및 보안 이벤트 발생 횟수를 측정할 수 있습니다. 전체 개발 상황을 추적하고 개선 기회를 찾으려면 이러한 KPI를 정기적으로 모니터링하고 평가합니다.

지속적 개선

이해관계자의 의견과 인사이트를 이끌어내는 시스템을 구축하면 지속적인 개선 문화를 조성하는 데 도움이 됩니다. 직원들이 클라우드 환경의 보안, 효과 및 사용자 경험을 개선하기 위한 생각과 제안을 제공하도록 장려합니다. 이 입력 내용을 활용하여 절차를 간소화하고, 보안 조치를 개선하고, 혁신을 촉진합니다.

## 섹션 요약

이러한 조직적, 문화적 고려 사항을 해결함으로써 조직은 제로 트러스트 보안 모델의 클라우드 도입을 위한 지원 환경을 조성할 수 있습니다. 다음 섹션에서는 단계적 도입 접근 방식을 살펴보고 실용적이고 관리 가능한 방식으로 제로 트러스트 원칙을 점진적으로 구현하는 방법에 대한 지침을 제공합니다.

# 제로 트러스트 사고방식 배양

제로 트러스트 구현은 기술적 구현을 넘어섭니다. 이를 위해서는 조직 내 문화적 변화가 필요합니다. 제로 트러스트 사고방식을 육성하려면 다음과 같은 주요 측면을 강조해야 합니다.

## 제로 트러스트 교육 및 훈련

직원들에게 제로 트러스트 아키텍처 (ZTA) 의 가치와 이점에 대해 교육합니다. 교육 세션, 워크숍 및 기타 리소스를 통해 ZTA 개념 및 접근 방식에 대한 기술적 및 비기술적 설명을 제공합니다. 직원들이 제로 트러스트 보안 패러다임을 수립하고 유지하는 데 따르는 책임을 인식하도록 장려하세요.

## 협업 및 커뮤니케이션

ZTA 구현에 관련된 모든 팀과 부서의 협업과 투명성을 촉진하세요. 모든 사람이 계획을 완전히 이해할 수 있도록 부서 간 커뮤니케이션, 지식 공유 및 정보 교환을 장려하십시오. 모든 사람이 비즈니스의 전반적인 보안에 대한 기여의 중요성을 인식하는 책임 공유 문화를 조성하세요.

## 지속적인 학습 및 개선

제로 트러스트의 맥락에서 지속적인 학습과 개선을 우선시하세요. 직원들이 최신 보안 동향, 기술 및 모범 사례에 대한 최신 정보를 숙지하도록 권장합니다. 직원들이 조직의 보안 태세를 강화하기 위한 새로운 솔루션과 접근 방식을 모색하도록 장려하는 혁신과 실험의 문화를 조성하십시오.

## 지표 및 책임

제로 트러스트 전략의 효과를 측정하기 위한 명확한 지표와 책임 메커니즘을 수립하세요. 조직의 보안 목표에 맞는 핵심 성과 지표 (KPI) 를 정의하고 진행 상황을 정기적으로 추적하세요. 제로 트러스트 원칙의 구현과 유지에 기여한 개인과 팀에 책임을 물으세요.

## 섹션 요약

이러한 측면을 해결하고 제로 트러스트 사고방식을 함양함으로써 조직은 제로 트러스트의 성공적인 채택 및 구현을 위한 견고한 토대를 마련할 수 있습니다. 이러한 문화적 변화는 조직 내 모든 사람이 제로 트러스트의 중요성을 이해하고 성공에 적극적으로 기여할 수 있도록 돕는 데 필수적입니다.

다음 섹션에서는 단계적 채택 접근 방식을 살펴보고 실용적이고 관리 가능한 방식으로 제로 트러스트 원칙을 점진적으로 구현하는 방법에 대한 지침을 제공합니다.

# 제로 트러스트에 대한 단계적 접근 방식

제로 트러스트 아키텍처(ZTA)를 도입하려면 신중한 계획과 구현이 필요합니다. 원활한 전환과 비즈니스 운영 중단 최소화를 위해 단계적 도입 접근 방식을 권장합니다. 이 섹션에서는 ZTA 도입과 관련된 주요 단계에 대한 지침을 제공합니다.

## 1단계: 평가 및 계획

제로 트러스트 구현의 첫 번째 단계는 평가 및 계획입니다. 이 단계는 조직의 현재 보안 태세에서 부족한 부분을 파악하고 해결하는 작업을 포함하므로 전체 구현의 성공에 매우 중요합니다. 시간을 내어 현재 상태를 평가하고 보안 목표를 정의하면 성공적인 제로 트러스트 구현을 위한 기반을 마련할 수 있습니다.

동시에 완벽하고 정확한 평가가 항상 현실적이지는 않을 수도 있습니다. 다음 단계로 넘어가지 못하게 하는 분석 마비를 방지하려면 일정 수준의 불완전성을 구분하거나 수용할 준비를 합니다.

1. 현재 상태 평가 - 기존 보안 인프라, 정책 및 제어 평가를 수행합니다. 잠재적 취약성, 보안의 격차, 제로 트러스트 원칙의 구현으로 개선이 가능한 영역을 파악합니다.
2. 보안 목표 정의 - 현재 상태 평가 조사 결과를 바탕으로 제로 트러스트 원칙에 부합하는 보안 목표를 정의합니다. 또한 이러한 보안 목표는 조직의 전체 보안 전략에 부합하고 식별된 취약성과 격차를 해소해야 합니다.
3. 아키텍처 설계 - 조직의 보안 목표를 지원하는 ZTA를 개발합니다. 이 아키텍처에는 ID 및 액세스 관리 솔루션, 네트워크 세분화 메커니즘, 지속적인 모니터링 시스템 등의 필수 구성 요소가 포함되어야 합니다. 또한 아키텍처는 확장 가능하고 적응력이 뛰어나며 미래의 성장 및 기술 발전을 수용할 수 있어야 합니다. 이 아키텍처는 문서나 다이어그램뿐만 아니라 AWS CloudFormation 템플릿과 같이 구현을 담당하는 팀이 쉽게 사용할 수 있는 형식으로 표현하는 것이 가장 이상적입니다.
4. 이해관계자 참여 - 사업부, IT 팀, 보안 팀을 비롯한 모든 이해관계자를 참여시켜 인사이트를 얻고 목표를 ZTA 구현 계획에 맞게 조정합니다. 협업과 소통을 장려하여 제로 트러스트 접근 방식의 이점과 요구 사항에 대한 공통된 이해를 확립합니다.

## 2단계: 파일럿 및 구현

제로 트러스트 구현의 두 번째 단계는 파일럿 및 구현입니다. 이 단계에서는 소규모의 통제된 환경에서 ZTA를 테스트한 다음, 조직 전체에 반복적으로 배포합니다. 직원들에게 새로운 보안 조치와 제로 트러스트 환경을 유지하기 위한 각자의 역할에 대해 교육하는 것이 중요합니다.

