AWS Well-Architected Framework

Pilier Sécurité

Pilier Sécurité: AWS Well-Architected Framework

Table of Contents

Pilier Sécurité - AWS Well-Architected Framework

Date de publication : 6 décembre 2023 (Révisions du document)

Ce document porte sur le pilier Sécurité du AWS Well-Architected Framework. Il fournit des conseils pour vous aider à appliquer les bonnes pratiques et les recommandations actuelles dans la conception, la distribution et la maintenance des charges de travail sécurisées sur AWAWS.

Introduction

La AWS Well-Architected Framework vous aide à comprendre les compromis des décisions que vous prenez lors du développement des charges de travail sur AWS. En utilisant le cadre, vous apprendrez les bonnes pratiques architecturales actuelles pour concevoir et exploiter des charges de travail fiables, sécurisées, efficaces et rentables dans le cloud. Il vous permet de mesurer systématiquement votre charge de travail par rapport aux bonnes pratiques et d'identifier les domaines à améliorer. Nous pensons que le fait d'avoir des charges de travail bien structurées augmente considérablement les chances de réussite métier.

Le cadre repose sur six piliers :

- Excellence opérationnelle
- Sécurité
- Fiabilité
- Efficacité des performances
- Optimisation des coûts
- Durabilité

Ce livre blanc porte sur le pilier Sécurité. Il vous aidera à répondre à vos exigences opérationnelles et réglementaires en suivant les recommandations actuelles AWS. Il s'adresse aux personnes qui occupent des fonctions technologiques, telles que les directeurs de la technologie (CTO), les responsables de la sécurité de l'information (CSO/CISO), les architectes, les développeurs et les membres des équipes opérationnelles.

Après avoir lu ce document, vous comprendrez les recommandations et les stratégies actuelles AWS à utiliser lors de la conception d'architectures cloud en tenant compte de la sécurité. Ce document ne fournit pas d'informations sur la mise en œuvre ni de modèles architecturaux, mais inclut des

références aux ressources appropriées pour obtenir ces informations. En adoptant les pratiques décrites dans ce document, vous pouvez créer des architectures qui protègent les données et les systèmes, contrôler les accès et répondre automatiquement aux événements de sécurité.

Bases du pilier Sécurité

Le pilier Sécurité décrit comment tirer parti des technologies du cloud pour protéger les données, les systèmes et les ressources de manière à améliorer votre niveau de sécurité. Ce document fournit de bonnes pratiques détaillées pour la création de charges de travail sécurisées sur AWS.

Principes de conception

Dans le cloud, il existe un certain nombre de principes qui peuvent vous aider à renforcer la sécurité de vos charges de travail :

- Mettre en place une solide base pour le contrôle des identités : mettez en œuvre le principe du moindre privilège et appliquez la séparation des responsabilités avec l'autorisation appropriée pour chaque interaction avec vos ressources AWS. Centralisez la gestion des identités et visez l'élimination de la dépendance aux informations d'identification statiques de longue durée.
- Assurer la traçabilité : Supervisez, alertez et contrôlez les actions et les modifications apportées à votre environnement en temps réel. Intégrez la collecte des journaux et des métriques aux systèmes pour effectuer des analyses et prendre des mesures automatiquement.
- Appliquer la sécurité à toutes les couches : Appliquez une approche approfondie de la défense avec plusieurs contrôles de sécurité. Appliquez-les à toutes les couches (par exemple, périphérie du réseau, VPC, équilibrage de charge, chaque instance et service de calcul, système d'exploitation, application et code).
- Automatiser les bonnes pratiques en matière de sécurité : Les mécanismes de sécurité automatisés basés sur les logiciels améliorent votre capacité à vous adapter de manière plus rapide et plus économique, et ce en toute sécurité. Créez des architectures sécurisées, y compris avec mise en œuvre des contrôles définis et gérés en tant que code dans les modèles de contrôle de versions.
- Protéger les données en transit et au repos : classez vos données selon différents niveaux de sensibilité et utilisez des mécanismes, tels que le chiffrement, la création de jetons et le contrôle d'accès, si nécessaire.
- Éviter les interventions humaines sur les données : Utilisez des mécanismes et outils pour réduire ou éliminer le besoin d'accès direct ou le traitement manuel des données. Cette approche permet de réduire les risques de mauvaise manipulation ou de modification ainsi que les erreurs humaines lors d'interventions sur des données sensibles.

- Se préparer aux incidents impliquant la sécurité : Préparez-vous à un incident en mettant en œuvre une stratégie et des processus de gestion et d'investigation des incidents conformes à vos besoins d'entreprise. Exécutez des simulations de réponse aux incidents et utilisez des outils d'automatisation pour améliorer votre vitesse de détection, d'investigation et de récupération.

Définition

La sécurité dans le cloud se compose de sept domaines :

- Bases du pilier Sécurité
- Identity and Access Management
- Détection
- Protection de l'infrastructure
- Protection des données
- Réponse aux incidents
- Sécurité des applications

Responsabilité partagée

La sécurité et la conformité sont une responsabilité partagée entre AWS et le client. Ce modèle peut atténuer la charge opérationnelle qui pèse sur le client, car les services AWS exploitent, gèrent et contrôlent 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. Le client assume toujours la responsabilité et la gestion du système d'exploitation « invité » (notamment les mises à jour et les correctifs de sécurité), d'autres éléments applicatifs connexes, de même que la configuration du pare-feu du groupe de sécurité fourni par AWS. Les clients doivent choisir avec soin les services, car leurs responsabilités varient en fonction des services utilisés, de l'intégration de ces services dans leur environnement informatique, ainsi que les cadres législatifs et règlementaires applicables. La nature de cette responsabilité partagée assure également la flexibilité et le contrôle client qui permettent le déploiement. Comme illustré dans le graphique suivant, cette distinction des responsabilités est communément appelée sécurité « du » cloud par rapport à la sécurité « dans » le cloud.

Responsabilité AWS « Sécurité du cloud » – AWSest responsable de la protection de l'infrastructure exécutant tous les services proposés dans le cloud AWS. Cette infrastructure se compose de matériels, de logiciels, de réseaux et d'installations exécutant les services de cloud AWS.

Responsabilité du client « Sécurité dans le cloud » – La responsabilité du client est déterminée par les services de cloud AWS qu'il sélectionne. Ils déterminent la quantité de travail de configuration que doit réaliser le client dans le cadre de ses responsabilités en matière de sécurité. Par exemple, les services, tels qu'Amazon Elastic Compute Cloud (Amazon EC2), sont classés dans la catégorie Infrastructure en tant que service (IaaS) et, en tant que tels, exigent du client qu'il effectue toutes les tâches de configuration et de gestion de la sécurité nécessaires. Les clients qui déploient une instance Amazon EC2 sont chargés de la gestion du système d'exploitation invité (notamment les mises à jour et les correctifs de sécurité), de tous les logiciels ou utilitaires qu'ils installent sur les instances, ainsi que de la configuration du pare-feu fourni par AWS (appelé groupe de sécurité) sur chaque instance. Dans le cas des services extraits, comme Amazon S3 et Amazon DynamoDB, AWS exploite la couche infrastructure, le système d'exploitation et les plateformes, et les clients accèdent aux points de terminaison pour stocker et récupérer les données. Les clients sont responsables de la gestion de leurs données (notamment les options de chiffrement), de la classification de leurs ressources et de l'utilisation d'outils IAM pour appliquer les autorisations appropriées.

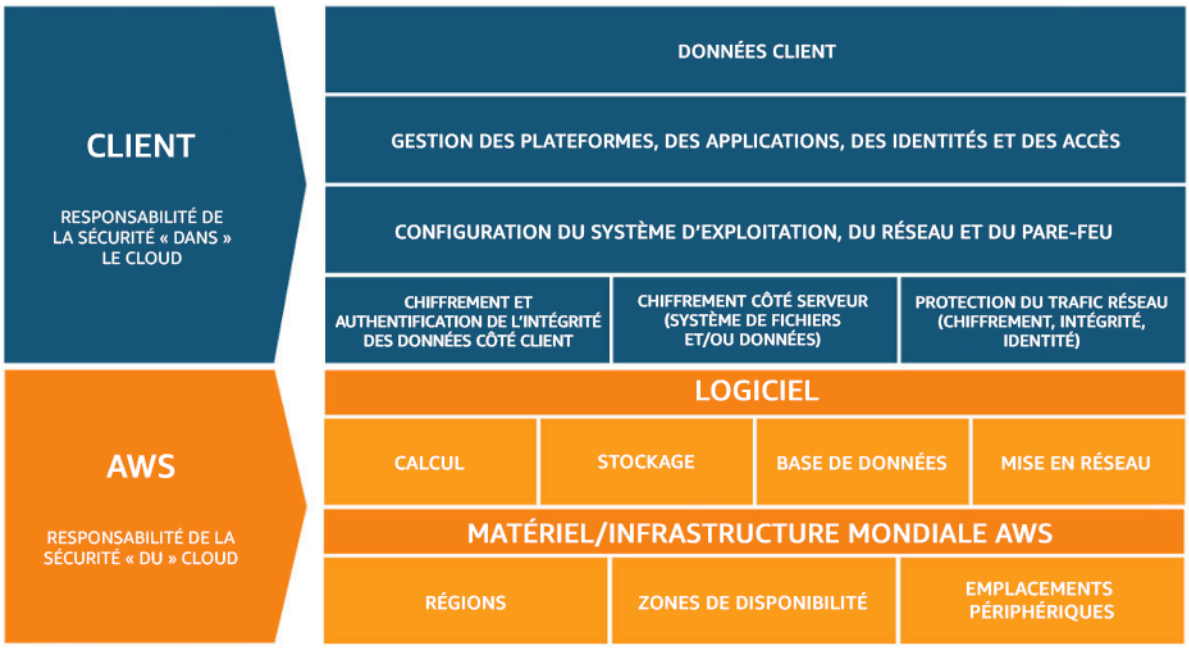


Figure 1 : Modèle de responsabilité partagée AWS

Ce modèle de responsabilité partagée entre AWS et le client s'étend également aux contrôles informatiques. Tout comme la responsabilité d'exploiter l'environnement informatique est partagée

entre AWS et ses clients, la gestion, l'exploitation et la vérification des contrôles informatiques sont également partagées. AWS peut soulager les clients au niveau de l'exécution des contrôles en gérant ceux associés à l'infrastructure physique déployée au sein de l'environnement AWS, lesquels étaient peut-être jusqu'à alors gérés par le client lui-même. Étant donné que chaque déploiement client sur AWS est différent, les clients peuvent tirer parti de ce transfert de gestion de certains contrôles informatiques vers AWS, donnant lieu à un (nouvel) environnement de contrôle distribué. Les clients peuvent ensuite utiliser la documentation AWS relative aux contrôles et à la mise en conformité qui est mise à leur disposition afin d'exécuter leurs propres procédures de vérification et d'évaluation des contrôles, si nécessaire. Voici des exemples de contrôles gérés par AWS, les clients AWS ou les deux.

Contrôles hérités – Contrôle qu'un client hérite entièrement d'AWS.

- Contrôles de l'environnement et de la couche physique

Contrôles partagés – Contrôles qui s'appliquent à la fois à la couche infrastructure et aux couches client, mais dans des contextes ou des perspectives distincts. Dans un contrôle partagé, AWS fournit les exigences pour l'infrastructure, et le client doit fournir sa propre implémentation de contrôle dans le cadre de son utilisation des services AWS. En voici quelques exemples :

- Gestion des correctifs – AWS est responsable de la correction des failles et de l'application des correctifs au sein de l'infrastructure, mais les clients sont responsables de la correction de leur système d'exploitation invité et de leurs applications.
- Gestion de la configuration – AWS gère la configuration de ses périphériques d'infrastructure, mais les clients sont responsables de la configuration de leurs propres systèmes d'exploitation invités, bases de données et applications.
- Sensibilisation et formation : AWS forme les employés AWS, mais les clients doivent former leurs propres employés.

Contrôles spécifiques au client – Contrôles qui relèvent de la seule responsabilité du client en fonction de l'application qu'il déploie au sein des services AWS. En voici quelques exemples :

- Protection des services et des communications ou zone de sécurité, qui peut nécessiter qu'un client achemine ou segmente les données dans des environnements de sécurité spécifiques.

Gouvernance

La gouvernance de la sécurité, en tant que sous-ensemble de l'approche globale, vise à soutenir les objectifs commerciaux en définissant des politiques et des objectifs de contrôle pour faciliter la gestion des risques. Pour assurer la gestion des risques, suivez une approche à plusieurs niveaux des objectifs de contrôle de sécurité. Chaque niveau s'appuie sur la précédente. La compréhension du modèle de responsabilité partagée AWS est le niveau de base. Ce niveau permet de clarifier ce dont vous êtes responsable côté client et ce dont vous héritez d'AWS. Une ressource utile est AWS Artifact, qui offre un accès à la demande aux rapports de sécurité et de conformité d'AWS, ainsi qu'à certains contrats en ligne.

Atteignez la plupart de vos objectifs de contrôle au niveau suivant. C'est là que se trouve la capacité à l'échelle de la plateforme. Par exemple, ce niveau inclut le processus de distribution de comptes AWS, l'intégration avec un fournisseur d'identité telle que AWS IAM Identity Center et les contrôles de détection communs. Certains des résultats du processus de gouvernance de la plateforme se trouvent également ici. Lorsque vous souhaitez commencer à utiliser un nouveau service AWS, mettez à jour les stratégies de contrôle de service (SCP) dans le service AWS Organisations afin de fournir les barrières de protection pour l'utilisation initiale du service. Vous pouvez utiliser d'autres SCP pour implémenter des objectifs de contrôle de sécurité communs, souvent appelés « invariants de sécurité ». Il s'agit d'objectifs de contrôle ou de configuration que vous appliquez à plusieurs comptes, unités organisationnelles ou à l'ensemble de l'organisation AWS. Des exemples typiques limitent les régions dans lesquelles l'infrastructure s'exécute ou empêchent la désactivation des contrôles de détection. Ce niveau intermédiaire contient également des politiques codifiées telles que des règles de configuration ou des vérifications dans les pipelines.

Le niveau supérieur est celui où les équipes produit répondent aux objectifs de contrôle. Cela est dû au fait que la mise en œuvre se fait dans les applications contrôlées par les équipes produit. Il peut s'agir d'implémenter la validation des entrées dans une application ou de s'assurer que l'identité passe correctement entre les microservices. Même si l'équipe produit est responsable de la configuration, elle peut toujours hériter de certaines fonctionnalités du niveau intermédiaire.

Quel que soit l'endroit où vous mettez en œuvre le contrôle, l'objectif est le même : gérer les risques. Divers frameworks de gestion des risques s'appliquent à des secteurs, des régions ou des technologies spécifiques. Votre objectif principal : mettre en évidence le risque en fonction de la probabilité et de la conséquence. C'est le risque inhérent. Vous pouvez ensuite définir un objectif de contrôle qui réduit soit la probabilité, soit la conséquence, soit les deux. Puis, avec un contrôle en place, vous pouvez voir quel est le risque qui est le plus susceptible d'en résulter. C'est le risque résiduel. Les objectifs de contrôle peuvent s'appliquer à une ou plusieurs charges de travail. Le

diagramme suivant illustre une matrice de risque typique. La probabilité est basée sur la fréquence des événements précédents, et la conséquence est basée sur le coût de l'événement en termes d'argent, de réputation et de durée.

