Partage de renseignements sur les cybermenaces sur AWS

AWS Conseils prescriptifs

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Conseils prescriptifs: Partage de renseignements sur les cybermenaces sur AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Introduction 1
Modèle de partage CTI 3
Sécurité du cloud 3
Sécurité dans le cloud 4
Architecture CTI 5
Déploiement d'une plateforme de renseignement sur les menaces 7
Ingestion de CTI 8
Automatiser les contrôles de sécurité 9
Amazon GuardDuty 11
Amazon Route 53 Resolver Pare-feu DNS 13
AWS Network Firewall 14
Gagner en visibilité 16
Enregistrement du trafic réseau 16
Centralisation des résultats de sécurité dans AWS 17
Intégration AWS données de sécurité avec d'autres données d'entreprise 19
Partage du CTI 19
Étapes suivantes 22
AWS ressources 22
Service AWS documentation 22
Ressources STIX 23
Plateformes de renseignement sur les menaces 23
Collaborateurs 24
Conception 24
Révision 24
Rédaction technique 24
Historique du document 25
..... xxvi

Partage de renseignements sur les cybermenaces sur AWS

Amazon Web Services (contributeurs)

Décembre 2024 (historique du document)

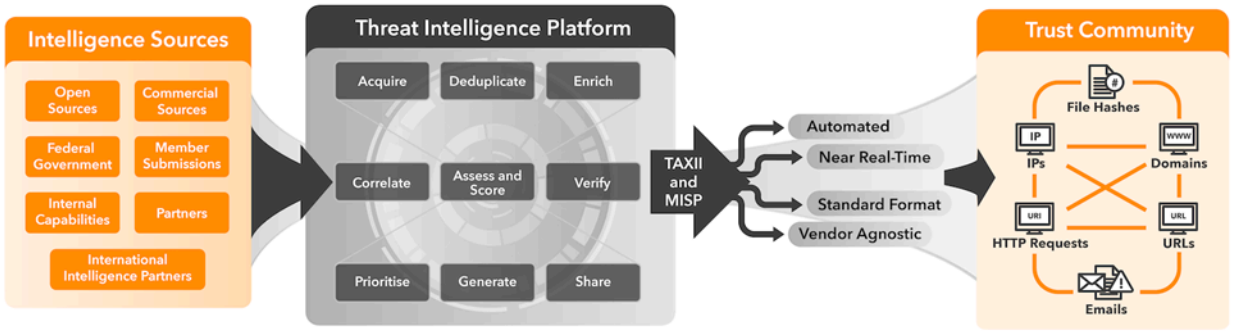
À mesure que de nouveaux risques apparaissent, les meilleures pratiques en matière de protection des charges de travail critiques dans le cloud évoluent en permanence. À mesure que le nombre d'actifs connectés à Internet nécessitant une protection augmente, le risque d'un événement de sécurité associé à des acteurs malveillants augmente également. Le renseignement sur les cybermenaces (CTI) est la collecte et l'analyse de données qui indiquent l'intention, l'opportunité et les capacités d'un acteur menaçant. Il est fondé sur des preuves et exploitable, et il oriente les activités de cyberdéfense. Il inclut souvent des informations relatives à l'attribution des acteurs, aux tactiques, aux techniques et procédures, aux motivations ou aux cibles.

Le CTI peut être partagé au sein d'une organisation, entre des organisations au sein d'une communauté de confiance, avec des centres de partage et d'analyse d'informations (ISAC) ou avec d'autres entités, telles que les autorités gouvernementales. Parmi les autorités gouvernementales, on peut citer le Centre australien de cybersécurité (ACSC) et l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA).

Comme toutes les formes de renseignement, le contexte des menaces est essentiel. Le partage des CTI contribue à la gestion dynamique des risques de cybersécurité. Il est essentiel pour assurer une défense, une réponse et une restauration rapides en matière de cybersécurité. Cela augmente l'efficience et l'efficacité des capacités de cybersécurité. Le contexte de menace est également essentiel pour faire la distinction entre les exigences de capacité du CTI relatives aux différentes cibles. Par exemple, les acteurs sophistiqués peuvent cibler des entreprises ou des gouvernements spécifiques, tandis que les acteurs du secteur des matières premières utilisent des outils et des techniques facilement accessibles pour attaquer à grande échelle des individus et des organisations.

La planification de la sécurité, l'observabilité, l'analyse des informations sur les menaces, l'automatisation des contrôles de sécurité et le partage au sein d'une communauté de confiance sont des éléments clés du cycle de vie des informations sur les menaces. AWS vous permet d'automatiser les tâches de sécurité manuelles afin de détecter les menaces avec une plus grande précision, de réagir plus rapidement et de générer des informations de haute qualité sur les menaces que vous pouvez partager. Vous pouvez découvrir une nouvelle cyberattaque, l'analyser, générer un CTI, la partager et l'appliquer, le tout à des vitesses conçues pour empêcher qu'une deuxième attaque ne se produise.

Ce guide explique comment déployer une plateforme de renseignement sur les menaces sur AWS. Les communautés de confiance fournissent des CTI, et la plateforme les ingère pour identifier les informations exploitables et automatiser les contrôles de protection et de détection dans l'environnement. AWS L'image suivante montre le cycle de vie des renseignements sur les menaces. Le CTI arrive de sa source, puis la plateforme de renseignement sur les menaces le traite. En utilisant le protocole TAXII (Trusted Automated Exchange of Intelligence Information) ou la plateforme MISP (Malware Information Sharing Platform), le CTI est partagé avec la communauté de confiance pour qu'elle passe à l'action.



La plateforme de renseignement sur les menaces utilise le CTI pour implémenter automatiquement des contrôles de sécurité dans votre AWS environnement ou pour informer votre équipe de sécurité si une action manuelle est requise. Un contrôle préventif est un contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Les exemples incluent l'automatisation des listes de blocage d'adresses IP ou de noms de domaine connus à l'aide de pare-feux réseau, de résolveurs DNS et d'autres systèmes de prévention des intrusions (IPS). Un contrôle de détection est un contrôle de sécurité conçu pour détecter, enregistrer et alerter après la survenue d'un événement. Les exemples incluent la surveillance continue des activités malveillantes et la recherche dans les journaux de recherche de preuves de problèmes ou d'événements.

Vous pouvez agréger tous les résultats dans un outil d'observabilité de sécurité centralisé, tel que AWS Security Hub CSPM. Vous pouvez ensuite partager les résultats avec une communauté de confiance afin de créer en collaboration une image complète des menaces.

Modèle de responsabilité partagée pour le partage des CTI

Le modèle de responsabilitéAWS partagée définit la manière dont vous partagez les responsabilités en AWS matière de sécurité et de conformité dans le cloud. AWS sécurise l'infrastructure qui exécute tous les services proposés dans le cadre de ce que l' AWS Cloud on appelle la sécurité du cloud. Vous êtes responsable de la sécurisation de votre utilisation de ces services, tels que vos données et applications. C'est ce que l'on appelle la sécurité dans le cloud.

Sécurité du cloud

La sécurité est la priorité absolue de AWS. Nous travaillons d'arrache-pied pour éviter que les problèmes de sécurité ne perturbent votre organisation. Alors que nous nous efforçons de défendre notre infrastructure et vos données, nous utilisons nos connaissances à l'échelle mondiale pour recueillir un volume important de renseignements de sécurité, à grande échelle et en temps réel, afin de vous protéger automatiquement. Dans la mesure du possible, AWS ses systèmes de sécurité neutralisent les menaces là où cette action a le plus d'impact. Souvent, ce travail se fait dans les coulisses.