1. 배포 파일럿 - 소규모의 통제된 환경에서 ZTA를 테스트합니다. 아키텍처 설계 단계에서 정의된 필수 구성 요소 및 보안 제어를 구현합니다. 파일럿 배포를 면밀히 모니터링하고 피드백을 수집하고 필요한 조정을 수행합니다. 제로 트러스트가 가상의 연습에서 실제 경험을 쌓는 과정으로 전환되는 프로세스 초기에 유연하게 대처할 수 있도록 준비합니다.
2. 반복적 배포 - 파일럿 배포에서 얻은 교훈을 바탕으로 조직 전체에 제로 트러스트를 반복적으로 배포하기 시작합니다. 중요한 배포 규모를 달성하기 위해 대규모 캠페인이 필요하지 않은 플라이휠 효과를 통해 추진력을 확보합니다. 롤아웃이 길어질 경우 필요할 수 있으므로 리더십 위임 또는 에스컬레이션을 예약하세요.
3. 사용자 교육 제공 및 인식 제고 - 직원들에게 새로운 보안 조치와 제로 트러스트 환경 유지 관리에 필요한 역할에 대해 교육합니다. 강력한 암호, 다중 인증, 정기적인 보안 업데이트와 같은 보안 관행의 중요성을 강조합니다.
4. 변경 관리 - 제로 트러스트 도입과 관련된 조직적, 문화적 변화에 대응하기 위한 포괄적인 변경 관리 계획을 수립합니다. 도입의 이점과 근거를 직원들에게 전달하고 우려 사항이나 저항이 있는 부분을 해결합니다. 원활한 전환을 위해 지속적인 지원과 지침을 제공합니다.

## 3단계: 모니터링 및 지속적인 개선

제로 트러스트 구현의 세 번째이자 마지막 단계는 모니터링과 지속적인 개선입니다. 이 단계에는 포괄적인 모니터링 및 분석 프로그램을 수립하고, 포괄적인 인시던트 대응 계획을 수립하고, 이해관계자와 사용자에게 정기적으로 피드백을 요청하는 작업이 포함됩니다.

1. 지속적인 모니터링 - 포괄적인 모니터링 및 분석 프로그램을 구축하여 보안 태세를 지속적으로 평가하고 잠재적 이상을 탐지합니다. 고급 보안 도구 및 기술을 사용하여 사용자 동작, 네트워크 트래픽 및 시스템 활동을 모니터링합니다.
2. 인시던트 대응 및 해결 계획 - 제로 트러스트 원칙에 부합하는 포괄적인 인시던트 대응 계획을 세웁니다. 명확한 에스컬레이션 경로를 설정하고, 역할과 책임을 정의하고, 가능한 경우 자동화된 인시던트 대응 메커니즘을 구현합니다. 인시던트 대응 계획을 정기적으로 테스트하고 업데이트합니다.
3. 피드백 및 평가 받기 - 이해관계자와 사용자에게 정기적으로 피드백을 요청하여 제로 트러스트 아키텍처(ZTA)의 효과에 대한 인사이트를 수집합니다. 보안 태세, 운영 효율성 및 사용자 경험에 미치는 영향을 측정하기 위해 정기적인 평가 및 평가를 수행합니다. 피드백 및 평가 결과를 사용하여 개선이 필요한 영역을 파악합니다. 시간이 지남에 따라 ZTA가 변경될 것으로 예상하고 개발 팀이 최소한의 노력이나 중단으로 이러한 업데이트를 구현하는 방법을 고려합니다.

# 섹션 요약

이러한 단계별 도입 접근 방식을 따라 조직은 위험과 중단을 최소화하면서 ZTA로 효과적으로 전환할 수 있습니다. 다음 섹션에서는 CXO, VP, 고위 관리자를 위한 주요 고려 사항과 권장 사항을 다루면서 제로 트러스트 구현으로 성공을 달성하기 위한 모범 사례를 논의합니다.

# 제로 트러스트로 성공을 거두기 위한 모범 사례

제로 트러스트 아키텍처(ZTA)를 성공적으로 도입하려면 전략적 접근 방식과 모범 사례 준수가 필요합니다. 이 섹션에서는 CXO, VP, 고위 관리자가 제로 트러스트를 성공적으로 도입하는 데 도움이 되는 일련의 모범 사례를 소개합니다. 조직은 다음 권장 사항을 따라 강력한 보안 기반을 구축하고 제로 트러스트 접근 방식의 이점을 실현할 수 있습니다.

- 명확한 목표 및 비즈니스 성과 정의 - 클라우드 운영의 목표와 원하는 비즈니스 성과를 명확하게 정의합니다. 이러한 목표를 제로 트러스트 원칙에 맞게 조정하여 비즈니스 성장과 혁신을 지원하는 동시에 강력한 보안 기반을 구축합니다.
- 포괄적인 평가 수행 - 현재 IT 인프라, 애플리케이션 및 데이터 자산에 대한 포괄적인 평가를 수행합니다. 종속성, 기술 부채, 잠재적인 호환성 문제를 파악합니다. 이 평가를 통해 도입 계획을 세우고 중요도, 복잡성, 비즈니스 영향에 따라 워크로드의 우선순위를 정할 수 있습니다.
- 도입 계획 개발 - 워크로드, 애플리케이션 및 데이터를 클라우드로 이동하기 위한 단계별 접근 방식을 설명하는 세부 도입 계획을 통합합니다. 도입 단계, 타임라인, 종속성을 정의합니다. 주요 이해관계자를 참여시키고 그에 따라 리소스를 할당합니다.
- 조기 구축 시작 – 제로 트러스트를 분석하고 논의하는 대신 실제로 구축하고 배포하기 시작하면 조직 내에서 제로 트러스트가 어떤 모습일지 확실하게 표현할 수 있는 능력이 크게 향상됩니다.
- 경영진 후원 확보 - 제로 트러스트 구현을 위한 경영진 후원 및 지원을 확보합니다. 이 이니셔티브를 지지하고 필요한 리소스를 할당할 수 있도록 다른 최고 경영진의 참여를 유도합니다. 성공적인 구현에 필요한 문화 및 조직 변화를 추진하려면 리더십의 의지가 반드시 있어야 합니다.
- 거버넌스 프레임워크 구현 - 제로 트러스트 구현을 위한 역할, 책임, 의사 결정 프로세스를 정의하는 거버넌스 프레임워크를 만듭니다. 보안 통제, 위험 관리 및 규정 준수의 책임과 소유권을 명확하게 정의합니다. 거버넌스 프레임워크를 정기적으로 검토하고 업데이트하여 진화하는 보안 요구 사항에 맞게 조정합니다.
- 부서 간 협업 지원 - 다양한 사업부, IT 팀 및 보안 팀 간의 협업과 커뮤니케이션을 장려합니다. 제로 트러스트 구현 전반에서 조율과 조정을 촉진하기 위해 공동 책임 문화를 조성합니다. 잦은 상호 작용, 지식 공유 및 공동 문제 해결을 장려합니다.
- 데이터 및 애플리케이션 보호 - 제로 트러스트는 리소스와 애플리케이션에 액세스하는 최종 사용자에만 적용되는 것이 아닙니다. 워크로드 내부와 워크로드 간에도 제로 트러스트 원칙을 구현해야 합니다. 데이터 센터 내에서도 사용 가능한 모든 컨텍스트를 사용하여 강력한 ID, 마이크로 세분화, 권한 부여 등의 동일한 기술 원칙을 적용합니다.
- 심층 방어 제공 - 여러 계층의 보안 제어를 사용하여 심층 방어 전략을 실행합니다. 다중 인증(MFA), 네트워크 세분화, 암호화, 이상 탐지와 같은 다양한 보안 기술을 결합하여 포괄적인 보호를 제공합니다. 각 계층이 다른 계층을 보완하여 강력한 방어 시스템을 구축해야 합니다.

