Guide technique AWS

Guide de réponse aux incidents de sécurité AWS

Guide de réponse aux incidents de sécurité AWS: Guide technique AWS

Table of Contents

Guide de réponse aux incidents de sécurité AWS

Date de publication : 23 novembre 2020 (Révisions du document)

Ce guide présente une vue d'ensemble des éléments fondamentaux de la réponse aux incidents de sécurité dans l'environnement de cloud AWS d'un client. Il offre une vue d'ensemble des concepts de la sécurité du cloud et de la réponse aux incidents, et identifie les capacités, les services et les mécanismes du cloud disponibles pour les clients qui doivent résoudre des problèmes de sécurité.

Ce document est destiné aux personnes occupant des postes techniques et suppose que vous êtes familiarisé avec les principes généraux de la sécurité des informations, que vous avez une compréhension de base de la réponse aux incidents dans vos environnements sur site actuels et que vous êtes familiarisé avec les services cloud.

Introduction

Chez AWS, la sécurité est la priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité. Le cloud AWS utilise un modèle de responsabilité partagée. AWS gère la sécurité du cloud. Vous êtes responsable de la sécurité dans le cloud. Cela signifie que vous conservez le contrôle de la sécurité que vous choisissez de mettre en œuvre. Vous avez accès à des centaines d'outils et de services pour vous aider à atteindre vos objectifs de sécurité. Ces fonctionnalités vous aident à établir une base de sécurité qui répond à vos objectifs pour vos applications exécutées dans le cloud.

Lorsqu'un écart par rapport à votre niveau de référence se produit (par exemple en raison d'une erreur de configuration), vous devrez peut-être réagir et enquêter. Pour y parvenir, vous devez comprendre les concepts de base de la réponse aux incidents de sécurité au sein de votre environnement AWS, ainsi que les problèmes que vous devez prendre en compte pour préparer, former et entraîner vos équipes cloud avant que des problèmes de sécurité ne surviennent. Il est important de savoir quels contrôles et capacités vous pouvez utiliser, pour examiner des exemples d'actualité afin de résoudre des problèmes potentiels et identifier les méthodes de correction que vous pouvez utiliser pour tirer parti de l'automatisation et améliorer votre vitesse de réponse.

Étant donné que la réponse aux incidents de sécurité peut être un sujet complexe, nous vous conseillons de commencer à petite échelle, de développer des runbooks, de tirer parti des capacités de base et de créer une bibliothèque initiale de mécanismes de réponse aux incidents à partir desquels vous pourrez itérer et améliorer. Ce travail initial doit impliquer votre service juridique ainsi que des équipes qui ne sont pas concernées par la sécurité, afin que vous soyez mieux en mesure de comprendre l'impact de la réponse aux incidents (IR) et des choix que vous avez faits sur vos objectifs d'entreprise.

Rubriques

Avant de commencer

En plus du présent document, nous vous encourageons à consulter Bonnes pratiques en matière de sécurité, d'identité et de conformité et le livre blanc Perspectives de sécurité du framework relatif à l'adoption du cloud AWS (CAF). L'AWS CAF fournit des conseils qui prennent en charge la coordination entre les différentes parties des organisations qui migrent vers le cloud. Les directives du framework CAF sont divisées en plusieurs domaines d'intérêt pertinents pour l'implémentation de systèmes informatiques basés sur le cloud, que nous appelons perspectives. La perspective Sécurité décrit comment implémenter un programme de sécurité sur plusieurs axes de travail, dont l'un se concentre sur la réponse aux incidents. Le présent document détaille certaines de nos expériences visant à aider les clients à évaluer et à implémenter des mécanismes efficaces dans cet axe de travail.

Perspective Sécurité du framework AWS CAF

La perspective Sécurité comprend quatre éléments :

- Les contrôles directifs définissent des modèles de gouvernance, de risque et de conformité qui serviront de cadre à l'environnement.
- Les contrôles préventifs protègent vos charges de travail et limitent les menaces et les vulnérabilités.
- Les contrôles de détection offrent une visibilité et une transparence complètes sur le fonctionnement des déploiements dans AWS.
- Les contrôles de réaction permettent de remédier à certains écarts potentiels par rapport à vos principes de sécurité de base.

Bien que la réponse aux incidents soit généralement associée aux contrôles de réaction, ceux-ci sont dépendants et influencés par les autres composants. Par exemple, les contrôles de sécurité directifs et préventifs permettent d'établir une base de référence, afin que vous puissiez surveiller et étudier tout écart par rapport à cette référence. Cette approche permet non seulement d'éliminer le bruit, mais elle contribue également à concevoir une sécurité défensive.

Base de la réponse aux incidents

Tous les utilisateurs AWS au sein d'une organisation doivent avoir une connaissance de base des processus de réponse aux incidents de sécurité, et le personnel de sécurité doit parfaitement

comprendre comment réagir aux problèmes de sécurité. Avant de gérer un événement de sécurité, vous devez impérativement avoir acquis l'expérience et la formation nécessaires au programme de réponse aux incidents dans le cloud. Les concepts de base d'un programme de réponse aux incidents réussi dans le cloud sont : former, préparer, simuler et itérer.

Pour comprendre chacun de ces aspects, examinez les descriptions suivantes :

- Formez votre personnel chargé des opérations de sécurité et de réponse aux incidents sur les technologies cloud et sur la façon dont votre organisation a l'intention de les utiliser.
- Préparez votre équipe de réponse aux incidents à détecter et réagir aux incidents dans le cloud, en activant les capacités de détection et en assurant un accès approprié aux outils et aux services cloud nécessaires. De plus, préparez les runbooks nécessaires, manuels et automatisés, pour garantir des réponses fiables et cohérentes. Collaborez avec d'autres équipes pour établir les opérations de base attendues, et utilisez ces connaissances pour identifier les écarts par rapport à ces opérations normales.
- Simulez des événements de sécurité attendus et inattendus dans votre environnement cloud pour déterminer l'efficacité de votre préparation.
- Itérez le résultat de votre simulation pour améliorer l'étendue de votre niveau de réponse et réduire le délai et les risques supplémentaires.

Former

Rubriques

Responsabilité partagée

La responsabilité en matière de sécurité et de conformité est partagée entre AWS et vous. Ce modèle partagé allège votre charge opérationnelle, car AWS exploite, gère et contrôle les composants depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles les services sont exploités.

Vous êtes responsable de la gestion des systèmes d'exploitation invités (y compris les mises à jour et les correctifs de sécurité) et des logiciels d'application, ainsi que de la configuration des contrôles de sécurité fournis par AWS, tels que les groupes de sécurité, les listes de contrôle d'accès réseau et la gestion des identités et des accès. Vous devez réfléchir attentivement aux services que vous choisissez, car vos responsabilités varient selon les services choisis, l'intégration de ces services dans votre environnement informatique et la législation et la réglementation en vigueur. La Figure 2 montre une représentation classique du modèle de responsabilité partagée tel qu'il s'applique aux services d'infrastructure, par exemple Amazon Elastic Compute Cloud (Amazon EC2). Il distingue la plupart des responsabilités en deux catégories : la sécurité du cloud (gérée par AWS) et la sécurité dans le cloud (gérée par le client). Les responsabilités peuvent changer en fonction des services que vous utilisez. Pour les services dissociés, tels qu'Amazon S3 et Amazon DynamoDB, AWS exploite la couche d'infrastructure, le système d'exploitation et les plateformes, tandis que les clients ont accès aux points de terminaison pour stocker et extraire des données. Le client est responsable de la gestion de ses données (y compris des options de chiffrement), du classement de ses ressources et de l'utilisation des outils IAM pour appliquer les autorisations appropriées.

Cependant, le modèle de responsabilité partagée évolue avec l'ajout de conteneurs et d'autres services qui transfèrent le modèle d'exploitation vers le fournisseur de services. Au fur et à mesure que nous nous dirigeons vers la gauche du modèle opérationnel, en nous éloignant de l'IaaS et des centres de données et en nous dirigeant vers le PaaS, la responsabilité du fournisseur de

services augmente. Un client a moins de responsabilités dans le cloud et profite d'une exploitation plus facile lorsqu'il utilise la migration vers la gauche du graphique. Examinez les figures suivantes et les différences dans la capacité à exploiter ou à fonctionner dans le cloud. À mesure que votre responsabilité partagée dans le cloud évolue, vos options en matière de réponse aux incidents ou d'analyse des attaques évoluent également. En tant que client, lorsque vous planifiez votre réponse aux incidents, vous devez également vous assurer que votre planification tient compte des capacités dont vous disposez dans votre modèle d'exploitation et que vous planifiez les interactions possibles avant qu'elles ne se produisent dans le modèle que vous avez choisi. La planification et la compréhension de ces compromis et leur adéquation à vos besoins en matière de gouvernance constituent une étape cruciale de la réponse aux incidents.

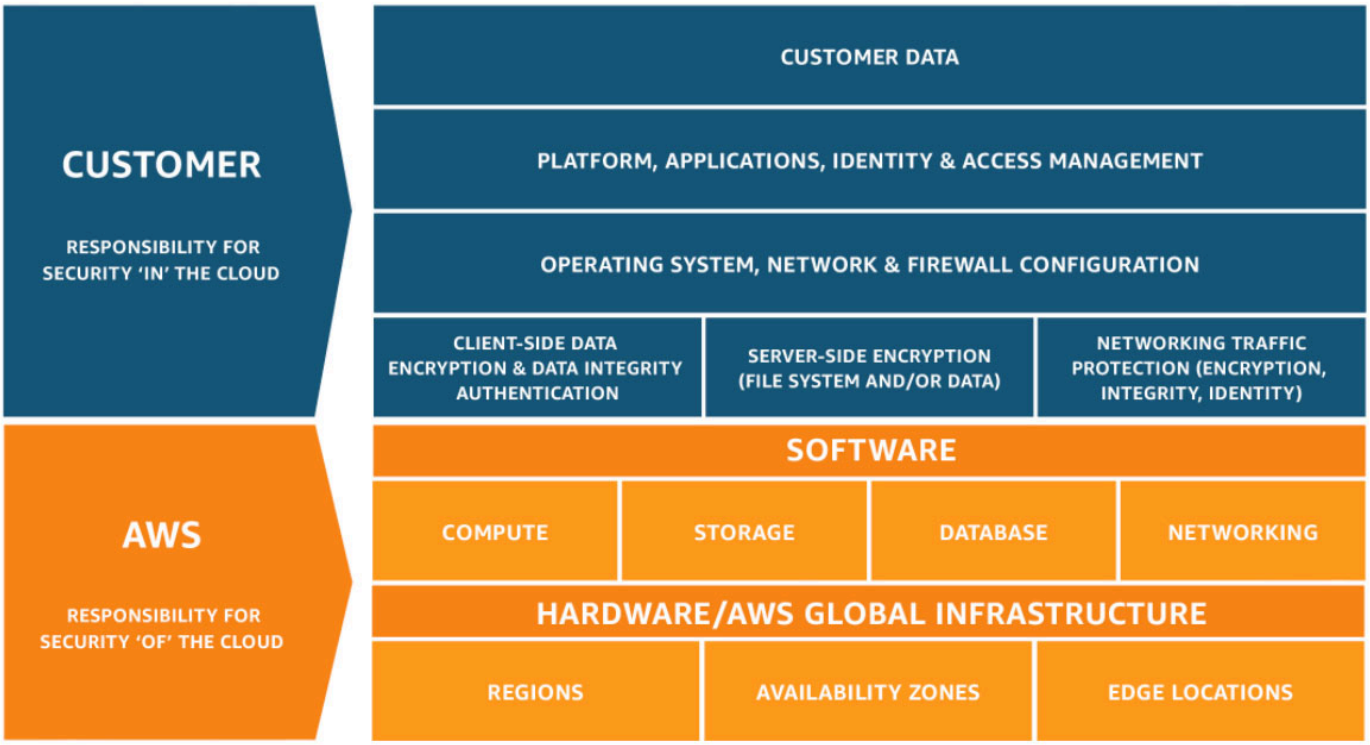

Figure 1 : Modèle de responsabilité partagée

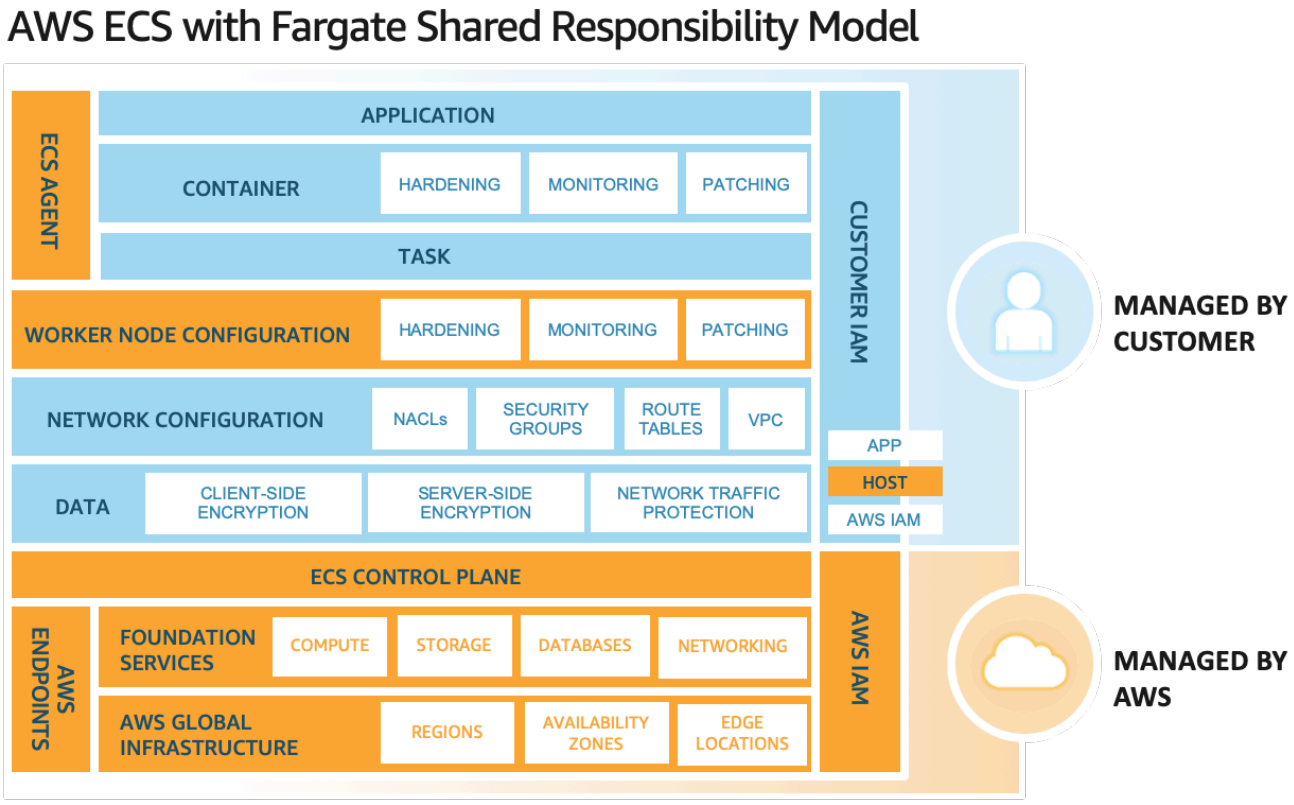

Figure 2 : Modèle de responsabilité partagée Amazon Elastic Container Service (Amazon ECS) avec AWS Fargate

Outre la relation directe que vous entretenez avec AWS, d'autres entités peuvent avoir des responsabilités dans votre modèle de responsabilité particulier. Par exemple, des unités d'organisation internes peuvent assumer la responsabilité de certains aspects de vos opérations. Des partenaires ou d'autres tiers peuvent également développer, gérer ou exploiter certaines de vos technologies de cloud.

Il est extrêmement important de créer un runbook de réponse aux incidents et d'analyse des attaques approprié qui correspond à votre modèle d'exploitation. Votre réussite dépend de votre compréhension des types d'outils que vous devez créer, ou des outils que vous devez acheter, pour le modèle d'exploitation que vous avez sélectionné. Plus votre organisation comprend les outils disponibles, mieux vous serez préparé à répondre aux besoins du modèle de gouvernance, de risque et de conformité (GRC) de votre entreprise.

Réponse aux incidents dans le cloud

Objectifs de conception de la réponse cloud

Bien que les processus et mécanismes généraux de réponse aux incidents, tels que ceux définis dans le document NIST SP 800-61 Computer Security Incident Handling Guide, restent valables, nous vous encourageons à prendre en compte ces objectifs de conception spécifiques qui sont pertinents pour répondre aux incidents de sécurité dans un environnement cloud :

- Définir des objectifs de réponse : collaborez avec les parties prenantes, vos conseillers juridiques et les responsables de votre organisation pour déterminer l'objectif de la réponse à un incident. Parmi les objectifs courants figurent la limitation et l'atténuation du problème, la récupération des ressources affectées, la conservation des données pour l'analyse et l'attribution.
- Répondre à l'aide du cloud : implémentez vos modèles de réponse où se trouvent l'événement et les données.
- Savoir ce dont vous disposez et ce dont vous avez besoin : conservez les journaux, les instantanés et les autres preuves en les copiant vers un compte cloud de sécurité centralisé. Utilisez des balises, des métadonnées et des mécanismes qui appliquent des stratégies de conservation. Par exemple, vous pouvez choisir d'utiliser la commande Linux dd ou un équivalent Windows pour copier la totalité des données à des fins d'investigation.
- Utiliser des mécanismes de redéploiement : si une anomalie de sécurité peut être attribuée à une mauvaise configuration, la correction peut se limiter à supprimer l'anomalie en redéployant les ressources avec la configuration appropriée. Dans la mesure du possible, faites en sorte que vos mécanismes de réponse puissent être exécutés en toute sécurité plusieurs fois et sur des états inconnus.
- Automatiser autant que possible : lorsque des problèmes ou des incidents se répètent, mettez en place des mécanismes qui permettent de trier par programme et de répondre aux situations courantes. Les incidents uniques, nouveaux et sensibles doivent être traités par des humains.
- Choisir des solutions évolutives : essayez d'adapter l'approche de votre organisation en matière de cloud computing et de réduire le délai entre la détection et la réponse.
- Apprendre et améliorer votre processus : lorsque vous identifiez des lacunes dans votre processus, vos outils ou votre personnel, comblez-les. Les simulations sont des méthodes sûres pour identifier les lacunes et améliorer les processus.