Chaque jour, dans l'ensemble de l' AWS Cloud infrastructure, nous détectons et déjouons avec succès des centaines de cyberattaques qui pourraient autrement être perturbatrices et coûteuses. Ces victoires importantes, mais pour la plupart inédites, sont remportées grâce à un réseau mondial de capteurs et à un ensemble d'outils de perturbation associés. Grâce à ces fonctionnalités, nous rendons les cyberattaques plus difficiles et plus coûteuses contre notre réseau et notre infrastructure.

AWS possède le réseau public le plus étendu de tous les fournisseurs de cloud. Cela donne AWS un aperçu inégalé en temps réel de certaines activités sur Internet. MadPotest un réseau mondial de capteurs de menaces (appelés honeypots). MadPot aide les équipes AWS de sécurité à comprendre les tactiques et les techniques des attaquants. Chaque fois qu'un attaquant tente de cibler l'un des capteurs de menaces, il AWS collecte et analyse les données.

Sonaris est un autre outil interne AWS utilisé pour analyser le trafic réseau. Il identifie et stoppe les tentatives non autorisées d'accès à un grand nombre de comptes et de ressources. Entre mai 2023 et avril 2024, Sonaris a démenti plus de 24 milliards de tentatives de numérisation des données clients stockées dans Amazon Simple Storage Service (Amazon S3). Il a également empêché près de 2,6 billions de tentatives visant à découvrir des charges de travail vulnérables exécutées sur Amazon Elastic Compute Cloud (Amazon EC2).

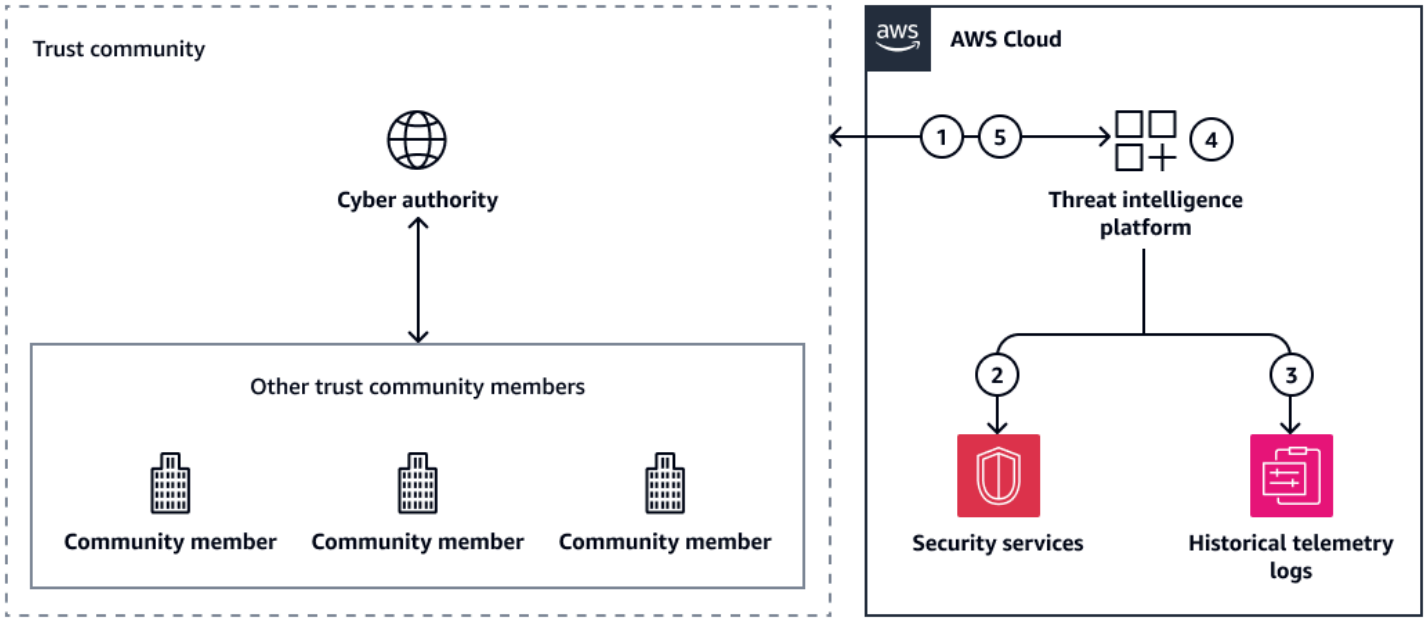
Sécurité dans le cloud

Ce guide se concentre sur les meilleures pratiques en matière de renseignement sur les cybermenaces (CTI) dans le AWS Cloud. Vous êtes chargé de générer des CTI localisés et contextualisés. Vous contrôlez où vos données sont stockées, comment elles sont sécurisées et qui y a accès. AWS n'a aucune visibilité sur vos données de journalisation, de surveillance et d'audit, ce qui est essentiel pour la sécurité basée sur le CTI dans le cloud.

L'expression structurée des informations sur les menaces (STIX) est un langage open source et un format de sérialisation utilisés pour échanger des CTI. Les indicateurs tels que les hachages de fichiers, les domaines URLs, les requêtes HTTP et les adresses IP sont des résultats importants à partager pour bloquer les menaces. Cependant, une action efficace repose sur des informations supplémentaires, telles que les cotes de certitude et les corrélations entre ensembles d'intrusions. STIX 2.1 définit 18 objets de domaine STIX, notamment le schéma d'attaque, le plan d'action, l'auteur de la menace, l'emplacement géographique et les informations sur les malwares. Il introduit également des concepts, tels que les cotes de confiance et les relations, qui aident les entités à déterminer le signal issu du bruit dans le grand volume de données collectées par la plateforme de renseignement sur les menaces. Vous pouvez détecter, analyser et partager ce niveau de détail sur les menaces présentes dans vos AWS environnements. Pour plus d’informations, consultez Automatiser les contrôles de sécurité préventifs et de détection dans ce guide.

Architecture de renseignement sur les cybermenaces sur AWS

La figure suivante décrit une architecture généralisée permettant d'utiliser un flux de menaces pour intégrer les informations sur les cybermenaces (CTI) dans votre AWS environnement. Le CTI est partagé entre votre plateforme de renseignement sur les menaces AWS Cloud, la cyberautorité sélectionnée et les autres membres de la communauté de confiance.



Il montre le flux de travail suivant :

1. La plateforme de renseignement sur les menaces reçoit des CTI exploitables de la part de la cyberautorité ou d'autres membres de la communauté de confiance.
2. La plateforme de renseignement sur les menaces charge les services de AWS sécurité de détecter et de prévenir les événements.
3. La plateforme de renseignement sur les menaces reçoit des informations sur les menaces provenant de Services AWS.
4. Si un événement se produit, la plateforme de renseignement sur les menaces organise de nouveaux CTI.
5. La plateforme de renseignement sur les menaces partage le nouveau CTI avec la cyberautorité. Il peut également partager le CTI avec d'autres membres de la communauté de confiance.

De nombreuses autorités cybernétiques proposent des flux CTI. Les exemples incluent le Centre australien de cybersécurité (ACSC), le programme Connect Inform Share Protect (CISP) proposé par le Centre national de cybersécurité du Royaume-Uni et le programme Malware Free Networks (MFN) proposé par le Bureau de la sécurité des communications du gouvernement de la Nouvelle Zélande. De nombreux AWS partenaires proposent également des flux de partage CTI.