- 강력한 인증 요구 - 모든 리소스에 액세스하는 모든 사용자에 대해 MFA와 같은 강력한 인증 메커니즘을 시행합니다. 제로 트러스트에 대한 높은 수준의 인증 보장을 제공하고 광범위한 보안 이점(예: 피싱 방지)을 제공하는 FIDO2 하드웨어 기반 보안 키와 같은 최신 MFA를 고려하는 것이 가장 좋습니다.
- 권한 부여 중앙 집중화 및 개선 - 특히 모든 액세스 시도를 승인합니다. 프로토콜 세부 사항에 따라 연결별 또는 요청별로 수행해야 합니다. 요청별이 이상적입니다. ID, 디바이스, 동작, 네트워크 정보 등 사용 가능한 모든 컨텍스트를 사용하여 보다 세분화되고 적응력이 뛰어나며 정교한 권한 부여 결정을 내릴 수 있습니다.
- 최소 권한 원칙 사용 - 최소 권한 원칙을 이행하여 사용자에게 직무 수행에 필요한 최소 액세스 권한을 부여합니다. 직무, 책임, 비즈니스 요구 사항에 따라 액세스 권한을 정기적으로 검토하고 업데이트합니다. 적시 액세스 프로비저닝 구현
- 권한이 필요한 액세스 관리 사용 - 권한이 필요한 액세스 관리(PAM) 솔루션을 구현하여 권한 있는 계정을 보호하고 중요 시스템에 대한 무단 액세스 위험을 줄입니다. PAM 솔루션은 권한이 필요한 액세스 제어, 세션 기록, 감사 기능을 제공하여 조직이 가장 민감한 데이터와 시스템을 보호하는 데 도움을 줍니다.
- 마이크로 분할 사용 - 네트워크를 더 작고 격리된 세그먼트로 나눕니다. 마이크로 분할을 사용하여 사용자 역할, 애플리케이션 또는 데이터 민감도를 기반으로 세그먼트 간에 엄격한 액세스 제어를 적용할 수 있습니다. 불필요한 네트워크 경로, 특히 데이터로 이어지는 경로를 모두 제거하도록 하세요.
- 보안 경고 모니터링 및 대응 - 클라우드 환경에서 포괄적인 보안 모니터링 및 인시던트 대응 프로그램을 구현합니다. 클라우드 네이티브 보안 도구 및 서비스를 사용하여 실시간으로 위협을 탐지하고, 로그를 분석하고, 인시던트 대응을 자동화합니다. 명확한 인시던트 대응 절차를 수립하고, 정기적인 보안 평가를 수행하고, 이상 또는 의심스러운 활동을 지속적으로 모니터링합니다.
- 지속적인 모니터링 사용 - 보안 인시던트를 빠르고 효과적으로 탐지하고 이에 대응하려면 지속적인 모니터링을 구현합니다. 고급 보안 분석 도구를 사용하여 사용자 동작, 네트워크 트래픽 및 시스템 활동을 모니터링합니다. 경고 및 알림을 자동화하여 적시에 인시던트에 대응할 수 있도록 합니다.
- 보안 및 규정 준수 문화 조성 - 조직 전체에 보안 및 규정 준수 문화를 장려합니다. 보안 모범 사례, 제로 트러스트 원칙 준수의 중요성, 안전한 클라우드 환경 유지를 직원의 역할에 대한 교육을 실시합니다. 정기적인 보안 인식 교육을 실시하여 직원들이 소셜 엔지니어링에 주의를 기울이고 데이터 보호 및 개인정보 보호와 관련된 책임을 이해하도록 합니다.
- 소셜 엔지니어링 시뮬레이션 사용 - 소셜 엔지니어링 시뮬레이션을 수행하여 소셜 엔지니어링 공격에 대한 사용자의 취약성을 평가합니다. 시뮬레이션 결과를 사용하여 사용자 인식을 개선하고 잠재적 위협에 대응할 수 있는 맞춤형 교육 프로그램을 마련합니다.

- 지속적인 교육 장려 - 계속되는 보안 교육 및 리소스를 제공하여 지속적인 교육 및 학습 문화를 구축합니다. 진화하는 보안 모범 사례에 대해 사용자에게 계속 알려줍니다. 사용자가 경계를 늦추지 않고 의심스러운 활동이 있으면 즉시 신고하도록 권장합니다.
- 지속적 평가 및 최적화 - 클라우드 환경을 정기적으로 평가하여 개선이 필요한 부분을 찾습니다. 클라우드 네이티브 도구를 사용하여 리소스 사용 및 성능을 모니터링하고 취약성 평가와 침투 테스트를 수행하여 약점을 식별하여 해결합니다.
- 거버넌스 및 규정 준수 프레임워크 수립 - 조직이 업계 표준 및 규제 요구 사항을 준수할 수 있도록 거버넌스 및 규정 준수 프레임워크를 개발합니다. 프레임워크에서 데이터 및 시스템을 무단 액세스, 사용, 공개, 중단, 수정 또는 파괴로부터 보호하기 위한 정책, 절차 및 제어를 정의합니다. 규정 준수 지표를 추적 및 보고하고, 정기적인 감사를 실시하고, 규정 미준수 문제를 즉시 해결하기 위한 메커니즘을 구현합니다.
- 협업 및 지식 공유 장려 - ZTA 도입에 관련된 팀 간의 협업과 지식 공유를 장려합니다. 이를 위해 IT, 보안 및 사업부 간의 부서 간 커뮤니케이션 및 협업을 촉진합니다. 또한 조직에서는 포럼, 워크숍, 지식 공유 세션을 마련하여 이해를 증진하고 문제를 해결하며 도입 과정 전반에 걸쳐 얻은 교훈을 공유할 수 있습니다.

# 핵심 고려 사항

이 가이드에서는 성공적인 제로 트러스트 아키텍처(ZTA) 전략을 개발하기 위한 필수적인 측면을 살펴보았습니다. 이 섹션에는 제시된 권장 가이드의 핵심 고려 사항이 요약되어 있습니다.