Les objectifs de conception NIST vous rappellent que vous devez passer en revue l'architecture afin de déterminer la capacité à procéder à la fois à la réponse aux incidents et à la détection des menaces. Lorsque vous planifiez votre implémentation du cloud, pensez à répondre à un incident ou à un événement d'analyse. Dans certains cas, cela signifie que plusieurs organisations, comptes et outils peuvent être spécifiquement configurés pour ces tâches de réponse. Ces outils et fonctions devraient être mis à la disposition du gestionnaire d'incident par pipeline de déploiement et ne doivent pas être statiques, car cela entraînerait un risque plus important.

Incidents de sécurité cloud

Rubriques

Domaines d'incidents

Les incidents de cybersécurité peuvent survenir dans trois domaines relevant de la responsabilité du client : le service, l'infrastructure et l'application. La différence entre les domaines est liée aux outils que vous utilisez lorsque vous apportez une réponse. Prenez en compte les domaines suivants :

- Domaine de service – Les incidents dans le domaine de service affectent le compte AWS d'un client, les autorisations IAM, les métadonnées des ressources, la facturation et d'autres domaines. Un événement dans le domaine de service est un événement auquel vous répondez exclusivement à l'aide des mécanismes d'API AWS, ou dont les causes d'origine sont associées à votre configuration ou aux autorisations de vos ressources, et qui peut être associé à une journalisation orientée service.
- Domaine de l'infrastructure – Les incidents dans le domaine de l'infrastructure comprennent les données ou l'activité liée au réseau, comme le trafic vers vos instances Amazon EC2 dans le VPC, les processus et les données sur vos instances Amazon EC2, et d'autres domaines, comme les conteneurs et d'autres services à venir. La réponse que vous apportez aux événements du domaine de l'infrastructure implique généralement la récupération, la restauration ou l'acquisition de données liées à l'incident à des fins d'analyse. Il est probable qu'elle comprenne une interaction avec le système d'exploitation d'une instance et, dans certains cas, elle peut également faire appel aux mécanismes d'API AWS.
- Domaine de l'application – Les incidents dans le domaine de l'application se produisent dans le code de l'application ou dans le logiciel déployé dans les services ou l'infrastructure. Ce domaine

doit être inclus dans vos runbooks de détection et de réponse aux menaces liées au cloud, et peut intégrer des réponses similaires à celles du domaine de l'infrastructure. Avec une architecture d'application appropriée et bien pensée, vous pouvez gérer ce domaine à l'aide d'outils de cloud, en utilisant des outils automatisés d'analyse, de récupération et de déploiement.

Dans ces domaines, vous devez prendre en compte les acteurs susceptibles d'agir contre votre compte, vos ressources ou vos données. Utilisez un cadre de gestion des risques interne ou externe pour déterminer quels sont les risques spécifiques pour votre organisation et vous préparer en conséquence.

Dans le domaine de service, vous vous efforcez d'atteindre vos objectifs exclusivement avec les API AWS. Par exemple, le traitement d'un incident de divulgation de données à partir d'un compartiment Amazon S3 implique des appels d'API pour récupérer la politique du compartiment, en analysant les journaux d'accès S3 et éventuellement en examinant les journaux AWS CloudTrail. Dans cet exemple, il est peu probable que votre enquête fasse appel à des outils d'analyse des données ou à des outils d'analyse du trafic réseau.

Dans le domaine de l'infrastructure, vous pouvez utiliser une combinaison d'API AWS et de logiciels courants d'analyse/de réponse aux incidents (DFIR) au sein du système d'exploitation d'un poste de travail, tel qu'une instance Amazon EC2 que vous avez préparée pour le travail de réponse aux incidents. Les incidents dans le domaine de l'infrastructure peuvent impliquer l'analyse de captures de paquets réseau, de blocs de disque sur un volume Amazon Elastic Block Store (Amazon EBS) ou de la mémoire volatile d'une instance.

Indicateurs des événements de sécurité liés au cloud

Il existe de nombreux événements de sécurité que vous ne pouvez pas classer comme incidents, mais il peut s'avérer prudent de les étudier. Pour détecter les événements liés à la sécurité dans votre environnement cloud AWS, vous pouvez utiliser ces mécanismes. Cette liste n'est pas exhaustive, mais nous vous invitons à prendre en compte les exemples suivants de certains indicateurs potentiels :

- Journaux et moniteurs : consultez les journaux AWS (tels qu'Amazon CloudTrail, les journaux d'accès Amazon S3 et les journaux de flux VPC) et les services de surveillance de la sécurité (tels qu'Amazon GuardDuty, Amazon Detective AWS Security Hub et Amazon Macie). En outre, utilisez des moniteurs tels que les surveillances de l'état Amazon Route 53 et les alarmes Amazon CloudWatch. De même, utilisez les événements Windows, les journaux Syslog Linux et

d'autres journaux spécifiques aux applications que vous pouvez générer dans vos applications, et connectez-vous à Amazon CloudWatch à l'aide d'agents CloudWatch.

- Activité de facturation : un changement soudain dans l'activité de facturation peut indiquer un événement de sécurité.
- Détection des menaces : si vous vous abonnez à un flux de détection des menaces tiers, vous pouvez mettre en corrélation ces informations avec d'autres outils de journalisation et de surveillance afin d'identifier les indicateurs d'événements potentiels.
- Outils partenaires : les partenaires du réseau de partenaires AWS (APN) proposent des centaines de produits leaders du secteur qui peuvent vous aider à atteindre vos objectifs de sécurité. Pour de plus amples informations, veuillez consulter Solutions des partenaires de sécurité et Solutions de sécurité dans AWS Marketplace.
- AWS Outreach : AWS Support peut vous contacter si nous identifions une activité abusive ou malveillante. Pour de plus amples informations, veuillez consulter la section Réponse d'AWS aux abus et aux compromissions.
- Contact ponctuel : étant donné que ce sont vos clients, vos développeurs ou d'autres membres du personnel de votre organisation qui remarquent quelque chose d'inhabituel, il est important de disposer d'une méthode connue et ayant fait l'objet d'une bonne communication pour contacter votre équipe de sécurité. Les systèmes de tickets, les adresses e-mail de contact et les formulaires web figurent parmi les choix les plus courants. Si votre organisation travaille auprès du grand public, vous pouvez également avoir besoin d'un mécanisme de contact de sécurité destiné au public.

L'un des outils proposés par AWS pour l'automatisation et la détection est AWS Security Hub. Security Hub vous offre une vue complète de vos alertes de sécurité hautement prioritaires et de l'état de conformité de vos comptes AWS en un seul endroit, ce qui permet une meilleure visibilité de ces indicateurs. AWS Security Hub n'est pas un logiciel de gestion des informations et des événements de sécurité (SIEM) et ne stocke pas de données de journal, mais agrège, organise et hiérarchise vos alertes de sécurité, ou vos résultats, provenant de plusieurs services AWS. Security Hub vous permet également de créer des informations personnalisées pouvant provenir de plusieurs sources. Cela donne à l'équipe des opérations de sécurité des options et des informations supplémentaires lorsqu'un événement se produit. Security Hub contrôle en permanence votre environnement à l'aide de contrôles de conformité automatisés basés sur les bonnes pratiques d'AWS et les normes sectorielles suivies par votre organisation.

Vous pouvez également prendre des mesures concernant ces résultats liés à la sécurité et à la conformité en les analysant dans Amazon Detective ou Amazon Athena, ou en utilisant

des règles Amazon CloudWatch Events ou du bus d'événement pour envoyer les résultats au système de tickets, à la messagerie instantanée, aux outils SIEM, à la plateforme d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR), aux outils de gestion des incidents ou à des manuels de remédiation personnalisés. L'automatisation basée sur les événements vous permet de répondre automatiquement aux incidents ou aux événements qui se produisent. Cette approche modifie la sécurité et la façon dont vous gérez les événements dans le cloud par rapport aux environnements sur site.

Comprendre les fonctionnalités du cloud

AWS propose un large éventail de fonctionnalités de sécurité que vous pouvez utiliser pour enquêter sur les événements de sécurité dans les domaines. Par exemple, AWS fournit des mécanismes de journalisation, tels que les journaux AWS CloudTrail, les journaux Amazon CloudWatch Logs, les journaux d'accès Amazon S3, etc. Vous devez prendre en compte les services que vous utilisez et vous assurer que vous avez activé les journaux correspondants. AWS propose également une solution de journalisation centralisée, qui peut vous aider à comprendre comment centraliser et stocker les types les plus courants de journaux cloud. Après avoir activé ces sources de journalisation, vous devez décider de la manière dont vous souhaitez les analyser, par exemple en utilisant Amazon Athena pour interroger les journaux conservés dans vos compartiments Amazon S3.

En outre, un certain nombre de produits partenaires APN peuvent simplifier votre processus lors de l'analyse de ces journaux, comme ceux décrits dans le programme de compétences en sécurité APN. Il existe également plusieurs services AWS qui peuvent vous aider à obtenir des informations précieuses sur ces données, comme Amazon GuardDuty (service de détection des menaces) et AWS Security Hub, qui peuvent vous offrir une vue complète de vos alertes de sécurité hautement prioritaires et de votre état de conformité sur l'ensemble des comptes AWS. En outre, Amazon Detective collecte des données de journal à partir de vos ressources AWS et utilise le machine learning, l'analyse statistique et la théorie des graphes pour vous aider à identifier la cause première des problèmes de sécurité potentiels ou des activités suspectes. Pour de plus amples informations sur les autres capacités du cloud que vous pouvez exploiter au cours de vos enquêtes, veuillez consulter l'Annexe A : Définitions des capacités du cloud.

Rubriques

- Confidentialité des données
- Réponse d'AWS aux abus et aux compromissions

Confidentialité des données

Nous savons que les clients se soucient profondément de la confidentialité et de la sécurité des données, c'est pourquoi nous mettons en œuvre un système élaboré responsable de contrôles techniques et physiques conçu pour empêcher l'accès non autorisé au contenu des clients, ou sa divulgation. Préserver la confiance client est un engagement permanent. Pour de plus amples informations sur les engagements concernant la confidentialité des données AWS, veuillez consulter notre page Questions fréquentes (FAQ) sur la confidentialité des données.

Ces contrôles intentionnels et auto-imposés limitent la capacité d'AWS à aider à répondre au sein de l'environnement d'un client. Pour cette raison, il est essentiel de se concentrer sur la compréhension et le renforcement des capacités au sein du modèle de responsabilité partagée pour réussir dans le cloud AWS. Bien qu'il soit important d'activer les capacités de journalisation et de surveillance dans vos comptes AWS avant qu'un incident ne se produise, la réponse aux incidents comporte d'autres aspects essentiels à la réussite d'un programme.

Confidentialité des données des consommateurs en Californie

La loi sur la confidentialité des données des consommateurs en Californie (CCPA, California Consumer Privacy Act) de 2018 accorde « au consommateur divers droits en ce qui concerne les informations personnelles relatives au consommateur qui sont détenues par une entreprise » soumis à la loi CCPA. Pour de plus amples informations et pour obtenir des conseils sur les politiques de confidentialité et de sécurité des données d'AWS relatives aux clients soumis à la CCPA, veuillez consulter le livre blanc Préparation à la loi sur la confidentialité des consommateurs en Californie.

Règlement général sur la protection des données

Le Règlement général sur la protection des données (RGPD) est une réglementation européenne relative à la protection de la vie privée (Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016) qui est entrée en vigueur le 25 mai 2018. Le RGPD remplace la Directive de l'UE sur la protection des données personnelles, aussi appelée Directive 95/46/CE, et vise l'harmonisation des législations relatives à la protection des données dans l'ensemble de l'Union européenne (UE) en proposant une loi unique relative à la protection des données personnelles, obligatoire et directement applicable dans tout État membre. Pour de plus amples informations sur la conformité d'AWS par rapport au RGPD, veuillez consulter le livre blancConsultation des conseils relatifs au RGPD sur AWS.

Réponse d'AWS aux abus et aux compromissions

Les activités abusives sont le fait d'instances de clients AWS ou d'autres ressources dont le comportement observé est de nature malveillante, inconvenante, illégale ou susceptible de porter atteinte à d'autres sites Internet. AWS œuvre à vos côtés pour détecter les activités suspectes et malveillantes de vos ressources AWS et y remédier. Des comportements inattendus ou suspects de la part de vos ressources peuvent suggérer que vos ressources AWS ont été mises en péril, ce qui représente un risque potentiel pour vos activités. Nous vous rappelons que vous disposez d'autres méthodes de contact dans votre compte AWS. Veillez à appliquer les bonnes pratiques lors de l'ajout de contacts, tant pour la sécurité que pour la facturation. Bien que l'e-mail de votre compte racine soit la principale cible des communications d'AWS, AWS communique également les problèmes de sécurité et les problèmes de facturation aux adresses e-mail secondaires. Si vous ajoutez une adresse e-mail qui n'est attribuée qu'à une seule personne, cela signifie que vous avez ajouté un point unique de défaillance à votre compte AWS. Assurez-vous d'ajouter au moins une liste de distribution à vos contacts.

AWS détecte les activités abusives dans vos ressources à l'aide de mécanismes tels que :

- La surveillance des événements internes AWS
- L'analyse de l'espace réseau AWS à la lumière de renseignements de sécurité externes
- L'analyse des ressources AWS à la lumière de plaintes d'abus Internet

Même si l'équipe de réponse aux abus AWS assure une surveillance agressive et stoppe les activités non autorisées sur AWS, la majorité des plaintes d'abus concernent des clients qui ont une activité légitime sur AWS. Voici quelques exemples de causes fréquentes d'activités abusives involontaires :

- Ressource compromise : par exemple, une instance Amazon EC2 non corrigée risque d'être infectée et devenir un agent botnet.
- Abus involontaire : par exemple, un robot d'indexation trop agressif peut être pris pour un pirate DOS par certains sites Internet.
- Abus secondaire : par exemple, un utilisateur final du service fourni par un client AWS peut publier des fichiers de programme malveillant sur un compartiment Amazon S3 public.
- Fausses plaintes : il arrive que des internautes signalent par erreur des activités légitimes comme des abus.

AWS s'engage à œuvrer avec les clients AWS pour empêcher, détecter et limiter les effets des abus et se prémunir contre les récidives futures. Nous vous encourageons à consulter la Politique d'utilisation acceptable d'AWS, qui décrit les utilisations interdites des services web proposés par Amazon Web Services et ses filiales. Pour favoriser une réponse rapide aux notifications d'abus d'AWS, assurez-vous que les informations de contact de votre compte AWS sont correctes. Lorsque vous recevez un avis d'abus AWS, votre personnel en charge de la sécurité et de l'exploitation doit immédiatement mener une enquête. Un retard peut prolonger l'impact sur votre réputation, ainsi que les implications juridiques pour vous-même et pour d'autres. Plus important encore, la ressource abusive en question peut avoir été mise en péril par des utilisateurs malveillants : ignorer cette mise en péril peut aggraver les dégâts à vos activités.

Préparation – Personnes

Les processus automatisés permettent aux organisations de consacrer plus de temps aux mesures visant à accroître la sécurité de leur environnement cloud et de leurs applications. La réponse automatisée aux incidents rend également les personnes disponibles pour corréler les événements, pratiquer des simulations, concevoir de nouvelles procédures de réponse, effectuer des recherches, développer de nouvelles compétences et tester ou créer de nouveaux outils. Malgré l'automatisation croissante, les spécialistes de l'analyse et les intervenants au sein d'une organisation de sécurité sont toujours très occupés. Les équipes homogènes peuvent créer des angles morts. Il est donc essentiel de constituer une équipe hétérogène qui offre différents systèmes de pensée, différentes perspectives culturelles et différentes expériences de travail et de vie dans des situations complexes et fluides. Lors de la planification d'événements, nous devons impérativement nous assurer que nos équipes et nos plans d'intervention sont basés sur la diversité. Une équipe offrant différents points de vue peut potentiellement identifier les angles morts qui n'auraient peut-être pas été détectés par une équipe homogène, et identifier des solutions qui n'auraient peut-être pas été envisagées autrement.

Rubriques

Définition des rôles et des responsabilités

Les compétences et les mécanismes de réponse aux incidents sont essentiels lors de la gestion de nouveaux événements ou d'événements de grande envergure. Ces événements reposent sur les normes écrites que votre équipe a développées et sur l'expérience de votre équipe. Étant donné que nous ne pouvons pas prévoir ni codifier toutes les directions potentielles que prendre un événement, nous nous appuyons sur l'automatisation pour les tâches simples et répétitives, telles que la collecte de la mémoire des instances ou des journaux de diagnostic, et laissons les intervenants humains prendre les décisions difficiles. La gestion des événements de sécurité peu clairs nécessite une discipline inter-organisationnelle, une propension aux actions décisives et la capacité à produire des résultats. Au sein de votre structure organisationnelle, de nombreuses personnes doivent être responsables, consultées ou informées lors d'un incident, telles que des représentants des ressources humaines (RH), de votre équipe de direction et du service juridique. Examinez ces rôles

et responsabilités et déterminez si des tiers doivent être impliqués. Notez que dans de nombreuses régions géographiques, des lois locales régissent ce qu'il est possible ou non de faire. Malgré l'aspect bureaucratique de la création d'un tableau des personnes responsables, consultées et informées pour un incident, cette opération permet de communiquer rapidement et directement, et décrit clairement le leadership dans les différentes étapes de l'événement.

Des partenaires de confiance peuvent participer à l'enquête ou à la réponse, et ils fournissent une expertise supplémentaire et un examen minutieux. Lorsque votre équipe ne possède pas ces compétences, vous pouvez obtenir l'aide d'un tiers externe. Si vous avez recours à un tiers externe, assurez-vous que ce tiers forme les membres de votre équipe. Lorsque ces tiers externes collaborent avec vos développeurs et opérateurs internes, ils contribuent à développeur les compétences des membres de votre équipe et cette nouvelle expertise peut être précieuse pour votre programme de réponse aux incidents à l'avenir.

Lors d'un incident, il est essentiel d'inclure les propriétaires et les développeurs des applications et des ressources touchées, car ce sont des experts qui peuvent fournir des informations et un contexte. Assurez-vous de collaborer avec les développeurs et les propriétaires des applications et d'établir avec eux des relations avant de vous fier à leur expertise en matière de réponse aux incidents. Les propriétaires d'applications ou les experts peuvent devoir intervenir dans des situations où l'environnement n'est pas familier, où l'environnement présente une complexité imprévue ou dans lesquelles les intervenants n'ont pas accès à l'environnement. Les experts des applications doivent s'entraîner et acquérir l'aisance nécessaire pour travailler avec l'équipe de réponse aux incidents.