Probabilité	Niveau de risque				
Très probable	Faible	Moyenne entreprise	Débit	Critique	Critique
Probable	Faible	Moyenne entreprise	Moyenne entreprise	Débit	Critique
Possible	Faible	Faible	Moyenne entreprise	Moyenne entreprise	Débit
Peu probable	Faible	Faible	Moyenne entreprise	Moyenne entreprise	Débit
Très improbable	Faible	Faible		Moyenne entreprise	Débit
Conséquence	Minime	Faible	Moyenne entreprise	Débit	Sévère

Figure 2 : Matrice de probabilité du niveau de risque

Gestion et séparation des comptes AWS

Nous vous recommandons d'organiser les charges de travail dans des comptes et des comptes de groupe distincts suivant la fonction, les exigences de conformité ou un ensemble commun de contrôles plutôt que de mettre en miroir la structure de rapport de votre organisation. Dans AWS, les comptes constituent un conteneur hermétique. Par exemple, la séparation au niveau du compte est fortement recommandée pour isoler les charges de travail de production des charges de travail de développement et de test.

Gérer les comptes de manière centralisée : AWS Organizations automatise la création et la gestion de comptes AWS, ainsi que le contrôle de ces comptes après leur création. Lorsque vous créez un compte dans AWS Organizations, il est important de tenir compte de l'adresse électronique que vous utilisez, car il s'agit de l'identifiant racine qui permet de réinitialiser le mot de passe. Organizations vous permet de regrouper des comptes en unités d'organisation (UO), ce qui peut représenter différents environnements en fonction des besoins et de l'objectif de la charge de travail.

Définir les contrôles de manière centralisée : Contrôlez ce que vos comptes AWS peuvent faire en autorisant uniquement des services, régions et actions de service spécifiques au niveau approprié. AWS Organizations vous permet d'utiliser des politiques de contrôle des services (SCP) pour appliquer des protections par autorisation au niveau de l'organisation, de l'unité d'organisation ou du compte, qui s'appliquent à tous les utilisateurs et rôles AWS Identity and Access Management (IAM). Par exemple, vous pouvez appliquer une politique de contrôle des services qui empêche les utilisateurs de lancer des ressources dans des régions que vous n'avez pas explicitement autorisées. AWS Control Tower offre un moyen simplifié de configurer et de gérer plusieurs comptes. Il automatise la configuration des comptes dans votre organisation AWS et la mise en service, applique des détection/correction (qui incluent la prévention et la détection) et vous fournit un tableau de bord pour plus de visibilité.

Configurer les services et les ressources de manière centralisée : AWS Organizations vous aide à configurer les services AWS qui s'appliquent à tous vos comptes. Par exemple, vous pouvez configurer la journalisation centrale de toutes les actions effectuées dans votre organisation à l'aide d' AWS CloudTrailet empêcher les comptes membres de désactiver la journalisation. Vous pouvez également regrouper de manière centralisée les données pour les règles que vous avez définies à l'aide d' AWS Config, ce qui vous permet de vérifier la conformité de vos charges de travail et de réagir rapidement aux modifications. AWS CloudFormation StackSets permet de gérer de manière centralisée les piles AWS CloudFormation dans votre organisation dans plusieurs comptes et unités d'organisation. Cela vous permet de mettre automatiquement en service un nouveau compte pour répondre à vos exigences de sécurité.

Utilisez la fonction de délégation de l'administration des services de sécurité pour séparer les comptes utilisés pour la gestion du compte de facturation (compte de gestion) de l'organisation. Plusieurs services AWS, tels que GuardDuty, Security Hub et AWS Config, prennent en charge les intégrations avec les organisations AWS, y compris la désignation d'un compte spécifique pour les fonctions administratives.

Bonnes pratiques

- SEC01-BP01 Séparer les charges de travail à l'aide de comptes
- SEC01-BP02 Sécuriser l'utilisateur root et les propriétés du compte

SEC01-BP01 Séparer les charges de travail à l'aide de comptes

Établissez des barrières de protection et un isolement communs entre les environnements (par exemple, production, développement et test) et les charges de travail grâce à une stratégie

multicompte. La séparation au niveau des comptes est vivement recommandée, car elle fournit une solide limite d'isolement pour la sécurité, la facturation et les accès.

Résultat souhaité : une structure de compte qui isole les opérations cloud, les charges de travail non liées et les environnements dans des comptes séparés, ce qui permet de renforcer la sécurité dans l'infrastructure cloud.

Anti-modèles courants :

- Placer plusieurs charges de travail non liées avec différents niveaux de sensibilité des données dans le même compte.
- Structure d'unité d'organisation mal définie.

Avantages liés à l'instauration de cette bonne pratique :

- Réduction de la portée des répercussions si un utilisateur accède à une charge de travail par inadvertance.
- Gouvernance centralisée des services, ressources et régions AWS.
- Maintien de la sécurité de l'infrastructure cloud avec des politiques et une administration centralisée des services de sécurité.
- Processus automatisé de création et de gestion des comptes.
- Audit centralisé de votre infrastructure pour les exigences en matière de conformité et de réglementation.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Les Comptes AWS établissent une limite d'isolement de sécurité entre les charges de travail ou les ressources qui fonctionnent à différents niveaux de sensibilité. AWS fournit des outils permettant de gérer vos charges de travail cloud à grande échelle grâce à une stratégie multicompte pour tirer parti de cette limite d'isolement. Pour obtenir des conseils sur les concepts, les modèles et l'implémentation d'une stratégie multicompte sur AWS, consultez Organizing Your AWS Environment Using Multiple Accounts (Organisation de votre environnement AWS à l'aide de plusieurs comptes).

Lorsque plusieurs Comptes AWS sont gérés de façon centralisée, ils doivent être organisés selon une hiérarchie définie par des couches d'unités d'organisation. Les contrôles de sécurité peuvent

ensuite être organisés et appliqués aux unités d'organisation et aux comptes membres, ce qui permet d'établir des contrôles préventifs uniformes sur les comptes membres au sein de l'organisation. Les contrôles de sécurité sont hérités, vous pouvez donc filtrer les autorisations disponibles pour les comptes membres situés aux niveaux inférieurs d'une hiérarchie d'unités d'organisation. Une bonne conception tire parti de cet héritage pour réduire le nombre et la complexité des politiques de sécurité nécessaires afin de mettre en place les contrôles de sécurité souhaités pour chaque compte membre.

Les services AWS Organizations et AWS Control Tower peuvent être utilisés pour implémenter et gérer cette structure multicompte dans votre environnement AWS. AWS Organizations vous permet d'organiser les comptes dans une hiérarchie définie par une ou plusieurs couches d'unités d'organisation, chacune de ces dernières contenant un certain nombre de comptes membres. Les politiques de contrôle des services (SCP) permettent à l'administrateur de l'organisation d'établir des contrôles préventifs granulaires sur les comptes membres et AWS Config peut être utilisé pour établir des contrôles proactifs et de détection sur les comptes membres. Un grand nombre de services AWS s'intègrent à AWS Organizations pour fournir des contrôles administratifs délégués et effectuer des tâches propres aux services dans tous les comptes membres de l'organisation.

Ajouté au-dessus d'AWS Organizations, AWS Control Tower fournit une configuration en un clic des bonnes pratiques pour un environnement AWS multicompte avec une zone de destination. La zone de destination est le point d'entrée de l'environnement multicompte établi par Control Tower. Control Tower offre plusieurs avantages par rapport à AWS Organizations. Les trois avantages qui permettent d'améliorer la gouvernance des comptes sont les suivants :

- Des barrières de protection obligatoires intégrées qui sont automatiquement appliquées aux comptes admis dans l'organisation.
- Des barrières de protection facultatives qui peuvent être activées ou désactivées pour un ensemble donné d'unités d'organisation.
- AWS Control Tower Account Factory fournit un déploiement automatisé des comptes contenant des bases de référence préapprouvées et des options de configuration au sein de votre organisation.

Étapes d'implémentation

1. Concevez une structure d'unités d'organisation : une structure d'unités d'organisation bien conçue réduit la charge de gestion liée à la création et à l'application des politiques de contrôle des services et d'autres contrôles de sécurité. Votre structure d'unités d'organisation doit être alignée sur les besoins opérationnels, la sensibilité des données et la structure des charges de travail.

2. Créez une zone de destination pour votre environnement multicompte : une zone de destination fournit une base cohérente de sécurité et d'infrastructure à partir de laquelle votre organisation peut rapidement développer, lancer et déployer des charges de travail. Vous pouvez utiliser une zone de destination personnalisée ou AWS Control Tower pour orchestrer votre environnement.
3. Établissez des barrières de protection : implémentez des barrières de protection de sécurité uniformes pour votre environnement dans votre zone de destination. AWS Control Tower fournit une liste de contrôles obligatoires et facultatifs qui peuvent être déployés. Les contrôles obligatoires sont déployés automatiquement lors de l'implémentation de Control Tower. Passez en revue la liste des contrôles hautement recommandés et facultatifs, puis implémentez les contrôles adaptés à vos besoins.
4. Limitez l'accès aux régions qui viennent d'être ajoutées : pour les nouvelles Régions AWS, les ressources IAM telles que les utilisateurs et les rôles sont uniquement propagées vers les régions que vous spécifiez. Cette action peut être effectuée via la console lorsque vous utilisez Control Tower ou en modifiant les politiques d'autorisations IAM dans AWS Organizations.
5. Envisagez l'utilisation d'AWS CloudFormation StackSets : les StackSets vous permettent de déployer des ressources, dont les politiques, rôles et groupes IAM dans différentes régions et différents Comptes AWS à partir d'un modèle approuvé.

Ressources

Bonnes pratiques associées :

- SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé

Documents connexes :

- AWS Control Tower
- AWS Security Audit Guidelines (Consignes pour les audits de sécurité AWS)
- Bonnes pratiques dans IAM
- Use CloudFormation StackSets to provision resources across multiple Comptes AWS and regions (Utiliser CloudFormation StackSets pour provisionner les ressources sur plusieurs comptes et régions AWS)
- FAQ sur AWS Organizations
- Terminologie et concepts relatifs à AWS Organizations

- Best Practices for Service Control Policies in an AWS Organizations Multi-Account Environment (Bonnes pratiques pour les politiques de contrôle des services d'AWS Organizations dans un environnement multicompte)
- AWS Account Management Reference Guide (Guide de référence de la gestion des comptes AWS)
- Organizing Your AWS Environment Using Multiple Accounts (Organisation de votre environnement AWS à l'aide de plusieurs comptes)

Vidéos connexes :

- Enable AWS adoption at scale with automation and governance
- Security Best Practices the Well-Architected Way
- Building and Governing Multiple Accounts using AWS Control Tower
- Enable Control Tower for Existing Organizations

Ateliers connexes :

- Journée d'immersion Control Tower

SEC01-BP02 Sécuriser l'utilisateur root et les propriétés du compte

L'utilisateur root est celui qui dispose du plus de privilèges dans un Compte AWS, avec un accès administratif complet à toutes les ressources du compte. De plus, dans certains cas, il ne peut pas être limité par les politiques de sécurité. Si vous désactivez l'accès par programmation pour l'utilisateur root, établissez des contrôles appropriés pour l'utilisateur root et évitez l'utilisation de routine de l'utilisateur root, vous réduirez le risque d'exposition accidentelle des informations d'identification root et de compromission ultérieure de l'environnement cloud.

Résultat souhaité : la sécurisation de l'utilisateur root permet de réduire les risques de dommages accidentels ou intentionnels en raison de l'utilisation inappropriée des informations d'identification de l'utilisateur root. La mise en place de contrôles de détection permet également d'alerter le personnel approprié lorsque des mesures sont prises à l'aide de l'utilisateur root.

Anti-modèles courants :

- Se servir de l'utilisateur root pour des tâches autres que celles nécessitant des informations d'identification de l'utilisateur root.

- Omettre de tester régulièrement des plans d'urgence pour vérifier le fonctionnement de l'infrastructure, des processus et du personnel essentiels dans les situations d'urgence.
- Ne tenir compte que du flux de connexion type du compte et omettre d'envisager ou de tester d'autres méthodes de récupération de compte.
- Ne pas gérer les DNS, les serveurs de messagerie et les fournisseurs de services téléphoniques dans le cadre du périmètre de sécurité critique, car ils sont utilisés dans le flux de récupération de compte.

Avantages liés à l'instauration de cette bonne pratique : la sécurisation de l'accès à l'utilisateur root permet de garantir le contrôle et la vérification des actions effectuées dans votre compte.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

AWS propose plusieurs outils afin de vous aider à sécuriser votre compte. Toutefois, étant donné que certaines de ces mesures ne sont pas activées par défaut, vous devez intervenir directement pour les implémenter. Considérez ces recommandations comme des étapes fondamentales pour sécuriser votre Compte AWS. À mesure que vous mettez en œuvre ces étapes, il est important d'établir un processus permettant d'évaluer et de surveiller continuellement les contrôles de sécurité.

Lorsque vous créez un compte Compte AWS, vous commencez avec une seule identité disposant d'un accès complet à toutes les ressources et à tous les services AWS de ce compte. Cette identité est appelée l'utilisateur root du Compte AWS. Vous pouvez vous connecter en tant qu'utilisateur root en utilisant l'adresse e-mail et le mot de passe utilisés pour créer le compte. En raison de l'accès élevé accordé à l'utilisateur root AWS, vous devez limiter l'utilisation de cet utilisateur root AWS à l'exécution de tâches qui en ont spécifiquement besoin. Les informations d'identification de l'utilisateur root doivent être étroitement protégées et l'authentification multifactorielle (MFA) doit toujours être activée pour l'utilisateur root du Compte AWS.

Outre le flux d'authentification normal pour vous connecter à votre utilisateur root en utilisant un nom d'utilisateur, un mot de passe et un dispositif d'authentification multifactorielle (MFA), il y a des flux de récupération de compte pour vous connecter à l'utilisateur root de votre Compte AWS, à condition de disposer d'un accès à l'adresse e-mail et au numéro de téléphone associés à votre compte. Par conséquent, il est tout aussi important de sécuriser le compte de messagerie de l'utilisateur root là où l'e-mail de récupération est envoyé, ainsi que le numéro de téléphone associé au compte. Il est également nécessaire de tenir compte des dépendances circulaires possibles lorsque l'adresse e-

mail associée à l'utilisateur root est hébergée sur des serveurs de messagerie ou des ressources du service de noms de domaine (DNS) à partir du même Compte AWS.