Pour commencer à utiliser le partage de CTI, nous vous recommandons de procéder comme suit :

1. Déploiement d'une plateforme de renseignement sur les menaces — Déployez une plateforme qui ingère, agrège et organise les données de renseignement sur les menaces provenant de sources multiples et dans différents formats.
2. Ingestion de renseignements sur les cybermenaces : intégrez votre plateforme de renseignements sur les menaces à un ou plusieurs fournisseurs de flux d'informations sur les menaces. Lorsque vous recevez un flux de menaces, utilisez votre plateforme de renseignement sur les menaces pour traiter le nouveau CTI et identifier les informations exploitables pertinentes pour les opérations de sécurité de votre environnement. Automatisez autant que possible, mais certaines situations nécessitent une prise de décision humaine.
3. Automatisation des contrôles de sécurité préventifs et de détection : déployez le CTI sur les services de sécurité de votre architecture qui fournissent des contrôles préventifs et de détection. Ces services sont communément appelés systèmes de prévention des intrusions (IPS). Activé AWS, vous utilisez les API de service pour configurer des listes de blocage qui refusent l'accès depuis les adresses IP et les noms de domaine fournis dans les flux de menaces.
4. Gagner en visibilité grâce aux mécanismes d'observabilité : pendant que les opérations de sécurité ont lieu dans votre environnement, vous collectez de nouveaux CTI. Par exemple, vous pouvez observer une menace qui a été incluse dans le fil des menaces, ou vous pouvez observer des indicateurs de compromission associés à une intrusion (comme un exploit Zero-Day). La centralisation des informations sur les menaces fournit une meilleure connaissance de la situation dans votre environnement, de sorte que vous pouvez examiner les CTI existants et les CTI récemment découverts dans un seul système.
5. Partage des CTI avec votre communauté de confiance — Pour terminer le cycle de vie du partage des CTI, générez votre propre CTI et partagez-le à nouveau avec votre communauté de confiance.

La vidéo suivante, intitulée Scaling cyber threat intelligence sharing with the AUS Cyber Security Center, décrit ces étapes plus en détail. Bien que cette vidéo présente les capacités de partage CTI du Centre australien de cybersécurité, les étapes sont les mêmes, quel que soit le flux de menaces que vous choisissez ou votre localisation.

Déploiement d'une plateforme de renseignement sur les menaces

Une plateforme de renseignement sur les menaces ingère, agrège et organise les données de renseignement sur les menaces provenant de sources multiples et dans différents formats. Il permet aux analystes de consulter, de hiérarchiser et d'agir en fonction des informations sur les cybermenaces (CTI) reçues de leur communauté de confiance.

OpenCTI et MISP sont des plateformes open source courantes de renseignement sur les menaces. Des solutions sont également disponibles auprès des AWS partenaires sur le AWS Marketplace. Vous devez tenir compte du niveau de compétence de votre équipe de sécurité lorsque vous choisissez une plateforme de renseignement sur les menaces. Le MISP peut être puissant mais complexe, et OpenCTI possède une interface utilisateur plus intuitive.

Lorsque vous choisissez une plateforme de renseignement sur les menaces, tenez compte des points suivants :

- Fonctionnalités — La plateforme offre-t-elle des fonctionnalités telles que la surveillance en temps réel, la détection et l'analyse des menaces ?
- Sources de données — La plateforme utilise-t-elle diverses sources, notamment des flux de menaces, des informations sur le Dark Web, des réseaux sociaux et des informations open source ?
- Qualité des données — La plateforme dispose-t-elle de processus garantissant l'exactitude et la fiabilité des informations ?
- Évolutivité : la plateforme peut-elle s'adapter à l'évolution des besoins de votre entreprise, tels que la croissance et l'évolution des menaces ?
- Intégration — La plateforme peut-elle s'intégrer à vos outils et infrastructures de sécurité existants ?
- Expérience utilisateur — La plateforme est-elle facile à naviguer et à utiliser ?
- Personnalisation — La plateforme peut-elle être personnalisée pour répondre aux besoins spécifiques de votre organisation ?
- Coût — La plateforme est-elle rentable, y compris les coûts de licence et les exigences de maintenance ?

Vous pouvez déployer votre plateforme de renseignement sur les menaces au sein de votre cloud privé virtuel (VPC). Vous pouvez le déployer directement sur une instance Amazon Elastic Compute

Cloud (Amazon EC2) ou en utilisant une technologie de conteneur, telle qu'Amazon Elastic Container Service (Amazon ECS) ou. AWS Fargate Pour plus d'informations sur le choix du service de AWS conteneur adapté au développement de vos applications modernes, voir Choisir un service de AWS conteneur.

Ingestion de renseignements sur les cybermenaces

La première étape du processus d'ingestion consiste à convertir les données de renseignement sur les cybermenaces (CTI) issues des flux de menaces dans un format que votre plateforme de renseignement sur les menaces peut ingérer. C'est ce qu'on appelle la conversion CTI. Les données issues des flux de menaces peuvent être disponibles dans différents formats, tels que STIX (Structured Threat Information Expression). Vous devez restructurer les données entrantes dans un format prévisible et facile à utiliser, adapté aux produits de sécurité que vous utilisez dans votre AWS environnement.

Pour une compatibilité maximale, nous vous recommandons de convertir les données au format JSON. Par exemple, ils AWS Step Functionspeuvent consommer des données au format JSON, et les flux de travail automatisés peuvent utiliser ce format plus facilement et de manière plus cohérente. De plus amples informations sur la création de flux de travail automatisés sont fournies dans la section suivante, Automatisation des contrôles de sécurité préventifs et de détection.

Pour accélérer l'ingestion des données CTI, vous pouvez automatiser les transformations des données. Les données sont converties au fur et à mesure de leur ingestion, puis transmises directement à la plateforme de renseignement sur les menaces. Vous pouvez utiliser une AWS Lambda fonction pour terminer la transformation, et vous pouvez orchestrer le processus via Services AWS telle que AWS Step Functions ou Amazon EventBridge.

Lorsque vous ingérez du CTI, vous pouvez choisir les attributs à extraire et à conserver. La quantité exacte de détails requise peut varier en fonction des besoins de votre entreprise. Toutefois, pour mettre à jour les pare-feux et autres services de sécurité, nous recommandons les attributs minimaux suivants :

- Adresse IP et domaine
- Menace
- Ajouter ou supprimer de vos listes de menaces internes

Extrayez les attributs que vous souhaitez utiliser, puis formatez-les dans un modèle JSON structuré.