Formation

Pour réduire la dépendance et le temps de réponse, veillez à ce que vos équipes de sécurité et les intervenants soient formés aux services cloud que vous utilisez et aient la possibilité d'effectuer des exercices pratiques avec les plateformes cloud utilisées par votre organisation. Cette formation tire parti de la cohésion de l'équipe et de la création de runbooks, qui ont lieu au début du processus. Vos équipes internes accèdent à une meilleure compréhension si vous incluez le plus de personnes possible dans la phase initiale de formation des runbooks. Cette formation devient plus réelle au fur et à mesure que ces équipes commencent à mettre en pratique ces runbooks dans des exercices de simulation.

AWS et d'autres tiers proposent également des ateliers de sécurité en ligne (ateliers de sécurité AWS) que vous pouvez télécharger et suivre. Votre organisation peut en tirer des avantages en fournissant au personnel des formations supplémentaires pour apprendre à programmer, apprendre

les processus de développement (y compris les systèmes de contrôle de version et les pratiques de déploiement) et l'automatisation de l'infrastructure.

AWS propose un certain nombre d'options de formation et de parcours d'apprentissage par le biais de formations numériques, de formations en classe, de partenaires APN et de certifications. Pour de plus amples informations, veuillez consulter AWS Training & Certification.

Définition des mécanismes de réponse

Votre mécanisme de réponse dépend de votre modèle de gouvernance, de risque et de conformité (GRC). Idéalement, votre modèle GRC est conçu avant de planifier la réponse aux incidents. Si ce n'est pas déjà fait, concevez un modèle GRC. Il s'agit d'une première étape nécessaire à la mise en place d'un mécanisme de réponse aux incidents performant. Lorsque vous réfléchissez à votre approche de réponse aux incidents dans le cloud, en accord avec d'autres équipes (votre service juridique, vos dirigeants, les parties prenantes de l'entreprise, etc.), vous devez identifier ce que vous avez et ce dont vous avez besoin. Identifiez les parties prenantes et les contacts pertinents, et assurez-vous de disposer d'un accès approprié pour fournir la réponse nécessaire.

Bien que le cloud puisse vous fournir une visibilité et des capacités accrues grâce aux API de service, votre modèle GRC vous montre comment les utiliser dans votre réponse. Identifiez les numéros de compte AWS de votre équipe, les plages d'adresses IP de vos VPC, les diagrammes réseau, les journaux, les emplacements de données et les classifications de données correspondants. Bon nombre de ces processus technologiques sont abordés dans la section Préparation – Technologie. Commencez ensuite à documenter vos procédures de réponse aux incidents, souvent appelées « procédures » ou « runbooks », qui définissent les étapes à suivre pour enquêter sur un incident et le corriger.

Création d'une culture de sécurité réceptive et adaptative

Chez AWS, nous avons appris que nos clients et nos propres équipes internes réussissent mieux lorsque les équipes de sécurité favorisent la coopération pour leur entreprise et les développeurs, favorisent une culture qui garantit que toutes les parties prenantes coopèrent et s'efforcent de maintenir une posture de sécurité agile et hautement réactive. Bien que l'amélioration de la culture de sécurité de votre organisation ne soit pas le sujet de ce document, sachez que vous pouvez obtenir des renseignements pertinents auprès de collaborateurs qui ne sont pas responsables de la sécurité, à condition que l'équipe de sécurité soit réceptive. Lorsque votre équipe de sécurité est ouverte et accessible, et qu'elle bénéficie du soutien de la direction, elle est plus susceptible de recevoir des

notifications, des actes de coopération et des réponses supplémentaires en temps opportun aux événements de sécurité.

Dans certaines organisations, les collaborateurs peuvent craindre les conséquences en cas de signalement d'un problème de sécurité. Parfois, les collaborateurs ne savent tout simplement pas comment signaler un problème. Dans d'autres cas, ils peuvent ne pas vouloir perdre de temps, ou avoir peur de signaler un incident de sécurité qui n'en serait finalement pas un. De l'ensemble de l'organisation, à partir de l'équipe dirigeante, il est important de promouvoir une culture d'acceptation et d'inviter tout le monde à participer à la sécurité de l'organisation. Indiquez un canal clair qui permettra à chacun d'ouvrir un ticket de niveau de gravité élevé chaque fois qu'il peut y avoir une menace ou un risque potentiel. Accueillez ces notifications avec un esprit enthousiaste et ouvert, mais surtout, faites savoir clairement au personnel qui n'est pas responsable de la sécurité que vous accueillez favorablement ces notifications. Insistez sur le fait que vous préférez recevoir trop de notifications de problèmes potentiels plutôt que de ne recevoir aucune notification. Il est de loin préférable qu'un développeur informe d'une erreur qu'il a commise, plutôt qu'un chercheur la signale dans une publication.

Ces notifications offrent de précieuses opportunités de mener des enquêtes réactives dans des situations de stress. Elles peuvent constituer des boucles de rétroaction importantes lorsque vous développez vos procédures de réponse.

Prédiction des réponses

Comme il est impossible de prévoir tous les événements potentiels, vous devez continuer à vous fier à l'analyse humaine. Prenez le temps de former soigneusement votre personnel et de préparer votre organisation. Cela vous aide à anticiper les imprévus. Votre organisation n'est toutefois pas obligée de se préparer seule. Pour bénéficier d'une visibilité et d'informations supplémentaires, les organisations peuvent collaborer avec des partenaires de sécurité de confiance qui leur permettront d'identifier les événements de sécurité imprévus.

Partenaires et fenêtre de réponse

La transition vers le cloud est unique pour chaque organisation. Il existe cependant des modèles et des pratiques auxquels d'autres organisations ont déjà été confrontées et sur lesquels un partenaire de sécurité de confiance peut attirer votre attention. Nous vous encourageons à identifier des partenaires APN de sécurité AWS externes qui peuvent vous apporter une expertise extérieure et une perspective différente pour accroître vos capacités d'intervention. Vos partenaires de sécurité

de confiance peuvent vous aider à identifier des risques ou des menaces potentiels que vous ne connaissez peut-être pas.

En 1955, Joseph Luft et Harrington Ingham ont créé la fenêtre Johari, un exercice permettant de faire correspondre des caractéristiques à des catégories. La fenêtre est représentée sous la forme d'une grille composée de quatre quadrants, comme dans le schéma suivant.

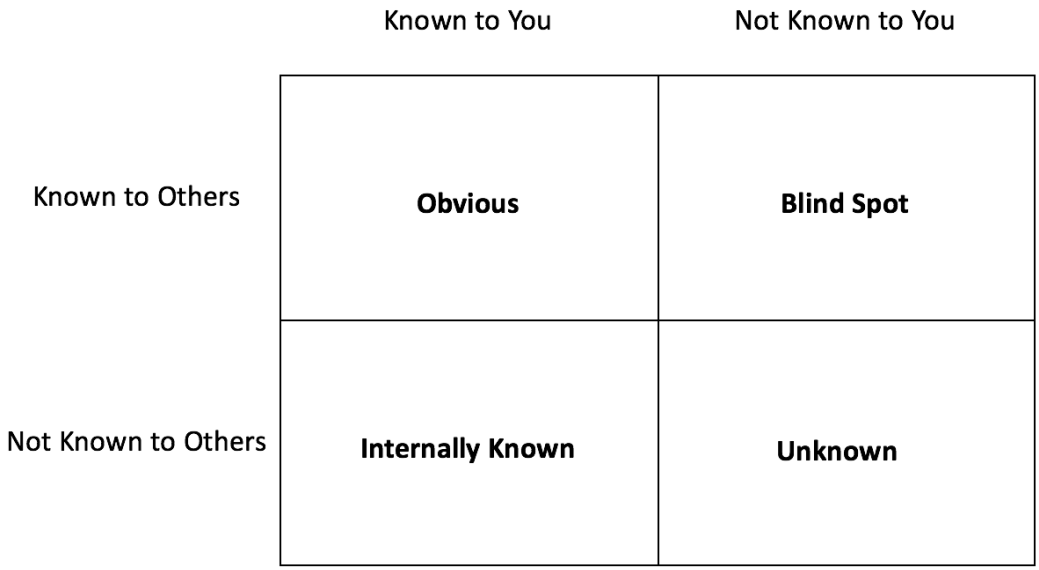

Figure 3 : Fenêtre Johari adaptée à la réponse aux incidents

Bien que la fenêtre Johari n'ait pas été conçue pour la sécurité des informations, nous pouvons ajuster le concept pour l'utiliser comme un simple modèle mental permettant de prendre en compte la difficulté d'évaluer les menaces qui pèsent sur une organisation. Dans notre concept modifié, les quatre quadrants sont les suivants :

- Évident : risque dont votre équipe et votre partenaire APN sont conscients.
- Connu en interne : risque que votre équipe connaît bien, mais que votre partenaire APN ne connaît pas. Cela peut signifier que vous avez une expertise interne ou des connaissances propres à votre organisation.
- Angle mort : risque que votre partenaire APN connaît bien, mais que votre équipe ne connaît pas.
- Inconnu : risque que ni vous ni votre partenaire APN ne connaissez.

Bien que ce diagramme soit simple, il représente la valeur que représente le fait d'avoir des partenaires APN de confiance. Vous devez être conscient des angles morts éventuels, dont vous

n'êtes pas au courant, mais sur lesquels un partenaire APN possédant l'expertise appropriée peut attirer votre attention. Bien que votre organisation et le partenaire APN connaissent les risques du quadrant Évident, il est possible que votre partenaire APN vous recommande des contrôles et des solutions que vous ne connaissez pas. En outre, bien que vous puissiez attirer l'attention de votre partenaire APN sur les risques du quadrant Connu en interne, votre partenaire peut également être en mesure d'identifier des contrôles optimisés pour atténuer ces risques. Lorsque vous évaluez votre niveau d'amélioration, contactez votre partenaire APN pour obtenir des conseils d'experts.

Risque inconnu

Si vous vous êtes concentré sur la personnalisation des alertes, l'amélioration de vos procédures de réponse aux incidents grâce à l'automatisation et l'amélioration de vos défenses de sécurité, vous vous demandez peut-être ce que vous devez faire ensuite. Vous êtes peut-être curieux de connaître les risques inconnus, représentés dans la catégorie Inconnu de la Figure 3. Les méthodes suivantes peuvent vous aider à réduire les risques inconnus :

- Définir les affirmations de sécurité : quelles sont les vérités que vous pouvez affirmer ? Quelles sont les primitives de sécurité qui devraient absolument être vraies dans votre environnement ? En les définissant clairement, vous pouvez rechercher l'inverse. Cela est plus facile à faire dès le début de votre transition vers le cloud, plutôt que d'essayer de faire machine arrière sur vos affirmations de sécurité ultérieurement.
- Formation, communication et recherche : intégrez des experts en sécurité dans le cloud à votre personnel ou faites appel à des partenaires experts pour vous aider à examiner minutieusement votre environnement. Remettez en question vos hypothèses et méfiez-vous des raisonnements subtils. Créez des boucles de rétroaction dans vos processus et proposez des mécanismes permettant à vos équipes d'ingénierie de communiquer avec les équipes de sécurité. Vous pouvez également développer votre approche pour surveiller les listes de diffusion de sécurité pertinentes et les divulgations de sécurité des informations.
- Réduction de la surface d'attaque : améliorez votre défense pour éviter les risques et vous donner plus de temps pour contrer les attaques inconnues. Bloquez et ralentissez les personnes malveillantes, et amenez-les à la faute.
- Détection des menaces : abonnez-vous à un flux continu de menaces, de risques et d'indicateurs actuels et pertinents du monde entier.
- Alertes : générez des notifications qui vous alertent en cas d'activités inhabituelles, malveillantes ou coûteuses. Par exemple, vous pouvez créer une notification pour vous alerter en cas d'activités qui se produisent dans des régions ou des services que vous n'utilisez pas.

- Machine learning : utilisez le machine learning pour identifier des anomalies complexes pour une organisation ou des personas spécifiques. Pour vous aider à identifier les comportements inhabituels, vous pouvez également profiler les caractéristiques normales de vos réseaux, utilisateurs et systèmes.

Les renseignements sur les menaces deviennent le principal sujet lorsque vous examinez les angles morts et les inconnues non connues. La fenêtre Johari montre comment classer ce que vous savez et ce que vous ne savez pas, mais la détection des menaces montre comment tenir compte de ce que vous ne savez pas encore. La détection des menaces est une discipline qui aide les entreprises à voir au-delà du modèle de menace, pour identifier des menaces dont votre entreprise ne connaît peut-être pas encore l'existence.

En général, la détection des menaces implique les actions suivantes :

1. Recherche de nouvelles menaces
2. Définition de nouveaux modèles
3. Définition de nouvelles techniques d'acquisitions automatisées
4. Répétition de ces processus

Bien que ce type de pratique puisse être utile, le fonctionnement et la maintenance d'une équipe de détection des menaces peuvent surcharger de nombreuses entreprises, même de grandes entreprises. En fin de compte, la question est de réussir à faire correspondre votre modèle de menace, votre taille et l'adversité des risques. Prenez en compte ces questions :

- Votre modèle de menace est-il suffisamment différent du secteur standard dans lequel se trouve l'entreprise ?
- Votre goût du risque est-il suffisamment faible pour qu'une telle équipe soit nécessaire ?
- Est-il judicieux sur le plan financier de mettre en place une équipe pour votre entreprise ?
- Votre profil de risque est-il suffisamment intéressant pour rallier les talents adaptés à votre cause ?

Si vous répondez Non à l'une de ces questions, vous devriez probablement rechercher un partenaire de détection des menaces. De nombreuses grandes entreprises renommées proposent ce service.

AWS vous fournit les outils et les services qui permettent de gérer vous-même ces problèmes. L'utilisation du machine learning pour identifier les modèles malveillants est un domaine d'étude bien documenté, avec des modèles implémentés par les clients, AWS Professional Services, les

partenaires APN et par le biais de services AWS tels qu'Amazon GuardDuty et Amazon Macie. Certains de ces modèles ont été abordés lors des sessions de conférence AWS re:Invent. Pour de plus amples informations, veuillez consulte la section Médias de ce livre blanc.

Les clients étendent également leurs lacs de données traditionnellement centrés sur l'entreprise afin de tirer parti de modèles d'architecture similaires lorsqu'ils développent des lacs de données de sécurité. Les équipes chargées des opérations de sécurité étendent également leur utilisation des outils de journalisation et de surveillance traditionnels, tels que Amazon OpenSearch Service et les tableaux de bord OpenSearch, aux architectures big data.

Ces clients collectent des données internes à partir de journaux d'événements AWS CloudTrail, de journaux de flux VPC, de journaux d'accès Amazon CloudFront, de journaux de base de données et de journaux d'applications, puis combinent ces données avec des données publiques et la détection des menaces. Grâce à ces précieuses données, les clients ont développé leurs compétences en science des données et en ingénierie des données au sein de leurs équipes chargées des opérations de sécurité afin de tirer parti d'outils tels qu'Amazon EMR, Amazon Kinesis Data Analytics, Amazon Redshift, Amazon QuickSight, AWS Glue, Amazon SageMaker et Apache MXNet sur AWS. Cela leur permet de créer des solutions qui identifient et prédisent les anomalies propres à leur activité.

Pour terminer, nous vous invitons à consulter Solutions des partenaires de sécurité afin d'accéder aux centaines de produits de pointe proposés par des partenaires APN, qui sont équivalents, identiques ou intégrés à des contrôles existants dans vos environnements sur site. Ces produits complètent les services AWS existants pour vous permettre de déployer une architecture de sécurité exhaustive et une expérience plus homogène dans vos environnements cloud et sur site.

Préparation – Technologie

Rubriques

Préparation de l'accès aux comptes AWS

Lors d'un incident, vos équipes de réponse aux incidents doivent avoir accès aux environnements et aux ressources impliqués dans l'incident. Assurez-vous que vos équipes disposent d'un accès approprié pour accomplir leurs tâches avant qu'un événement ne se produise. Pour cela, vous devez connaître le niveau d'accès dont les membres de votre équipe ont besoin (par exemple, quels types d'actions ils sont susceptibles d'entreprendre) et vous devez leur fournir un accès à l'avance. Cet accès est dérivé des politiques de gouvernance, de gestion des risques et de conformité (GRC) de votre entreprise. L'authentification et l'autorisation des membres de votre équipe doivent être documentées et testées bien avant qu'un événement ne se produise afin de s'assurer que les membres peuvent répondre rapidement et sans retard. Pour répondre correctement à un incident, vous devez notamment vous préparer à examiner la façon dont les comptes AWS sont présentés et comment les rôles entre comptes sont autorisés et organisés.

À ce stade, vous devez travailler en étroite collaboration avec vos développeurs, architectes, partenaires, équipes de gouvernance et équipes de conformité pour comprendre quel niveau d'accès est nécessaire pour les intervenants. Identifiez et abordez la stratégie de compte AWS et la stratégie d'identité cloud avec les architectes cloud de votre organisation afin de comprendre quelles méthodes d'authentification et d'autorisation sont configurées, par exemple :

- Fédération : un utilisateur assume un rôle IAM dans un compte AWS auprès d'un fournisseur d'identité.
- Accès entre comptes : un utilisateur assume un rôle IAM entre plusieurs comptes AWS.
- Authentification : un utilisateur s'authentifie en tant qu'utilisateur AWS IAM créé au sein d'un seul compte AWS.

Ces options définissent les choix techniques pour l'authentification auprès d'AWS et la manière dont vous pouvez obtenir l'accès pendant une réponse. Cependant, certaines organisations peuvent

se reposer sur une autre équipe ou sur un partenaire pour vous aider à répondre. Les comptes utilisateurs créés spécifiquement pour répondre à un incident de sécurité sont souvent privilégiés afin de fournir un accès suffisant. Par conséquent, l'utilisation de ces comptes utilisateur doit être limitée ; ils ne doivent pas être utilisés pour les activités quotidiennes.

Avant de créer de nouveaux mécanismes d'accès, vous devez collaborer avec vos équipes cloud afin de comprendre comment vos comptes AWS sont organisés et régis. De nombreux clients utilisent AWS Organizations pour centraliser la gestion de la facturation, le partage des ressources dans l'ensemble de leurs comptes AWS et le contrôle des accès, la conformité et la sécurité. L'une des principales caractéristiques d'Organizations est la possibilité d'exploiter ce service pour appliquer des politiques de contrôle des services à des groupes de comptes, ce qui vous permet d'obtenir une gestion des politiques à grande échelle. Pour de plus amples informations sur l'implémentation de mécanismes de gouvernance à grande échelle, veuillez consulter Gouvernance AWS à grande échelle. Une fois que vous avez compris la manière dont votre organisation organise et régit vos comptes AWS, examinez les modèles de réponse généralisée suivants pour vous aider à identifier les approches adaptées à votre organisation.