- 제로 트러스트 원칙 이해 - 제로 트러스트는 기존 네트워크 제어나 네트워크 경계에만 전적으로 또는 근본적으로 의존하지 않는 디지털 자산에 대한 보안 제어를 제공하는 데 초점을 맞춘 개념적 모델이자 관련 메커니즘입니다. 대신 네트워크 제어에는 ID, 디바이스, 동작 및 기타 풍부한 컨텍스트와 신호가 추가되어 보다 세분화되고 지능적이며 적응력이 뛰어나고 지속적인 액세스 결정을 내릴 수 있습니다. 최소 권한, 마이크로 분할, 지속적 인증, 적응형 권한 부여와 같은 제로 트러스트의 핵심 원칙을 숙지하세요.
- 명확한 목표 정의 - ZTA 도입의 목표와 원하는 비즈니스 성과를 명확하게 정의합니다. 이러한 목표를 제로 트러스트 원칙에 맞게 조정하여 비즈니스 성장과 혁신을 지원하는 동시에 강력한 보안 기반을 보장합니다.
- 포괄적인 평가 수행 - 기존 IT 인프라, 애플리케이션 및 데이터 자산에 대한 철저한 평가를 수행합니다. 종속성, 기술적 부채, 호환성 문제를 파악하여 도입 전략을 수립합니다.
- ZTA 도입 계획 개발 - 워크로드, 애플리케이션 및 데이터를 클라우드로 이동하기 위한 단계별 접근 방식을 설명하는 세부 계획을 세웁니다. 규정 준수 요구 사항 및 애플리케이션 현대화와 같은 요소를 고려합니다.
- 강력한 ZTA 구현 - 세분화된 액세스 제어, 강력한 인증 메커니즘 및 지속적인 모니터링을 시행하는 ZTA를 설계하고 구현합니다. 보다 효율적인 ZTA 도입을 위해 AWS Verified Access, Amazon VPC Lattice 등의 클라우드 네이티브 제로 트러스트 서비스를 사용합니다.
- 데이터 및 애플리케이션 보안의 우선순위 지정 - 강력한 ID, 마이크로 분할, 권한 부여 등의 제로 트러스트 원칙을 적용하여 사용 가능한 모든 컨텍스트를 제공하십시오. 시스템 및 리소스에 액세스하는 사용자와 백엔드 구성 요소 내부 및 백엔드 구성 요소 간의 통신 및 데이터 흐름에 이 컨텍스트를 사용합니다.
- 모니터링 및 인시던트 대응 프레임워크 수립 - 클라우드 환경에서 강력한 보안 모니터링 및 인시던트 대응 기능을 구현합니다. 실시간 위협 탐지, 로그 분석 및 인시던트 대응 자동화에 Amazon Inspector, AWS Security Hub, Amazon GuardDuty 등의 클라우드 네이티브 보안 도구를 사용합니다.
- 보안 및 규정 준수 문화 조성 - 조직 전체에 보안 인식 및 규정 준수 문화를 장려합니다. 보안 모범 사례와 안전한 클라우드 환경 유지를 직원의 역할에 대한 교육을 실시합니다.
- 지속적인 평가 및 최적화 - 클라우드 환경, 보안 제어, 운영 프로세스를 정기적으로 평가합니다. 인사이트를 수집하고 리소스 사용률, 비용 관리 및 성능을 최적화하려면 Amazon CloudWatch, AWS Security Hub 등의 클라우드 네이티브 분석 및 모니터링 도구를 사용합니다.

- 거버넌스 및 규정 준수 프레임워크 수립 - 업계 표준과 규제 요구 사항에 부합하는 거버넌스 및 규정 준수 프레임워크를 개발합니다. 보안, 개인정보 보호 및 규정 준수 표준을 준수하는 데 도움이 되는 정책, 절차 및 제어를 정의합니다.

# 다음 단계

제로 트러스트 아키텍처(ZTA) 도입은 조직의 태세를 개선하고 위험을 줄이는 가장 안전한 방법 중 하나입니다. 이 권장 가이드는 원칙 이해부터 준비 상태 평가, 필요한 구성 요소 구현에 이르기까지 제로 트러스트를 구현하기 위한 포괄적인 로드맵을 제공합니다.

이 워크스트림 또는 도메인의 다음 단계에는 다음이 포함됩니다.

- 도입 계획 구현
- ZTA 구현
- 정기 보안 평가 수행
- 지속적으로 클라우드 환경 및 보안 제어 최적화

ZTA는 강력한 보안 기반을 확보하기 위해 지속적인 모니터링, 평가 및 조정이 필요한 지속적인 프로세스입니다. 이 가이드에 설명된 모범 사례를 따라 조직은 보안 태세를 강화하고, 규정 준수를 보장하고, 민감한 데이터를 보호할 수 있습니다.

# FAQ

이 섹션에서는 제로 트러스트 아키텍처(ZTA) 설계 및 구현에 대해 자주 묻는 질문에 대한 답변을 제공합니다.

## 제로 트러스트란 무엇인가요?

제로 트러스트는 기존 네트워크 제어나 네트워크 경계에만 전적으로 또는 근본적으로 의존하지 않는 디지털 자산에 대한 보안 제어를 제공하는 데 초점을 맞춘 개념적 모델이자 관련 메커니즘입니다. 대신 네트워크 제어에는 ID, 디바이스, 동작 및 기타 풍부한 컨텍스트와 신호가 추가되어 보다 세분화되고 지능적이며 적응력이 뛰어나고 지속적인 액세스 결정을 내릴 수 있습니다.

## 제로 트러스트 아키텍처를 구현하는 데 어떤 AWS 서비스가 도움이 되나요?

AWS는 AWS Verified Access, AWS Identity and Access Management(IAM), Amazon Virtual Private Cloud(VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway, Amazon GuardDuty 등 제로 트러스트 구현에 도움이 되는 여러 서비스를 제공합니다.

## AWS로 데이터 보안을 확보하려면 어떻게 해야 하나요?

AWS는 저장 및 전송 중 데이터 암호화를 위한 AWS Key Management Service(AWS KMS), 네트워크 격리를 위한 Amazon Virtual Private Cloud(VPC), 안전한 저장 및 보안 인증 검색을 위한 AWS Secrets Manager와 같은 서비스를 제공합니다.

## AWS는 제로 트러스트 환경의 규정 준수 요구 사항을 지원할 수 있나요?

예, AWS에는 다양한 규제 요구 사항을 충족하는 데 도움이 되는 규정 준수 프로그램과 서비스가 있습니다. AWS Artifact는 AWS 규정 준수 보고서에 대한 액세스를 제공하고, AWS Config는 규정 준수에 대한 지속적인 모니터링 및 평가를 지원합니다.

# 제로 트러스트 환경에서 보안을 자동화하기 위한 AWS 도구나 서비스가 있나요?

AWS는 보안 검색 결과를 중앙 집중화하고 자동화하는 AWS Security Hub, 보안 정책을 정의하고 실행하기 위한 AWS Config 규칙 등의 서비스를 제공합니다.

# AWS를 사용하여 제로 트러스트 클라우드 환경에서 지속적인 모니터링 및 인시던트 대응을 보장하려면 어떻게 해야 하나요?

AWS는 실시간 모니터링을 위한 Amazon CloudWatch, 로깅 및 분석을 위한 AWS CloudTrail과 같은 서비스를 제공합니다. 인시던트 대응 모범 사례를 보려면 AWS 보안 사고 대응 안내서를 참조하세요.

# 리소스

## 참조

- What is a cloud center of excellence and why should your organization create one? - 이 블로그 게시물에서는 CCoE의 개요, 효과적인 CCoE를 만드는 방법에 대한 모범 사례 등을 제공합니다.
- AWS 기반 제로 트러스트 – 이 페이지에서는 AWS 환경의 제로 트러스트 보안 원칙과 모범 사례의 개요를 제공합니다.
- Zero Trust architecture: An AWS perspective – 이 블로그 게시물은 AWS에서 제로 트러스트가 구현되는 방식에 대한 정의와 지침 원칙을 공유합니다.
- AWS Identity and Access Management(IAM) 사용 설명서 - 이 설명서에서는 제로 트러스트 아키텍처의 중요한 구성 요소인 IAM의 사용자 액세스 및 권한 관리에 대한 포괄적인 문서를 제공합니다.
- AWS Security Hub – AWS 계정 전체의 보안 경고 및 규정 준수 상태를 종합적으로 볼 수 있는 서비스인 Security Hub에 대해 알아보세요.
- AWS Well-Architected Framework – AWS에서 안전하고 성능이 뛰어나고 복원력이 뛰어나고 효율적인 아키텍처를 구축하는 방법에 대한 지침을 제공하는 Well-Architected Framework를 살펴보세요.
- AWS Security Incident Response Guide – 이 안내서에서는 조직의 AWS 클라우드 환경 내에서 보안 인시던트에 대응하기 위한 기본 사항을 개략적으로 설명합니다. 클라우드 보안 및 인시던트 대응 개념의 개요를 제공하고 보안 문제에 대응하는 고객이 사용할 수 있는 클라우드 기능, 서비스 및 메커니즘을 파악합니다.