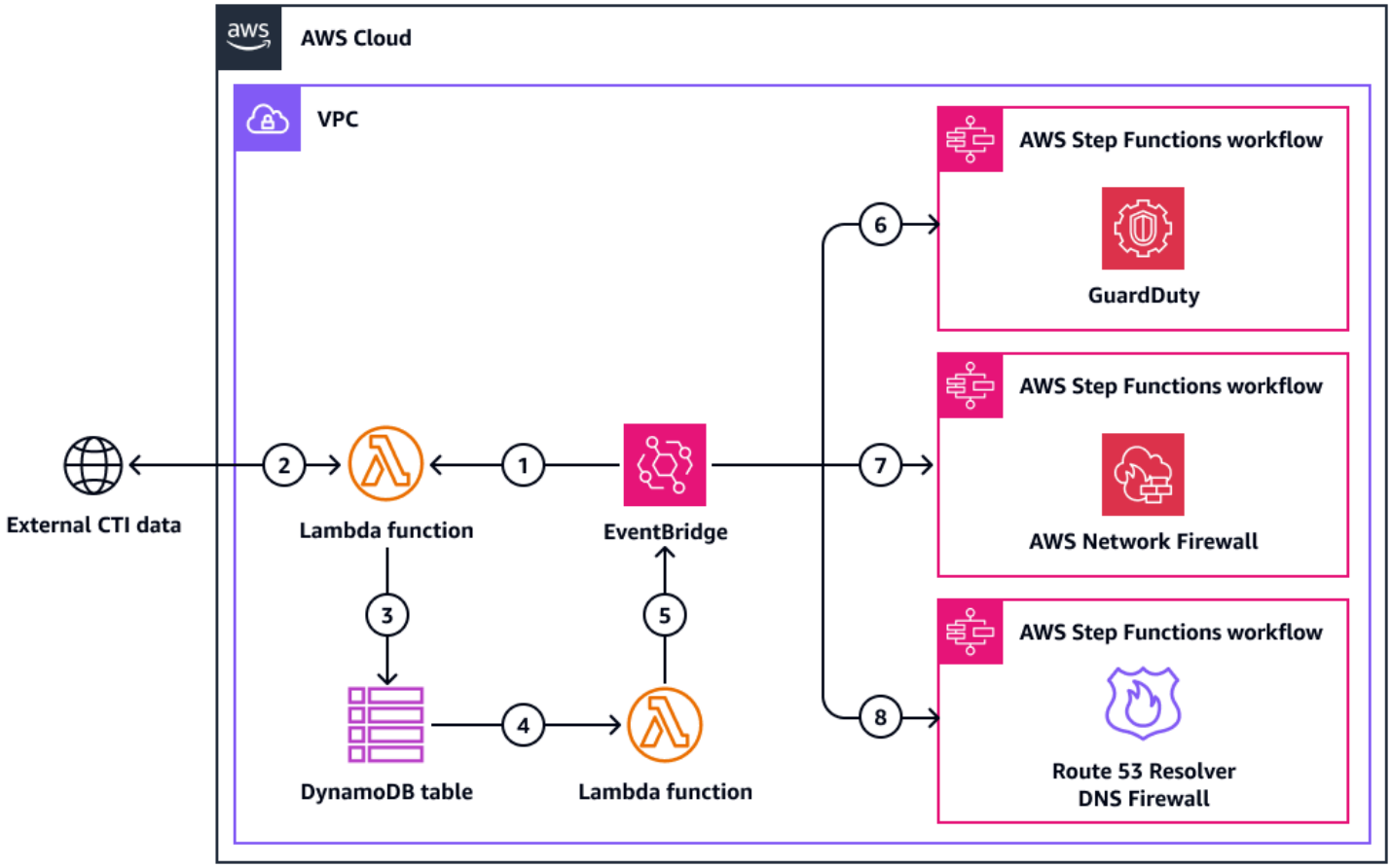
Automatiser les contrôles de sécurité préventifs et de détection

Une fois que les informations sur les cybermenaces (CTI) ont été intégrées à la plateforme de renseignement sur les menaces, vous pouvez automatiser le processus de modification de configuration en réponse aux données. Les plateformes de renseignement sur les menaces vous aident à gérer les informations sur les cybermenaces et à observer votre environnement. Ils permettent de structurer, de stocker, d'organiser et de visualiser des informations techniques et non techniques sur les cybermenaces. Ils peuvent vous aider à vous faire une idée des menaces et à combiner diverses sources de renseignement pour profiler et suivre les menaces, telles que les menaces persistantes avancées (APT).

L'automatisation peut réduire le délai entre la réception des informations sur les menaces et la mise en œuvre des modifications de configuration dans l'environnement. Toutes les réponses du CTI ne peuvent pas être automatisées. Cependant, l'automatisation du plus grand nombre de réponses possible permet à votre équipe de sécurité de hiérarchiser et d'évaluer les CTI restants plus rapidement. Chaque organisation doit déterminer quels types de réponses CTI peuvent être automatisés et lesquels nécessitent une analyse manuelle. Prenez cette décision en fonction du contexte organisationnel, tel que les risques, les actifs et les ressources. Par exemple, certaines organisations peuvent choisir d'automatiser le blocage de domaines ou d'adresses IP erronés connus, mais elles peuvent avoir besoin d'une enquête d'un analyste avant de bloquer les adresses IP internes.

Cette section fournit des exemples de configuration de réponses CTI automatisées dans Amazon GuardDuty et Amazon Route 53 Resolver DNS Firewall. AWS Network Firewall Vous pouvez implémenter ces exemples indépendamment les uns des autres. Laissez les exigences et les besoins de sécurité de votre entreprise guider vos décisions. Vous pouvez automatiser les modifications de configuration Services AWS par le biais d'un AWS Step Functionsflux de travail (également appelé machine à états). Lorsqu'une AWS Lambdafonction termine la conversion du CTI au format JSON, elle déclenche un EventBridge événement Amazon qui lance le flux de travail Step Functions.

Le schéma suivant montre un exemple d'architecture. Les flux de travail Step Functions mettent automatiquement à jour la liste des menaces dans GuardDuty, la liste des domaines dans Route 53 Resolver DNS Firewall et le groupe de règles dans Network Firewall.



La figure montre le flux de travail suivant :

1. Un EventBridge événement est lancé selon un calendrier régulier. Cet événement lance une AWS Lambda fonction.
2. La fonction Lambda récupère les données CTI du flux de menaces externe.
3. La fonction Lambda écrit les données CTI récupérées dans une table Amazon DynamoDB.
4. L'écriture de données dans la table DynamoDB déclenche un événement de flux de capture des données de modification qui lance une fonction Lambda.
5. En cas de modification, une fonction Lambda lance un nouvel événement dans. EventBridge Si aucune modification n'est survenue, le flux de travail se termine.
6. Si le CTI concerne les enregistrements d'adresses IP, il EventBridge lance un flux de travail Step Functions qui met automatiquement à jour la liste des menaces sur Amazon GuardDuty. Pour plus d'informations, consultez Amazon GuardDuty dans cette section.
7. Si le CTI concerne l'adresse IP ou les enregistrements de domaine, il EventBridge lance un flux de travail Step Functions qui met automatiquement à jour le groupe de règles dans AWS Network Firewall. Pour plus d'informations, consultez AWS Network Firewallcette section.

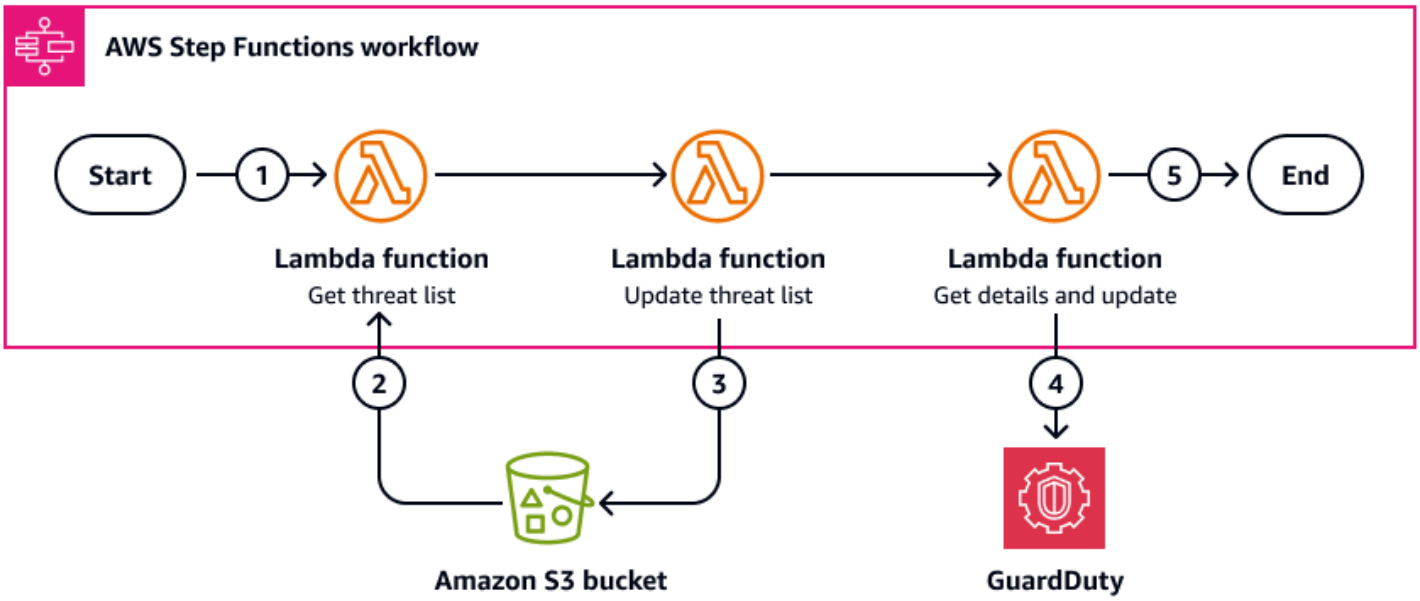
8. Si le CTI concerne les enregistrements de domaine, EventBridge lance un flux de travail Step Functions qui met automatiquement à jour la liste des domaines dans Amazon Route 53 Resolver DNS Firewall. Pour plus d'informations, consultez la section Pare-feu Amazon Route 53 Resolver DNS dans cette section.