Rubriques

Accès indirect

Si vous utilisez l'accès indirect, les propriétaires de votre compte ou vos équipes d'application sont tenus d'effectuer des corrections autorisées dans leurs comptes AWS en suivant les conseils tactiques de l'équipe de réponse aux incidents, votre expert en sécurité. Cette méthode est plus lente et plus complexe pour exécuter des tâches, mais elle peut s'avérer efficace lorsque les intervenants ne sont pas familiarisés avec le compte ou l'environnement cloud.

Accès direct

Pour accorder un accès direct aux gestionnaires d'incident, déployez un rôle IAM AWS sur les comptes AWS que vos ingénieurs en sécurité ou vos gestionnaires d'incident peuvent assumer lors d'un événement de sécurité. Le gestionnaire d'incident s'authentifie soit par le biais d'un processus

fédéré normal, soit par le biais d'un processus d'urgence spécial, si l'incident a un impact sur votre processus d'authentification normal. Les autorisations que vous accordez au rôle IAM de réponse aux incidents dépendent des actions qui doivent être effectuées par les gestionnaires d'incident.

Autre accès

Si vous pensez qu'un événement de sécurité a un impact sur votre sécurité, votre identité ou vos systèmes de communication, vous devrez peut-être rechercher d'autres mécanismes et accès pour enquêter et corriger cet impact. En utilisant un nouveau compte AWS spécialement conçu, les intervenants peuvent collaborer et travailler à partir d'une autre infrastructure sécurisée.

Par exemple, les intervenants peuvent tirer parti de la nouvelle infrastructure lancée dans le cloud, par exemple les postes de travail distants à l'aide d'Amazon WorkSpaces et les services de messagerie fournis par Amazon WorkMail. Vous devez préparer des contrôles d'accès appropriés (à l'aide de politiques IAM) pour déléguer l'accès afin que votre autre compte AWS sécurisé puisse assumer des autorisations pour le compte AWS concerné.

Après avoir délégué l'accès approprié, vous pouvez utiliser les API AWS du compte concerné pour partager des données pertinentes, comme des journaux et des instantanés de volumes, afin d'effectuer un travail d'enquête dans un environnement isolé. Pour de plus amples informations sur cet accès entre comptes, veuillez consulter Didacticiel IAM : déléguer l'accès entre des comptes AWS à l'aide des rôles IAM.

Accès à l'automatisation

Lorsque vous migrez vers l'automatisation pour répondre aux événements de sécurité, vous devez créer des rôles IAM qui seront spécifiquement utilisés par vos ressources d'automatisation (telles que les instances Amazon EC2 ou les fonctions AWS Lambda). Ces ressources peuvent ensuite assumer les rôles IAM et hériter des autorisations attribuées au rôle. Au lieu de créer et de distribuer des informations d'identification AWS, vous déléguez l'autorisation à votre fonction AWS Lambda ou à votre instance Amazon EC2. La ressource AWS reçoit automatiquement un ensemble d'informations d'identification temporaires qu'elle utilise pour signer des demandes d'API.

Vous pouvez également envisager une méthode sécurisée pour votre automatisation ou vos outils afin de vous authentifier et de l'exécuter au sein du système d'exploitation de votre instance Amazon EC2. Bien qu'il existe de nombreux outils capables d'effectuer cette automatisation, pensez à utiliser la fonctionnalité Exécuter la commande d'AWS Systems Manager, qui vous permet d'administrer des instances à distance et en toute sécurité en utilisant un agent que vous installez sur le système d'exploitation de votre instance Amazon EC2.

AWS Systems Manager Agent (SSM Agent) est installé par défaut sur certaines images Amazon Machine Image (AMI) Amazon EC2, par exemple pour Microsoft Windows Server et Amazon Linux. Toutefois, vous devrez peut-être installer manuellement l'agent sur d'autres versions de Linux et sur des instances hybrides. Que vous utilisiez la fonctionnalité Exécuter la commande ou un autre outil, effectuez toutes les opérations d'installation et de configuration préalables avant de recevoir la première alerte de sécurité sur laquelle vous devrez enquêter.

Accès aux services managés

Votre organisation est peut-être déjà associée à un fournisseur de technologies de l'information qui gère les services et les solutions en votre nom. Ces partenaires exercent une responsabilité partagée pour la prise en charge de la sécurité de votre organisation, et il est important de bien comprendre cette relation avant qu'une anomalie ne se produise. Que vous travailliez déjà avec un partenaire Fournisseur de service managé (MSP) AWS, AWS Managed Services ou un partenaire de services de sécurité gérés, vous devez identifier les responsabilités de chaque partenaire concernant vos environnements cloud, les accès à vos services cloud dont disposent les fournisseurs, les accès dont ils ont besoin, ainsi que les points de contact ou les voies de remontée d'informations lorsque vous avez besoin d'assistance. Enfin, vous devrez vous entraîner avec votre partenaire afin de vous assurer que vos plans d'intervention sont prévisibles et opérationnels.

Préparation des processus

Une fois que l'accès approprié a été attribué et testé, votre équipe de réponse aux incidents doit définir et préparer les processus connexes nécessaires à l'enquête et à la résolution des problèmes. Cette étape demande beaucoup d'efforts, car vous devez planifier correctement la réponse appropriée aux événements de sécurité au sein de vos environnements cloud.

Travaillez en étroite collaboration avec vos équipes internes dédiées aux services cloud et avec vos partenaires afin d'identifier les tâches nécessaires pour garantir que les processus sont possibles. Collaborez ou attribuez-vous mutuellement des tâches d'activité de réponse, et assurez-vous que les configurations de compte nécessaires sont effectives. Nous vous recommandons de préparer les processus et les configurations préalables à l'avance afin que votre organisation aient les capacités de réponse suivantes.

Rubriques

- Arbres de décision
- Utilisation d'autres comptes

- Affichage ou copie de données
- Partage d'instantanés Amazon EBS
- Partage de journaux Amazon CloudWatch Logs
- Utilisation d'un stockage immuable
- Lancement de ressources à proximité de l'événement
- Isolation des ressources
- Lancement de stations de travail d'analyse

Arbres de décision

En fonction des conditions, des actions ou des étapes différentes doivent parfois être appliquées. Vous pouvez par exemple prendre des mesures différentes en fonction du type de compte AWS (développement ou production), des balises des ressources, de l'état de conformité aux règles AWS Config de ces ressources ou d'autres informations.

Pour vous aider à créer et à documenter ces décisions, nous vous recommandons d'élaborer un arbre de décision avec vos autres équipes et avec les parties prenantes. Semblable à un organigramme, un arbre de décision est un outil qui peut être utilisé pour soutenir la prise de décision. Il vous aide à déterminer les actions et les résultats optimaux en fonction des conditions et des informations potentielles, y compris des probabilités.

Utilisation d'autres comptes

Même s'il peut être nécessaire de répondre à un événement dans le compte concerné, il est préférable d'examiner les données en dehors du compte concerné. Certains clients disposent d'un processus pour créer des environnements de comptes AWS distincts et isolés, à l'aide de modèles qui préconfigurent les ressources qu'ils doivent allouer. Ces modèles sont déployés par le biais d'un service, tel que AWS CloudFormation ou Terraform, qui fournit une méthode simple pour créer un ensemble de ressources AWS associées et les allouer de manière ordonnée et prévisible.

La préconfiguration de ces comptes à l'aide de mécanismes modélisés permet d'éliminer les interactions humaines au cours des premières étapes d'un incident et de garantir que l'environnement et les ressources sont préparés de manière reproductible et prévisible, ce qui peut être vérifié par un audit. En outre, ce mécanisme augmente également la capacité de maintenir la sécurité et le confinement des données dans l'environnement d'analyse.

Cette approche nécessite de travailler avec vos services cloud et vos équipes d'architectes pour déterminer un processus de compte AWS approprié qui peut être utilisé pour les enquêtes. Vos équipes de services cloud peuvent par exemple utiliser AWS Organizations pour générer de nouveaux comptes et vous aider à préconfigurer ces comptes à l'aide d'une méthode modélisée ou basée sur des scripts.

Cette méthode de segmentation est idéale lorsqu'une organisation de plus grande envergure doit être tenue à l'écart d'une menace potentielle. Cette segmentation, qui utilise un nouveau compte AWS en grande partie non connecté, signifie qu'un utilisateur de l'organisation, marquée dans la documentation multi-comptes comme l'unité d'organisation (UO) de sécurité, est en mesure d'accéder au compte, d'effectuer les activités d'analyse nécessaires et éventuellement de transférer le compte dans son ensemble. à une entité juridique, si nécessaire. Cette méthode d'analyse et d'attribution nécessite un examen et une planification importants, et doit respecter les politiques GRC de l'entreprise. Bien que ce travail ne soit pas facile, il est beaucoup plus facile à mener avant de constituer une base de comptes importante.

Affichage ou copie de données

Les intervenants doivent avoir accès à des journaux ou à d'autres preuves à analyser, et doivent s'assurer qu'ils sont en mesure de visualiser ou de copier des données. Au minimum, la politique d'autorisation IAM pour les intervenants doit fournir un accès en lecture seule afin qu'ils puissent mener leur enquête. Pour activer un accès approprié, vous pouvez envisager certaines politiques gérées AWS prédéfinies, telles que SecurityAudit ou ViewOnlyAccess.

Par exemple, les intervenants peuvent souhaiter effectuer une copie ponctuelle des données, par exemple les journaux AWS CloudTrail, à partir d'un compartiment Amazon S3 d'un compte vers un compartiment Amazon S3 d'un autre compte. Les autorisations fournies par la politique gérée ReadOnlyAccess, par exemple, permettent à l'intervenant d'effectuer ces actions. Pour comprendre comment utiliser l'interface de ligne de commande (CLI) AWS à cette fin, veuillez consulter Comment puis-je copier tous les objets d'un compartiment Amazon S3 vers un autre compartiment ?.

Partage d'instantanés Amazon EBS

De nombreux clients utilisent des instantanés Amazon Elastic Block Store (Amazon EBS) dans le cadre de leur enquête sur des événements de sécurité impliquant leurs instances Amazon EC2. Les instantanés des volumes Amazon EBS sont des sauvegardes incrémentielles. Pour de plus amples informations sur les instantanés incrémentiels Amazon EBS, veuillez consulter Instantanés Amazon EBS.

Pour mener une enquête sur un volume Amazon EBS dans un compte séparé et isolé, vous devez modifier les autorisations de l'instantané pour le partager avec les autres comptes AWS spécifiés. Les utilisateurs qui bénéficient de votre autorisation peuvent utiliser les instantanés que vous partagez comme base de création de leurs propres volumes EBS. Votre instantané d'origine n'est alors pas affecté. Pour de plus amples informations, veuillez consulter Partager un instantané Amazon EBS.

Si votre instantané est chiffré, vous devez également partager la clé gérée par le client (CMK) AWS Key Management Service (AWS KMS) personnalisée utilisée pour chiffrer l'instantané. Vous pouvez appliquer des autorisations entre comptes à une clé CMK personnalisée lors de sa création ou ultérieurement. Les instantanés sont limités à la région dans laquelle ils ont été créés, mais vous pouvez partager un instantané avec une autre région en le copiant dans cette région. Pour de plus amples informations, veuillez consulter Copier un instantané Amazon EBS.

Partage de journaux Amazon CloudWatch Logs

Les journaux enregistrés dans Amazon CloudWatch Logs, comme les journaux de flux Amazon VPC, peuvent être partagés avec un autre compte (par exemple votre compte de sécurité centralisé) via un abonnement CloudWatch Logs. Par exemple, les données d'événements de journaux peuvent être lues à partir d'un flux Amazon Kinesis centralisé pour effectuer un traitement et une analyse personnalisés. Le traitement personnalisé est particulièrement utile lorsque vous collectez des données de journalisation sur plusieurs comptes. L'idéal est de créer cette configuration au début de votre transition vers le cloud, avant qu'un événement lié à la sécurité ne se produise. Pour de plus amples informations, veuillez consulter Partage de données du journal entre comptes avec les abonnements.

Utilisation d'un stockage immuable

Lorsque vous copiez des journaux et d'autres preuves sur un autre compte, assurez-vous que les données répliquées sont protégées. En plus de protéger les preuves secondaires, vous devez également protéger l'intégrité des données à la source. Ces mécanismes, connus sous le nom de stockage immuable, protègent l'intégrité de vos données en empêchant la falsification ou la suppression des données.

Vous pouvez configurer un compartiment Amazon S3 pour protéger l'intégrité de vos données à l'aide des fonctionnalités natives d'Amazon S3. Par exemple, en utilisant le verrouillage des objets S3, vous pouvez empêcher qu'un objet soit supprimé ou remplacé sur une période déterminée ou indéfinie. La gestion des autorisations d'accès avec les politiques de compartiment S3, la configuration du contrôle de version S3 et l'activation de la fonction Supprimer MFA sont d'autres moyens de restreindre

la façon dont les données peuvent être écrites ou lues. Ce type de configuration est utile pour stocker les journaux d'enquête et les preuves, et est souvent appelé (WORM (Write Once, Read Many ; une écriture, plusieurs lecteurs). Vous pouvez également protéger les données en utilisant le chiffrement côté serveur avec AWS Key Management Service (AWS KMS) et en vérifiant que seuls les mandataires IAM appropriés sont autorisés à déchiffrer les données.

En outre, si vous souhaitez conserver les données en toute sécurité dans un stockage à long terme une fois l'enquête terminée, envisagez de déplacer les données d'Amazon S3 vers Amazon S3 Glacier à l'aide de politiques de cycle de vie des objets. Amazon S3 Glacier est un service de stockage dans le cloud sécurisé, durable à très faible coût qui permet l'archivage et la sauvegarde des données à long terme. Il est conçu pour offrir une durabilité de 99,999999999 % et fournit des fonctionnalités complètes de sécurité et de conformité.

En outre, vous pouvez protéger les données dans Amazon S3 Glacier en utilisant le verrouillage de coffre Amazon S3 Glacier, qui vous permet de déployer et d'appliquer facilement des contrôles de conformité pour des coffres Amazon S3 Glacier individuels avec une politique de verrouillage de coffre. Vous pouvez définir des contrôles de sécurité, tels que la technique WORM, dans une politique de verrouillage de coffre et empêcher que la politique fasse l'objet de modifications ultérieures. Une fois verrouillée, la politique ne peut pas être modifiée. Amazon S3 Glacier applique les contrôles définis dans la stratégie de verrouillage de coffre afin de vous aider à atteindre vos objectifs de conformité, par exemple la conservation des données. Vous pouvez déployer différents contrôles de la conformité dans une politique de verrouillage de coffre en utilisant le langage de politique AWS Identity and Access Management (IAM).

Lancement de ressources à proximité de l'événement

Les intervenants qui débutent dans le cloud peuvent être tentés d'essayer de mener sur site (où se trouvent vos outils existants) des enquêtes concernant le cloud. D'après notre expérience, les clients AWS qui réagissent aux incidents à l'aide de technologies cloud obtiennent de meilleurs résultats : les isolations peuvent être automatisées, les copies peuvent être effectuées plus facilement, les preuves sont prêtes à être analysées plus rapidement et l'analyse peut être réalisée plus rapidement.

La bonne pratique consiste à mener des enquêtes et des analyses dans le cloud, là où se trouvent les données, plutôt que d'essayer de transférer les données vers un centre de données avant d'enquêter. Vous pouvez utiliser les fonctionnalités de calcul et de stockage sécurisées du cloud pratiquement n'importe où dans le monde pour effectuer les opérations de réponse sécurisées. De nombreux clients choisissent de pré-créer un compte AWS distinct pour mener une enquête, mais vous pouvez, dans certains cas, choisir d'effectuer votre analyse dans le même compte AWS. Si

votre organisation doit conserver des enregistrements pour des raisons juridiques et de conformité, il peut être prudent de conserver des comptes séparés pour le stockage à long terme et les activités juridiques.

Il est également recommandé de mener l'enquête dans la région AWS où l'événement s'est produit, plutôt que de répliquer les données vers une autre région. Nous recommandons cette pratique avant tout pour éviter le temps supplémentaire requis pour transférer les données entre les régions. Pour chaque région AWS dans laquelle vous opérez, assurez-vous que votre processus de réponse aux incidents et les intervenants respectent les lois applicables en matière de confidentialité des données. Si vous devez déplacer des données entre des régions, tenez compte des implications juridiques du déplacement de données d'une juridiction à une autre. Il est généralement recommandé de conserver les données dans la même juridiction nationale.

Si vous pensez qu'un événement de sécurité a un impact sur votre sécurité, votre identité ou vos systèmes de communication, vous devrez peut-être rechercher d'autres mécanismes et accès pour enquêter et corriger cet impact. AWS vous offre la possibilité de lancer rapidement une nouvelle infrastructure pouvant être utilisée pour des environnements de travail différents et sécurisés. Par exemple, pendant que vous enquêtez sur la sévérité potentielle de la situation, vous pouvez créer un nouveau compte AWS avec les outils sécurisés dont ont besoin le service juridique, les relations publiques et les équipes de sécurité pour communiquer et continuer à travailler. Des services tels qu'AWS WorkSpaces (pour les bureaux virtuels), AWS WorkMail (pour les e-mails) et Amazon Chime (pour la communication) peuvent fournir à vos équipes d'intervention, à vos dirigeants et aux autres participants les fonctionnalités et la connectivité dont ils ont besoin pour communiquer, étudier et résoudre un problème.

Isolation des ressources

Au cours de votre enquête, vous devrez peut-être isoler des ressources pour répondre à une anomalie de sécurité. L'objectif de l'isolement des ressources est de limiter l'impact potentiel, d'empêcher la propagation ultérieure des ressources affectées, de limiter l'exposition involontaire des données et d'empêcher tout accès non autorisé supplémentaire.

Comme pour toute réponse, des considérations opérationnelles, réglementaires, juridiques ou autres peuvent s'appliquer. Assurez-vous d'évaluer les conséquences prévues et non prévues des actions que vous souhaitez mener. Si vos équipes cloud utilisent des balises de ressources, ces balises peuvent vous aider à identifier l'importance de la ressource ou du propriétaire à contacter.

Lancement de stations de travail d'analyse

Certaines de vos activités de réponse aux incidents peuvent inclure l'analyse des images des disques, des systèmes de fichiers, des déchargements de RAM ou d'autres artefacts qui sont impliqués dans un incident. De nombreux clients créent un poste de travail d'analyse personnalisé qu'ils peuvent utiliser pour monter des copies de tous les volumes de données concernés (appelés instantanés EBS). Pour cela, suivez la procédure suivante :

1. Choisissez une image Amazon Machine Image (AMI) de base (par exemple Linux ou Microsoft Windows) qui peut être utilisée comme station de travail d'analyse.
2. Lancez une instance Amazon EC2 à partir de cette AMI de base.
3. Renforcez le système d'exploitation, supprimez les packages logiciels inutiles et configurez les mécanismes d'audit et de journalisation appropriés.
4. Installez votre suite préférée de boîtes à outils open source ou privées, ainsi que tous les logiciels et packages dont vous avez besoin.
5. Arrêtez l'instance Amazon EC2 et créez une nouvelle AMI à partir de l'instance arrêtée.
6. Créez un processus hebdomadaire ou mensuel pour mettre à jour et recréer l'AMI avec les derniers correctifs logiciels.