## 도구

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Key Management Service

- AWS Secrets Manager
- AWS Security Hub
- AWS Verified Access

# 문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 업데이트 추가됨 | 제로 트러스트 아키텍처의 주요 구성 요소 섹션에 정보가 추가되고, 제로 트러스트 도입을 위한 조직 준비 상태 평가 섹션이 변경되고, 모범 사례 섹션에 정보가 추가되고, FAQ가 변경되었습니다. | 2023년 12월 4일 |
| 최초 게시 | — | 2023년 6월 19일 |

# AWS 규범적 지침 용어집

다음은 AWS 규범적 지침에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

## 숫자

7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora Postgre SQL-Compatible Edition으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예: 에서 온프레미스 Oracle 데이터베이스를 Oracle용 Amazon Relational Database Service(AmazonRDS)로 마이그레이션합니다 AWS 클라우드.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예: 의 EC2 인스턴스에서 온프레미스 Oracle 데이터베이스를 Oracle로 마이그레이션합니다 AWS 클라우드.
- 재배치(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: 마이그레이션 Microsoft Hyper-V 에 대한 애플리케이션입니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중으로 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

# A

ABAC

속성 기반 액세스 제어 를 참조하세요.

추상화된 서비스

관리형 서비스 를 참조하세요.

ACID

원자성, 일관성, 격리, 내구성을 참조하세요.

능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. 유연성은 뛰어나지만 능동 수동 마이그레이션보다 더 많은 작업이 필요합니다.

능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 소스 데이터베이스만 연결 애플리케이션의 트랜잭션을 처리하고 데이터는 대상 데이터베이스로 복제되는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

집계 함수

행 그룹에서 작동하고 그룹의 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로는 `SUM` 및 가 있습니다`MAX`.

AI

인공 지능 을 참조하세요.

AIOps

인공 지능 작업 을 참조하세요.

익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

애플리케이션 제어

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용할 수 있도록 허용하는 보안 접근 방식입니다.

애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 포트폴리오 검색 및 분석 프로세스의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 What is Artificial Intelligence?를 참조하십시오.

인공 지능 작업(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AIOps 가 마이그레이션 전략에 사용되는 AWS 방법에 대한 자세한 내용은 운영 통합 가이드 섹션을 참조하세요.

비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

원자성, 일관성, 격리, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

속성 기반 액세스 제어(ABAC)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management (IAM) 설명서ABAC AWS의 섹션을 참조하세요.

신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

가용 영역

다른 가용 영역의 장애로부터 절연 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내 고유 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환하기 위한 효율적이고 효과적인 계획을 개발하는 AWS 데 도움이 되는 의 지침 및 모범 사례 프레임워크입니다. AWS CAF 는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이 관점에서 AWS CAF는 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 훈련 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 AWS CAF 웹 사이트 및 AWS CAF 백서를 참조하세요.

AWS 워크로드 검증 프레임워크(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 권장하고, 작업 추정치를 제공하는 도구입니다. AWS WQF 는 AWS Schema Conversion Tool (AWS SCT)에 포함되어 있습니다. 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

# B

잘못된 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

BCP

비즈니스 연속성 계획 을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 통화 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 Data in a behavior graph를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. Endianness 도 참조하세요.

바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 “이 이메일이 스팸인가요, 스팸이 아닌가요?”, '이 제품은 책인가요, 자동차인가요?' 등의 문제를 예측해야 할 수 있습니다.

블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

블루/그린(Blue/Green) 배포

별개의 동일한 두 환경을 생성하는 배포 전략입니다. 현재 애플리케이션 버전은 한 환경(파란색)에서 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 빠르게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 작업을 실행하고 인적 활동 또는 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같은 일부 봇은 유용하거나 유용합니다. 잘못된 봇 이라고 하는 다른 봇은 개인 또는 조직에 방해가 되거나 피해를 입히기 위한 것입니다.

봇넷

맬웨어에 감염되고 봇 셰더 또는 봇 운영자 라고 하는 단일 당사자의 제어 하에 있는 봇 네트워크입니다. Botnet은 봇과 그 영향을 확장하는 가장 잘 알려진 메커니즘입니다.

브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 브랜치 정보(GitHub 문서)를 참조하세요.

브레이크 글라스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는 에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 Well-Architected 지침의 브레이크 글라스 절차 구현 표시기를 AWS 참조하세요.

브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

# C

CAF

AWS Cloud Adoption Framework 를 참조하세요.

canary 배포

최종 사용자에게 버전의 느린 증분 릴리스입니다. 확신이 드는 경우 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

Cloud Center of Excellence를 참조하세요.

CDC

데이터 캡처 변경 을 참조하세요.

데이터 캡처 변경(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 사항을 감사하거나 복제하는 등 동기화를 유지하기 CDC 위한 다양한 용도로 를 사용할 수 있습니다.

혼돈 엔지니어링

시스템 복원력을 테스트하기 위해 의도적으로 장애 또는 중단 이벤트를 도입합니다. AWS Fault Injection Service (AWS FIS)를 사용하여 AWS 워크로드에 스트레스를 가하고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전송을 참조하세요.

분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

클라이언트측 암호화

대상에서 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 암호화합니다.

Cloud Center of Excellence(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 CCoE 게시물을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 엣지 컴퓨팅 기술에 연결됩니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 클라우드 운영 모델 구축을 참조하십시오.

클라우드 채택 단계

조직이 로 마이그레이션할 때 일반적으로 거치는 4단계: AWS 클라우드

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 파운데이션 - 클라우드 채택을 확장하기 위한 기본 투자(예: 랜딩 영역 생성, 정의CCoE, 운영 모델 설정)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 블로그 게시물 The Journey Toward Cloud-First 및 Enterprise Strategy 블로그의 채택 단계에 정의했습니다. AWS 클라우드 AWS 마이그레이션 전략과 관련된 방법에 대한 자세한 내용은 마이그레이션 준비 가이드 섹션을 참조하세요.

CMDB

구성 관리 데이터베이스 를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리에는 GitHub 또는 가 포함됩니다 AWS CodeCommit. 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

컴퓨터 비전(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 AI 필드입니다. 예를 들어 는 온프레미스 카메라 네트워크에 CV를 추가하는 디바이스를 AWS Panorama 제공하고 Amazon은 CV에 대한 이미지 처리 알고리즘을 SageMaker 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상 상태에서 변경됩니다. 이로 인해 워크로드가 규정 미준수가 될 수 있으며 일반적으로 점진적이고 의도하지 않습니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션CMDB의 포트폴리오 검색 및 분석 단계에서 의 데이터를 사용합니다.

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다. YAML 템플릿을 사용하여 AWS 계정 및 리전 또는 조직 전체에서 적합성 팩을 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 적합성 팩을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 지속적 전달의 이점을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 참조하십시오.

CV

컴퓨터 비전 을 참조하세요.

# D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected 프레임워크의 보안 기둥 구성 요소입니다. 자세한 내용은 데이터 분류를 참조하십시오.

데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

데이터 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 분산된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 프라이버시 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스할 수 있도록 하는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 에서 데이터 경계 구축을 AWS 참조하세요.

데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

데이터 주체

데이터를 수집 및 처리하는 개인입니다.