Amazon GuardDuty

Amazon GuardDuty est un service de détection des menaces qui surveille en permanence votre activité Comptes AWS et votre charge de travail pour détecter toute activité non autorisée et fournit des résultats de sécurité détaillés à des fins de visibilité et de correction. En mettant automatiquement à jour la liste des GuardDuty menaces à partir des flux CTI, vous pouvez obtenir des informations sur les menaces susceptibles d'accéder à vos charges de travail. GuardDuty améliore vos capacités de contrôle des détectives.

> **Tip**
>
> GuardDuty s'intègre nativement à AWS Security Hub CSPM. Security Hub CSPM fournit une vue complète de votre état de sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Lorsque vous GuardDuty intégrez Security Hub CSPM, vos GuardDuty résultats sont automatiquement envoyés à Security Hub CSPM. Security Hub CSPM peut ensuite inclure ces résultats dans son analyse de votre posture de sécurité. Pour plus d'informations, consultez la section Intégration avec AWS Security Hub CSPM dans la GuardDuty documentation. Dans Security Hub CSPM, vous pouvez utiliser des automatisations pour améliorer vos capacités de détection et de contrôle de sécurité réactives.

L'image suivante montre comment un flux de travail Step Functions peut utiliser le CTI d'un flux de menaces pour mettre à jour la liste des menaces dans GuardDuty. Lorsqu'une fonction Lambda finit de convertir le CTI au format JSON, elle déclenche un EventBridge événement qui démarre le flux de travail.



Le schéma montre les étapes suivantes :

1. Si le CTI concerne les enregistrements d'adresses IP, EventBridge démarre le flux de travail Step Functions.
2. Une fonction Lambda extrait la liste des menaces, qui est stockée sous forme d'objet dans un bucket Amazon Simple Storage Service (Amazon S3).
3. Une fonction Lambda met à jour la liste des menaces avec les modifications d'adresse IP dans le CTI. Il enregistre la liste des menaces en tant que nouvelle version de l'objet dans le compartiment Amazon S3 d'origine. Le nom de l'objet est inchangé.
4. Une fonction Lambda utilise des appels d'API pour récupérer l'identifiant du GuardDuty détecteur et l'identifiant du set d'informations sur les menaces. Il utilise ces identifiants pour effectuer une mise GuardDuty à jour afin de faire référence à la nouvelle version de la liste des menaces.

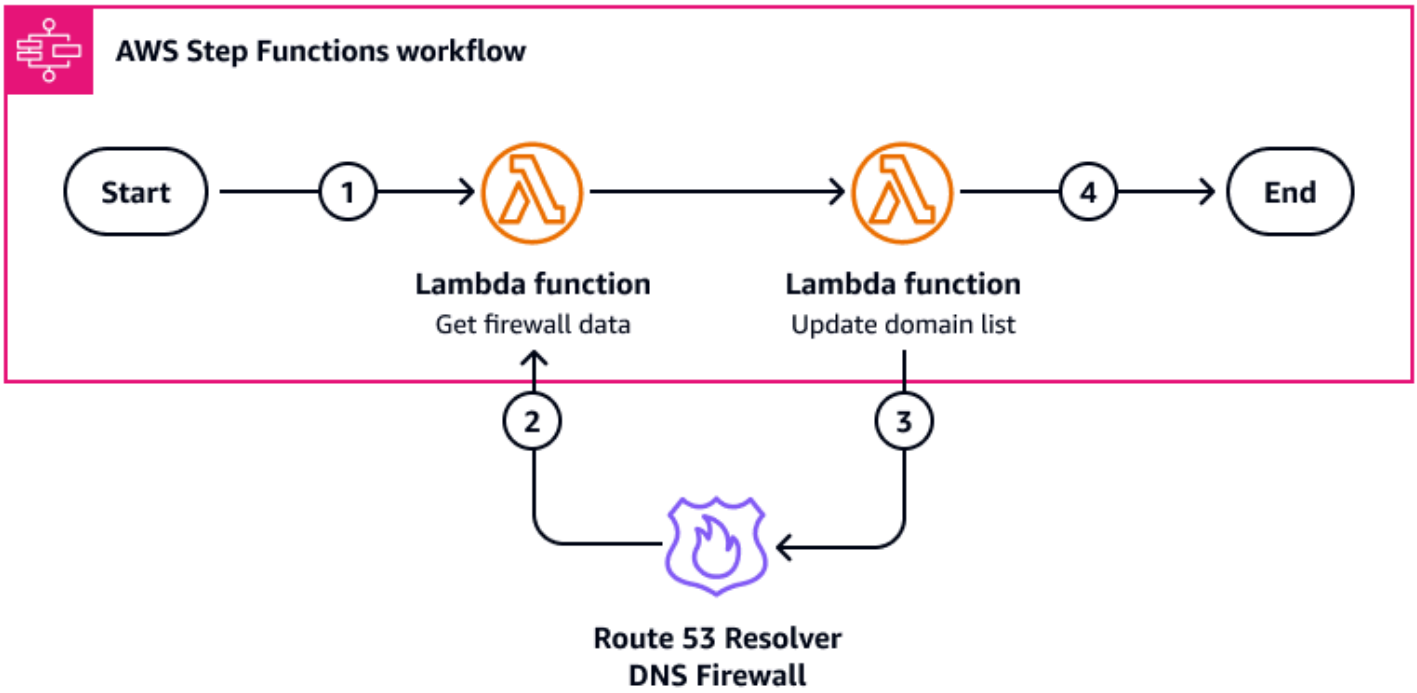
> **Note**
>
> Vous ne pouvez pas récupérer un GuardDuty détecteur et une liste d'adresses IP spécifiques car ils sont récupérés sous forme de matrice. Par conséquent, nous vous recommandons de n'en avoir qu'un seul dans la cible Compte AWS. Si vous en avez plusieurs, vous devez vous assurer que les données correctes sont extraites dans la fonction Lambda finale de ce flux de travail.

5. Le flux de travail Step Functions se termine.

Amazon Route 53 Resolver Pare-feu DNS

Amazon Route 53 Resolver Le pare-feu DNS vous aide à filtrer et à réguler le trafic DNS sortant pour votre cloud privé virtuel (VPC). Dans le pare-feu DNS, vous créez un groupe de règles qui bloque les adresses de domaine identifiées par le flux CTI. Vous configurez un flux de travail Step Functions pour ajouter et supprimer automatiquement des domaines de ce groupe de règles.