Une fois que le système d'analyse est configuré à l'aide d'une AMI, votre équipe de réponse aux incidents peut utiliser ce modèle pour créer une nouvelle AMI afin de lancer un nouveau poste de travail d'analyse pour chaque enquête. Le processus de lancement de l'AMI en tant qu'instance Amazon EC2 peut être préconfiguré pour simplifier le processus de déploiement. Par exemple, vous pouvez créer un modèle des ressources d'infrastructure d'analyse dont vous avez besoin dans un fichier texte et le déployer sur votre compte AWS à l'aide d'AWS CloudFormation.

Lorsque vos ressources sont disponibles pour être déployées rapidement à partir d'un modèle, vos experts formés à l'analyse peuvent utiliser de nouveaux postes de travail d'analyse pour chaque enquête, au lieu de réutiliser l'infrastructure. Grâce à ce processus, vous pouvez vous assurer qu'il n'y a pas de contamination croisée due à d'autres examens d'analyse.

Types et emplacements d'instance

Amazon EC2 fournit un vaste éventail de types d'instances optimisés pour différents cas d'utilisation. Ces types d'instance correspondent à différentes combinaisons en termes de capacités de CPU, de mémoire, de stockage et de mise en réseau. Vous pouvez ainsi choisir un ensemble de ressources parfaitement adapté à vos applications. De nombreux types d'instance incluent plusieurs tailles

d'instance, ce qui vous permet de mettre à l'échelle vos ressources en fonction des besoins de votre charge de travail cible. Pour les instances de réponse aux incidents, suivez les politiques GRC de votre entreprise en matière de localisation et de segmentation à partir du réseau qui exécute les instances de production.

La mise en réseau améliorée AWS utilise la virtualisation d'I/O d'une racine unique (SR-IOV) pour fournir des fonctionnalités de mise en réseau hautes performances sur les types d'instance pris en charge. La méthode SR-IOV de virtualisation des appareils fournit de meilleures performances des E/S et une utilisation de la CPU réduite par rapport aux interfaces réseau virtualisées traditionnelles. La mise en réseau améliorée offre une bande passante supérieure, des performances de paquet par seconde (PPS) nettement plus élevées, ainsi que des latences réduites entre les instances. L'utilisation de la mise en réseau améliorée n'implique aucun coût supplémentaire. Pour de plus amples informations sur les types d'instance qui prennent en charge des vitesses réseau de 10 ou 25 Gbit/s et sur d'autres fonctionnalités avancées, veuillez consulter Types d'instance Amazon EC2.

Support pour les fournisseurs de cloud

Rubriques

- AWS Managed Services
- AWS Support
- Support de réponse DDoS

AWS Managed Services

AWS Managed Services (AMS) fournit une gestion continue de votre infrastructure AWS de telle sorte que vous puissiez vous concentrer sur vos applications. En implémentant les bonnes pratiques pour gérer votre infrastructure, AMS vous aide à réduire les coûts et risques de fonctionnement. AMS automatise les activités courantes telles que les demandes de modification, la surveillance, la gestion des correctifs, la sécurité et les services de sauvegarde, et fournit des services pour l'intégralité du cycle de vie pour mettre en service, exécuter et soutenir votre infrastructure.

En tant qu'opérateur d'infrastructure, AMS est responsable du déploiement d'une série de contrôles de détection de sécurité et fournit une première ligne de réponse aux alertes 24 /24 et 7 j/7, grâce au suivi global sur différents fuseaux horaires (modèle « follow-the-sun »). Lorsqu'une alerte est déclenchée, AMS suit un ensemble standard de runbooks automatisés et manuels pour garantir une réponse cohérente. Ces runbooks sont partagés avec les clients AMS lors de l'intégration afin qu'ils

puissent développer et coordonner la réponse avec AMS. AMS encourage l'exécution conjointe de simulations de réponse de sécurité avec les clients afin de développer la force opérationnelle avant qu'un incident réel ne se produise.

AWS Support

AWS Support offre une large gamme de plans qui vous permettent d'accéder à des outils et au savoir-faire nécessaires pour garantir la réussite et l'état opérationnel de vos solutions AWS. Tous les plans de support offrent un accès 24 /24 et 7 j/7 au service client, une documentation AWS, des livres blancs et des forums de support. Si vous avez besoin d'un support technique et d'autres ressources qui vous aideront à planifier, déployer et optimiser votre environnement AWS, vous pouvez sélectionner le plan de support le plus adapté à votre cas d'utilisation d'AWS.

Le centre de support d'AWS Management Console est le point de contact central pour obtenir de l'assistance pour les problèmes qui affectent vos ressources AWS. L'accès à AWS Support est contrôlé par IAM. Pour de plus amples informations sur l'accès aux fonctionnalités AWS support, veuillez consulter Accès au support.

En outre, si vous devez signaler un abus d'Amazon EC2, contactez l'équipe AWS Abuse.

Support de réponse DDoS

Une attaque par déni de service (DoS) rend votre site web ou votre application indisponible pour les utilisateurs finaux. Les personnes malveillantes utilisent diverses techniques qui consomment de la bande passante réseau ou d'autres ressources, perturbant ainsi l'accès des utilisateurs finaux légitimes. Dans sa forme la plus simple, une attaque DoS contre une cible est exécutée par une personne malveillante isolée à partir d'une source unique.

Lors d'une attaque par déni de service distribué (DDoS), une personne malveillante utilise plusieurs sources, qui peuvent être compromises ou contrôlées par un groupe de collaborateurs, pour orchestrer une attaque contre une cible. Lors d'une attaque DDoS, chacun des collaborateurs ou hôtes compromis participe à l'attaque, générant un flot de paquets ou de demandes visant à submerger la cible visée.

AWS propose aux clients le service AWS Shield. Il s'agit d'un service de protection DDoS (Distributed Denial of Service) managé qui protège les applications web exécutées sur AWS. AWS Shield offre des fonctions de détection continue et d'atténuation automatique qui peuvent minimiser les temps d'arrêt et la latence des applications. Il n'est donc pas nécessaire de faire appel à AWS Support pour bénéficier de la protection DDoS. Il existe deux niveaux AWS Shield : Standard et Avancé.

Tous les clients AWS bénéficient des protections automatiques d'AWS Shield Standard. AWS Shield Standard protège contre les attaques DDoS les plus fréquentes de la couche réseau et de transport qui ciblent les sites web et les applications. Lorsque vous utilisez AWS Shield Standard avec Amazon CloudFront et Amazon Route 53, vous recevez une protection complète contre toutes les attaques connues contre l'infrastructure (Couche 3 et 4) qui assure la disponibilité.

Pour obtenir des niveaux de protection supérieurs contre les attaques ciblant vos applications web s'exécutant sur des ressources Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront et Amazon Route 53, vous pouvez souscrire à AWS Shield Advanced. En outre, AWS Shield Advanced vous permet d'accéder 24 h/24 et 7 j/7 à l'équipe de réponse DDoS (DRT) AWS. Pour de plus amples informations sur AWS Shield Standard et AWS Shield Advanced, veuillez consulter AWS Shield.

Simuler

Rubriques

Simulations de réponse aux incidents de sécurité

Les simulations de réponse aux incidents de sécurité (SIRS) sont des événements internes qui permettent de mettre en pratique de manière structurée vos plans et procédures de réponse aux incidents au cours d'un scénario réaliste. Les événements SIRS consistent principalement en la préparation et en l'amélioration itérative de vos capacités de réponse. Voici quelques-unes des raisons pour lesquelles des activités SIRS peuvent s'avérer utiles :

- Validation de l'état de préparation
- Confiance accrue grâce aux simulations et à la formation du personnel
- Respect des obligations contractuelles ou de conformité
- Génération d'artefacts pour l'accréditation
- Agilité et amélioration progressive grâce à la concentration
- Amélioration de la vitesse et des outils
- Affinage de la communication et de la remontée des informations
- Plus grande sérénité face aux scénarios extraordinaires et inattendus

Pour ces raisons, la valeur apportée par la participation à une activité SIRS (Security Incident Report System) augmente l'efficacité d'une organisation lors d'événements stressants. Il peut s'avérer difficile de développer une activité SIRS à la fois réaliste et bénéfique. Bien que tester vos procédures ou l'automatisation qui gère des événements déjà connus présente certains avantages, il est tout aussi important de participer à des activités SIRS créatives pour vous tester par rapport à des événements inattendus.

Étapes de simulation

Que vous conceviez votre propre système SIRS ou que vous ayez un partenaire de confiance pour vous fournir les bases, les simulations suivent généralement les étapes suivantes :

1. Trouver un problème important : définissez le déclencheur qui doit provoquer une réponse.
2. Identifier les ingénieurs en sécurité compétents : une simulation nécessite l'intervention d'un créateur et d'un testeur.
3. Construire un système de modèle réaliste : la simulation doit être réaliste et appropriée. Si elle n'est pas réaliste, les participants risquent de ne pas apprécier l'exercice. Si elle est minimaliste, l'exercice peut être considéré comme sans importance. Commencez par des exercices simples et progressez vers un événement complet.
4. Créer et tester les éléments du scénario : il peut être nécessaire de créer un support de simulation pertinent, tel que des artefacts de journalisation, des notifications et des alertes par e-mail, ainsi que des runbooks potentiels.
5. Inviter d'autres responsables de la sécurité et des participants d'autres organisations : invitez tous ceux qui ont besoin de se former et de participer. Si votre service juridique général, les cadres et le service relations publiques de votre organisation participent à la simulation, vous devez également les inviter.
6. Exécuter la simulation : décidez si le personnel doit être informé de l'événement SIRS ou si la simulation doit rester inopinée.
7. Encourager, mesurer, améliorer et répéter : la simulation entraîne du stress, il est donc important d'encourager et de complimenter les efforts des participants. Après les encouragements vient l'occasion de mesurer, d'améliorer et d'itérer pour la prochaine simulation. AWS vous encourage créer une habitude autour de ces activités.

> **Important**
>
> Si vous planifiez une simulation de réponse aux incidents de sécurité (SIRS), veuillez consulter Test d'intrusion et lire la section Autres événements simulés pour obtenir les dernières informations concernant la procédure à suivre.

Exemples de simulation

Les simulations de sécurité doivent être réalistes pour apporter la valeur attendue. Lorsque vous ou vos partenaires vous efforcez de créer vos propres simulations, considérez toujours les événements du monde réel qui se sont déjà produits comme une source précieuse pour d'éventuels exercices de simulation. Voici quelques exemples que des clients AWS ont trouvé utiles pour leurs simulations initiales :

- Modifications non autorisées de la configuration ou des ressources réseau.
- Informations d'identification exposées publiquement par erreur en raison d'une mauvaise configuration du développeur.
- Contenu sensible rendu accessible au public par erreur en raison d'une mauvaise configuration par un développeur.
- Isolement d'un serveur web qui communique avec des adresses IP présumées malveillantes.

En plus de l'apprentissage empirique précieux, la réalisation d'activités SIRS génère des résultats, tels que les leçons apprises, sur lesquels vous pouvez vous appuyer dans le processus suivant de votre programme : l'itération.

Itérer

Dans la section précédente, certains des avantages des activités SIRS ont été définis. Le gain d'agilité grâce à des améliorations progressives constitue l'un de ces avantages. Les simulations doivent générer des résultats intéressants dont vous pouvez tirer parti pour améliorer votre réponse en matière de sécurité. Elles fournissent une boucle de rétroaction à l'organisation, sur ce qui fonctionne et ce qui ne fonctionne pas. Grâce à ces connaissances, vous pouvez créer progressivement de nouvelles procédures ou mettre à jour des procédures existantes pour améliorer votre réponse.

Rubriques

Runbooks

Lorsqu'une anomalie de sécurité est détectée, la maîtrise de l'événement et le retour à un état correct connu constituent une partie importante d'un plan de réponse. Par exemple, si l'anomalie est survenue en raison d'une mauvaise configuration de la sécurité, la correction peut se limiter à supprimer l'écart en redéployant les ressources avec la configuration appropriée. Pour ce faire, vous devez planifier à l'avance et définir vos propres procédures de réponse de sécurité, souvent appelées runbooks.

Un runbook est la forme documentée des procédures d'une organisation visant à exécuter une tâche ou une série de tâches. Cette documentation est généralement stockée soit dans un système numérique interne, soit imprimée sur papier. Vous disposez peut-être déjà de runbooks de réponse aux incidents ou vous devez les créer pour vous conformer à un cadre d'assurance de sécurité. Cependant, lorsque vous suivez manuellement les runbooks écrits, vous augmentez le risque de commettre des erreurs. Nous vous recommandons plutôt d'automatiser toutes vos tâches reproductibles. L'automatisation libère les membres de votre équipe de réponse des tâches courantes et les rend disponibles pour des tâches plus importantes, telles que la corrélation d'événements, les simulations, la conception de nouvelles procédures de réponse, la réalisation de recherches, le développement de nouvelles compétences et le test ou la création de nouveaux outils. Cependant, avant de pouvoir décomposer les tâches en logique programmable et itérer vers une automatisation appropriée, vous devez commencer par écrire un runbook.

Création de Runbooks

Pour créer des runbooks pour le cloud, nous vous recommandons de commencer par vous concentrer sur les alertes que vous générez actuellement. Si vous générez une alerte, il est important de l'examiner. Commencez par définir les descriptions des processus manuels que vous effectuez. Ensuite, testez les processus et itérez sur le modèle de runbook pour améliorer la logique de base de votre réponse. Déterminez les exceptions et les autres résolutions de ces scénarios. Par exemple, dans un environnement de développement, vous pouvez mettre fin à une instance Amazon EC2 mal configurée. Cependant, si le même événement se produisait dans un environnement de production, au lieu de mettre fin à l'instance, vous pourriez l'arrêter et vérifier avec les parties prenantes que les données critiques ne sont pas perdues et vérifier si la résiliation est acceptable.

Après avoir déterminé la meilleure solution, vous pouvez déconstruire la logique en une solution basée sur le code, qui peut être utilisée comme outil par de nombreux intervenants pour automatiser la réponse et supprimer les écarts ou les conjectures de vos intervenants. Cela accélère le cycle de vie d'une réponse. L'objectif suivant est de permettre à ce code d'être entièrement automatisé en étant appelé par les alertes ou les événements eux-mêmes, plutôt que d'être exécuté par un intervenant humain.

Mise en route

Si vous ne savez pas par où commencer, envisagez de commencer par les alertes qui pourraient être générées par AWS Trusted Advisor, les bonnes pratiques de sécurité fondamentales d'AWS Security Hub et AWS Config Rules (y compris le référentiel Github AWS Config Rules). Ensuite, concentrez-vous sur les événements générés par les services qui décriront les systèmes qui vous préoccupent.

Il est souvent suggéré d'utiliser Amazon GuardDuty et Access Analyzer, car ils décrivent de nombreux domaines qu'une application utilisera dans AWS. Cependant, Amazon Inspector et Amazon Macie proposent des utilisations spécifiques en cas de préoccupations au niveau des données et des points de terminaison. Les informations sur les résultats d'Amazon GuardDuty sont disponibles dans le Guide de l'utilisateur Amazon GuardDuty. Les résultats d'Access Analyzer sont disponibles dans le Guide de l'utilisateur Amazon Access Analyzer. Les résultats de Macie sont disponibles dans le Guide de l'utilisateur Amazon Macie. Les résultats d'Amazon Inspector sont disponibles dans le Guide de l'utilisateur Amazon Inspector. Security Hub est suggéré comme emplacement central pour la correction, car il vous permet d'unifier ces découvertes en un seul endroit et d'y réagir avec une faible latence.

Tous les services ci-dessus envoient des notifications via Amazon CloudWatch Events en cas de modification des résultats ou des alertes, y compris en cas d'alerte nouvellement générée et de

mise à jour des alertes existantes. Vous pouvez configurer les règles Amazon CloudWatch Events pour déclencher des fonctions AWS Lambda afin d'offrir une réponse basée sur un événement. Cependant, des critères importants font pencher la balance vers Security Hub : il offre la possibilité de créer des informations personnalisées et d'ajouter vos propres conclusions à partir du domaine d'application. Pour de plus amples informations, veuillez consulter la section Réponse basée sur les événements.

Automatisation

L'automatisation est un multiplicateur de force, ce qui signifie qu'elle adapte les efforts de vos intervenants à la vitesse de l'organisation. Passer de processus manuels à des processus automatisés vous permet de passer plus de temps à renforcer la sécurité de votre environnement cloud AWS.

Rubriques

- Automatisation de la réponse aux incidents
- Réponse basée sur les événements

Automatisation de la réponse aux incidents

Pour automatiser les fonctions d'ingénierie et d'exploitation de la sécurité, vous pouvez utiliser un ensemble complet d'API et d'outils AWS. Vous pouvez entièrement automatiser la gestion des identités, la sécurité du réseau, la protection des données et les fonctionnalités de surveillance. Lorsque vous automatisez la sécurité, vous autorisez votre système à surveiller, examiner et déclencher une réponse, plutôt que d'avoir à demander à des personnes de surveiller votre posture de sécurité et de réagir manuellement aux événements.

Si vos équipes de réponse aux incidents continuent de répondre aux alertes de la même manière, elles risquent de se lasser des alertes. Au fil du temps, l'équipe peut faire moins attention aux alertes et soit faire des erreurs en gérant des situations ordinaires, soit manquer des alertes inhabituelles. L'automatisation permet d'éliminer la lassitude liée aux alertes en utilisant des fonctions qui traitent les alertes répétitives et ordinaires, laissant aux personnes le soin de gérer les incidents sensibles et uniques.

Vous pouvez améliorer les processus manuels en automatisant par programmation les étapes du processus. Une fois que vous avez défini le modèle de correction d'un événement, vous pouvez le décomposer en logique exploitable et écrire le code pour exécuter la logique. Les

intervenants peuvent ensuite exécuter ce code pour corriger le problème. Au fil du temps, vous pouvez automatiser un nombre croissant d'étapes et, enfin, gérer automatiquement des catégories entières d'incidents courants.

Cependant, votre objectif devrait être de réduire davantage l'intervalle de temps entre les mécanismes de détection et les mécanismes de réaction. D'après l'historique, cet intervalle de temps peut prendre des heures, des jours, voire des mois. Une enquête sur la réponse aux incidents menée par SANS en 2016 a révélé que 21 % des personnes interrogées ont déclaré que leur délai de détection avait pris entre deux et sept jours, et seulement 29 % des personnes interrogées étaient en mesure de remédier aux événements dans le même délai. Dans le cloud, vous pouvez réduire cet intervalle de temps de réponse à quelques secondes en créant des capacités de réponse basées sur les événements.