Lorsque vous utilisez AWS Organizations, il y a plusieurs Comptes AWS, chacun d'entre eux ayant un utilisateur root. Un compte est désigné comme compte de gestion et plusieurs couches de comptes membres peuvent alors être ajoutées sous le compte de gestion. Privilégiez la sécurisation de l'utilisateur root de votre compte de gestion, puis occupez-vous des utilisateurs root des comptes membres. La stratégie de sécurisation de l'utilisateur root de votre compte de gestion peut différer de celle des utilisateurs root des comptes membres et vous pouvez placer des contrôles de sécurité préventifs sur les utilisateurs root des comptes membres.

Étapes d'implémentation

Les étapes d'implémentation suivantes sont recommandées afin d'établir des contrôles pour l'utilisateur root. Le cas échéant, les recommandations comportent des renvois vers les contrôles de référence CIS AWS Foundations version 1.4.0. Outre ces étapes, consultez Consignes en matière de bonnes pratiques avec AWS pour sécuriser vos ressources et votre Compte AWS.

Contrôles préventifs

1. Configurez des coordonnées exactes pour le compte.
    a. Ces informations sont utilisées pour le flux de récupération de mot de passe perdu, le flux de récupération de compte d'authentification multifactorielle perdu et pour les communications critiques liées à la sécurité avec votre équipe.
    b. Utilisez une adresse e-mail hébergée par votre domaine d'entreprise, de préférence une liste de distribution, comme adresse e-mail de l'utilisateur root. L'utilisation d'une liste de distribution plutôt que d'un compte de messagerie individuel fournit une redondance et une continuité supplémentaires pour l'accès au compte root sur de longues périodes.
    c. Le numéro de téléphone indiqué pour les coordonnées doit correspondre à un téléphone dédié et sécurisé à cette fin. Ce numéro de téléphone ne doit figurer sur aucune liste ni être communiqué à personne.
2. Ne créez pas de clés d'accès pour l'utilisateur root. Si des clés d'accès existent, retirez-les (CIS 1.4).
    a. Éliminez les informations d'identification par programmation de longue durée (clés d'accès et secrètes) pour l'utilisateur root.
    b. S'il existe déjà des clés d'accès pour l'utilisateur root, vous devez effectuer la transition des processus en utilisant ces clés afin de vous servir de clés d'accès temporaires issues d'un rôle

AWS Identity and Access Management (IAM), puis supprimer les clés d'accès de l'utilisateur root.

3. Déterminez si vous devez stocker les informations d'identification de l'utilisateur root.
   a. Si vous utilisez AWS Organizations pour créer de nouveaux comptes membres, le mot de passe initial pour l'utilisateur root sur ces nouveaux comptes est une valeur aléatoire à laquelle vous n'avez pas accès. Envisagez d'utiliser le flux de réinitialisation du mot de passe à partir de votre compte de gestion AWS Organization pour accéder au compte membre si nécessaire.
   b. Pour les Comptes AWS autonomes ou le compte de gestion AWS Organization, envisagez de créer et de stocker en toute sécurité les informations d'identification de l'utilisateur root. Activez l'authentification multifactorielle pour l'utilisateur root.
4. Activez les contrôles préventifs pour les utilisateurs root des comptes membres dans les environnements AWS multicomptes.
   a. Envisagez d'activer la barrière de protection préventive Désactiver la création des clés d'accès root pour l'utilisateur root pour les comptes membres.
   b. Envisagez d'activer la barrière de protection préventive Désactiver les actions en tant qu'utilisateur root pour les comptes membres.
5. Si vous avez besoin d'informations d'identification pour l'utilisateur root :
   a. Utilisez un mot de passe complexe.
   b. Activez l'authentification multifactorielle (MFA) pour l'utilisateur root, plus particulièrement pour les comptes de gestion (payeur) AWS Organizations (CIS 1.5).
   c. Envisagez l'utilisation des appareils d'authentification multifactorielle pour la résilience et la sécurité, car les appareils à usage unique peuvent réduire les risques de réutilisation des appareils contenant vos codes d'authentification multifactorielle à d'autres fins. Vérifiez que les appareils d'authentification multifactorielle alimentés par une batterie sont remplacés régulièrement. (CIS 1.6)
      - Si vous souhaitez configurer l'authentification multifactorielle pour l'utilisateur root, suivez les instructions d'activation d'une authentification multifactorielle virtuelle ou d'un appareil d'authentification multifactorielle.
   d. Envisagez d'inscrire plusieurs appareils d'authentification multifactorielle pour la sauvegarde. Jusqu'à 8 appareils d'authentification multifactorielle sont autorisés par compte.
      - Notez que l'inscription de plusieurs appareils d'authentification multifactorielle pour l'utilisateur root désactive automatiquement le flux de récupération de votre compte si l'appareil d'authentification multifactorielle est perdu.

e. Stockez le mot de passe en sécurité et tenez compte des dépendances circulaires si vous le stockez électroniquement. Ne stockez pas le mot de passe de manière à ce qu'il nécessite un accès au même Compte AWS pour l'obtenir.

6. Facultatif : envisagez d'établir un calendrier périodique de rotation des mots de passe pour l'utilisateur root.
   - Les bonnes pratiques relatives à la gestion des informations d'identification dépendent de vos exigences en matière de réglementation et de politiques. Les utilisateurs root protégés par l'authentification multifactorielle ne dépendent pas du mot de passe comme facteur d'authentification unique.
   - La modification périodique du mot de passe de l'utilisateur root réduit le risque d'utilisation inappropriée d'un mot de passe exposé par inadvertance.

Contrôles de détection

- Créez des alarmes pour détecter l'utilisation des informations d'identification root (CIS 1.7). L'activation d'Amazon GuardDuty permettra de surveiller et d'alerter sur l'utilisation des informations d'identification de l'API de l'utilisateur root via la recherche RootCredentialUsage.
- Évaluez et implémentez les contrôles de détection inclus dans le pack de conformité du pilier Sécurité AWS Well-Architected pour AWS Config ou, si vous utilisez AWS Control Tower, les contrôles vivement recommandés disponibles dans Control Tower.

Conseils opérationnels

- Déterminez qui, au sein de l'organisation, doit avoir accès aux informations d'identification de l'utilisateur root.
  - Utilisez la règle des deux personnes pour éviter qu'une seule personne ait accès à toutes les informations d'identification et à l'authentification multifactorielle nécessaires pour obtenir l'accès à l'utilisateur root.
  - Vérifiez que l'organisation, et non une seule personne, conserve le contrôle du numéro de téléphone et de l'alias d'e-mail associés au compte (qui sont utilisés pour la réinitialisation du mot de passe et l'authentification multifactorielle).
- Utilisez l'utilisateur root uniquement de façon exceptionnelle (CIS 1.7).
  - L'utilisateur root AWS ne doit pas être employé pour des tâches quotidiennes, même les tâches d'administration. Connectez-vous en tant qu'utilisateur root uniquement pour effectuer des

tâches AWS qui requièrent l'utilisateur root. Toutes les autres actions doivent être effectuées par d'autres utilisateurs assumant les rôles appropriés.

- Vérifiez régulièrement que l'accès à l'utilisateur root fonctionne afin que les procédures soient testées avant une situation d'urgence nécessitant l'utilisation des informations d'identification de l'utilisateur root.
- Vérifiez régulièrement que l'adresse e-mail associée au compte et les adresses répertoriées sous Autres contacts fonctionnent. Vérifiez dans ces boîtes de réception si vous avez reçu des notifications de sécurité de la part de `<abuse@amazon.com>`. Assurez-vous également que les numéros de téléphone associés au compte fonctionnent.
- Préparez les procédures d'intervention en cas d'incident pour réagir face à une utilisation inappropriée du compte root. Consultez le guide AWS Security Incident Response Guide (Guide d'intervention en cas d'incident de sécurité) et les bonnes pratiques dans la section sur le pilier Sécurité du livre blanc consacré aux réponses face aux incidents pour plus d'informations sur l'élaboration d'une stratégie de réponse face aux incidents pour votre Compte AWS.

Ressources

Bonnes pratiques associées :

- SEC01-BP01 Séparer les charges de travail à l'aide de comptes
- SEC02-BP01 Utiliser de solides mécanismes d'authentification
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège
- SEC03-BP03 Établir un processus d'accès d'urgence
- SEC10-BP05 Préallouer les accès

Documents connexes :

- AWS Control Tower
- AWS Security Audit Guidelines (Consignes pour les audits de sécurité AWS)
- Bonnes pratiques dans IAM
- Amazon GuardDuty – root credential usage alert (Alerte d'utilisation des informations d'identification root)
- Step-by-step guidance on monitoring for root credential use through CloudTrail (Conseils étape par étape sur la surveillance de l'utilisation des informations d'identification root via Control Tower)

- MFA tokens approved for use with AWS (Jetons d'authentification multifactorielle approuvés pour une utilisation avec AWS)
- Implementing break glass access on AWS
- Top 10 security items to improve in your Compte AWS
- Que faire si je remarque une activité non autorisée dans mon Compte AWS ?

Vidéos connexes :

- Enable AWS adoption at scale with automation and governance
- Bonnes pratiques de sécurité : une approche Well-Architected
- Limitation de l'utilisation des AWS informations d'identification root de AWS re:inforce 2022 – Bonnes pratiques de sécurité avec AWS IAM

Exemples et ateliers connexes :

- Atelier : Compte AWS and root user

Gestion sécurisée de votre charge de travail

La gestion sécurisée de votre charge de travail couvre en toute sécurité l'ensemble du cycle de vie d'une charge de travail, de la conception à l'amélioration continue, en passant par la construction et l'exécution. L'une des façons d'améliorer votre capacité à opérer en toute sécurité dans le cloud consiste à adopter une approche organisationnelle de la gouvernance. La gouvernance est la façon dont les décisions sont guidées en permanence sans dépendre uniquement du bon jugement des personnes impliquées. Le modèle et le processus de gouvernance sont la façon dont vous déterminer comment savoir que les objectifs de contrôle pour une charge de travail donnée sont atteints et sont appropriés pour cette charge de travail. Adopter une approche cohérente pour prendre des décisions accélère le déploiement des charges de travail et contribue à renforcer la sécurité dans votre organisation.

Vous devez appliquer de bonnes pratiques générales à chaque domaine de la sécurité pour réussir à gérer votre charge de travail en toute sécurité. Appliquez à tous les domaines les conditions et les processus que vous avez définis en matière d'excellence opérationnelle au niveau de l'organisation et de la charge de travail. La connaissance des recommandations actuelles d'AWS et du secteur ainsi que des renseignements sur les menaces vous aide à faire évoluer votre modèle de menace et vos

objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous permet de mettre à l'échelle vos opérations de sécurité.

L'automatisation permet la cohérence et la répétabilité des processus. Nous avons tous des talents multiples, mais répéter constamment la même action de la même manière et sans jamais faire d'erreurs n'en fait pas partie. Même avec les runbooks les plus précis, vous courez le risque que les utilisateurs n'exécutent pas les tâches répétitives de manière cohérente. Cela est particulièrement vrai lorsqu'ils ont des responsabilités diverses et qu'ils doivent répondre à des alertes inconnues. En revanche, l'automatisation répond de la même manière à chaque fois. L'automatisation est donc la meilleure façon de déployer des applications. Le code qui exécute le déploiement peut être testé, puis utilisé pour effectuer le déploiement. Cette approche renforce la confiance dans le processus de modification et limite le risque d'échec des modifications.

Pour vérifier que la configuration répond à vos objectifs de contrôle, testez d'abord l'automatisation et l'application déployée dans un environnement hors production. De cette façon, vous pouvez tester l'automatisation pour prouver qu'elle a suivi toutes les étapes correctement. Vous bénéficiez également d'un retour d'information précoce sur le cycle de développement et de déploiement, ce qui évite les retouches. Pour réduire les risques d'erreurs de déploiement, effectuez les modifications de configuration par programmation et non en faisant appel à des humains. Si vous avez besoin de redéployer une application, l'automatisation facilite le processus. Lorsque vous définissez des objectifs de contrôle supplémentaires, vous pouvez facilement les ajouter à l'automatisation pour toutes les charges de travail.

Au lieu de demander aux responsables de charge de travail individuels d'investir dans des options de sécurité spécifiques à leurs charges de travail, vous gagnez du temps en utilisant des fonctionnalités communes et des composants partagés. Parmi les exemples de services que plusieurs équipes peuvent utiliser, citons le processus de création de compte AWS, l'identité centralisée des personnes, la configuration de la journalisation commune et la création d'images de base d'AMI et de conteneur. Cette approche peut aider les concepteurs de builds à améliorer les temps de cycle de la charge de travail et à atteindre systématiquement les objectifs de contrôle de sécurité. Lorsque les équipes sont constantes, vous pouvez valider les objectifs de contrôle et faire part de votre niveau de contrôle et de votre niveau de risque aux parties prenantes avec plus de confiance.

Bonnes pratiques

- SEC01-BP03 Identifier et valider les objectifs de contrôle
- SEC01-BP04 Rester informé des menaces de sécurité
- SEC01-BP05 Connaître les recommandations de sécurité

- SEC01-BP06 Automatiser les tests et la validation des contrôles de sécurité dans les pipelines
- SEC01-BP07 Identifier les menaces et hiérarchiser les atténuations à l'aide d'un modèle de menaces
- SEC01-BP08 Évaluer et mettre en œuvre régulièrement de nouveaux services et de nouvelles fonctions de sécurité

SEC01-BP03 Identifier et valider les objectifs de contrôle

Fixez et validez les objectifs de contrôle et les contrôles que vous devez appliquer à votre charge de travail en fonction de vos exigences de conformité et des risques identifiés à partir de votre modèle de menace. La validation continue des objectifs de contrôle et des contrôles permet de mesurer l'efficacité de l'atténuation des risques.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Débit

Directives d'implémentation

- Identifier les exigences de conformité : découvrez les exigences organisationnelles, juridiques et de conformité que votre charge de travail doit nécessairement respecter.
- Identifier les ressources de conformité AWS : identifiez les ressources que propose AWS pour vous aider à rester conforme.
  - https://aws.amazon.com/compliance/
  - https://aws.amazon.com/artifact/

Ressources

Documents connexes :

- Directives d'audit de sécurité AWS
- Bulletins de sécurité

Vidéos connexes :

- AWS Security Hub : gérer les alertes de sécurité et automatiser la conformité
- Bonnes pratiques de sécurité : une approche Well-Architected

SEC01-BP04 Rester informé des menaces de sécurité

Identifiez les vecteurs d'attaque en restant informé des dernières menaces de sécurité afin de définir et de mettre en œuvre les contrôles appropriés. Utilisez AWS Managed Services pour faciliter la réception des notifications de comportement inattendu ou inhabituel dans vos comptes AWS. Réalisez vos investigations à l'aide d'outils partenaires AWS ou de flux d'informations sur les menaces tiers dans le cadre de votre flux d'informations de sécurité. La liste des vulnérabilités et risques communs (CVE) contient des vulnérabilités de cybersécurité divulguées publiquement, que vous pouvez utiliser pour rester à jour.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Débit

Directives d'implémentation

- S'abonner aux sources d'informations sur les menaces : consultez régulièrement les informations sur les menaces issues de plusieurs sources spécifiques aux technologies utilisées dans votre charge de travail.
  - Liste des vulnérabilités et risques communs (CVE)
- Envisager le service AWS Shield Advanced : offre une visibilité quasiment en temps réel sur les sources d'informations si votre charge de travail est accessible sur Internet.