데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템입니다. 데이터 웨어하우스에는 일반적으로 많은 양의 기록 데이터가 포함되어 있으며 일반적으로 쿼리 및 분석에 사용됩니다.

데이터베이스 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

DDL

데이터베이스 정의 언어 를 참조하세요.

딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

defense-in-depth

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 에서 이 전략을 채택 AWS하면 AWS Organizations 구조의 여러 계층에 여러 제어를 추가하여 리소스를 보호하는 데 도움이 됩니다. 예를 들어, 접근 방식은 다중 인증, 네트워크 세분화 및 암호화를 defense-in-depth 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고 합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 AWS Organizations와 함께 사용할 수 있는 AWS 서비스를 참조하십시오.

배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

개발 환경

환경 을 참조하세요.

탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Detective controls를 참조하십시오.

개발 값 스트림 매핑(DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM 는 원래 린 제조 관행을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

차원 테이블

스타 스키마에서 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트 필드 또는 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 쿼리 제약, 필터링 및 결과 세트 레이블 지정에 일반적으로 사용됩니다.

재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

재해 복구(DR)

재해로 인한 가동 중지 시간과 데이터 손실을 최소화하기 위해 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 클라우드에서 AWS: 복구에서 워크로드의 재해 복구를 참조하세요.

DML

데이터베이스 조작 언어 를 참조하세요.

도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. 스트랭글러 무화과 패턴으로 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 컨테이너 및 Amazon API Gateway를 사용하여 레거시 Microsoft ASP.NET (ASMX) 웹 서비스 점진적으로 현대화를 참조하세요.

DR

재해 복구를 참조하세요.

드리프트 감지

기준 구성과의 편차 추적. 예를 들어 AWS CloudFormation 를 사용하여 시스템 리소스의 드리프트를 감지하거나 를 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 랜딩 존의 변경 사항을 감지할 수 있습니다.

DVSM

개발 값 스트림 매핑을 참조하세요.

# E

EDA

탐색적 데이터 분석 을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 클라우드 컴퓨팅 과 비교할 때 엣지 컴퓨팅은 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 암호 텍스트로 변환하는 컴퓨팅 프로세스입니다.

암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

엔드포인트

서비스 엔드포인트 를 참조하세요.

엔드포인트 서비스

가상 프라이빗 클라우드(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 보안 주체 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 엔드포인트를 생성하여 VPC 엔드포인트 서비스에 비공개로 연결할 수 있습

니다. 자세한 내용은 Amazon Virtual Private Cloud(AmazonVPC) 설명서의 엔드포인트 서비스 생성을 참조하세요.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, 및 프로젝트 관리)를 자동화MES하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 봉투 암호화를 참조하세요.

환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어 보안 AWS CAF 에픽에는 자격 증명 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획 을 참조하세요.

탐색적 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA 는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

# F

팩트 테이블

별표 스키마 의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블에는 측정값이 포함된 열과 차원 테이블에 대한 외부 키가 포함된 열의 두 가지 유형이 있습니다.

빠른 실패

자주 증분 테스트를 사용하여 개발 수명 주기를 줄이는 철학입니다. 애자일 접근 방식의 중요한 부분입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 제어 영역 또는 데이터 영역과 같은 AWS 클라우드경계입니다. 자세한 내용은 AWS 장애 격리 경계를 참조하세요.

기능 브랜치

브랜치를 참조하세요.

기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 Shapley Additive Explanations(SHAP) 및 통합 그라데이션과 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 를 사용한 기계 학습 모델 해석 가능성을 참조하세요AWS.

기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용할 수 있습니다. 예를 들어, 날짜 '2021-05-27 00:15:37'을 '2021년', '5월', '목', '15일'로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

FGAC

세분화된 액세스 제어 를 참조하세요.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 변경 데이터 캡처를 통해 지속적인 데이터 복제를 사용하여 가능한 최단 시간 내에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

# G

지리적 차단

지리적 제한 사항 을 참조하세요.

지리적 제한(지리적 차단)

Amazon 에서는 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 CloudFront옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하세요.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 트렁크 기반 워크플로는 현대적이고 선호하는 접근 방식입니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 브라운필드라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

가드레일

조직 단위 전반의 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 상위 수준 규칙입니다 (OUs). 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책 및 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, AWS Config,, Amazon AWS Security Hub, GuardDuty, AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

# H

HA

고가용성 섹션을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스키마를 변환하는 것은 복잡한 작업일 수 있습니다.AWS 는 스키마 변환에 도움이 되는 AWS SCT를 제공합니다.

높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

동종 데이터베이스 마이그레이션

소스 데이터베이스를 동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로). 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫포밍 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 긴급성으로 인해 핫픽스는 일반적으로 일반적인 DevOps 릴리스 워크플로 외부에서 이루어집니다.

하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

## I

IaC

인프라를 코드 로 참조하세요.

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

IIoT

산업용 사물 인터넷을 참조하세요.

변경할 수 없는 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드를 위해 새 인프라를 배포하는 모델입니다. 변경 가능한 인프라는 본질적으로 변경 가능한 인프라보다 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 변경할 수 없는 인프라를 사용한 배포 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅VPC 하는 . AWS Security Reference Architecture는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 VPCs 위해 인바운드, 아웃바운드 및 검사로 네트워크 계정을 설정하는 것이 좋습니다.

증분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스

또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통한 제조 프로세스의 현대화를 언급하기 위해 2016년에 Klaus Schwab에서 도입한 용어입니다.

인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 산업용 사물 인터넷 구축(IIoT) 디지털 변환 전략 단원을 참조하세요.

검사 VPC

AWS 다중 계정 아키텍처에서 (VPCs동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 VPC 관리하는 중앙 집중식 아키텍처입니다. AWS Security Reference Architecture는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 VPCs 위해 인바운드, 아웃바운드 및 검사로 네트워크 계정을 설정하는 것이 좋습니다.

사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 IoT란?을 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 를 사용한 기계 학습 모델 해석 가능성을 AWS참조하세요.

IoT

사물 인터넷을 참조하세요.

IT 정보 라이브러리(ITIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL 는 의 기반을 제공합니다ITSM.

IT 서비스 관리(ITSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 작업을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 작업 통합 가이드 단원을 참조하세요.

ITIL

IT 정보 라이브러리 를 참조하세요.

ITSM

IT 서비스 관리 섹션을 참조하세요.

## L

레이블 기반 액세스 제어(LBAC)

사용자와 데이터 자체에 각각 보안 레이블 값이 명시적으로 할당되는 필수 액세스 제어(MAC)의 구현입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

랜딩 존

랜딩 존은 확장 가능하고 안전한 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 안전하고 확장 가능한 다중 계정 AWS 환경 설정을 참조하십시오.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어 섹션을 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 최소 권한 적용을 참조하세요.

리프트 앤드 시프트

7 Rs 를 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. Endianness 를 참조하세요.

하위 환경

환경 을 참조하세요.

# M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 참조하십시오.

기본 브랜치

브랜치를 참조하세요.

맬웨어

컴퓨터 보안 또는 프라이버시를 손상시키도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 중단하거나 민감한 정보를 유출하거나 무단 액세스를 가져올 수 있습니다. 맬웨어의 예로는 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스 는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하고 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB는 관리형 서비스의 예입니다. 이를 추상화된 서비스 라고도 합니다.

제조 실행 시스템(MES)

원재료를 생산 현장의 완제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

마이그레이션 가속화 프로그램 단원을 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 결과를 검사하여 조정하는 전체 프로세스입니다. 메커니즘은 작동하면서 자체를 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 메커니즘 구축을 참조하세요.