Rubriques

Options d'automatisation des réponses

Il est important de veiller à équilibrer l'implémentation de l'entreprise et la structure de l'organisation. La Figure 4 illustre les différences d'attributs techniques pour chaque option de réponse automatisée dans votre implémentation AWS à l'aide d'un graphique en radar. Dans le graphique, plus l'attribut technique s'éloigne du centre du graphique, plus la force de cet attribut technique pour la réponse d'automatisation correspondante est grande. Par exemple, AWS Lambda offre plus de vitesse et nécessite moins de compétences techniques. AWS Fargate offre plus de flexibilité et nécessite moins de maintenance et de compétences techniques. Le Tableau 1 offre un aperçu de ces options d'automatisation et un résumé des attributs techniques de chacune.

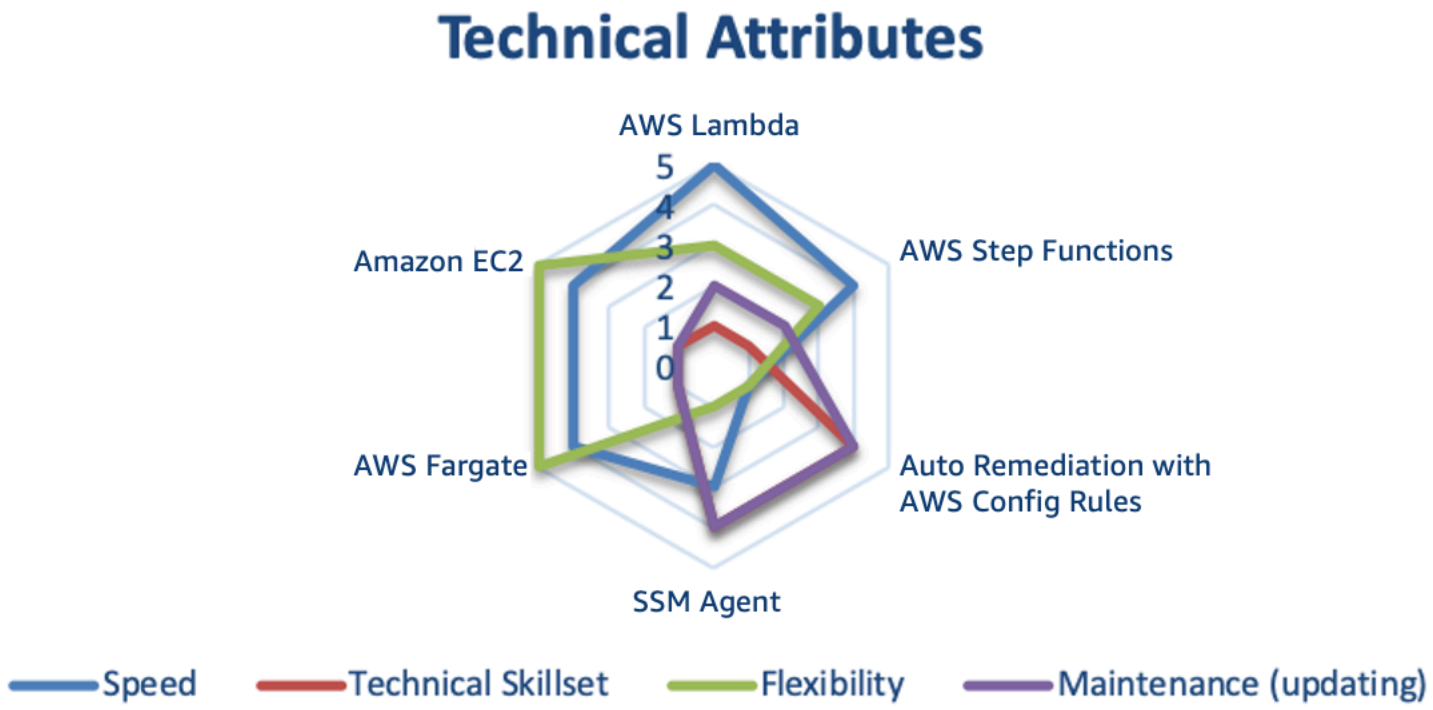

Figure 4 : Comparaison des attributs techniques entre les approches de réponse automatisée

Tableau 1 : Options pour les réponses automatisées

Service ou fonction AWS	Description	Résumé des attributs*
AWS Lambda	Système utilisant AWS Lambda uniquement et utilisant la langue d'entreprise de votre organisation.	Vitesse Flexibilité Maintenance Compétences
AWS Step Functions	Système utilisant AWS Step Functions, Lambda et SSM Agent.	Vitesse Flexibilité Maintenance Compétences
Correction automatique avec AWS Config Rules	Ensemble de règles AWS Config Rules et de mesures	Maintenance et compétences

Service ou fonction AWS	Description	Résumé des attributs*
	correctives automatiques qui évaluent l'environnement et le replacent dans la spécification approuvée.	Vitesse et flexibilité
SSM Agent	Ensemble de règles et de documents d'automatisation examinant de nombreux éléments des environnements et des systèmes internes et apportant des corrections.	Maintenance et compétences Vitesse Flexibilité
AWS Fargate	Système AWS Fargate utilisant le code de fonction step open source et les événements d'Amazon CloudWatch, et d'autres systèmes, pour stimuler la détection et la correction.	Flexibilité Vitesse Maintenance et compétences
Amazon EC2	Système s'exécutant sur une instance complète, similaire à l'option AWS Fargate.	Flexibilité Vitesse Maintenance Compétences

* Les attributs sont répertoriés par ordre décroissant pour chaque service ou fonction. Par exemple, AWS Lambda offre plus de vitesse et nécessite moins de compétences techniques. AWS Fargate offre plus de flexibilité et nécessite moins de maintenance et de compétences techniques.

Lorsque vous envisagez d'utiliser ces options d'automatisation dans votre environnement AWS, vous devez également prendre en compte la centralisation et la période d'analyse (événements par seconde, EPS).

La centralisation fait référence à un compte central qui gère toutes les opérations de détection et de correction pour une organisation. Cette approche peut sembler être le meilleur choix prêt à l'emploi, et constitue actuellement la bonne pratique. Cependant, certaines circonstances exigent que vous n'utilisiez pas cette approche. Vous devez comprendre quelles sont ces circonstances, en fonction de la façon dont vous gérez vos comptes subordonnés. Nous vous invitons à commencer par tirer parti de l'approche du compte Outils de sécurité dans le cadre multi-compte dans AWS Organizations ou dans AWS Control Tower.

Tableau 2 : Avantages et inconvénients de la centralisation

	Centralisation	Décentralisation
Avantages	Configuration plus simple à gérer Impossible d'annuler ou de modifier une réponse	Architecture simple Configuration initiale plus rapide
Inconvénients	Architecture plus complexe Inscription / désinscription des comptes et des ressources	Plus de ressources à gérer Base logicielle de référence difficile à maintenir

Une comparaison des coûts de ces implémentations peut également orienter votre entreprise dans le choix de la meilleure option. La métrique Événements par seconde (EPS) est celle que vous utilisez pour mieux estimer le coût. En fin de compte, il est peut-être beaucoup plus facile et moins coûteux d'utiliser des approches centralisées ou décentralisées. Mais il nous est impossible d'examiner la façon dont vous allez évaluer ce coût spécifiquement dans votre compte. Assurez-vous de prendre en compte les données Événements par seconde lorsque vous envoyez ces événements vers un compte central pour y répondre. Plus il y a d'événements par seconde, plus le coût d'envoi de ces événements vers un compte centralisé est élevé.

Comparaison des coûts dans les méthodes d'analyse

Les coûts sont par ailleurs déterminés par la méthode d'analyse qui permet de détecter une anomalie ainsi que par le délai entre les validations. Pour les méthodes d'analyse, vous pouvez choisir entre une analyse basée sur les événements ou une analyse périodique. Le Tableau 3 montre les avantages et les inconvénients des deux approches.

Tableau 3 : Avantages et inconvénients des différentes méthodes d'analyse

	Analyse basée sur les événements	Analyse périodique
Avantages	Moins de temps entre l'événement et la réponse Besoin limité d'interroger des appels d'API supplémentaires	Image complète à un moment donné
Inconvénients	Contexte limité concernant l'état de la ressource Les événements déclenchés peuvent concerner une ressource qui n'est pas facilement accessible	Limites de service pour les grands comptes Peut éventuellement se heurter à une limitation en raison d'un volume élevé d'appels d'API

Dans de nombreux cas, la combinaison des deux approches d'analyse constitue probablement le meilleur choix dans une organisation arrivée à maturité. AWS Security Hub et la norme des bonnes pratiques de sécurité de base AWS offrent une combinaison des deux méthodes d'analyse.

Le graphique en radar de la Figure 5 illustre la comparaison des coûts des événements par seconde pour chacune des approches d'automatisation. Par exemple, Amazon EC2 et AWS Fargate affichent les coûts les plus élevés pour l'exécution de 0 à 10 événements par seconde, tandis que AWS Lambda et AWS Step Functions affichent les coûts les plus élevés pour l'exécution de plus de 76 événements par seconde.

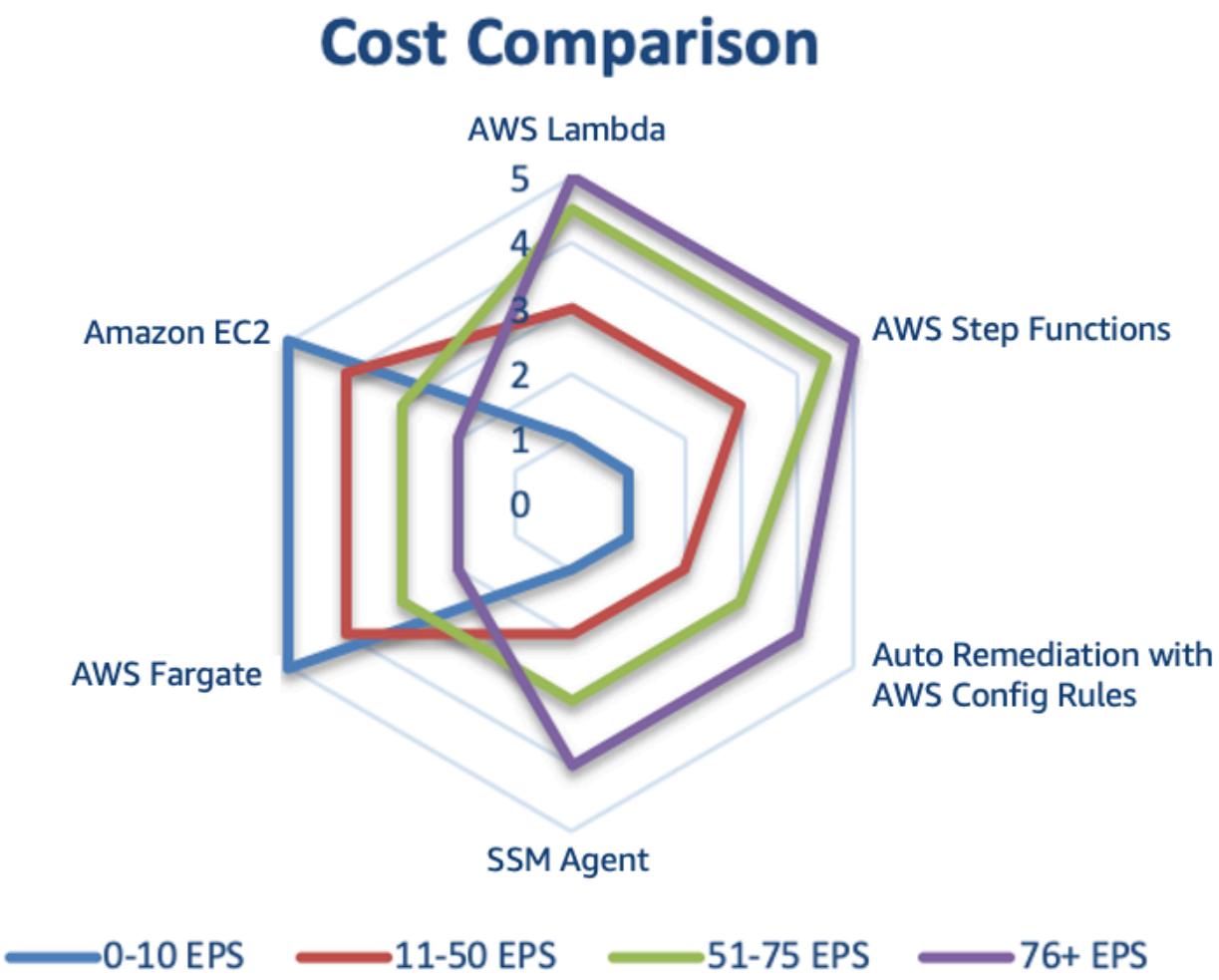

Figure 5 : Comparaison des coûts des méthodes d'analyse des options d'automatisation (événements par seconde)

Réponse basée sur les événements

Avec un système de réponse basée sur les événements, un mécanisme de détection déclenche un mécanisme de réaction pour répondre automatiquement à l'événement. Vous pouvez utiliser des fonctionnalités de réaction basées sur les événements pour réduire le délai entre les mécanismes de détection et les mécanismes de réaction. Pour créer cette architecture basée sur les événements, vous pouvez utiliser AWS Lambda, un service de calcul sans serveur qui exécute votre code en réponse à des événements et gère automatiquement les ressources de calcul sous-jacentes.

Supposons que disposez d'un compte AWS avec le service AWS CloudTrail activé. Si AWS CloudTrail est désactivé (via l'API `cloudtrail:StopLogging`), la procédure de réponse consiste à réactiver le service et à rechercher l'utilisateur qui a désactivé la journalisation AWS CloudTrail. Au

lieu d'effectuer ces étapes manuellement dans AWS Management Console, vous pouvez réactiver la journalisation par programme (via l'API `cloudtrail:StartLogging`). Si vous implémentez cela avec du code, l'objectif de votre réponse est d'effectuer cette tâche le plus rapidement possible et d'informer les intervenants que la réponse a été effectuée.

Vous pouvez décomposer la logique en code simple à exécuter dans une fonction AWS Lambda pour effectuer ces tâches. Vous pouvez ensuite utiliser Amazon CloudWatch Events pour surveiller l'événement `cloudtrail:StopLogging` spécifique et appeler la fonction s'il se produit. Lorsque cette fonction de répondeur AWS Lambda est appelée par Amazon CloudWatch Events, vous pouvez lui transmettre les détails de l'événement spécifique avec les informations sur le principal qui a désactivé AWS CloudTrail, la date de la désactivation, la ressource spécifique qui a été affectée et d'autres informations pertinentes. Vous pouvez utiliser ces informations pour enrichir les résultats des journaux, puis générer une notification ou une alerte avec uniquement les valeurs spécifiques dont un une personne chargée de l'analyse de la réponse aurait besoin.

Idéalement, la réponse basée sur les événements a pour objectif de faire exécuter la fonction répondeur par Lambda, puis informe le répondeur que l'anomalie a été résolue avec succès à l'aide de toute information contextuelle pertinente. Il appartient ensuite à l'intervenant humain chargé de la réponse de décider comment déterminer pourquoi cela s'est produit et comment éviter que cela se reproduise. Cette boucle de rétroaction permet d'améliorer encore la sécurité de vos environnements cloud. Pour atteindre cet objectif, votre culture doit permettre à votre équipe de sécurité de travailler plus étroitement avec vos équipes de développement et d'exploitation.

Exemples de réponse aux incidents

Rubriques

Incidents de domaine de service

Les incidents de domaine de service sont généralement gérés exclusivement par le biais des API AWS.

Identités

AWS fournit des API à nos services cloud qui sont utilisés par des millions de clients pour créer de nouvelles applications et générer des résultats opérationnels. Ces API peuvent être invoquées par le biais de nombreuses méthodes, comme les kits SDK, l'AWS CLI et AWS Management Console. Pour interagir avec AWS par le biais de ces méthodes, le service IAM vous aide à contrôler en toute sécurité l'accès aux ressources AWS. Vous pouvez utiliser IAM pour contrôler les personnes qui s'authentifient (qui sont connectées) et qui sont autorisées (qui disposent d'autorisations) à utiliser des ressources au niveau du compte. Pour connaître la liste des services AWS prenant en charge IAM, veuillez consulter Services AWS qui fonctionnent avec IAM.

Lorsque vous créez un compte AWS, vous commencez avec une identité d'authentification unique (SSO) disposant d'un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée utilisateur racine du compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, et notamment pour les tâches administratives. Respectez plutôt la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM. Stockez en sécurité les informations d'identification de l'utilisateur racine et exécutez seulement certaines tâches de gestion de comptes et de services. Pour de plus amples informations, veuillez consulter Créer des utilisateurs IAM individuels.

Bien que ces API apportent de la valeur à des millions de clients, certaines d'entre elles peuvent être utilisées à mauvais escient si de mauvaises personnes ont accès à votre compte IAM ou à vos informations d'identification racine. Par exemple, vous pouvez utiliser les API pour activer la journalisation au sein de votre compte, par exemple AWS CloudTrail. Toutefois, si des personnes

malveillantes obtiennent vos informations d'identification, elles peuvent également utiliser l'API pour désactiver ces journaux. Vous pouvez empêcher ce type d'abus en configurant des autorisations IAM appropriées qui suivent un modèle de moindre privilège, et en protégeant correctement vos informations d'identification IAM. Pour de plus amples informations, veuillez consulter Bonnes pratiques IAM dans le Guide de l'utilisateur AWS Identity and Access Management. Si ce type d'événement se produit, plusieurs contrôles de détection permettent d'identifier que votre journalisation AWS CloudTrail a été désactivée, notamment AWS CloudTrail, AWS Config, AWS Trusted Advisor, Amazon GuardDuty et AWS CloudWatch Events.

Ressources

Les autres fonctionnalités qui peuvent être utilisées à mauvais escient ou mal configurées varient d'une organisation à l'autre, en fonction de la façon dont chaque client utilise le cloud. Par exemple, certaines organisations prévoient de rendre certaines données ou applications accessibles au public, tandis que d'autres gardent leurs applications et leurs données confidentielles et en interne. Les événements de sécurité ne sont pas tous de nature malveillante ; certains événements peuvent résulter de configurations non intentionnelles ou incorrectes. Déterminez quelles API ou fonctions ont un impact important sur votre organisation et déterminez si vous les utilisez fréquemment ou rarement.