Ressources

Documents connexes :

- Directives d'audit de sécurité AWS
- AWS Shield
- Bulletins de sécurité

Vidéos connexes :

- Bonnes pratiques de sécurité : une approche Well-Architected

SEC01-BP05 Connaître les recommandations de sécurité

Tenez-vous au courant des recommandations AWS et des recommandations de sécurité pertinentes pour faire évoluer le niveau de sécurité de votre charge de travail. Les bulletins de sécurité AWS contiennent des informations importantes sur les notifications de sécurité et de confidentialité.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Débit

Directives d'implémentation

- Suivre l'actualité AWS : abonnez-vous ou consultez régulièrement les nouvelles recommandations, ainsi que les conseils et astuces.
  - Ateliers AWS Well-Architected
  - Blog sur la sécurité AWS
  - Documentation des services AWS
- S'abonner aux sources d'actualité sur le secteur : consultez régulièrement les flux d'actualités issus de plusieurs sources pertinentes pour les technologies qui sont utilisées dans votre charge de travail.
  - Exemple : liste des vulnérabilités et risques communs (CVE)

Ressources

Documents connexes :

- Bulletins de sécurité

Vidéos connexes :

- Bonnes pratiques de sécurité : une approche Well-Architected

SEC01-BP06 Automatiser les tests et la validation des contrôles de sécurité dans les pipelines

Établissez des bases et des modèles sécurisés pour les mécanismes de sécurité qui sont testés et validés dans le cadre de votre version, de vos pipelines et de vos processus. Utilisez des outils et l'automatisation pour tester et valider en continu tous les contrôles de sécurité. Par exemple,

analysez des éléments tels que les images machine et les modèles d'infrastructure en tant que de code pour détecter les failles, les irrégularités et les dérives de sécurité par rapport à des points de référence établis à chaque étape. AWS CloudFormation Guard permet de vérifier que les modèles CloudFormation sont sûrs, vous font gagner du temps et réduisent le risque d'erreur de configuration.

Il est essentiel de réduire le nombre d'erreurs de configuration de sécurité introduites dans un environnement de production : plus vous contrôlez la qualité et réduisez les défauts dans le processus de génération, mieux c'est. Concevez des pipelines d'intégration et de déploiement continus (CI/CD, continuous integration and continuous deployment) pour tester la sécurité dans la mesure du possible. Les pipelines CI/CD offrent la possibilité d'améliorer la sécurité à chaque étape de la création et de la distribution. Les outils de sécurité CI/CD doivent être également maintenus à jour pour atténuer l'évolution des menaces.

Suivez les modifications apportées à la configuration de votre charge de travail pour faciliter les audits de conformité, la gestion des modifications et les enquêtes susceptibles de vous concerner. Vous pouvez utiliser AWS Config pour enregistrer et évaluer vos ressources AWS et tierces. Il vous permet d'auditer et d'évaluer en continu la conformité globale avec les règles et les packs de conformité, qui sont des ensembles de règles avec des actions correctives.

Le suivi des modifications doit inclure les modifications planifiées, qui font partie du processus de contrôle des modifications de votre organisation (parfois appelé MACD), les modifications non planifiées et les modifications inattendues, telles que les incidents. Des modifications peuvent se produire sur l'infrastructure, mais elles peuvent également être liées à d'autres catégories, telles que des changements dans les référentiels de code, des modifications au niveau des images machine et de l'inventaire d'applications, des modifications de processus et de politique ou des modifications de documentation.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

- Automatiser la gestion de la configuration : appliquez et validez des configurations sécurisées automatiquement à l'aide d'un service ou d'un outil de gestion de la configuration.
  - AWS Systems Manager
  - AWS CloudFormation
  - Configuration d'un pipeline CI/CD sur AWS

Ressources

Documents connexes :

- Comment utiliser des politiques de contrôle des services pour définir des protections par autorisation dans les comptes de votre organisation AWS

Vidéos connexes :

- Managing Multi-Account AWS Environments Using AWS Organizations
- Bonnes pratiques de sécurité : une approche Well-Architected

SEC01-BP07 Identifier les menaces et hiérarchiser les atténuations à l'aide d'un modèle de menaces

Effectuez une modélisation des menaces pour identifier et gérer un registre actualisé des menaces potentielles et des mesures d'atténuation connexes pour votre charge de travail. Hiérarchisez vos menaces et adaptez vos atténuations des contrôles de sécurité pour les prévenir, les détecter et y répondre. Ajustez et maintenez ces mesures en fonction de votre charge de travail et de l'évolution de l'environnement de sécurité.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Qu'est-ce que la modélisation des menaces ?

« La modélisation des menaces permet d'identifier, de communiquer et de comprendre les menaces et les atténuations dans le contexte de la protection de quelque chose de valeur. » – The Open Web Application Security Project (OWASP) Application Threat Modeling

Quel est l'intérêt de la modélisation des menaces ?

Les systèmes sont complexes et deviennent de plus en plus complexes et compétents au fil du temps, offrant plus de valeur opérationnelle, ainsi qu'une satisfaction et un engagement client accrus. Cela signifie que les décisions de conception informatique doivent tenir compte d'un nombre toujours croissant de cas d'utilisation. Cette complexité et ce nombre de permutations des cas d'utilisation nuisent généralement à l'efficacité des approches non structurées pour trouver et atténuer les menaces. Dans ces conditions, il est préférable d'adopter une approche systématique pour recenser

les menaces potentielles qui pèsent sur le système, concevoir les atténuations et d'établir la priorité de ces atténuations afin de veiller à ce que les ressources limitées de votre organisation aient un impact maximal sur l'amélioration de la posture de sécurité globale du système.

La modélisation des menaces est conçue pour fournir cette approche systématique, dans le but de trouver et de régler les problèmes au début du processus de conception, lorsque les atténuations impliquent un coût relatif et des efforts limités par rapport à plus tard dans le cycle de vie. Cette approche est conforme au principe de sécurité shift left. Au final, la modélisation des menaces s'intègre au processus de gestion des risques d'une organisation et aide à prendre des décisions sur les contrôles à mettre en œuvre en utilisant une approche axée sur les menaces.

Quand la modélisation des menaces doit-elle être effectuée ?

Commencez la modélisation des menaces le plus tôt possible dans le cycle de vie de votre charge de travail, afin de bénéficier de plus de flexibilité pour la gestion des menaces identifiées. Comme pour les bogues logiciels, plus vous identifiez les menaces rapidement, plus leur résolution est économique. Un modèle de menace est un document évolutif et il doit continuer à évoluer avec vos charges de travail. Revoyez vos modèles de menaces au fil du temps, y compris lorsqu'il y a un changement majeur, une évolution du contexte des menaces ou lorsque vous adoptez une nouvelle fonctionnalité ou un nouveau service.

Étapes d'implémentation

Comment pouvons-nous modéliser les menaces ?

Il existe de nombreuses façons de modéliser les menaces. Comme pour les langages de programmation, chaque méthode a ses avantages et ses inconvénients. À vous de choisir celle qui fonctionne le mieux pour votre organisation. Une approche consiste à commencer par le cadre des 4 questions de Shostack pour la modélisation des menaces, qui pose des questions ouvertes afin de structurer votre exercice de modélisation des menaces :

1. Sur quoi travaillons-nous ?

   Le but de cette question est de vous aider à comprendre et à vous mettre d'accord sur le système que vous créez et les détails associés qui sont pertinents pour la sécurité. La création d'un modèle ou d'un diagramme est la solution la plus populaire pour répondre à cette question, car elle vous aide à visualiser ce que vous créez, par exemple en utilisant un diagramme de flux des données. Le fait de noter les hypothèses et les détails importants sur votre système vous aide également à définir ce qui est inclus dans le champ d'application. Cela permet à tous ceux qui contribuent au modèle de menaces de se concentrer sur la même chose et d'éviter les détours

fastidieux pour étudier des sujets qui ne rentrent pas dans le champ d'application (y compris les versions obsolètes de votre système). Par exemple, si vous créez une application web, il n'est probablement pas intéressant de consacrer du temps à la modélisation de la séquence de démarrage autorisé du système d'exploitation pour les clients du navigateur, car vous ne pouvez pas avoir un impact sur ce point avec votre conception.

2. Quels problèmes pouvez-vous rencontrer ?

   C'est là que vous identifiez les menaces qui pèsent sur votre système. Les menaces sont des actions ou des événements accidentels ou intentionnels qui ont des impacts indésirables et pourraient affecter la sécurité de votre système. Sans une compréhension claire de ce qui pourrait poser un problème, vous n'avez aucun moyen de faire quoi que ce soit.

   Il n'existe pas de liste standard des problèmes potentiels. La création de cette liste nécessite un brainstorming et une collaboration entre tous les membres de votre équipe et les décideurs pertinents impliqués dans l'exercice de modélisation des menaces. Vous pouvez faciliter votre brainstorming en utilisant un modèle pour identifier les menaces, par exemple STRIDE, qui suggère différentes catégories à évaluer : Usurpation d'identité, Altération, Répudiation, Divulgation d'informations, Déni de service et Élévation de privilège. De plus, vous pouvez faciliter le brainstorming en examinant les listes et les recherches existantes afin de vous en inspirer, y compris l'OWASP Top 10, le HiTrust Threat Catalog, ainsi que le catalogue des menaces de votre organisation.

3. Qu'allons-nous faire à ce sujet ?

   Comme pour la question précédente, il n'existe pas de liste standard avec toutes les atténuations possibles. Lors de cette étape, les informations utilisées sont les menaces, les acteurs et les domaines d'amélioration identifiés par rapport à l'étape précédente.

   La sécurité et la conformité sont une responsabilité partagée entre vous et AWS. Il est important de comprendre que lorsque vous demandez « Qu'allons-nous faire à ce sujet ? », vous demandez également qui est responsable de ce qui doit être fait. En comprenant l'équilibre des responsabilités entre vous-même et AWS, vous pouvez évaluer votre exercice de modélisation des menaces en fonction des atténuations qui sont sous votre contrôle, c'est-à-dire, en règle générale, une combinaison des options de configuration du service AWS et vos propres atténuations spécifiques au système.

   Pour la partie AWS de la responsabilité partagée, vous constaterez que les services AWS sont couverts par de nombreux programmes de conformité. Ces programmes vous aident à comprendre les contrôles rigoureux en place chez AWS afin de garantir la sécurité et la conformité

du cloud. Les rapports d'audit de ces programmes peuvent être téléchargés pour les clients AWS à partir d'AWS Artifact.

Quels que soient les services AWS utilisés, il y a toujours un élément de responsabilité client et les atténuations correspondant à ces responsabilités doivent être incluses dans votre modèle de menaces. En ce qui concerne les atténuations en matière de contrôle de sécurité pour les services AWS eux-mêmes, envisagez l'implémentation de contrôles de sécurité dans tous les domaines, y compris la gestion des identités et des accès (authentification et autorisation), la protection des données (au repos et en transit), la sécurité de l'infrastructure, la journalisation et la surveillance. La documentation de chaque service AWS comporte un chapitre dédié à la sécurité qui fournit des conseils sur les contrôles de sécurité à implémenter à des fins d'atténuation. Il est surtout important de réfléchir au code que vous écrivez et à ses dépendances, ainsi que de penser aux contrôles que vous pourriez mettre en place pour résoudre ces menaces. Ces contrôles peuvent notamment prendre les formes suivantes : validation des entrées, gestion des sessions et gestion des limites. La plupart des vulnérabilités sont souvent introduites dans le code personnalisé, c'est pourquoi il est important de se concentrer sur ce domaine.

4. Avons-nous fait du bon travail ?

   L'objectif est que votre équipe et votre organisation améliorent la qualité des modèles de menaces et la vitesse à laquelle vous effectuez la modélisation des menaces au fil du temps. Ces améliorations découlent d'une combinaison de pratique, d'apprentissage, d'enseignement et de révision. Pour approfondir ces notions et vous exercer, votre équipe et vous-même pouvez suivre le cours de formation ou l'atelier sur les bons principes de modélisation des menaces pour les créateurs. De plus, si vous souhaitez obtenir des conseils sur l'intégration de la modélisation des menaces dans le cycle de développement des applications de votre organisation, consultez la publication How to approach threat modeling sur le Blog de sécurité d'AWS.

Threat Composer

Pour vous aider et vous guider dans la modélisation des menaces, pensez à utiliser l'outil Threat Composer, qui vise à réduire le délai de modélisation des menaces. L'outil vous permet d'effectuer les opérations suivantes :

- Rédiger des déclarations de menaces utiles, qui respectent la grammaire des menaces et fonctionnent dans un flux de travail naturel et non linéaire
- Générer un modèle de menaces lisible par l'homme

- Générer un modèle de menaces lisible par machine pour vous permettre de traiter les modèles de menaces comme du code
- Identifier rapidement les domaines dans lesquels la qualité et la couverture peuvent être améliorées à l'aide du tableau de bord

Pour en savoir plus, accédez à Threat Composer et basculez vers l'exemple d'espace de travail défini par le système.