L'image suivante montre comment un flux de travail Step Functions peut utiliser le CTI d'un flux de menaces pour mettre à jour la liste des domaines dans le pare-feu Amazon Route 53 Resolver DNS. Lorsqu'une fonction Lambda finit de convertir le CTI au format JSON, elle déclenche un EventBridge événement qui démarre le flux de travail.



Le schéma montre les étapes suivantes :

1. Si le CTI concerne des enregistrements de domaine, EventBridge démarre le flux de travail Step Functions.
2. Une fonction Lambda récupère les données de la liste de domaines pour le pare-feu. Pour plus d'informations sur la création de cette fonction Lambda, consultez get_firewall_domain_list dans la documentation. AWS SDK pour Python (Boto3)
3. Une fonction Lambda utilise le CTI et les données récupérées pour mettre à jour la liste des domaines. Pour plus d'informations sur la création de cette fonction Lambda, consultez

update_firewall_domains dans la documentation de Boto3. La fonction Lambda permet d'ajouter, de supprimer ou de remplacer des domaines.

4. Le flux de travail Step Functions se termine.

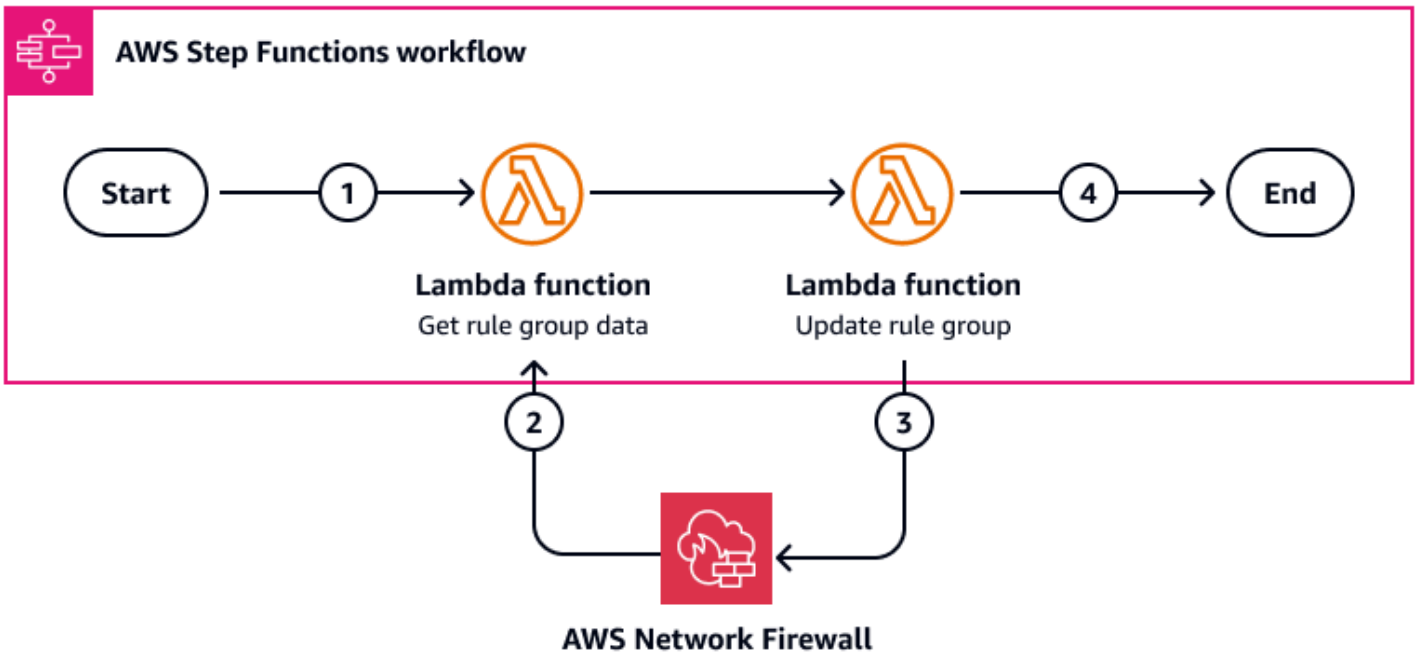
Nous recommandons les bonnes pratiques suivantes :

- Nous vous recommandons d'utiliser à la fois le pare-feu DNS Route 53 Resolver et AWS Network Firewall. Le pare-feu DNS filtre le trafic DNS et le Network Firewall filtre tous les autres types de trafic.
- Nous vous recommandons d'activer la journalisation pour le pare-feu DNS. Vous pouvez créer des contrôles de détection qui surveillent les données du journal et vous alertent si un domaine restreint tente de faire passer le trafic par le pare-feu. Pour plus d'informations, consultez la section Surveillance des groupes de règles du pare-feu DNS Route 53 Resolver avec Amazon CloudWatch.

AWS Network Firewall

AWS Network Firewallest un pare-feu réseau dynamique et géré, ainsi qu'un service de détection et de prévention des intrusions pour les VPC du. AWS Cloud Il filtre le trafic sur le périmètre de votre VPC pour vous aider à bloquer les menaces. L'utilisation de flux de renseignements sur les menaces pour mettre à jour automatiquement les groupes de règles du Network Firewall peut contribuer à protéger les charges de travail et les données du cloud de votre entreprise contre les acteurs malveillants.

L'image suivante montre comment un flux de travail Step Functions peut utiliser le CTI d'un flux de menaces pour mettre à jour un ou plusieurs groupes de règles dans Network Firewall. Lorsqu'une fonction Lambda finit de convertir le CTI au format JSON, elle déclenche un EventBridge événement qui démarre le flux de travail.



Le schéma montre les étapes suivantes :

1. Si le CTI concerne l'adresse IP ou les enregistrements de domaine, il EventBridge lance un flux de travail Step Functions qui met automatiquement à jour le groupe de règles dans Network Firewall.
2. Une fonction Lambda extrait les données du groupe de règles auprès de Network Firewall.
3. Une fonction Lambda utilise le CTI pour mettre à jour le groupe de règles. Il ajoute ou supprime des adresses IP ou des domaines.
4. Le flux de travail Step Functions se termine.

Nous recommandons les bonnes pratiques suivantes :

- Network Firewall peut avoir plusieurs groupes de règles. Créez des groupes de règles distincts pour les domaines et les adresses IP.
- Nous vous recommandons d'activer la journalisation pour Network Firewall. Vous pouvez créer des contrôles de détection qui surveillent les données du journal et vous alertent si un domaine restreint ou une adresse IP tente de faire passer le trafic via le pare-feu. Pour plus d'informations, consultez la section Enregistrement du trafic réseau depuis AWS Network Firewall.
- Nous vous recommandons d'utiliser à la fois le pare-feu DNS Route 53 Resolver et AWS Network Firewall. Le pare-feu DNS filtre le trafic DNS et le Network Firewall filtre tous les autres types de trafic.

Gagner en visibilité grâce aux mécanismes d'observabilité

La possibilité de visualiser les événements de sécurité survenus est tout aussi importante que la mise en place de contrôles de sécurité appropriés. Dans le pilier de sécurité du AWS Well-Architected Framework, les meilleures pratiques de détection incluent la configuration de la journalisation des services et des applications et la capture des journaux, des résultats et des métriques dans des emplacements standardisés. Pour mettre en œuvre ces meilleures pratiques, vous devez enregistrer les informations qui vous aident à identifier les événements, puis les traiter dans un format utilisable par l'homme, idéalement dans un emplacement centralisé.

Ce guide vous recommande d'utiliser Amazon Simple Storage Service (Amazon S3) pour centraliser les données des journaux. Amazon S3 prend en charge le stockage des journaux à la fois pour le pare-feu Amazon Route 53 Resolver DNS AWS Network Firewall et pour le DNS. Vous utilisez AWS Security Hub CSPMensuite Amazon Security Lake pour centraliser les résultats d'Amazon et GuardDuty les autres résultats de sécurité en un seul endroit.