Vous pouvez identifier de nombreuses erreurs de configuration de sécurité à l'aide d'outils et de services. Par exemple, AWS Trusted Advisor fournit un certain nombre de vérifications des bonnes pratiques. Les partenaires APN proposent également des centaines de produits leaders du secteur qui sont équivalents, identiques ou s'intègrent aux contrôles existants dans vos environnements sur site. Un certain nombre de ces produits et solutions ont été présélectionnés par le programme de compétences des partenaires AWS. Nous vous encourageons à consulter la section Configuration et analyse des vulnérabilités du programme de compétences en sécurité APN pour parcourir ces solutions et déterminer si elles peuvent répondre à vos exigences.

Incidents de domaine de l'infrastructure

Le domaine de l'infrastructure inclut généralement les données de votre application ou les activités liées au réseau, telles que le trafic vers vos instances Amazon EC2 au sein du VPC et les processus exécutés dans vos systèmes d'exploitation d'instance Amazon EC2.

Supposons par exemple que votre solution de surveillance vous a signalé une anomalie de sécurité potentielle sur votre instance Amazon EC2. Les actions suivantes constituent des étapes courantes pour résoudre ce problème :

1. Capturez les métadonnées de l'instance Amazon EC2, avant d'apporter des modifications à votre environnement.
2. Protégez l'instance Amazon EC2 contre les mises hors service accidentelles en activant la protection contre la mise hors service pour l'instance.
3. Isolez l'instance Amazon EC2 en changeant le groupe de sécurité du VPC. Toutefois, soyez conscient du suivi des connexions VPC et des autres techniques de confinement.
4. Détachez l'instance Amazon EC2 de tous les groupes AWS Auto Scaling.
5. Annulez l'inscription de l'instance Amazon EC2 de tout service Elastic Load Balancing associé.
6. Réalisez un instantané des volumes de données Amazon EBS attachés à l'instance EC2 à des fins de conservation et de suivi.
7. Marquez l'instance Amazon EC2 comme étant mise en quarantaine à des fins d'enquête et ajoutez toutes les métadonnées pertinentes, telles que le ticket d'incident associé à l'enquête.

Vous pouvez effectuer toutes les étapes précédentes à l'aide des API AWS, des kits SDK AWS, de l'AWS CLI et d'AWS Management Console. Pour interagir avec AWS à l'aide de ces méthodes, le service IAM vous aide à contrôler en toute sécurité l'accès aux ressources AWS. Vous pouvez utiliser IAM pour contrôler les personnes qui sont authentifiées et qui sont autorisées à utiliser des ressources au niveau du compte. Le service IAM fournit l'authentification et l'autorisation qui vous permettent d'effectuer ces actions et d'interagir avec le domaine de service.

Un instantané d'un volume Amazon EBS est une copie ponctuelle au niveau du bloc d'un volume de données EBS, qui se produit de manière asynchrone et dont l'exécution peut prendre du temps. Il s'agit d'un delta de ces données à partir de ce moment. Vous pouvez créer de nouveaux volumes EBS à partir de ces copies et les monter sur l'instance EC2 d'enquête afin qu'une analyse approfondie hors ligne soit menée par des enquêteurs. Le diagramme suivant montre une version simplifiée du résultat et ne décrit pas tous les composants réseau (tels que les sous-réseaux, les tables de routage et les listes de contrôle d'accès au réseau).

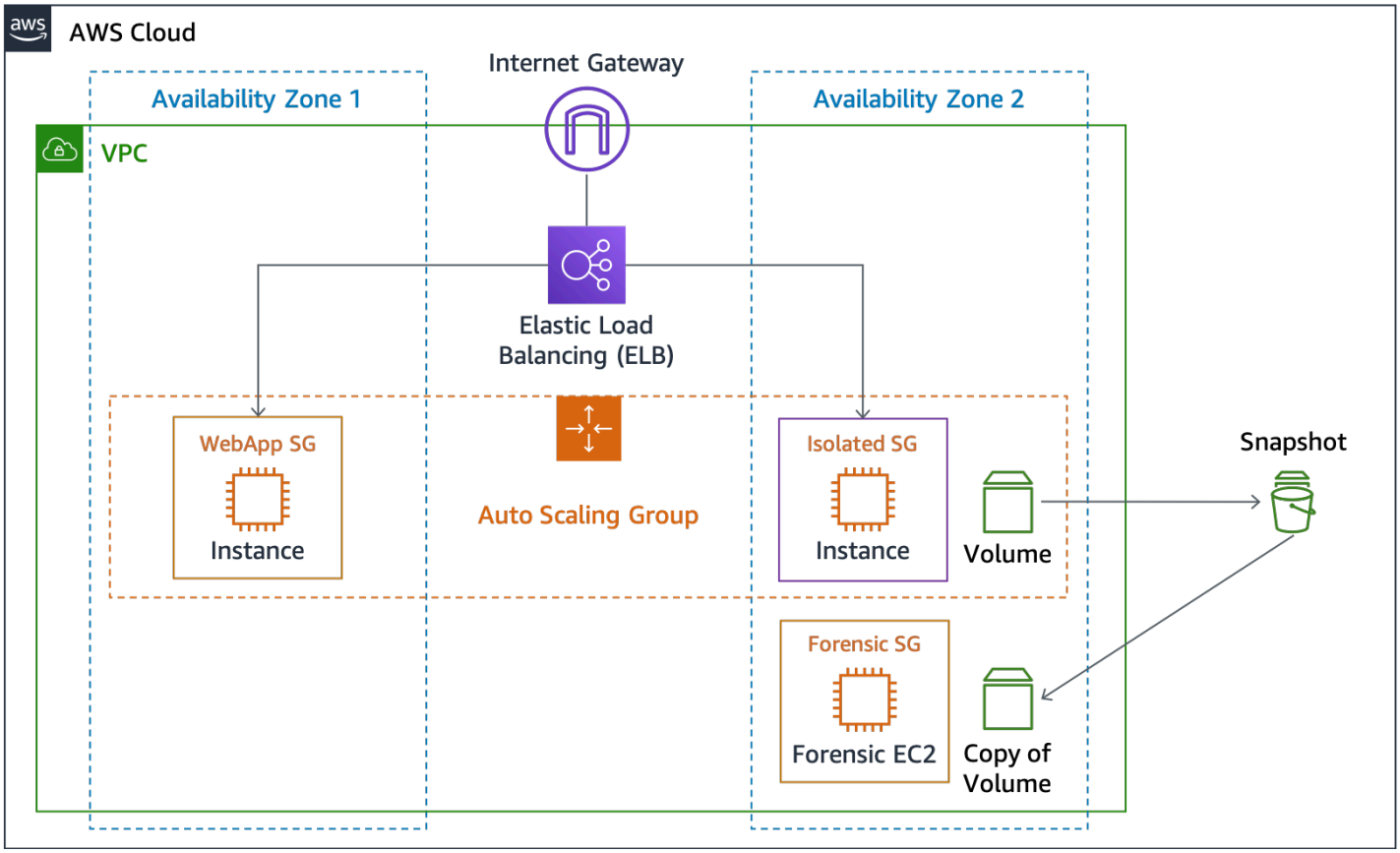

Figure 6 : Isolation d'instance EC2 et instantanés

Rubriques

- Décisions relatives aux enquêtes
- Capture de données dynamiques
- Utilisation d'AWS Systems Manager
- Automatisation de la capture

Décisions relatives aux enquêtes

À ce stade, vous pouvez choisir entre une enquête hors ligne (arrêt immédiat de l'instance) ou une enquête en ligne (maintien de l'exécution de l'instance). L'un des avantages de l'enquête hors ligne est qu'une fois que l'instance a été arrêtée, elle ne peut plus affecter l'environnement existant. En outre, vous pouvez créer une copie de l'instance affectée à partir des instantanés EBS et l'examiner dans un compte AWS isolé avec un environnement isolé spécialement conçu pour votre enquête. Toutefois, vous pouvez choisir de ne pas arrêter l'instance immédiatement, si une enquête en ligne

vous permet de capturer des preuves dynamiques provenant du système d'exploitation hôte, telles que la mémoire ou le trafic réseau.

Capture de données dynamiques

Même si vous ne choisissiez pas d'effectuer l'enquête en ligne, il est important de comprendre les mécanismes nécessaires pour capturer les données dynamiques d'une instance. Une enquête en ligne nécessite une interaction avec le système d'exploitation qui s'exécute sur l'instance Amazon EC2. Dans ce scénario, le service AWS IAM ne suffit pas pour exécuter des tâches sur une instance Amazon EC2. Bien que vous puissiez vous authentifier directement auprès de la machine à l'aide d'une méthode standard (telle que Linux Secure Shell (SSH) ou Microsoft Windows Remote Desktop (RDP)), l'interaction manuelle avec le système d'exploitation ne constitue pas une bonne pratique. Nous vous recommandons d'utiliser par programme un outil d'automatisation pour exécuter des tâches sur un hôte.

Utilisation d'AWS Systems Manager

La fonctionnalité Exécuter la commande d'AWS Systems Manager vous permet d'effectuer à distance et en toute sécurité des modifications à la demande en exécutant des scripts shell Linux et des commandes Windows PowerShell sur une instance ciblée. Bien que vous puissiez invoquer la fonctionnalité Exécuter la commande via les autorisations du service AWS IAM, vous devez d'abord activer vos instances Amazon EC2 en tant qu'instances gérées, installer SSM Agent sur vos machines (s'il n'est pas installé par défaut) et configurer les autorisations AWS IAM. Si vous souhaitez utiliser la fonctionnalité Exécuter la commande pour des activités d'automatisation ou de réponse, assurez-vous de terminer les activités préalables avant de mener une enquête.

AWS Systems Manager, qui inclut la fonctionnalité Exécuter la commande, est intégré à AWS CloudTrail, service qui capture les appels d'API effectués par ou pour le compte de Systems Manager et transmet les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les informations collectées par AWS CloudTrail vous permettent de déterminer quelle demande a été envoyée, l'adresse IP source à partir de laquelle la demande a été effectuée, qui a effectué la demande, quand, etc. CloudTrail crée des journaux de toutes les actions d'API Systems Manager, y compris les demandes d'API pour exécuter des commandes à l'aide de la fonctionnalité Exécuter la commande ou créer des documents Systems Manager.

Vous pouvez utiliser le service Exécuter la commande d'AWS Systems Manager pour appeler SSM Agent qui exécute les scripts shell Linux et les commandes Windows PowerShell. Ces scripts peuvent charger et exécuter des outils spécifiques pour capturer des données supplémentaires

à partir de l'hôte, tels que le module noyau Linux Memory Extractor (LiME). Vous pouvez ensuite transférer la capture de mémoire vers votre instance Amazon EC2 sur laquelle vous enquêtez dans le réseau VPC ou vers un compartiment Amazon S3 pour un stockage durable.

Automatisation de la capture

Pour appeler SSM Agent, une méthode consiste à cibler la fonctionnalité Exécuter la commande via Amazon CloudWatch Events lorsque l'instance est marquée avec une balise spécifique. Par exemple, si vous appliquez la balise `Response=Isolate+MemoryCapture` à une instance affectée, vous pouvez configurer Amazon CloudWatch Events pour déclencher deux actions :

- Une fonction Lambda qui effectue les activités d'isolation
- Une fonctionnalité Exécuter la commande qui exécute une commande shell pour exporter la mémoire Linux via SSM Agent

Cette réponse pilotée par des balises est une autre méthode de réponse basée sur les événements.

Conclusion

Au fur et à mesure de votre transition vers le cloud, il est important que vous preniez en compte les concepts fondamentaux de réponse aux incidents de sécurité mentionnés ci-dessus pour votre environnement AWS. Vous pouvez combiner les contrôles disponibles, les fonctionnalités cloud et les options de correction pour vous aider à améliorer la sécurité de votre environnement cloud. Vous pouvez également commencer à petite échelle et itérer les actions à mesure que vous adoptez des fonctionnalités d'automatisation qui améliorent votre vitesse de réponse, afin d'être mieux préparé en cas d'événements de sécurité.

Ressources supplémentaires

Pour de plus amples informations, veuillez consulter :

- AWS Well-Architected
- Page Cadre d'adoption du cloud AWS
- Solution de journalisation centralisée AWS
- Visualisez les AWS CloudTrail Logs à l'aide d'AWS GlueAmazon QuickSight
- How to Monitor Host-Based Intrusion Detection System Alerts on Amazon EC2 Instances
- Store and Monitor OS & Application Log Files with Amazon CloudWatch
- Identity and Access Management dans Amazon S3
- Gestion des versions (Amazon S3)
- Utilisation de la fonction Supprimer MFA
- Protection des données grâce au chiffrement côté serveur avec les clés gérées par AWS KMS (SSE-KMS)
- Réponse aux incidents avec la console AWS et l'interface de ligne de commande (CLI)
- Préparation à la loi sur la confidentialité des consommateurs en Californie

Multimédia

- AWS re:Invent 2014 (SEC402) : Intrusion Detection in the Cloud
- AWS re:Invent 2014 (SEC404) : Incident Response in the Cloud
- AWS re:Invent 2015 (SEC308) : Wrangling Security Events in The Cloud
- AWS re:Invent 2015 (SEC316) : Harden Your Architecture with Security Incident Response Simulations
- AWS re:Invent 2016 (SEC313) : Automating Security Event Response, from Idea to Code to Execution
- AWS re:Invent 2017 (SID302) : Force Multiply Your Security Team with Automation and Alexa
- AWS re:Invent 2016 (SAC316) : Security Automation: Spend Less Time Securing Your Applications
- AWS re:Invent 2016 (SAC304) : Predictive Security: Using Big Data to Fortify Your Defenses
- AWS re:Invent 2017 (SID325) : Amazon Macie: Data Visibility Powered by Machine Learning for Security and Compliance Workloads

- AWS London Summit 2018 : Automating Incident Response and Forensics in AWS

Outils tiers

Les liens suivants vers des outils tiers sont externes et ne sont pas approuvés par AWS. AWS n'offre aucune garantie ou représentation de quelque nature que ce soit concernant ces outils ou ces pages.

- AWS_IR – Utilitaire de ligne de commande installable en Python pour atténuer les compromissions d'hôte et de clé.
- MargaritaShotgun – Outil d'acquisition de mémoire à distance.
- ThreatPrep – Module Python pour l'évaluation des bonnes pratiques des comptes AWS en matière de préparation à la gestion des incidents.
- ThreatResponse Web – plateforme d'analyse basée sur le web à utiliser avec l'outil de ligne de commande AWS_IR.
- Réponse rapide GRR – Analyse en direct à distance pour la réponse aux incidents.
- Bloqueur d'écriture Linux – Correctif du noyau et outils d'espace utilisateur pour activer le blocage d'écriture du logiciel Linux.

Références sectorielles

- NIST SP 800-61R2 : Computer Security Incident Handling Guide

Révisions du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

update-history-change	update-history-description	update-history-date
Mises à jour mineures	Correctifs de bogues et nombreux changements mineurs.	2 juin 2021
Mise à jour mineure	Correction de liens brisés.	5 mars 2021
Livre blanc mis à jour	Correction de liens brisés et nombreuses modifications du texte afin d'améliorer la lisibilité.	23 novembre 2020
Mise à jour mineure	Correction du lien vers Réponse aux incidents avec la console AWS et l'interface de ligne de commande (CLI).	30 juin 2020
Livre blanc mis à jour	Mises à jour concernant les nouveaux services de sécurité, la détection des menaces, la responsabilité partagée pour les conteneurs, l'automatisation et la loi sur la confidentialité des consommateurs en Californie (CCPA). Ajout d'annexes avec un exemple d'arbre de décision et de runbook.	11 juin 2020
Publication initiale	Première publication du livre blanc	1 juin 2019

Annexe A : Définitions des capacités du cloud

AWS propose plus de 150 services cloud et des milliers de fonctions. Bon nombre de ces services et fonctions offrent des fonctionnalités natives de détection, de prévention et de réaction, tandis que d'autres peuvent être utilisés pour concevoir des solutions de sécurité personnalisées. Cette section inclut un sous-ensemble des services les plus pertinents pour la réponse aux incidents dans le cloud.

Rubriques

Journalisation et événements

AWS CloudTrail – AWS CloudTrail est un service qui permet la gouvernance, la conformité, l'audit opérationnel et l'audit des risques de votre compte AWS. Avec CloudTrail, vous pouvez journaliser, surveiller en continu et conserver l'activité de votre compte relative aux actions effectuées sur l'ensemble de votre infrastructure AWS. CloudTrail fournit l'historique des événements intervenus sur votre compte AWS, y compris les actions prises via AWS Management Console, les SDK AWS, les outils de ligne de commande et d'autres services AWS. Cet historique des événements simplifie l'analyse de la sécurité, le suivi des modifications de ressources et le dépannage.

Les fichiers journaux validés s'avèrent utiles lors d'enquêtes de sécurité et d'analyse. Afin de déterminer si des fichiers journaux ont été modifiés ou supprimés, ou s'ils restent inchangés après avoir été livrés par CloudTrail, vous pouvez utiliser la validation d'intégrité des fichiers journaux de CloudTrail. Cette fonction est intégrée l'aide d'algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est alors impossible de modifier, supprimer ou falsifier des fichiers journaux CloudTrail par traitement informatique sans être détecté.

Par défaut, les fichiers journaux livrés par CloudTrail à votre compartiment sont chiffrés à l'aide du chiffrement côté serveur Amazon. Vous pouvez éventuellement utiliser les clés gérées AWS Key Management Service (AWS KMS) (SSE-KMS) pour vos fichiers journaux CloudTrail.

Amazon CloudWatch Events – Amazon CloudWatch Events fournit un flux d'événements système en quasi temps réel décrivant les modifications apportées aux ressources AWS ou lorsque des appels d'API sont publiés par AWS CloudTrail. À l'aide de règles simples et rapidement configurées, vous pouvez faire correspondre des événements et les acheminer vers un ou plusieurs flux, ou vers une ou plusieurs fonctions cibles. CloudWatch Events prend connaissance des changements opérationnels au fur et à mesure qu'ils surviennent. CloudWatch Events peut répondre à ces changements opérationnels et, le cas échéant, prend des mesures correctives en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en procédant à des modifications et en capturant des informations d'état. Certains services de sécurité, tels qu'Amazon GuardDuty, produisent leur sortie sous la forme d'événements CloudWatch Events.

AWS Config – AWS Config est un service qui vous permet d'apprécier, d'auditer et d'évaluer les configurations de vos ressources AWS. Config surveille et enregistre en permanence les configurations de vos ressources AWS et vous permet d'automatiser l'évaluation des configurations enregistrées par rapport aux configurations souhaitées. Avec Config, vous pouvez examiner l'évolution des configurations et des relations entre les ressources AWS, manuellement ou automatiquement. Vous pouvez consulter des historiques de configuration des ressources détaillés et déterminer votre conformité globale aux configurations spécifiées dans vos directives internes. Cela vous permet de simplifier l'audit de la conformité, l'analyse de la sécurité, la gestion des modifications et le diagnostic des défaillances opérationnelles.