Ressources

Bonnes pratiques associées :

- SEC01-BP03 Identifier et valider les objectifs de contrôle
- SEC01-BP04 Rester informé des menaces de sécurité
- SEC01-BP05 Connaître les recommandations de sécurité
- SEC01-BP08 Évaluer et mettre en œuvre régulièrement de nouveaux services et de nouvelles fonctions de sécurité

Documents connexes :

- How to approach threat modeling (AWS Security Blog)
- NIST: Guide to Data-Centric System Threat Modelling

Vidéos connexes :

- AWS Summit ANZ 2021 - How to approach threat modelling
- AWS Summit ANZ 2022 - Scaling security – Optimise for fast and secure delivery

Formations associées :

- Threat modeling the right way for builders – AWS Skill Builder virtual self-paced training
- Threat modeling the right way for builders – AWS Workshop

Outils associés :

- Threat Composer

SEC01-BP08 Évaluer et mettre en œuvre régulièrement de nouveaux services et de nouvelles fonctions de sécurité

Évaluez et mettez en œuvre les services et fonctions de sécurité proposés par AWS et les partenaires AWS qui vous permettent de faire évoluer le niveau de sécurité de votre charge de travail. Le blog sur la sécurité AWSmet en évidence les nouveaux services et fonctionnalités AWS, les guides de mise en œuvre et des conseils généraux de sécurité. Les nouveautés AWS représentent un excellent moyen de se tenir au courant de tous les nouveaux services, fonctionnalités et annonces AWS.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Planifier des vérifications régulières : créez un calendrier d'activités de révision qui inclut les exigences de conformité, l'évaluation des nouvelles fonctionnalités et des nouveaux services de sécurité AWS et des créneaux pour rester informé des actualités du secteur.
- Découvrir les services et fonctions AWS : découvrez les fonctions de sécurité qui sont disponibles pour les services que vous utilisez. Évaluez les nouvelles fonctions au fur et à mesure qu'elles sont publiées.
  - Blog sur la sécurité AWS
  - Bulletins de sécurité AWS
  - Documentation des services AWS
- Définir le processus d'intégration des services AWS : définissez les processus d'intégration des nouveaux services AWS. Incluez la manière d'évaluer le fonctionnement des nouveaux services AWS et les exigences en matière de conformité pour votre charge de travail.
- Tester les nouveaux services et les nouvelles fonctions : testez les nouveaux services et les nouvelles fonctions au fil de leur publication dans un environnement hors production qui réplique fidèlement votre environnement de production.
- Mettre en place d'autres mécanismes de défense : implémentez des mécanismes automatisés pour défendre votre charge de travail et explorez les options disponibles.
  - Correction des ressources AWS non conformes à l'aide de règles AWS Config Rules

Ressources

Vidéos connexes :

- Bonnes pratiques de sécurité : une approche Well-Architected

Identity and Access Management

Pour utiliser les services AWS, vous devez accorder à vos utilisateurs et applications l'accès aux ressources de vos comptes AWS. Au fur et à mesure que vous exécutez davantage de charges de travail sur AWS, vous devrez mettre en place une gestion d'identité et des autorisations solides pour garantir que les bonnes personnes ont accès aux bonnes ressources dans les bonnes conditions. AWS propose un large choix de fonctionnalités pour vous aider à gérer vos identités humaines et machines, ainsi que leurs autorisations. Les bonnes pratiques concernant ces capacités se répartissent dans deux domaines principaux.

Rubriques

Gestion des identités

Il existe deux types d'identités à gérer dans le cadre de l'exploitation de charges de travail AWS sécurisées.

- Identités humaines : les administrateurs, développeurs, opérateurs et utilisateurs de vos applications ont besoin d'une identité pour accéder à vos environnements et application AWS. Il peut s'agir des membres de votre organisation ou des utilisateurs externes avec lesquels vous collaborez et qui interagissent avec vos ressources AWS via un navigateur Web, une application cliente, une application mobile ou des outils de ligne de commande interactifs.
- Identités de machines : vos applications de charge de travail, outils opérationnels et composants nécessitent une identité pour envoyer des demandes aux services AWS, par exemple pour lire des données. Ces identités comprennent des machines s'exécutant dans votre environnement AWS, telles que des instances Amazon EC2 ou des fonctions AWS Lambda. Vous pouvez également gérer les identités de machines pour les tiers qui ont besoin d'un accès. De plus, certaines machines en dehors d'AWS peuvent avoir besoin d'accéder à votre environnement AWS.

Bonnes pratiques

- SEC02-BP03 Stocker et utiliser des secrets en toute sécurité
- SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé
- SEC02-BP05 Contrôler et effectuer régulièrement une rotation des informations d'identification
- SEC02-BP06 Tirer parti des groupes d'utilisateurs et des attributs

SEC02-BP01 Utiliser de solides mécanismes d'authentification

Les connexions (authentification au moyen d'informations d'identification de connexion) peuvent présenter des risques lorsque l'on n'utilise pas des mécanismes tels que l'authentification multifactorielle (MFA), surtout dans les situations où les informations d'identification de connexion ont été divulguées par inadvertance ou peuvent être devinées facilement. Vous devez utiliser de solides mécanismes d'authentification pour réduire ces risques en exigeant l'authentification multifactorielle (MFA) et des politiques strictes de gestion des mots de passe.

Résultat souhaité : réduire les risques d'accès involontaire aux informations d'identification dans AWS en utilisant des mécanismes de connexion solides pour les utilisateurs AWS Identity and Access Management (IAM), l'utilisateur root Compte AWS, AWS IAM Identity Center (successeur d'AWS Single Sign-On [AWS SSO]), et les fournisseurs d'identité tiers. Cela signifie que vous devez exiger une authentification multifactorielle, appliquer des politiques strictes de gestion des mots de passe et détecter les comportements de connexion anormaux.

Anti-modèles courants :

- Ne pas appliquer de politique stricte de gestion des mots de passe pour vos identités, notamment des mots de passe complexes et l'authentification multifactorielle (MFA).
- Utiliser les mêmes informations d'identification pour différents utilisateurs.
- Ne pas utiliser de contrôles de détection pour les connexions suspectes.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Les identités humaines peuvent se connecter à AWS de plusieurs façons. Une bonne pratique AWS consiste à faire appel à un fournisseur d'identité centralisé utilisant la fédération (fédération directe ou AWS IAM Identity Center) lors de l'authentification auprès d'AWS. Dans ce cas, vous devez établir une connexion sécurisée avec votre fournisseur d'identité ou Microsoft Active Directory.

Lorsque vous ouvrez pour la première fois un Compte AWS, vous commencez avec un utilisateur root de Compte AWS. Vous devez utiliser uniquement l'utilisateur root du compte afin de configurer l'accès pour vos utilisateurs (et pour les tâches qui requièrent l'utilisateur root). Il est important d'activer l'authentification multifactorielle pour l'utilisateur root du compte immédiatement après l'ouverture de votre Compte AWS et de sécuriser l'utilisateur root en s'appuyant sur le Guide des bonnes pratiques AWS.

Si vous créez des utilisateurs dans AWS IAM Identity Center, sécurisez le processus de connexion dans ce service. Pour les identités des consommateurs, vous pouvez utiliser Amazon Cognito user pools et sécuriser le processus de connexion dans ce service, ou utiliser l'un des fournisseurs d'identité pris en charge par Amazon Cognito user pools.

Si vous employez des utilisateurs AWS Identity and Access Management (IAM), vous devez sécuriser le processus de connexion à l'aide d'IAM.

Quelle que soit la méthode de connexion, il est essentiel d'appliquer une politique de connexion rigoureuse.

Étapes d'implémentation

Voici des recommandations générales en matière de connexion. Les paramètres réels que vous configurez doivent être définis par votre politique d'entreprise ou utiliser une norme telle que NIST 800-63.

- Exigez l'authentification multifactorielle. Dans le cadre des bonnes pratiques IAM, il est recommandé d'exiger l'authentification multifactorielle pour les identités et les charges de travail humaines. L'activation de l'authentification multifactorielle fournit une couche de sécurité supplémentaire en exigeant que les utilisateurs fournissent des informations d'identification et un mot de passe unique (OTP) ou une chaîne de caractères générée et vérifiée cryptographiquement à partir d'un appareil physique.
- Mettez en place une longueur de mot de passe minimale, il s'agit d'un facteur essentiel pour garantir la force du mot de passe.
- Appliquez la complexité des mots de passe pour les rendre plus difficiles à deviner.
- Permettez aux utilisateurs de changer leurs propres mots de passe.
- Créez des identités individuelles plutôt que des informations d'identification partagées. En créant des identités individuelles, vous pouvez attribuer à chaque utilisateur un ensemble unique d'informations d'identification de sécurité. Les utilisateurs individuels offrent la possibilité d'auditer l'activité de chaque utilisateur.

Recommandations IAM Identity Center :

- IAM Identity Center fournit une politique de mot de passe prédéfinie lorsque vous utilisez le répertoire par défaut qui établit la longueur, la complexité et les exigences de réutilisation du mot de passe.
- Activez l'authentification multifactorielle et configurez le paramètre contextuel ou toujours activé pour l'authentification multifactorielle lorsque la source d'identité est le répertoire par défaut, AWS Managed Microsoft AD ou AD Connector.
- Autorisez les utilisateurs à enregistrer leurs propres appareils d'authentification multifactorielle (MFA).

Recommandations pour les répertoires Amazon Cognito user pools :

- Configurez les paramètres de force des mots de passe.
- Exigez l'authentification multifactorielle pour les utilisateurs.
- Utilisez les paramètres de sécurité avancés Amazon Cognito user pools pour les fonctionnalités telles que l'authentification adaptative qui peut bloquer les connexions suspectes.

Recommandations pour les utilisateurs IAM :

- Idéalement, vous utilisez IAM Identity Center ou la fédération directe. Cependant, vous aurez peut-être besoin d'utilisateurs IAM. Le cas échéant, définissez une politique de mot de passe pour les utilisateurs IAM. Vous pouvez utiliser la politique de gestion des mots de passe pour définir des exigences telles que la longueur minimale ou la nécessité d'utiliser des caractères non alphabétiques.
- Créez une politique IAM pour appliquer la connexion avec authentification multifactorielle afin que les utilisateurs puissent gérer leurs propres mots de passe et appareils d'authentification multifactorielle.

Ressources

Bonnes pratiques associées :

- SEC02-BP03 Stocker et utiliser des secrets en toute sécurité
- SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé
- SEC03-BP08 Partager des ressources en toute sécurité au sein de votre organisation

Documents connexes :

- AWS IAM Identity Center (successor to AWS Single Sign-On)
- Définition d'une politique de mot de passe du compte pour les utilisateurs IAM
- Utilisateur root Compte AWS
- Amazon Cognito password policy
- AWS Credentials (Informations d'identification AWS)
- Bonnes pratiques de sécurité dans IAM

Vidéos connexes :

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

SEC02-BP02 Utiliser des informations d'identification temporaires

Lors de tout type d'authentification, il est préférable d'utiliser des informations d'identification temporaires plutôt que des informations d'identification à long terme afin de réduire ou d'éliminer les risques, tels que la divulgation, le partage ou le vol des informations d'identification par inadvertance.

Résultat souhaité : réduire les risques liés aux informations d'identification à long terme, utiliser des informations d'identification temporaires dès que possible pour les identités humaines et machine. Les informations d'identification à long terme créent de nombreux risques, par exemple lorsqu'ils sont téléchargés dans du code dans des référentiels GitHub publics. En utilisant des informations d'identification temporaires, vous réduisez considérablement les risques de compromission de ces informations.

Anti-modèles courants :

- Les développeurs utilisent des clés d'accès à long terme issues des IAM users au lieu d'obtenir des informations d'identification temporaires de la CLI à l'aide de la fédération.
- Les développeurs intègrent des clés d'accès à long terme dans leur code et téléchargent ce code dans des référentiels Git publics.
- Les développeurs intègrent des clés d'accès à long terme dans les applications mobiles qui sont ensuite disponibles dans les boutiques d'applications.

- Les utilisateurs partagent des clés d'accès à long terme avec d'autres utilisateurs ou des employés quittent l'entreprise avec des clés d'accès à long terme toujours en leur possession.
- Utilisation des clés d'accès à long terme pour les identités machine lorsque des informations d'identification temporaires peuvent être utilisées.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Utilisez des informations d'identification de sécurité temporaires plutôt que des informations d'identification à long terme pour toutes les demandes d'API et de CLI AWS. Les demandes d'API et CLI transmises aux services AWS doivent, dans presque tous les cas, être signées en utilisant des clés d'accès AWS. Ces demandes peuvent être signées avec des informations d'identification temporaires ou à long terme. Le seul moment où vous devez utiliser des informations d'identification à long terme, également connues sous le nom de clés d'accès à long terme, est si vous employez un utilisateur IAM ou l'utilisateur root du Compte AWS. Lorsque vous fédérez sur AWS ou si vous assumez un rôle IAM via d'autres méthodes, des informations d'identification temporaires sont générées. Même lorsque vous accédez à la AWS Management Console à l'aide des informations d'identification de connexion, des informations d'identification temporaires sont gérées pour vous permettre d'appeler les services AWS. Vous avez rarement besoin d'informations d'identification à long terme et vous pouvez accomplir presque toutes les tâches en utilisant des informations d'identification temporaires.

Privilégiez les informations d'identification temporaires plutôt que les informations d'identification à long terme et, parallèlement, mettez en place une stratégie de réduction des utilisateurs IAM au profit de la fédération et des rôles IAM. Bien que les utilisateurs IAM aient été employés pour les identités humaines et machine dans le passé, nous recommandons désormais de ne plus procéder ainsi afin d'éviter les risques liés à l'utilisation de clés d'accès à long terme.

Étapes d'implémentation

Pour les identités humaines comme les employés, les administrateurs, les développeurs, les opérateurs et les clients :

- faites appel à un fournisseur d'identité centralisé et exigez des utilisateurs humains qu'ils se servent de la fédération avec un fournisseur d'identité pour accéder à AWS à l'aide d'informations d'identification temporaires. La fédération pour vos utilisateurs peut être mise en place soit avec une fédération directe à chaque Compte AWS, soit en utilisant AWS IAM Identity Center

(successeur d'AWS IAM Identity Center) et le fournisseur d'identité de votre choix. La fédération offre un certain nombre d'avantages par rapport aux utilisateurs IAM, outre l'élimination des informations d'identification à long terme. Les utilisateurs peuvent également demander des informations d'identification temporaires à partir de la ligne de commande pour une fédération directe ou en utilisant IAM Identity Center. Cela signifie que peu de cas d'utilisation nécessitent des utilisateurs IAM ou des informations d'identification à long terme pour vos utilisateurs.

- Lors de l'octroi d'accès aux ressources à des tiers, par exemple les fournisseurs de logiciels en tant que service (SaaS) dans votre Compte AWS, vous pouvez utiliser des rôles intercomptes et des politiques basées sur les ressources.
- Si vous devez accorder à des consommateurs ou des clients des autorisations d'accès à vos ressources AWS, vous pouvez utiliser des groupes d'identités Amazon Cognito ou Amazon Cognito user pools pour fournir des informations d'identification temporaires. Les autorisations pour les informations d'identification sont configurées via des rôles IAM. Vous pouvez également définir un rôle IAM distinct avec des autorisations limitées pour les utilisateurs invités qui ne sont pas authentifiés.

Pour les identités machine, vous devrez peut-être utiliser des informations d'identification à long terme. Le cas échéant, vous devez exiger que les charges de travail utilisent des informations d'identification temporaires avec des rôles IAM pour accéder à AWS.

- Pour Amazon Elastic Compute Cloud (Amazon EC2), vous pouvez utiliser des rôles pour Amazon EC2.

- AWS Lambda vous permet de configurer un rôle d'exécution Lambda afin d'octroyer au service les autorisations permettant d'effectuer des actions AWS en utilisant des informations d'identification temporaires. Il existe de nombreux modèles similaires pour permettre aux services AWS d'octroyer des informations d'identification temporaires à l'aide des rôles IAM.
- Pour les appareils IoT, vous pouvez utiliser le fournisseur d'informations d'identification AWS IoT Core afin de demander des informations d'identification temporaires.
- Pour les systèmes sur site ou les systèmes qui fonctionnent en dehors d'AWS et qui ont besoin d'accéder aux ressources AWS, vous pouvez utiliser IAM Roles Anywhere.