멤버 계정

에서 조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정입니다 AWS Organizations. 하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

제조 실행 시스템 을 참조하세요.

메시지 대기열 원격 측정 전송(MQTT)

리소스가 제한된 IoT 디바이스에 대한 게시/구독 패턴을 기반으로 하는 경량 machine-to-machine(M2M) 통신 프로토콜입니다.

마이크로서비스

잘 정의된 를 통해 통신APIs하고 일반적으로 소규모 독립 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 AWS 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하세요.

마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 를 사용하여 잘 정의된 인터페이스를 통해 통신합니다APIs. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 에서 마이크로서비스 구현을 참조하세요 AWS.

마이그레이션 가속화 프로그램(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 컨설팅 지원, 훈련 및 서비스를 제공하는 AWS 프로그램입니다. MAP 에는 체계적인 방식으로 레거시 마이그레이션을 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하기 위한 도구 세트가 포함되어 있습니다.

대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 AWS 마이그레이션 전략의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 작업하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자 및 DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 클라우드 마이그레이션 팩토리 가이드와 마이그레이션 팩토리에 대한 설명을 참조하십시오.

마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예: AWS Application Migration Service를 EC2 사용하여 Amazon으로 마이그레이션을 다시 호스팅합니다.

마이그레이션 포트폴리오 평가(MPA)

로 마이그레이션하기 위한 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다 AWS 클라우드. MPA 는 자세한 포트폴리오 평가(서버 적정 규모, 요금, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선 순위 지정 및 웨이브 계획)을 제공합니다. MPA 도구(로그인 필요)는 모든 AWS 컨설턴트 및 APN 파트너 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 평가(MRA)

를 사용하여 조직의 클라우드 준비 상태에 대한 통찰력을 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 실행 계획을 수립하는 프로세스입니다 AWS CAF. 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오. MRA 는 AWS 마이그레이션 전략의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 로 마이그레이션하는 데 사용되는 접근 방식입니다 AWS 클라우드. 자세한 내용은 이 용어집의 7 Rs 항목을 참조하고 대규모 마이그레이션을 가속화하기 위해 조직 동원을 참조하세요.

ML

기계 학습을 참조하세요.

현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 의 애플리케이션 현대화 전략을 참조하세요 AWS 클라우드.

현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는 로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 의 애플리케이션에 대한 현대화 준비 상태 평가를 참조하세요 AWS 클라우드.

모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 마이크로서비스로 모놀리식 유형 분해를 참조하십시오.

MPA

마이그레이션 포트폴리오 평가 단원을 참조하세요.

MQTT

메시지 대기열 원격 측정 전송을 참조하세요.

멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

변경 가능한 인프라

프로덕션 워크로드에 대한 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework는 변경할 수 없는 인프라를 모범 사례로 사용할 것을 권장합니다.

# O

OAC

오리진 액세스 제어 섹션을 참조하세요.

OAI

오리진 액세스 자격 증명 을 참조하세요.

OCM

조직 변경 관리 를 참조하세요.

오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

OI

작업 통합을 참조하세요.

OLA

운영 수준 계약 을 참조하세요.

온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

OPC- UA

Open Process Communications - 통합 아키텍처를 참조하세요.

Open Process Communications - 통합 아키텍처(OPC-UA)

산업 자동화를 위한 machine-to-machine (M2M) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계와 상호 운용성 표준을 제공합니다.

운영 수준 계약(OLA)

서비스 수준 계약()을 지원하기 위해 기능 IT 그룹이 서로에게 제공할 것을 명확히 하는 계약입니다 SLA.

운영 준비 검토(ORR)

인시던트 및 가능한 장애의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 및 관련 모범 사례 체크리스트입니다. 자세한 내용은 AWS Well-Architected 프레임워크의 운영 준비 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경과 협력하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조에서 OT와 정보 기술(IT) 시스템의 통합은 Industry 4.0 혁신의 핵심 초점입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 운영 통합 가이드를 참조하십시오.

조직 트레일

에서 생성한 추적으로 의 조직 AWS 계정 내 모든 에 대한 모든 이벤트를 AWS CloudTrail 기록합니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 설명서의 조직에 대한 추적 생성을 참조하세요 CloudTrail.

조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM 는 변화 채택을 가속화하고, 전환 문제를 해결하고, 문화적 및 조직적 변화를 주도하여 조직이 새로운 시스템 및 전략에 대비하고 전환하도록 지원합니다. AWS 마이그레이션 전략에서 이 프레임워크는 클라우드 채택 프로젝트에 필요한 변경 속도 때문에 인력 가속화 라고 합니다. 자세한 내용은 OCM 안내서를 참조하세요.

오리진 액세스 제어(OAC)

에서는 Amazon Simple Storage Service(Amazon S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 CloudFront향상된 옵션입니다. OAC 는 모든 의 모든 S3 버킷 AWS 리전, AWS KMS (-SSEKMS)를 사용한 서버 측 암호화, S3 버킷에 대한 동적 PUT 및 DELETE 요청을 지원합니다.

오리진 액세스 자격 증명(OAI)

에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 CloudFront옵션입니다. OAI를 사용하면 Amazon S3가 인증할 수 있는 보안 주체가 CloudFront 생성됩니다. 인증된 보안 주체는 특정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더욱 세분화되고 향상된 액세스 제어를 OAC제공하는 도 참조하세요.

ORR

운영 준비 검토 섹션을 참조하세요.

OT

운영 기술 을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 VPC 처리하는 입니다. AWS Security Reference Architecture는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 VPCs 위해 인바운드, 아웃바운드 및 검사로 네트워크 계정을 설정하는 것이 좋습니다.

# P

권한 경계

보안 IAM 주체에 연결되어 사용자 또는 역할이 가질 수 있는 최대 권한을 설정하는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 권한 경계를 참조하세요.

개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. 의 예로는 이름, 주소 및 연락처 정보가 PII 있습니다.

PII

개인 식별 정보 를 참조하세요.

플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

PLC

프로그래밍 가능한 로직 컨트롤러 를 참조하세요.

PLM

제품 수명 주기 관리 섹션을 참조하세요.

정책

권한을 정의하거나( 자격 증명 기반 정책 참조), 액세스 조건을 지정하거나(리소스 기반 정책 참조), 조직의 모든 계정에 대한 최대 권한을 정의할 수 있는 객체입니다 AWS Organizations (서비스 제어 정책 참조).

다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 스토어를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다. 자세한 내용은 마이크로서비스에서 데이터 지속성 활성화를 참조하십시오.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 참조하십시오.

조건자

`WHERE` 절에서 `false`일반적으로 위치한 `true` 또는 를 반환하는 쿼리 조건입니다.

조건부 푸시다운

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄어들고 쿼리 성능이 향상됩니다.

예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Preventative controls를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 AWS 있는 엔터티입니다. 이 엔터티는 일반적으로 AWS 계정, IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 역할의 보안 주체 용어 및 개념을 참조하세요. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html#id_roles_terms-and-concepts

개인 정보 보호 중심 설계

전체 엔지니어링 프로세스에서 개인 정보를 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

프라이빗 호스팅 영역

Amazon Route 53이 하나 이상의 내에서 도메인 및 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보를 포함하는 컨테이너입니다VPCs. 자세한 내용은 Route 53 설명서의 프라이빗 호스팅 영역 작업을 참조하십시오.