Journaux d'accès Amazon S3 – Si vous stockez des informations sensibles dans un compartiment Amazon S3, vous pouvez activer les journaux d'accès S3 pour enregistrer chaque chargement, téléchargement et modification de ces données. Ce journal est distinct et complémentaire des journaux CloudTrail qui enregistrent les modifications apportées au compartiment lui-même (telles que la modification des politiques d'accès et des politiques de cycle de vie).

Amazon CloudWatch Logs – Vous pouvez utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder à vos fichiers journaux (tels que votre système d'exploitation, votre application et vos fichiers journaux personnalisés) à partir de vos instances Amazon Elastic Compute Cloud (Amazon EC2) à l'aide de l'agent CloudWatch Logs. En outre, Amazon CloudWatch Logs peut capturer des journaux à partir de AWS CloudTrail, de requêtes DNS Amazon Route 53, de journaux de flux VPC, de fonctions Lambda et d'autres sources. Vous pouvez ensuite récupérer les données de journaux associées depuis CloudWatch Logs.

Journaux de flux VPC – Les journaux de flux VPC vous permettent de capturer des informations sur le trafic IP vers et depuis les interfaces réseau dans votre VPC. Une fois que vous avez créé un journal de flux, vous pouvez afficher et extraire ses données dans Amazon CloudWatch Logs. Les

journaux de flux VPC peuvent vous aider à réaliser un certain nombre de tâches. Par exemple, vous pouvez utiliser des journaux de flux pour déterminer pourquoi un trafic spécifique n'atteint pas une instance, ce qui peut vous aider à diagnostiquer des règles de groupe de sécurité trop restrictives. Vous pouvez également utiliser les journaux de flux comme outil de sécurité pour surveiller le trafic qui atteint votre instance.

Journaux AWS WAF – AWS WAF prend désormais en charge la journalisation complète de toutes les demandes web inspectées par le service. Vous pouvez stocker ces journaux dans Amazon S3 à des fins de conformité et d'audit, ainsi que les utiliser pour le débogage et d'autres analyses. Ces journaux vous aideront à comprendre pourquoi certaines règles sont déclenchées, alors que certaines demandes web sont bloquées. Vous pouvez également intégrer les journaux à vos services SIEM et à vos outils d'analyse des journaux.

Autres journaux AWS – Au fur et à mesure des innovations, nous continuons à déployer de nouvelles fonctions et capacités pour les clients pratiquement tous les jours, ce qui signifie qu'il existe des dizaines de services AWS qui fournissent des fonctions de journalisation et de surveillance. Pour de plus amples informations sur les fonctionnalités disponibles pour chaque service AWS, veuillez consulter la documentation AWS relative à chaque service.

Visibilité et alertes

AWS Security Hub – AWS Security Hub fournit une vue complète de vos alertes de sécurité hautement prioritaires et de l'état de conformité de vos comptes AWS. Avec Security Hub, vous disposez d'un emplacement unique qui regroupe, organise et hiérarchise vos alertes de sécurité ou vos conclusions à partir de plusieurs services AWS, tels qu'Amazon GuardDuty, Amazon Inspector et Amazon Macie, ainsi que des solutions AWS Partner. Vos résultats sont résumés visuellement dans des tableaux de bord intégrés qui contiennent des graphiques et des tableaux exploitables. Vous pouvez également contrôler en permanence votre environnement à l'aide de contrôles de conformité automatiques fondés sur les bonnes pratiques AWS et les normes du secteur que votre organisation suit.

Amazon GuardDuty – Amazon GuardDuty est un service géré de détection des menaces qui surveille en permanence les comportements malveillants ou non autorisés pour vous aider à protéger vos comptes et charges de travail AWS. Il contrôle les activités telles que les appels d'API inhabituels ou les déploiements potentiellement non autorisés qui peuvent indiquer un compte compromis. GuardDuty détecte également les instances potentiellement compromises ou les missions de reconnaissance de pirates.

GuardDuty identifie les personnes suspectées d'être malveillantes grâce à des flux intégrés de détection des menaces et utilise le machine learning pour détecter les anomalies dans les activités des comptes et des charges de travail. Quand une menace potentielle est détectée, le service envoie une alerte de sécurité détaillée à la console GuardDuty et à AWS CloudWatch Events. Ainsi, les alertes sont exploitables et faciles à intégrer aux systèmes existants de flux et de gestion des événements.

Amazon Macie – Amazon Macie est un service de sécurité basé sur l'IA qui vous aide à éviter toute perte de données en identifiant, répertoriant et protégeant automatiquement les données sensibles dans AWS. Amazon Macie utilise le machine learning pour reconnaître les données sensibles comme les données d'identification personnelle (PII) ou la propriété intellectuelle. Le service attribue une valeur opérationnelle à ces données et fournit une visibilité sur leur emplacement de stockage et la façon dont elles sont exploitées dans votre organisation. Amazon Macie contrôle en permanence l'activité liée à l'accès aux données et génère des alertes lorsqu'un risque d'accès non autorisé ou de fuite accidentelle de données est détecté.

AWS Config Rules – Une règle AWS Config représente les configurations préférées pour une ressource ; elle est comparée aux changements de configuration apportés aux ressources correspondantes et enregistrés par AWS Config. Vous pouvez consulter les résultats de l'évaluation d'une règle par rapport à la configuration d'une ressource dans un tableau de bord. En utilisant les règles Config, vous pouvez évaluer votre état global en termes de conformité et de risques du point de vue de la configuration, afficher les tendances de conformité au fil du temps et trouver les changements de configuration à l'origine du non-respect d'une règle par une ressource.

AWS Trusted Advisor – AWS Trusted Advisor est une ressource en ligne qui vous permet de réduire les coûts, d'augmenter les performances et d'améliorer la sécurité en optimisant votre environnement AWS. Trusted Advisor fournit des conseils en temps réel pour vous aider à mettre en service vos ressources AWS en suivant les bonnes pratiques AWS. L'ensemble des vérifications Trusted Advisor, y compris l'intégration avec CloudWatch Events, est accessible aux clients bénéficiant du programme de support niveau Business ou Enterprise.

Amazon CloudWatch – Amazon CloudWatch est un service de surveillance pour les ressources du cloud AWS et les applications que vous exécutez sur AWS. Vous pouvez utiliser Amazon CloudWatch pour collecter et suivre des métriques, regrouper et contrôler des fichiers journaux, régler des alarmes et réagir automatiquement aux modifications apportées à vos ressources AWS. Amazon CloudWatch peut surveiller les ressources AWS de la même façon que les instances Amazon EC2, les tables Amazon DynamoDB et les instances de base de données Amazon RDS, ainsi que les métriques personnalisées générées par vos applications et services, et tous les fichiers

journaux générés par vos applications. Vous pouvez utiliser Amazon CloudWatch pour gagner une visibilité à l'échelle du système sur l'utilisation des ressources, la performance de l'application et l'état opérationnel. Vous pouvez utiliser ces informations pour réagir de façon appropriée et faire en sorte que votre application continue de fonctionner sans heurt.

AWS Inspector – Amazon Inspector est un service automatique d'évaluation de la sécurité qui permet d'améliorer la sécurité et la conformité des applications déployées sur AWS. Amazon Inspector analyse automatiquement les applications afin de détecter les failles ou les écarts par rapport aux bonnes pratiques. Après avoir effectué une évaluation, Amazon Inspector produit une liste détaillée de constatations en matière de sécurité, classées par niveau de gravité. Ces résultats peuvent être analysés directement ou dans le cadre de rapports d'évaluation détaillés disponibles via l'API ou la console Amazon Inspector.

Amazon Detective – Amazon Detective est un service de sécurité qui collecte automatiquement les données de journal de vos ressources AWS et utilise le machine learning, l'analyse statistique et la théorie des graphes pour créer un ensemble de données liées qui vous permet de mener facilement des enquêtes de sécurité plus rapides et plus efficaces. Amazon Detective peut analyser des milliards d'événements à partir de plusieurs sources de données, telles que les journaux de flux Virtual Private Cloud (VPC), AWS CloudTrail et Amazon GuardDuty, et crée automatiquement une vue interactive et unifiée de vos ressources, de vos utilisateurs et des interactions mutuelles au fil du temps. Avec cette vue unifiée, vous pouvez visualiser toutes les informations et le contexte dans un même endroit pour identifier les raisons sous-jacentes des résultats, explorer en détail les activités d'historique pertinentes et déterminer rapidement la cause principale.

Automatisation

AWS Lambda – AWS Lambda est un service de calcul sans serveur qui exécute votre code en réponse à des événements et gère automatiquement les ressources de calcul sous-jacentes pour vous. Vous pouvez utiliser Lambda pour étendre d'autres services AWS grâce à une logique personnalisée ou créer vos propres services dorsaux, tout en bénéficiant du dimensionnement, des performances et de la sécurité d'AWS. Lambda exécute votre code sur une infrastructure de calcul à haute disponibilité et s'occupe de toute l'administration de vos ressources de calcul pour vous. Cette tâche comprend la maintenance des serveurs et des systèmes d'exploitation, l'approvisionnement en capacité et la scalabilité automatique, le déploiement du code et des correctifs de sécurité, ainsi que la surveillance et la journalisation du code. Il vous suffit de fournir le code.

AWS Step Functions – AWS Step Functions facilite la coordination des composants des applications distribuées et des microservices à l'aide de flux de travail visuels. Step Functions fournit une console

graphique pour que vous puissiez organiser et visualiser les composants de votre application en une série d'étapes. Vous pouvez donc développer et exécuter des applications à plusieurs étapes plus facilement. Step Functions déclenche automatiquement chaque étape, en fait le suivi et la relance en cas d'erreur. Votre application est donc exécutée dans l'ordre et comme prévu.

Step Functions consigne l'état de chaque étape pour que vous puissiez diagnostiquer et résoudre rapidement les problèmes éventuels. Vous pouvez modifier et ajouter des étapes sans écrire de code, ce qui vous permet de faire évoluer facilement votre application et d'innover plus rapidement. AWS Step Functions fait partie de la plateforme sans serveur d'AWS et facilite l'orchestration des fonctions AWS Lambda pour les applications sans serveur. Vous pouvez également utiliser Step Functions pour orchestrer les microservices en utilisant des ressources de calcul, telles qu'Amazon EC2 et Amazon ECS.

AWS Systems Manager – AWS Systems Manager vous donne la visibilité et le contrôle nécessaires sur votre infrastructure sur AWS. Il fournit une interface utilisateur unifiée qui vous permet d'afficher les données opérationnelles de plusieurs services AWS et d'automatiser les tâches opérationnelles pour vos ressources AWS. Avec Systems Manager, vous pouvez regrouper les ressources par application, visualiser les données opérationnelles pour la surveillance et le dépannage, et effectuer des actions sur ses groupes de ressources. Systems Manager peut conserver vos instances à leur état défini, appliquer des modifications à la demande, telles que la mise à jour d'application ou l'exécution de scripts de Shell et l'exécution d'autres tâches d'automatisation et d'application de correctifs.

Stockage sécurisé

Amazon S3 – Amazon S3 est un stockage d'objets conçu pour stocker et récupérer n'importe quelle quantité de données, n'importe où. Conçu pour offrir 99,999999999 % de durabilité, ce service stocke les données de millions d'applications utilisées par des leaders de tous les secteurs. Amazon S3 fournit une sécurité complète et est conçu pour répondre à vos exigences réglementaires. Ce service apporte davantage de flexibilité dans la manière de gérer les données pour l'optimisation des coûts, le contrôle des accès et la conformité. Amazon S3 fournit une fonctionnalité de requête en place, qui vous permet d'exécuter des analyses puissantes directement sur vos données au repos dans Amazon S3. Amazon S3 est le service de stockage dans le cloud disponible le plus pris en charge, étant intégré dans la plus grande communauté de fournisseurs de solutions tiers, de partenaires d'intégration système et d'autres services AWS.

Amazon S3 Glacier – Amazon S3 Glacier est un service de stockage dans le cloud sécurisé, durable et à très faible coût qui permet l'archivage et la sauvegarde des données à long terme. Il est conçu

pour offrir une durabilité de 99,999999999 %, fournit une sécurité complète et est conçu pour répondre à vos exigences réglementaires. Amazon S3 Glacier offre des fonctionnalités de requête sur place, qui vous permettent d'exécuter des analyses puissantes directement sur vos données d'archives au repos. Afin de proposer des coûts bas tout en restant adapté à différents cas de récupération, Amazon S3 Glacier offre trois options pour l'accès aux archives, avec des délais allant de quelques minutes à plusieurs heures.

Personnalisé

Les services et fonctionnalités mentionnés ci-dessus ne constituent pas une liste exhaustive. AWS propose continuellement de nouvelles fonctionnalités. Pour de plus amples informations, nous vous encourageons à consulter les pages Nouveautés AWS et Sécurité du cloud AWS. Outre les services de sécurité proposés par AWS en tant que services cloud natifs, vous pouvez souhaiter développer vos propres capacités en plus des services AWS.

Bien que nous vous recommandions d'activer un ensemble de base de services de sécurité au sein de vos comptes, tels que AWS CloudTrail, Amazon GuardDuty et Amazon Macie, vous pouvez souhaiter étendre ces fonctionnalités afin de tirer une valeur supplémentaire des ressources de vos journaux. Un certain nombre d'outils partenaires sont disponibles, tels que ceux répertoriés dans notre programme de compétences en sécurité APN. Vous pouvez également écrire vos propres requêtes pour effectuer des recherches dans vos journaux. Cela n'a jamais été aussi simple, grâce au grand nombre de services managés proposés par AWS. Il existe de nombreux services AWS supplémentaires qui peuvent vous aider dans vos enquêtes et qui ne sont pas abordés dans ce document, tels qu'Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning et Amazon EMR.

Annexe B : Exemple de code

Exemple d'évènement AWS CloudTrail

L'exemple suivant montre qu'un utilisateur IAM nommé `Alice` a utilisé l'AWS CLI pour appeler `StopInstancesaction` Amazon EC2 à l'aide de `ec2-stop-instances`.


```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

Exemple AWS CloudWatch Events

L'exemple d'événement Amazon CloudWatch suivant montre qu'un utilisateur IAM AWS nommé `jane-roe-test` a été publiquement exposé sur `www.github.com` et pourrait faire l'objet d'abus par des utilisateurs non autorisés.

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

Exemples d'activités d'interface de ligne de commande (CLI) du domaine de l'infrastructure

Les commandes de l'AWS CLI suivantes présentent un exemple de réponse à un événement au sein du domaine de l'infrastructure. Cet exemple utilise les API AWS pour effectuer de nombreuses activités initiales de réponse aux incidents décrites dans cet article.

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
```

```
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

Annexe C : Exemple de runbook

L'exemple de runbook suivant représente une seule entrée d'un runbook plus important. Ce runbook n'est pas officiel et n'est fourni qu'à titre d'exemple. Au fur et à mesure que vous concevez vos runbooks, chacun de vos scénarios peut évoluer vers des éléments plus importants ayant des débuts et des indicateurs de compromis différents, mais ayant tous des résultats similaires ou des actions similaires qui doivent être entreprises. Ce changement peut également offrir des réponses meilleures ou plus pertinentes pour d'autres situations.

Runbook de réponse aux incidents – Utilisation du compte racine

Objectif

L'objectif de ce runbook est de fournir des conseils spécifiques sur la façon de gérer l'utilisation du compte AWS racine. Ce runbook ne remplace pas une stratégie approfondie de réponse aux incidents. Ce runbook se concentre sur le cycle de vie des réponses aux incidents :

- Établir le contrôle
- Déterminer l'impact
- Procéder à la récupération en fonction des besoins
- Déterminer la cause première
- Améliorer

Les indicateurs de compromission, les étapes initiales (arrêter l'hémorragie) et les commandes CLI détaillées nécessaires pour exécuter ces étapes sont répertoriés ci-dessous.

Hypothèses

- Interface de ligne de commande (CLI) configurée et installée.
- Le processus de signalement est déjà en place.
- Trusted Advisor est activé.
- Security Hub est activé.

Indicateurs de compromission

- Activité anormale pour le compte.
  - Création d'utilisateurs IAM.
  - CloudTrail est désactivé.
  - Cloudwatch est désactivé.
  - SNS est mis en pause.
  - Step Functions est mis en pause.
- Lancement d'AMI nouvelles ou inattendues.
- Modifications apportées aux contacts du compte.

Étapes permettant de corriger la situation – Établir le contrôle

En cas de suspicion de compte compromis, la documentation AWS indique les tâches spécifiques répertoriées ci-dessous. La documentation relative à la suspicion de compte compromis se trouve sur la page suivante : Que faire si je remarque une activité non autorisée dans mon compte AWS ?

1. Contactez AWS Support et le gestionnaire technique du compte (TAM) dès que possible.
2. Modifiez et procédez à la rotation du mot de passe racine, et ajoutez un dispositif MFA associé à la racine.
3. Procédez à la rotation des mots de passe, des clés d'accès/des clés secrètes et des commandes CLI pertinentes pour les étapes de correction.
4. Passez en revue les actions entreprises par l'utilisateur racine.
5. Ouvrez les runbooks qui correspondent à ces actions.
6. Procédez à la fermeture de l'incident.
7. Examinez l'incident. Vous devez comprendre ce qui s'est passé.
8. Corrigez les problèmes sous-jacents, implémentez des améliorations et mettez à jour le runbook si nécessaire.

Autres mesures à prendre — Déterminer l'impact

Passez en revue les éléments créés et les appels mutants. Certains éléments ont peut-être été créés pour autoriser l'accès à l'avenir. Quelques points à examiner :

- Rôles entre comptes IAM
- Utilisateurs IAM
- Compartiments S3
- Instances EC2
- [Élaborez cette liste en fonction de votre application et de votre infrastructure.]

Mentions légales

Les clients sont responsables de leur propre évaluation indépendante des informations contenues dans ce document. Le présent document : (a) est fourni à titre informatif uniquement, (b) représente les offres et pratiques actuelles de produits AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ou assurance de la part d'AWS et de ses affiliés, fournisseurs ou concédants de licences. Les produits ou services AWS sont fournis « en l'état » sans garantie, représentation ou condition, de quelque nature que ce soit, explicite ou implicite. Les responsabilités et obligations d'AWS envers ses clients sont déterminées par les contrats AWS, et le présent document ne fait pas partie d'un contrat entre AWS et ses clients, ni le modifie.