Dans certains cas, il est impossible d'utiliser des informations d'identification temporaires et vous devrez alors opter pour des informations d'identification à long terme. Le cas échéant, auditez et effectuez une rotation des informations d'identification périodiquement et effectuez une rotation des

clés d'accès régulièrement pour les cas d'utilisation qui requièrent des informations d'identification à long terme. Parmi les exemples qui peuvent exiger des informations d'identification à long terme, citons notamment les plug-ins WordPress et les clients AWS tiers. Dans les situations où vous devez utiliser des informations d'identification à long terme ou des informations d'identification autres que les clés d'accès AWS, comme les connexions aux bases de données, vous pouvez utiliser un service conçu pour gérer la gestion des secrets, par exemple AWS Secrets Manager. Secrets Manager facilite la gestion, la rotation et le stockage sécurisé des secrets chiffrés à l'aide des services pris en charge. Pour plus d'informations sur la rotation des informations d'identification à long terme, consultez Rotation des clés d'accès.

Ressources

Bonnes pratiques associées :

- SEC02-BP03 Stocker et utiliser des secrets en toute sécurité
- SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé
- SEC03-BP08 Partager des ressources en toute sécurité au sein de votre organisation

Documents connexes :

- Informations d'identification de sécurité temporaires
- AWS Credentials (Informations d'identification AWS)
- Bonnes pratiques de sécurité dans IAM
- Rôles IAM
- IAM Identity Center
- Fournisseurs d'identité et fédération
- Rotating Access Keys (Rotation des clés d'accès)
- Solutions partenaires de sécurité : accès et contrôle d'accès
- Utilisateur root Compte AWS

Vidéos connexes :

- Managing user permissions at scale with AWS IAM Identity Center (successor to AWS IAM Identity Center)
- Mastering identity at every layer of the cake

SEC02-BP03 Stocker et utiliser des secrets en toute sécurité

Une charge de travail nécessite une capacité automatisée pour prouver son identité aux bases de données, aux ressources et aux services tiers. Cela se fait à l'aide d'identifiants d'accès secrets, tels que des clés d'accès à l'API, des mots de passe et des jetons OAuth. L'utilisation d'un service spécialement conçu pour stocker, gérer et faire tourner ces informations d'identification permet de réduire les risques de compromission de ces informations d'identification.

Résultat souhaité : implémentation d'un mécanisme de gestion sécurisée des informations d'identification des applications qui atteint les objectifs suivants :

- Identification des secrets nécessaires pour la charge de travail.
- Réduction du nombre d'informations d'identification à long terme requis en les remplaçant par des informations d'identification à court terme, dans la mesure du possible.
- Établissement d'un stockage sécurisé et d'une rotation automatisée des informations d'identification à long terme restantes.
- Audit de l'accès aux secrets qui existent dans la charge de travail.
- Surveillance continue pour vérifier qu'aucun secret n'est intégré dans le code source pendant le processus de développement.
- Réduction des risques de divulgation des informations d'identification par inadvertance.

Anti-modèles courants :

- Aucune rotation des informations d'identification.
- Stockage des informations d'identification à long terme dans le code source ou les fichiers de configuration.
- Stockage des informations d'identification au repos non chiffrées.

Avantages liés à l'instauration de cette bonne pratique :

- Les secrets sont chiffrés au repos et en transit.
- L'accès aux informations d'identification est sécurisé par une API (il s'agit plus ou moins d'un distributeur d'informations d'identification).
- L'accès à une information d'identification (en lecture et en écriture) est audité et consigné.

- Séparation des préoccupations : la rotation des informations d'identification est effectuée par un composant distinct, qui peut être séparé du reste de l'architecture.
- Les secrets sont distribués automatiquement à la demande aux composants logiciels et la rotation se produit dans un emplacement central.
- L'accès aux informations d'identification peut être contrôlé de façon précise.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Dans le passé, les informations d'identification utilisées pour s'authentifier auprès des bases de données, des API tierces, des jetons et d'autres secrets pouvaient être intégrées dans du code source ou des fichiers d'environnement. AWS fournit plusieurs mécanismes pour stocker ces informations d'identification en toute sécurité, en effectuer la rotation automatiquement et vérifier leur utilisation.

Pour gérer les secrets de façon optimale, la meilleure solution consiste à suivre les directives de suppression, de remplacement et de rotation. Les informations d'identification les plus sûres sont celles que vous n'avez pas à stocker, gérer ou manipuler. Certaines informations d'identification qui ne sont plus nécessaires au fonctionnement de la charge de travail peuvent être supprimées en toute sécurité.

Pour les informations d'identification qui restent nécessaires au bon fonctionnement de la charge de travail, il peut être possible d'opter pour une solution temporaire ou à court terme au lieu d'utiliser des informations à long terme. Par exemple, au lieu de coder en dur une clé d'accès secrète AWS, envisagez de remplacer les informations d'identification à long terme par des informations d'identification temporaires à l'aide de rôles IAM.

Certains secrets de longue durée ne peuvent pas être supprimés ni remplacés. Ces secrets peuvent être stockés dans un service tel qu'AWS Secrets Manager, où ils peuvent être stockés, gérés et mis en rotation de façon centralisée.

Un audit du code source de la charge de travail et des fichiers de configuration peut révéler de nombreux types d'informations d'identification. Le tableau suivant résume les stratégies de traitement des types courants d'informations d'identification :

Credential type	Description	Suggested strategy
IAM access keys	AWS IAM access and secret keys used to assume IAM roles inside of a workload	Replace: Use Rôles IAM assigned to the compute instances (such as Amazon EC2 or AWS Lambda) instead. For interoperability with third parties that require access to resources in your Compte AWS, ask if they support Accès intercompte AWS. For mobile apps, consider using temporary credentials through Groupes d'identités Amazon Cognito (identités fédérées). For workloads running outside of AWS, consider IAM Roles Anywhere or AWS Systems Manager Hybrid Activations.
SSH keys	Secure Shell private keys used to log into Linux EC2 instances, manually or as part of an automated process	Replace: Use AWS Systems Manager or EC2 Instance Connect to provide programmatic and human access to EC2 instances using IAM roles.
Application and database credentials	Passwords – plain text string	Rotate: Store credentials in AWS Secrets Manager and establish automated rotation if possible.
Amazon RDS and Aurora Admin Database credentials	Passwords – plain text string	Replace: Use the Intégration d'Secrets Manager à Amazon RDS or Amazon Aurora. In addition, some RDS database

Credential type	Description	Suggested strategy
		types can use IAM roles instead of passwords for some use cases (for more detail, see Authentification de base de données IAM).
OAuth tokens	Secret tokens – plain text string	Rotate: Store tokens in AWS Secrets Manager and configure automated rotation.
API tokens and keys	Secret tokens – plain text string	Rotate: Store in AWS Secrets Manager and establish automated rotation if possible.

Parmi les anti-modèles courants, citons l'intégration des clés d'accès IAM dans le code source, les fichiers de configuration ou les applications mobiles. Lorsqu'une clé d'accès IAM est requise pour communiquer avec un service AWS, utilisez des informations d'identification de sécurité temporaires (à court terme). Ces informations d'identification à court terme peuvent être fournies via des rôles IAM pour les instances EC2, des rôles d'exécution pour les fonctions Lambda, des rôles IAM Cognito pour l'accès des utilisateurs mobiles et des politiques IoT Core pour les appareils IoT. Lorsque vous interagissez avec des tiers, privilégiez la délégation des accès à un rôle IAM avec l'accès nécessaire aux ressources de votre compte au lieu de configurer un utilisateur IAM et d'envoyer au tiers la clé d'accès secrète pour cet utilisateur.

Dans de nombreux cas, la charge de travail exige le stockage de secrets nécessaires pour interagir avec d'autres services et ressources. AWS Secrets Manager est conçu pour gérer en toute sécurité ces informations d'identification, ainsi que le stockage, l'utilisation et la rotation des jetons d'API, mots de passe et autres informations d'identification.

AWS Secrets Manager fournit cinq capacités clés pour assurer le stockage et la manipulation sécurisés des informations d'identification sensibles : chiffrement au repos, chiffrement en transit, audit complet, contrôle d'accès détaillé et rotation extensible des informations d'identification. D'autres services de gestion des secrets créés par des partenaires AWS ou des solutions développées localement qui offrent des capacités et des assurances similaires sont également acceptables.

Étapes d'implémentation

1. Identifiez les chemins de code contenant des informations d'identification codées en dur à l'aide d'outils automatisés tels que Amazon CodeGuru.
   - Utilisez Amazon CodeGuru pour analyser vos référentiels de code. Une fois la vérification terminée, filtrez sur `Type=Secrets` dans CodeGuru afin de trouver les lignes de code qui posent problème.
2. Identifiez les informations d'identification qui peuvent être supprimées ou remplacées.
   a. Identifiez les informations d'identification qui ne sont plus nécessaires et marquez-les en vue de leur suppression.
   b. Pour les clés secrètes AWS qui sont intégrées au code source, remplacez-les par des rôles IAM associés aux ressources nécessaires. Si une partie de votre charge de travail se trouve en dehors d'AWS mais requiert des informations d'identification IAM pour accéder aux ressources AWS, envisagez l'utilisation d'IAM Roles Anywhere ou d'AWS Systems Manager Hybrid Activations.
3. Pour les autres secrets tiers de longue durée qui nécessitent l'utilisation de la stratégie de rotation, intégrez Secrets Manager dans votre code afin d'extraire les secrets tiers au moment de l'exécution.
   a. La console CodeGuru peut créer automatiquement un secret dans Secrets Manager à l'aide des informations d'identification découvertes.
   b. Intégrez l'extraction des secrets d'Secrets Manager dans votre code d'application.
      - Les fonctions Lambda sans serveur peuvent utiliser une extension Lambda qui ne dépend pas du langage.
      - Pour les instances ou conteneurs EC2, AWS fournit un exemple de code côté client permettant d'extraire les secrets d'Secrets Manager dans plusieurs langages de programmation populaires.
4. Examinez régulièrement votre base de code et effectuez une nouvelle analyse afin de vérifier qu'aucun nouveau secret n'a été ajouté au code.
   - Envisagez d'utiliser un outil tel que git-secrets pour éviter d'intégrer de nouveaux secrets dans votre référentiel de code source.
5. Surveillez l'activité d'Secrets Manager afin de détecter toute utilisation inattendue, tout accès aux secrets inapproprié ou toute tentative de suppression de secrets.
6. Réduisez l'exposition humaine aux informations d'identification. Limitez l'accès à la lecture, à l'écriture et à la modification des informations d'identification à un rôle IAM dédié à cette fin et

fournissez un accès uniquement pour assumer le rôle à un petit sous-ensemble d'utilisateurs opérationnels.

Ressources

Bonnes pratiques associées :

- SEC02-BP02 Utiliser des informations d'identification temporaires
- SEC02-BP05 Contrôler et effectuer régulièrement une rotation des informations d'identification

Documents connexes :

- Getting Started with AWS Secrets Manager (Démarrer avec AWS Secrets Manager)
- Fournisseurs d'identité et fédération
- Amazon CodeGuru Introduces Secrets Detector (Amazon DevOps Guru présente le détecteur de secrets)
- Comment AWS Secrets Manager utilise AWS Key Management Service
- Chiffrement et déchiffrement de secrets dans Secrets Manager
- Entrées de blog sur Secrets Manager
- Amazon RDS annonce l'intégration avec AWS Secrets Manager

Vidéos connexes :

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale
- Find Hard-Coded Secrets Using Amazon CodeGuru Secrets Detector
- Securing Secrets for Hybrid Workloads Using AWS Secrets Manager

Ateliers connexes :

- Store, retrieve, and manage sensitive credentials in AWS Secrets Manager
- AWS Systems Manager Hybrid Activations

SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé

Pour les identités du personnel (employés et sous-traitants), faites confiance à un fournisseur d'identité qui vous permet de gérer les identités de manière centralisée. Cela facilite la gestion de l'accès entre plusieurs applications et systèmes, car vous créez, attribuez, gérez, révoquez et auditez l'accès depuis un seul emplacement.

Résultat souhaité : Vous disposez d'un fournisseur d'identité centralisé dans lequel vous gérez de manière centralisée les utilisateurs faisant partie du personnel, les politiques d'authentification (telles que l'exigence d'authentification multifactorielle (MFA)) et les autorisations accordées aux systèmes et aux applications (telles que l'attribution de l'accès en fonction de l'appartenance à un groupe ou des attributs d'un utilisateur). Les utilisateurs en interne se connectent au fournisseur d'identité central et se fédèrent (authentification unique) avec les applications internes et externes, ce qui leur évite d'avoir à mémoriser différentes informations d'identification. Votre fournisseur d'identité est intégré à vos systèmes de ressources humaines (RH) afin que les changements de personnel soient automatiquement synchronisés avec lui. Par exemple, si quelqu'un quitte votre organisation, vous pouvez automatiquement révoquer l'accès aux applications et systèmes fédérés (y compris AWS). Vous avez activé la journalisation détaillée des audits dans votre fournisseur d'identité et vous surveillez ces journaux pour détecter tout comportement inhabituel des utilisateurs.

Anti-modèles courants :

- Vous n'utilisez pas la fédération ni l'authentification unique. Les utilisateurs en interne créent des comptes utilisateur et des informations d'identification distincts dans plusieurs applications et systèmes.
- Vous n'avez pas automatisé le cycle de vie des identités pour les utilisateurs en interne, par exemple en intégrant votre fournisseur d'identité à vos systèmes RH. Lorsqu'un utilisateur quitte votre organisation ou change de rôle, vous suivez un processus manuel pour supprimer ou mettre à jour ses enregistrements dans plusieurs applications et systèmes.

Avantages liés au respect de cette bonne pratique : En utilisant un fournisseur d'identité centralisé, vous disposez d'un emplacement unique pour gérer les identités et les politiques des utilisateurs en interne, de la possibilité d'attribuer l'accès aux applications, aux utilisateurs et aux groupes, et de la capacité de surveiller l'activité de connexion des utilisateurs. Grâce à l'intégration du fournisseur d'identité dans vos systèmes de ressources humaines (RH), lorsqu'un utilisateur change de rôle, ces modifications sont synchronisées avec le fournisseur d'identité et mettent automatiquement à jour les applications et les autorisations qui lui ont été attribuées. Lorsqu'un utilisateur quitte votre

organisation, son identité est automatiquement désactivée dans le fournisseur d'identité, révoquant ainsi son accès aux applications et systèmes fédérés.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Conseils pour les utilisateurs en interne accédant à AWS

Les utilisateurs en interne, tels que les employés et les sous-traitants de votre organisation, peuvent avoir besoin d'accéder à AWS avec la AWS Management Console ou AWS Command Line Interface (AWS CLI) pour exécuter leurs tâches. Vous pouvez accorder l'accès AWS aux utilisateurs en interne en les fédérant avec AWS à deux niveaux à partir de votre fournisseur d'identité centralisé : fédération directe vers chaque Compte AWS ou fédération vers plusieurs comptes dans votre organisation AWS.