Enregistrement du trafic réseau

La section Automatisation des contrôles de sécurité préventifs et de détection de ce guide décrit l'utilisation AWS Network Firewall d'un pare-feu Amazon Route 53 Resolver DNS pour automatiser les réponses aux informations sur les cybermenaces (CTI). Nous vous recommandons de configurer la journalisation pour ces deux services. Vous pouvez créer des contrôles de détection qui surveillent les données du journal et vous alertent si un domaine restreint ou une adresse IP tente de faire passer le trafic via le pare-feu.

Lors de la configuration de ces ressources, tenez compte de vos besoins individuels en matière de journalisation. Par exemple, la journalisation pour Network Firewall n'est disponible que pour le trafic que vous transférez vers le moteur de règles dynamiques. Nous vous recommandons de suivre un modèle de confiance zéro et de transférer tout le trafic vers le moteur de règles dynamiques. Toutefois, si vous souhaitez réduire les coûts, vous pouvez exclure le trafic auquel votre organisation fait confiance.

Network Firewall et DNS Firewall prennent tous deux en charge la connexion à Amazon S3. Pour plus d'informations sur la configuration de la journalisation pour ces services, consultez Journalisation du trafic réseau depuis AWS Network Firewall et Configuration de la journalisation pour le pare-feu DNS. Pour les deux services, vous pouvez configurer la journalisation dans un compartiment Amazon S3 via le Console de gestion AWS.

Centralisation des résultats de sécurité dans AWS

AWS Security Hub CSPMfournit une vue complète de votre état de sécurité AWS et vous aide à évaluer votre AWS environnement par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub CSPM peut générer des résultats associés à vos contrôles de sécurité. Il peut également recevoir les résultats d'autres Services AWS sources, comme Amazon GuardDuty. Vous pouvez utiliser Security Hub CSPM pour centraliser les résultats et les données provenant de vos produits tiers pris en charge et de ceux de Comptes AWS tiers Services AWS pris en charge. Pour plus d'informations sur les intégrations, consultez la section Comprendre les intégrations dans Security Hub CSPM dans la documentation de Security Hub CSPM.

Security Hub CSPM inclut également des fonctionnalités d'automatisation qui vous aident à trier et à résoudre les problèmes de sécurité. Par exemple, vous pouvez utiliser des règles d'automatisation pour mettre à jour automatiquement les résultats critiques en cas d'échec d'un contrôle de sécurité. Vous pouvez également utiliser l'intégration avec Amazon EventBridge pour lancer des réponses automatiques à des résultats spécifiques. Pour plus d'informations, consultez la section Modifier automatiquement les résultats du Security Hub CSPM et agir en conséquence dans la documentation du Security Hub CSPM.

Si vous utilisez Amazon GuardDuty, nous vous recommandons de configurer GuardDuty pour envoyer ses résultats à Security Hub CSPM. Security Hub CSPM peut ensuite inclure ces résultats dans son analyse de votre posture de sécurité. Pour plus d'informations, consultez la section Intégration avec AWS Security Hub CSPM dans la GuardDuty documentation.

Pour Network Firewall et Route 53 Resolver DNS Firewall, vous pouvez créer des résultats personnalisés à partir du trafic réseau que vous enregistrez. Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard. Vous pouvez créer des requêtes dans Athena qui analysent les journaux dans Amazon S3 et extraient les données pertinentes. Pour obtenir des instructions, consultez Getting Started dans la documentation d'Athena. Vous pouvez ensuite utiliser une AWS Lambda fonction pour convertir les données de journal pertinentes au format ASFF (AWS Security Finding Format) et envoyer les résultats au Security Hub CSPM. Voici un exemple de fonction Lambda qui convertit les données de journal de Network Firewall en résultats CSPM du Security Hub :

```
Import { SecurityHubClient, BatchImportFindingsCommand, GetFindingsCommand } from
 "@aws-sdk/client-securityhub";

Export const handler = async(event) => {
   const date = new Date().toISOString();
```

```
   const config = {
      Region: REGION
   };

   const input = {
      Findings: [
         {
            SchemaVersion: '2018-10-08',
            Id: ALERTLOGS3BUCKETID,
            ProductArn: FIREWALLMANAGERARN,
            GeneratorId: 'alertlogs-to-findings',
            AwsAccountId: ACCOUNTID,
            Types: 'Unusual Behaviours/Network Flow/Alert',
            CreatedAt: date,
            UpdatedAt: date,
            Severity: {
               Normalized: 80,
               Product: 8
            },
            Confidence: 100,
            Title: 'Alert Log to Findings',
            Description: 'Network Firewall Alert Log into Finding - add
               top level dynamic detail',
            Resources: [
               {
                  /*these are custom resources. Contain deeper details of your event
 here*/
                  firewallName: 'Example Name',
                  event: 'Example details here'
               }
            ]
         }
      ]
   };

   const client = new SecurityHubClient(config);
   const command = new BatchImportFindingsCommand(input);
   const response = await client.send(command);
   return { statusCode: 200, response };
};
```

Le modèle que vous suivez pour extraire et envoyer des informations à Security Hub CSPM dépend des besoins individuels de votre entreprise. Si vous avez besoin que les données soient envoyées selon un calendrier régulier, vous pouvez les utiliser EventBridge pour lancer le processus. Si vous souhaitez recevoir une alerte lorsque les informations sont ajoutées, vous pouvez utiliser Amazon Simple Notification Service (Amazon SNS). Il existe de nombreuses manières d'aborder cette architecture. Il est donc important de bien planifier afin de répondre aux besoins de votre entreprise.

Intégration AWS données de sécurité avec d'autres données d'entreprise

Amazon Security Lake peut automatiser la collecte des données des journaux et des événements liés à la sécurité à partir de services intégrés Services AWS et tiers. Il vous aide également à gérer le cycle de vie des données grâce à des paramètres de rétention et de réplication personnalisables. Security Lake convertit les données ingérées au format Apache Parquet et en un schéma open source standard appelé Open Cybersecurity Schema Framework (OCSF). Grâce au support OCSF, Security Lake normalise et combine les données de sécurité issues d' AWS un large éventail de sources de données de sécurité d'entreprise. Services AWS D'autres services tiers peuvent s'abonner aux données stockées dans Security Lake à des fins de réponse aux incidents et d'analyse des données de sécurité.

Vous pouvez configurer Security Lake pour recevoir les résultats de Security Hub CSPM. Pour activer cette intégration, vous devez activer les deux services et ajouter Security Hub CSPM en tant que source dans Security Lake. Une fois ces étapes terminées, Security Hub CSPM commence à envoyer tous les résultats à Security Lake. Security Lake normalise automatiquement les résultats du Security Hub CSPM et les convertit en OCSF. Dans Security Lake, vous pouvez ajouter un ou plusieurs abonnés pour consulter les résultats du Security Hub CSPM. Pour plus d'informations, consultez la section Intégration avec AWS Security Hub CSPM dans la documentation de Security Lake.

La vidéo suivante, AWS Re:inForce 2024 - Cyber Threat Intelligence sharing on AWS, explique comment utiliser les intégrations Security Hub CSPM et Security Lake pour partager des CTI.