사전 예방적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스가 프로비저닝되기 전에 스캔 리소스를 제어합니다. 리소스가 컨트롤을 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 제어 참조 가이드를 참조하고 의 보안 제어 구현의 사전 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도, 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리.

프로덕션 환경

환경 을 참조하세요.

프로그래밍 가능한 로직 컨트롤러(PLC)

제조에서 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

게시/구독(pub/sub)

마이크로서비스 간의 비동기 통신을 가능하게 하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 에서 MES마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

# Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 지침과 같은 일련의 단계입니다.

쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

# R

RACI 매트릭스

책임, 책임, 상담, 정보 제공(RACI)을 참조하세요.

랜섬웨어

결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

RASCI 매트릭스

책임, 책임, 상담, 정보 제공(RACI)을 참조하세요.

RCAC

행 및 열 액세스 제어 를 참조하세요.

읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의 로드를 줄일 수 있습니다.

재설계

7 Rs 를 참조하세요.

복구 시점 목표(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

복구 시간 목표(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터

7 Rs 를 참조하세요.

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전 는 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 계정에서 를 사용할 수 있는 항목 지정을 참조 AWS 리전 하세요.

회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

리호스팅

7 Rs 를 참조하세요.

release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7 Rs 를 참조하세요.

리플랫포밍

7 Rs 를 참조하세요.

재구매

7 Rs 를 참조하세요.

복원력

중단에 저항하거나 복구할 수 있는 애플리케이션의 기능입니다. 에서 복원력을 계획할 때 고가용성 및 재해 복구는 일반적인 고려 사항입니다 AWS 클라우드. 자세한 내용은 AWS 클라우드 복원력 섹션을 참조하세요.

리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

책임, 책임, 상담, 정보 제공(RACI) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다. 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조언자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원을 포함하는 경우 매트릭스를 RASCI 매트릭스 라고 하고, 매트릭스를 제외하면 RACI 매트릭스 라고 합니다.

대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 Implementing security controls on AWS의 Responsive controls를 참조하십시오.

retain

7 Rs 를 참조하세요.

사용 중지

7 Rs 를 참조하세요.

교체

공격자가 보안 인증 정보에 액세스하는 것을 더 어렵게 만들기 위해 보안 암호를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

액세스 규칙을 정의한 기본적이고 유연한 SQL 표현식의 사용. RCAC 는 행 권한과 열 마스크로 구성됩니다.

RPO

복구 시점 목표 를 참조하세요.

RTO

복구 시간 목표 를 참조하세요.

런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

# S

SAML 2.0

많은 자격 증명 공급자(IdPs)가 사용하는 개방형 표준입니다. 이 기능을 사용하면 페더레이션 Single Sign-On(SSO)을 사용할 수 있으므로 사용자는 조직의 모든 사용자에 AWS API IAM 대해 에서 사용자를 만들지 않고도 AWS Management Console 에 로그인하거나 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하세요.

SCADA

관리 제어 및 데이터 수집 을 참조하세요.

SCP

서비스 제어 정책 을 참조하세요.

secret

에서 암호 또는 사용자 자격 증명과 같이 암호화된 형식으로 저장하는 AWS Secrets Manager기밀 또는 제한된 정보입니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 Secrets Manager 설명서의 Secrets Manager 보안 암호의 내용을 참조하세요.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어에는 예방 , 탐지 , 대응 , 사전 예방 의 네 가지 기본 유형이 있습니다.

보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM) 및 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협 및 보안 위반을 탐지하고 알림을 생성합니다.

보안 응답 자동화

보안 이벤트에 자동으로 응답하거나 복구하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지적 또는 대응적 AWS 보안 제어 역할을 합니다. 자동 응답 작업의 예로는 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 보안 인증 정보 교체 등이 있습니다.

서버 측 암호화

대상에서 데이터를 수신하는 AWS 서비스 에 의한 데이터 암호화.

서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCPs 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대한 가드레일을 정의하거나 제한을

설정합니다. 허용 목록 또는 거부 목록SCPs으로 를 사용하여 허용되거나 금지된 서비스 또는 작업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 서비스 제어 정책을 참조하세요.

서비스 엔드포인트

에 대한 진입점URL의 입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

서비스 수준 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

서비스 수준 표시기(SLI)

오류율, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정치입니다.

서비스 수준 목표(SLO)

서비스 수준 지표 로 측정한 서비스의 상태를 나타내는 대상 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수에 AWS 대해 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 책임지고, 는 클라우드의 보안을 책임집니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

SIEM

보안 정보 및 이벤트 관리 시스템 을 참조하세요.

단일 장애 지점(SPOF)

시스템을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소 장애입니다.

SLA

서비스 수준 계약 을 참조하세요.

SLI

서비스 수준 표시기 를 참조하세요.

SLO

서비스 수준 목표 를 참조하세요.

split-and-seed 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 에서 애플리케이션 현대화에 대한 단계별 접근 방식을 참조하세요 AWS 클라우드.

SPOF

단일 장애 지점 을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스 또는 비즈니스 인텔리전스 용도로 설계되었습니다.

Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도하고 대체하는 것과 비슷합니다. Martin Fowler가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 컨테이너 및 Amazon API Gateway 를 사용하여 레거시 Microsoft ASP.NET (ASMX) 웹 서비스 점진적으로 현대화를 참조하세요.

서브넷

의 IP 주소 범위입니다VPC. 서브넷은 단일 가용 영역에 상주해야 합니다.

감독 제어 및 데이터 수집(SCADA)

제조에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 생산 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

잠재적 문제를 감지하거나 성능을 모니터링하기 위해 사용자 상호 작용을 시뮬레이션하는 방식으로 시스템을 테스트합니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

# T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색 및 필터링할 수 있습니다. 자세한 내용은 AWS 리소스에 태그 지정을 참조하십시오.

대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

테스트 환경

환경 을 참조하세요.

훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

전송 게이트웨이

VPCs 및 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 전송 게이트웨이란 무엇입니까?를 참조하세요.

트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

신뢰할 수 있는 액세스

사용자를 대신하여 및 해당 AWS Organizations 계정에서 조직에서 작업을 수행하도록 지정한 서비스에 대한 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여

관리 작업을 수행합니다. 자세한 내용은 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요 AWS Organizations .

튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

피자 두 판 팀

두 개의 피자로 먹을 수 있는 작은 DevOps 팀입니다. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

# U

불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다. 자세한 내용은 Quantifying uncertainty in deep learning systems 가이드를 참조하십시오.

차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

상위 환경

환경 을 참조하세요.

# V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수반하는 데이터베이스 유지 관리 작업입니다.

버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 VPCs 있는 두 연결입니다. 자세한 내용은 Amazon VPC 설명서의 VPC 피어링이란 무엇입니까?를 참조하세요.

취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

## W

웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에 대해 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대적 위치를 기반으로 행 값에 액세스하는 등의 작업을 처리하는 데 유용합니다.

워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

WORM

쓰기를 한 번 참조하고 많은 을 읽습니다.

WQF

AWS 워크로드 검증 프레임워크를 참조하세요.

한 번 쓰기, 많이 읽기(WORM)

데이터를 한 번에 쓰고 데이터가 삭제되거나 수정되는 것을 방지하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 데이터를 읽을 수 있지만 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 변경할 수 없는 로 간주됩니다.

## Z

제로데이 익스플로잇

제로데이 취약성 을 활용하는 공격, 일반적으로 맬웨어입니다.

제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.