- Pour fédérer les utilisateurs en interne directement avec chaque Compte AWS, vous pouvez utiliser un fournisseur d'identité centralisé afin de les fédérer à AWS Identity and Access Management sur ce compte. La flexibilité d'IAM vous permet d'activer un fournisseur d'identité SAML 2.0 ou OpenID Connect (OIDC) distinct pour chaque Compte AWS et d'utiliser les attributs des utilisateurs fédérés pour le contrôle de l'accès. Les utilisateurs en interne utiliseront leur navigateur web pour se connecter au fournisseur d'identité en indiquant leurs informations d'identification (telles que des mots de passe et des codes de jeton MFA). Le fournisseur d'identité enverra à son navigateur une assertion SAML soumise à l'URL de connexion de la AWS Management Console pour permettre à l'utilisateur de s'authentifier de manière unique auprès de la AWS Management Console en assumant un rôle IAM. Vos utilisateurs peuvent également obtenir des informations d'identification d'API AWS temporaires à utiliser dans AWS CLI ou les kits SDK AWS depuis AWS STS en endossant le rôle IAM à l'aide d'une assertion SAML auprès du fournisseur d'identité.
- Pour fédérer les utilisateurs en interne disposant de plusieurs comptes dans votre organisation AWS, vous pouvez utiliser AWS IAM Identity Center afin de gérer de manière centralisée l'accès des utilisateurs en interne aux Comptes AWS et aux applications. Activez Identity Center pour votre organisation et configurez votre source d'identité. IAM Identity Center fournit un annuaire source d'identités par défaut que vous pouvez utiliser pour gérer vos utilisateurs et vos groupes. Vous pouvez également choisir une source d'identité externe en vous connectant à votre fournisseur d'identité externe à l'aide de SAML 2.0 et en approvisionnant automatiquement les utilisateurs et les groupes avec SCIM, ou en vous connectant à votre annuaire Microsoft AD avec AWS Directory Service. Une fois qu'une source d'identité est configurée, vous pouvez attribuer aux utilisateurs et aux groupes l'accès aux Comptes AWS en définissant des politiques de moindre privilège dans vos

ensembles d'autorisations. Les utilisateurs en interne peuvent s'authentifier par le biais de votre fournisseur d'identité central pour se connecter au portail d'accès AWS et s'authentifier de manière unique aux Comptes AWS et aux applications cloud qui leur sont attribués. Vos utilisateurs peuvent configurer AWS CLI v2 pour s'authentifier auprès d'Identity Center et obtenir des informations d'identification pour exécuter des commandes AWS CLI. Identity Center permet également l'accès par authentification unique à des applications AWS comme Amazon SageMaker Studio et les portails AWS IoT Sitewise Monitor.

Une fois que vous aurez suivi les instructions précédentes, vos utilisateurs en interne n'auront plus besoin d'utiliser des IAM users et des groupes pour les opérations normales lors de la gestion des charges de travail sur AWS. Au lieu de cela, vos utilisateurs et vos groupes seront gérés en dehors d'AWS, et les utilisateurs pourront accéder aux ressources AWS en tant qu'identité fédérée. Les identités fédérées utilisent les groupes définis par votre fournisseur d'identité centralisé. Vous devez identifier et supprimer les groupes IAM, les IAM users et les informations d'identification utilisateur de longue durée (mots de passe et clés d'accès) dont vous n'avez plus besoin dans vos Comptes AWS. Vous pouvez trouver les informations d'identification non utilisées avec des rapports sur les informations d'identification IAM, supprimer les IAM users correspondants et supprimer les groupes IAM. Vous pouvez appliquer une politique de contrôle des services (SCP) à votre organisation afin d'empêcher la création d'autres groupes et IAM users, en vous assurant que cet accès à AWS se fasse via des identités fédérées.

Conseils pour les utilisateurs de vos applications

Vous pouvez gérer l'identité des utilisateurs de vos applications, telles qu'une application mobile, en utilisant Amazon Cognito en tant que fournisseur d'identité centralisé. Amazon Cognito permet l'authentification, l'autorisation et la gestion des utilisateurs pour vos applications web et mobiles. Amazon Cognito fournit une banque d'identités adaptée à des millions d'utilisateurs, prend en charge la fédération des identités sociales et d'entreprise et propose des fonctionnalités de sécurité avancées pour protéger vos utilisateurs et votre entreprise. Vous pouvez intégrer votre application web ou mobile personnalisée avec Amazon Cognito pour ajouter l'authentification des utilisateurs et le contrôle d'accès à vos applications en quelques minutes. Fondé sur des normes d'identité ouvertes telles que SAML et OpenID Connect (OIDC), Amazon Cognito prend en charge diverses réglementations de conformité et s'intègre aux ressources de développement frontend et backend.

Étapes d'implémentation

Étapes à suivre pour permettre aux utilisateurs en interne d'accéder à AWS

- Fédérez les utilisateurs en interne avec AWS pour qu'ils utilisent un fournisseur d'identité centralisé en utilisant l'une des approches suivantes :
  - Utilisez IAM Identity Center pour activer l'authentification unique à plusieurs Comptes AWS dans votre organisation AWS en vous fédérant avec votre fournisseur d'identité.
  - Utilisez IAM pour connecter votre fournisseur d'identité directement à chaque Compte AWS afin de permettre un accès fédéré précis.
- Identifiez et supprimez les groupes et IAM users qui seront remplacés par des identités fédérées.

Étapes à suivre pour les utilisateurs de vos applications

- Utilisez Amazon Cognito comme fournisseur d'identité centralisé pour vos applications.
- Intégrez vos applications personnalisées à Amazon Cognito à l'aide d'OpenID Connect et d'OAuth. Vous pouvez développer vos applications personnalisées à l'aide des bibliothèques Amplify qui fournissent des interfaces simples à intégrer à divers services AWS, tels que l'authentification Amazon Cognito.

Ressources

Bonnes pratiques Well-Architected connexes :

- SEC02-BP06 Tirer parti des groupes d'utilisateurs et des attributs
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège
- SEC03-BP06 Gérer l'accès en fonction du cycle de vie

Documents connexes :

- Fédération d'identité dans AWS
- Bonnes pratiques de sécurité dans IAM
- Bonnes pratiques AWS Identity and Access Management
- Commencer à utiliser l'administration déléguée IAM Identity Center
- Comment utiliser les politiques gérées par le client dans IAM Identity Center pour les cas d'utilisation avancés
- AWS CLI v2 : fournisseur d'informations d'identification IAM Identity Center

Vidéos connexes :

- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Invent 2018: Mastering Identity at Every Layer of the Cake

Exemples connexes :

- Atelier : utiliser AWS IAM Identity Center pour assurer une gestion solide de l'identité
- Atelier : identité sans serveur

Outils associés :

- Partenaires AWS disposant de la compétence Sécurité : gestion des identités et des accès
- saml2aws

SEC02-BP05 Contrôler et effectuer régulièrement une rotation des informations d'identification

Contrôlez et effectuez régulièrement une rotation des informations d'identification afin de limiter leur durée d'utilisation pour accéder à vos ressources. Les informations d'identification à long terme créent de nombreux risques qui peuvent être réduits par une rotation régulière de ces informations.

Résultat souhaité : implémenter la rotation des informations d'identification afin de réduire les risques associés à l'utilisation d'informations d'identification à long terme. Auditez et corrigez régulièrement toute non-conformité avec les politiques de rotation des informations d'identification.

Anti-modèles courants :

- Ne pas auditer l'utilisation des informations d'identification.
- Utiliser inutilement des informations d'identification à long terme.
- Utiliser des informations d'identification à long terme et ne pas effectuer de rotation régulièrement.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : moyen

Directives d'implémentation

Lorsque l'utilisation d'informations d'identification temporaires est impossible et que vous avez besoin d'informations d'identification à long terme, vérifiez les informations d'identification pour vous assurer que les contrôles définis, tels que l'authentification multifactorielle (MFA) sont appliqués, changés régulièrement et disposent du niveau d'accès approprié.

La validation régulière, de préférence via un outil automatisé, est nécessaire pour vérifier que les contrôles corrects sont appliqués. Pour les identités humaines, vous devez obliger les utilisateurs à modifier leurs mots de passe régulièrement et à abandonner les clés d'accès au profit d'informations d'identification temporaires. En passant des utilisateurs AWS Identity and Access Management (IAM) aux identités centralisées, vous pouvez générer un rapport des informations d'identification afin d'auditer vos utilisateurs.

Nous vous recommandons également d'appliquer les paramètres d'authentification multifactorielle dans votre fournisseur d'identité. Vous pouvez configurer AWS Config Rules ou utiliser les normes de sécurité AWS Security Hub, afin de surveiller si l'authentification multifactorielle est activée pour les utilisateurs. Envisagez d'utiliser IAM Roles Anywhere afin de fournir des informations d'identification temporaires pour les identités machine. Lorsque l'utilisation de rôles IAM et d'informations d'identification temporaires n'est pas possible, il est nécessaire de réaliser fréquemment des audits et la rotation des clés d'accès.

Étapes d'implémentation

- Auditez régulièrement les informations d'identification : l'audit des identités configurées dans votre fournisseur d'identité et dans IAM permet de s'assurer que seules les identités autorisées ont accès à votre charge de travail. Ces identités peuvent inclure, sans s'y limiter, des utilisateurs IAM, des utilisateurs AWS IAM Identity Center, des utilisateurs Active Directory ou des utilisateurs dans un autre fournisseur d'identité en amont. Par exemple, supprimez les personnes qui quittent l'organisation et supprimez les rôles intercomptes qui ne sont plus requis. Mettez en place un processus pour auditer périodiquement les autorisations aux services auxquels accède une entité IAM. Cela vous permet d'identifier les politiques à modifier afin de supprimer les autorisations inutilisées. Utilisez les rapports d'informations d'identification et AWS Identity and Access Management Access Analyzer pour auditer les informations d'identification et les autorisations IAM. Vous pouvez utiliser Amazon CloudWatch afin de configurer des alarmes pour des appels d'API spécifiques au sein de votre environnement AWS. Amazon GuardDuty peut également vous alerter en cas d'activité inattendue, ce qui peut indiquer un accès trop permissif ou involontaire à des informations d'identification IAM.

- Effectuez une rotation régulière des informations d'identification : lorsque vous ne pouvez pas utiliser d'informations d'identification temporaires, effectuez une rotation régulière des clés d'accès IAM (au maximum tous les 90 jours). Si une clé d'accès est divulguée involontairement à votre insu, cela limite la durée pendant laquelle les informations d'identification peuvent être utilisées pour accéder à vos ressources. Pour plus d'informations sur la rotation des clés d'accès pour les utilisateurs IAM, consultez Rotation des clés d'accès.
- Passez en revue les autorisations IAM : pour améliorer la sécurité de votre Compte AWS, passez en revue et surveillez régulièrement chacune de vos politiques IAM. Vérifiez que les politiques respectent le principe du moindre privilège.
- Envisagez d'automatiser la création et les mises à jour des ressources IAM : IAM Identity Center automatise de nombreuses tâches IAM, telles que la gestion des rôles et des politiques. Sinon, AWS CloudFormation peut être utilisé afin d'automatiser le déploiement des ressources IAM, y compris les rôles et les politiques, afin de réduire le risque d'erreur humaine, car les modèles peuvent être vérifiés et la version contrôlée.
- Utilisez IAM Roles Anywhere pour remplacer les utilisateurs IAM par des identités machine : IAM Roles Anywhere vous permet d'utiliser des rôles dans des domaines où cela était impossible auparavant, par exemple avec les serveurs sur site. IAM Roles Anywhere utilise un certificat X.509 autorisé afin de s'authentifier auprès d'AWS et de recevoir des informations d'identification temporaires. L'utilisation d'IAM Roles Anywhere vous évite d'avoir à effectuer des rotations de ces informations d'identification, car les informations d'identification à long terme ne sont plus stockées dans votre environnement sur site. Veuillez noter que vous devrez surveiller et faire tourner le certificat X.509 à l'approche de son expiration.

Ressources

Bonnes pratiques associées :

- SEC02-BP02 Utiliser des informations d'identification temporaires
- SEC02-BP03 Stocker et utiliser des secrets en toute sécurité

Documents connexes :

- Getting started with AWS Secrets Manager (Démarrer avec Amazon SQS)
- Bonnes pratiques de sécurité dans IAM
- Fournisseurs d'identité et fédération

- Solutions partenaires de sécurité : accès et contrôle d'accès
- Informations d'identification de sécurité temporaires
- Obtenir des rapports d'informations d'identification pour votre Compte AWS

Vidéos connexes :

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale
- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

Exemples connexes :

- Atelier Well-Architected – Automated IAM User Cleanup
- Atelier Well-Architected – Automated Deployment of IAM Groups and Roles

SEC02-BP06 Tirer parti des groupes d'utilisateurs et des attributs

Au fur et à mesure que le nombre d'utilisateurs que vous gérez augmente, vous devez déterminer les moyens de les organiser afin de pouvoir les gérer à grande échelle. Placez les utilisateurs ayant des exigences de sécurité communes dans des groupes définis par votre fournisseur d'identité et mettez en place des mécanismes pour s'assurer que les attributs pouvant être utilisés pour le contrôle d'accès (par exemple, service ou emplacement) sont corrects et mis à jour. Utilisez ces groupes et attributs pour contrôler l'accès plutôt que des utilisateurs individuels. Cela vous permet de gérer l'accès de manière centralisée en modifiant une fois l'appartenance à un groupe ou les attributs d'un utilisateur avec un jeu d'autorisations, plutôt que de mettre à jour de nombreuses stratégies individuelles lorsque les besoins d'accès d'un utilisateur changent. Vous pouvez utiliser AWS IAM Identity Center (IAM Identity Center) pour gérer les groupes d'utilisateurs et les attributs. IAM Identity Center prend en charge les attributs les plus couramment utilisés, qu'ils soient saisis manuellement lors de la création de l'utilisateur ou alloués automatiquement à l'aide d'un moteur de synchronisation, tel que défini dans la spécification SCIM (Cross-Domain Identity Management).