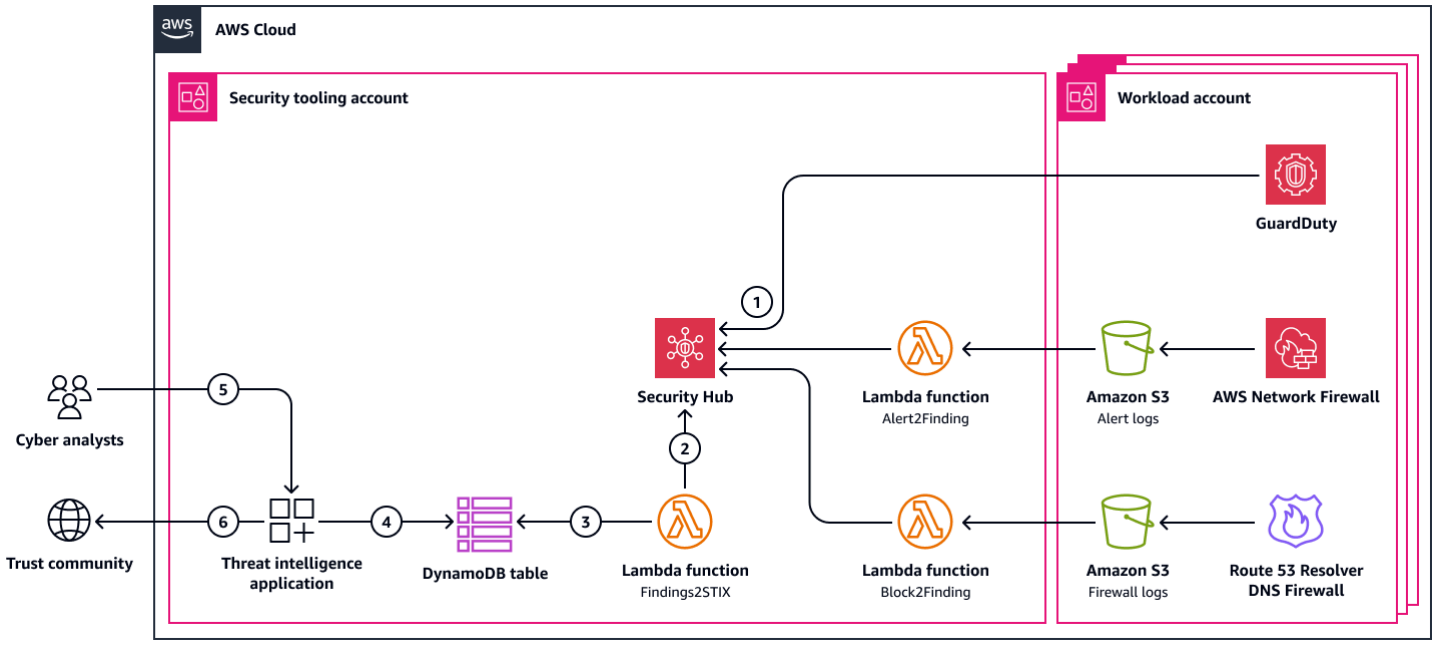
Partage du CTI avec votre communauté de confiance

La communauté à laquelle vous envoyez des informations sur les cybermenaces (CTI) est généralement la même que celle dont vous recevez les CTI. Cependant, vous pouvez choisir de partager avec un plus grand nombre de personnes. Par exemple, vous pouvez choisir de partager avec des organismes gouvernementaux ou réglementaires en qui vous avez confiance, tels que votre

centre national de cybersécurité ou vos centres de partage et d'analyse des informations (ISAC). L'objectif est de propager et de mettre en œuvre rapidement le CTI en mettant en commun les résultats de plusieurs organisations. Votre plateforme de renseignement sur les menaces gère les intégrations d'API pour le partage avec plusieurs flux.

L'envoi du CTI à la communauté de confiance se fait en même temps que la mise en œuvre de contrôles préventifs et de détection. Vous utilisez les journaux pour identifier les événements de sécurité. Ensuite, vous centralisez les événements et les résultats afin d'obtenir rapidement une vue d'ensemble de l'état de sécurité de votre Comptes AWS entreprise. Ensuite, vos équipes de sécurité, telles que vos cyber-analystes, peuvent identifier toute information susceptible d'être utile. Comme vous avez déjà enregistré des résultats AWS Security Hub CSPM, vous pouvez les convertir dans le format utilisé par le flux de menaces, tel que JSON ou STIX. Ensuite, vous envoyez le CTI au fournisseur d'alimentation. Leurs plateformes de renseignement sur les menaces ingèrent, anonymisent et valident le CTI que vous fournissez. Ensuite, votre CTI est partagé avec une communauté encore plus large.

L'image suivante montre comment vous pouvez l'utiliser Services AWS pour générer du CTI, puis le partager avec votre communauté de confiance, y compris les autorités cybernétiques et les autres membres de la communauté.



Ce diagramme montre le flux de travail suivant :

1. Les résultats sont créés dans AWS Security Hub CSPM.

2. Une AWS Lambda fonction extrait les résultats de Security Hub CSPM et les convertit dans un format partageable, tel que JSON ou STIX.
3. La fonction Lambda stocke les résultats dans une table Amazon DynamoDB.
4. La plateforme tierce de renseignement sur les menaces, qui fonctionne sur Amazon Elastic Compute Cloud (Amazon EC2) ou Amazon Elastic Container Service (Amazon ECS), extrait les résultats de la table DynamoDB.
5. Un cyber-analyste examine le CTI dans la plateforme de renseignement sur les menaces.
6. La plateforme de renseignement sur les menaces publie le CTI auprès de la communauté de confiance, composée d'autres producteurs et consommateurs de CTI.

Prochaines étapes et ressources

Tenez compte des actifs, du secteur et de l'environnement de menace de votre organisation. Ces facteurs devraient informer les communautés de confiance que vous choisissez de rejoindre pour partager des informations sur les cybermenaces. De nombreuses autorités cybernétiques du monde entier proposent des flux de renseignements sur les menaces. Réfléchissez à ce qui est proposé et choisissez celui qui convient le mieux au cas d'utilisation de votre organisation. Utilisez ce guide comme une approche modulaire et adaptez-le en conséquence à votre organisation.

Nous vous recommandons de consulter les ressources supplémentaires suivantes. Ces ressources peuvent vous aider à créer ou à déployer une plateforme de renseignement sur les menaces dans votre AWS environnement et à configurer le partage de renseignements sur les cybermenaces.

AWS ressources

- AWS Centre d'architecture
- AWS Re:inForce 2024 - Le partage de renseignements sur AWS les cybermenaces est activé (vidéo)
- AWS Sommet ANZ 2023 : Élargir le partage de renseignements sur les cybermenaces avec le centre de cybersécurité de l'AUS (vidéo)

Service AWS documentation

- Documentation Amazon DynamoDB
- EventBridge Documentation Amazon
- GuardDuty Documentation Amazon
- Documentation AWS Lambda
- AWS Network Firewall documentation
- Amazon Route 53 Resolver Documentation sur le pare-feu DNS
- Documentation AWS Security Hub CSPM
- Documentation Amazon Security Lake
- Documentation Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions documentation

Ressources STIX

- Exemples de STIX 2.1
- Indicateur d'URL malveillante

Plateformes de renseignement sur les menaces

- OpenCTI
- MISP

Collaborateurs

Les personnes suivantes ont contribué à ce guide.

Conception

- Jess Modini, technologue principale, AWS
- Alexa Donovan, architecte de solutions associée, AWS
- Steven Ryan, architecte de solutions pour les partenaires, AWS
- Byron Pogson, architecte de solutions de sécurité, AWS

Révision

- Brian Farnhill, ingénieur principal en développement logiciel, AWS
- Marc Luescher, architecte de solutions senior, AWS
- Stefan Mijic, spécialiste de l'assurance sécurité, AWS
- Timothy Woodill, architecte de solutions pour le secteur public, AWS

Rédaction technique

- Lilly AbouHarb, rédactrice technique senior, AWS

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Publication initiale	—	12 décembre 2024

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.