Placez les utilisateurs ayant des exigences de sécurité communes dans des groupes définis par votre fournisseur d'identité et mettez en place des mécanismes pour s'assurer que les attributs pouvant être utilisés pour le contrôle d'accès (par exemple, service ou emplacement) sont corrects et mis à jour. Utilisez ces groupes et attributs, plutôt que des utilisateurs individuels, pour contrôler l'accès. Cela vous permet de gérer l'accès de manière centralisée en modifiant l'appartenance à un

groupe ou les attributs d'un utilisateur une fois, plutôt que de mettre à jour de nombreuses stratégies individuelles lorsque les besoins d'accès d'un utilisateur changent.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Si vous utilisez AWS IAM Identity Center (IAM Identity Center), configurez des groupes : IAM Identity Center vous permet de configurer des groupes d'utilisateurs et d'attribuer aux groupes le niveau d'autorisation souhaité.
  - Authentification unique AWS : gérer les identités
- Familiarisez-vous avec le contrôle d'accès basé sur les attributs (ABAC) : l'ABAC est une stratégie d'autorisation qui définit les autorisations en fonction des attributs.
  - Qu'est-ce que l'ABAC pour AWS ?
  - Atelier : Contrôle d'accès basé sur les balises IAM pour EC2

Ressources

Documents connexes :

- Démarrer avec AWS Secrets Manager
- Bonnes pratiques IAM
- Fournisseurs d'identité et fédération
- Utilisateur racine d'un compte AWS

Vidéos connexes :

- Bonnes pratiques de gestion, d'extraction et de renouvellement des secrets à grande échelle
- Gestion des autorisations utilisateur à grande échelle avec AWS IAM Identity Center
- Maîtrise des identités dans chaque couche

Exemples connexes :

- Atelier : Contrôle d'accès basé sur les balises IAM pour EC2

Permissions management (Gestion des autorisations)

Gérez les autorisations des identités humaines et machines qui nécessitent un accès à AWS ainsi qu'à votre charge de travail. Les autorisations régissent les ressources accessibles et les conditions d'accès. Définissez des autorisations sur des identités humaines et machine spécifiques pour accorder l'accès à des actions de service spécifiques sur des ressources spécifiques. En outre, spécifiez les conditions qui doivent être remplies pour que l'accès soit accordé. Par exemple, vous pouvez autoriser les développeurs à créer de nouvelles fonctions Lambda, mais uniquement dans une région spécifique. Lorsque vous gérez vos environnements AWS à grande échelle, respectez les bonnes pratiques suivantes pour vous assurer que les identités ont uniquement l'accès dont elles ont besoin et rien de plus.

Il existe plusieurs façons d'accorder l'accès à différents types de ressources. L'une d'entre elles consiste à utiliser différents types de politiques.

Les politiques basées sur l'identité dans IAM sont gérées ou en ligne, et s'attachent aux identités IAM, y compris les utilisateurs, les groupes ou les rôles. Ces politiques vous permettent de spécifier ce que cette identité peut faire (ses autorisations). Les politiques basées sur l'identité peuvent être catégorisées davantage.

Politiques gérées – Politiques autonomes basées sur l'identité que vous pouvez attacher à plusieurs utilisateurs, groupes et rôles dans votre compte AWS. Il existe deux types de politiques gérées :

- Politiques gérées par AWS – Politiques gérées qui sont créées et gérées par AWS.
- Politiques gérées par le client – Politiques gérées que vous créez et gérez dans votre compte AWS. Les politiques gérées par le client offrent un contrôle plus précis de vos politiques que les politiques gérées par AWS.

Les politiques gérées sont la méthode privilégiée pour appliquer les autorisations. Cependant, vous pouvez également utiliser des politiques intégrées que vous ajoutez directement à un seul utilisateur, groupe ou rôle. Les politiques intégrées associent une politique spécifique à une identité. Elles sont éliminées lorsque vous supprimez l'identité.

Dans la plupart des cas, vous devez créer vos propres politiques gérées par le client en suivant le principe du moindre privilège.

Les politiques basées sur les ressources sont associées à une ressource. Par exemple, une politique de compartiment S3 est une politique basée sur les ressources. Ces politiques accordent une

autorisation à un mandataire qui peut se trouver dans le même compte que la ressource ou dans un autre compte. Pour obtenir une liste des services qui prennent en charge les politiques basées sur des ressources, consultez Services AWS qui fonctionnent avec IAM.

Les limites d'autorisation utilisent une politique gérée pour définir les autorisations maximales qu'un administrateur peut définir. Cela vous permet de déléguer aux développeurs la possibilité de créer et de gérer des autorisations, comme la création d'un rôle IAM, mais de limiter les autorisations qu'ils peuvent accorder afin qu'ils ne puissent pas faire remonter leur privilège grâce à ce qu'ils ont créé.

Le Contrôle d'accès basé sur les attributs (ABAC) vous permet d'accorder des autorisations en fonction des attributs. Dans AWS, on les appelle des balises. Les balises peuvent être associées à des mandataires IAM (utilisateurs ou rôles) et à des ressources AWS. Grâce aux stratégies IAM, les administrateurs peuvent créer une stratégie réutilisable qui applique des autorisations en fonction des attributs du mandataire IAM. Par exemple, en tant qu'administrateur, vous pouvez utiliser une seule stratégie IAM qui accorde aux développeurs de votre organisation l'accès aux ressources AWS qui correspondent aux balises de projet des développeurs. Lorsque l'équipe de développeurs ajoute des ressources aux projets, les autorisations sont automatiquement appliquées en fonction des attributs. Par conséquent, aucune mise à jour de stratégie n'est requise pour chaque nouvelle ressource.

Les politiques de contrôle des services (SCP) Organizations définissent les autorisations maximales des membres d'un compte d'une organisation ou d'une unité d'organisation (UO). Les politiques SCP limitent les autorisations que les politiques basées sur l'identité ou les politiques basées sur les ressources accordent aux entités (utilisateurs ou rôles) au sein du compte, mais n'accordent pas d'autorisations.

Les politiques de session assument un rôle ou un utilisateur fédéré. Transmettez des politiques de session lors de l'utilisation d'AWS CLI ou de l'API AWS. Ces politiques limitent les autorisations que les politiques basées sur l'identité du rôle ou de l'utilisateur accordent à la session. Ces politiques limitent les autorisations d'une session créée, mais n'accordent pas d'autorisations. Pour plus d'informations, consultez Politiques de session.

Bonnes pratiques

- SEC03-BP01 Définir les conditions d'accès
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège
- SEC03-BP03 Établir un processus d'accès d'urgence
- SEC03-BP04 Limiter les autorisations au minimum requis en permanence
- SEC03-BP05 Définir des protections par autorisation pour votre organisation

- SEC03-BP06 Gérer l'accès en fonction du cycle de vie
- SEC03-BP07 Analyser l'accès public et entre les comptes
- SEC03-BP08 Partager des ressources en toute sécurité au sein de votre organisation
- SEC03-BP09 Partager des ressources en toute sécurité avec un tiers

SEC03-BP01 Définir les conditions d'accès

Les administrateurs, utilisateurs finaux ou autres composants doivent pouvoir accéder à chaque composant ou ressource de votre charge de travail. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité et la méthode d'authentification et d'autorisation appropriés.

Anti-modèles courants :

- Codage en dur ou stockage de secrets dans votre application.
- Octroi d'autorisations personnalisées à chaque utilisateur.
- Utilisation d'informations d'identification durables.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : Élevé

Directives d'implémentation

Les administrateurs, utilisateurs finaux ou autres composants doivent pouvoir accéder à chaque composant ou ressource de votre charge de travail. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité et la méthode d'authentification et d'autorisation appropriés.

Un accès standard aux Comptes AWS de l'organisation doit être fourni à l'aide d'un accès fédéré ou d'un fournisseur d'identité centralisé. Vous devez également centraliser la gestion des identités et vous assurer qu'il existe une pratique établie pour intégrer l'accès à AWS au cycle de vie de l'accès des employés. Par exemple, lorsqu'un employé change de poste et de niveau d'accès, son appartenance à un groupe doit également évoluer de façon à refléter les nouvelles conditions d'accès qui lui sont associées.

Lorsque vous définissez des conditions d'accès pour des identités non humaines, déterminez quels applications et composants ont besoin d'un accès et comment les autorisations sont accordées. Dans

cette optique, il est recommandé d'utiliser les rôles IAM créés avec le modèle d'accès du moindre privilège. Les politiques gérées par AWS établissent des politiques IAM prédéfinies qui couvrent les cas d'utilisation les plus courants.

Les services AWS, tels qu' AWS Secrets Manager et AWS Systems Manager Parameter Store,peuvent permettre de dissocier les secrets de l'application ou de la charge de travail en toute sécurité lorsqu'il est impossible d'utiliser des rôles IAM. Dans Secrets Manager, vous pouvez établir une rotation automatique de vos informations d'identification. Vous pouvez utiliser Systems Manager de façon à référencer les paramètres dans vos scripts, commandes, documents SSM, configuration et flux de travail d'automatisation en utilisant le nom unique que vous avez spécifié lors de la création du paramètre.

Vous pouvez utiliser des rôles AWS Identity and Access Management partout de façon à obtenir des informations d'identification de sécurité temporaires dans IAM pour les charges de travail exécutées en dehors d'AWS. Vos charges de travail peuvent utiliser les mêmes politiques IAM et rôles IAM que ceux utilisés avec les applications AWS pour accéder aux ressources AWS.

Dans la mesure du possible, privilégiez les informations d'identification temporaires à court terme plutôt que les informations d'identification statiques à long terme. Pour les scénarios dans le cadre desquels les utilisateurs IAM doivent disposer d'un accès par programmation et d'informations d'identification à long terme, utilisez les dernières informations de clé d'accès utilisées pour effectuer la rotation des clés d'accès et supprimer ces dernières.

Ressources

Documents connexes :

- Contrôle d'accès basé sur les attributs (ABAC)
- AWS IAM Identity Center
- IAM Roles Anywhere
- AWS politiques gérées pour IAM Identity Center
- AWS IAM policy conditions
- IAM use cases
- Remove unnecessary credentials
- Gestion des politiques IAM
- How to control access to AWS resources based on Compte AWS, OU, or organization

- Identify, arrange, and manage secrets easily using enhanced search in AWS Secrets Manager

Vidéos connexes :

- Devenir un expert en stratégie IAM en 60 minutes maximum
- Separation of Duties, Least Privilege, Delegation, and CI/CD
- Streamlining identity and access management for innovation

SEC03-BP02 Accorder un accès selon le principe du moindre privilège

Une bonne pratique consiste à accorder uniquement l'accès dont les identités ont besoin pour effectuer des actions spécifiques sur des ressources spécifiques dans des conditions spécifiques. Faites appel à des groupes et des attributs d'identité pour définir de façon dynamique des autorisations à grande échelle, plutôt que pour des utilisateurs individuels. Par exemple, vous pouvez autoriser un groupe de développeurs à gérer uniquement les ressources de leur projet. Ainsi, si un développeur quitte le projet, son accès est automatiquement révoqué sans que les stratégies d'accès sous-jacentes soient modifiées.

Résultat souhaité : les utilisateurs doivent uniquement disposer des autorisations requises pour faire leur travail. Les utilisateurs ne doivent avoir accès qu'aux environnements de production pour effectuer une tâche précise dans un délai limité et cet accès doit être révoqué une fois la tâche terminée. Les autorisations doivent être révoquées lorsqu'elles ne sont plus nécessaires, y compris lorsqu'un utilisateur passe à un autre projet ou à une autre fonction. Les privilèges d'administrateur ne doivent être accordés qu'à un petit groupe d'administrateurs approuvés. Les autorisations doivent être examinées régulièrement pour éviter toute dérive. Les comptes des machines ou des systèmes doivent recevoir le plus petit ensemble d'autorisations nécessaires pour effectuer leurs tâches.

Anti-modèles courants :

- Octroi par défaut des autorisations d'administrateur aux utilisateurs.
- Utilisation de l'utilisateur root pour les activités quotidiennes.
- Création de politiques trop permissives, mais sans tous les privilèges d'administrateur.
- Absence de révision des autorisations pour comprendre si elles autorisent l'accès selon le principe du moindre privilège.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Le principe du moindre privilège établit que les identités ne doivent être autorisées à effectuer que le plus petit ensemble d'actions nécessaires pour accomplir une tâche spécifique. Il permet d'atteindre un équilibre entre la convivialité, l'efficacité et la sécurité. Le respect de ce principe permet de limiter l'accès non intentionnel et de déterminer qui a accès aux ressources. Les utilisateurs et les rôles IAM n'ont aucune autorisation par défaut. L'utilisateur root dispose d'une accès complet par défaut et doit être étroitement contrôle et surveillé. De plus, il doit être utilisé uniquement pour des tâches qui requièrent un accès root.

Les politiques IAM sont utilisées pour octroyer explicitement des autorisations aux rôles IAM ou à des ressources spécifiques. Par exemple, les politiques basées sur l'identité peuvent être attachées à des groupes IAM, tandis que les compartiments S3 peuvent être contrôlés par des politiques basées sur les ressources.

Lorsque vous créez une politique IAM, vous pouvez spécifier les actions de service, les ressources et les conditions qui doivent être remplies pour qu'AWS autorise ou refuse l'accès. AWS prend en charge diverses conditions pour vous aider à limiter l'accès. Par exemple, en utilisant la clé de condition `PrincipalOrgID`, vous pouvez refuser des actions si le demandeur ne fait pas partie de votre AWS Organization.

Vous pouvez également contrôler les demandes effectuées par les services AWS en votre nom, par exemple AWS CloudFormation qui crée une fonction AWS Lambda, en utilisant la clé de condition `CalledVia`. Vous devez superposer différents types de politiques pour établir une défense en profondeur et limiter les autorisations globales de vos utilisateurs. Vous pouvez également limiter les autorisations qui peuvent être accordées et sous quelles conditions. Par exemple, vous pouvez autoriser les équipes de votre application à créer leurs propres politiques IAM pour les systèmes qu'elles créent, mais vous devez également appliquer une limite d'autorisation afin de restreindre les autorisations maximum que le système peut recevoir.

Étapes d'implémentation

- Implémentez des politiques du moindre privilège : attribuez des politiques d'accès avec le moins de privilèges possibles aux groupes et rôles IAM pour rester cohérent avec le rôle ou la fonction de l'utilisateur que vous avez défini.
  - Politiques de base sur l'utilisation des API : pour déterminer les autorisations nécessaires, vous pouvez notamment passer en revue les journaux AWS CloudTrail. Cela vous permet de créer des autorisations adaptées aux actions généralement effectuées par l'utilisateur dans AWS. IAM

Access Analyzer peut générer automatiquement une politique IAM basée sur l'activité. Vous pouvez utiliser IAM Access Advisor au niveau de l'organisation ou du compte pour suivre les dernières informations consultées pour une politique particulière.

- Envisagez d'utiliser des politiques gérées par AWS pour les fonctions professionnelles. Lorsque vous commencez à créer des politiques d'autorisations détaillées, il peut être difficile de savoir par où commencer. AWS dispose de politiques gérées pour les rôles professionnels courants, par exemple la facturation, les administrateurs de bases de données et les scientifiques des données. Ces politiques peuvent permettre de restreindre l'accès des utilisateurs en déterminant comment mettre en œuvre les politiques reposant sur le principe du moindre privilège.
- Supprimez les autorisations inutiles : supprimez les autorisations qui ne sont pas nécessaires et réduisez les politiques trop permissives. La génération de politique IAM Access Analyzer peut vous aider à affiner les politiques d'autorisations.
- Assurez-vous que les utilisateurs ont un accès limité aux environnements de production : les utilisateurs ne doivent avoir accès aux environnements de production qu'avec un cas d'utilisation valide. Une fois que l'utilisateur a effectué les tâches précises qui nécessitent un accès en production, cet accès doit être révoqué. Le fait de limiter l'accès aux environnements de production permet de prévenir les événements imprévus ayant une incidence sur la production et réduit la portée des répercussions de l'accès involontaire.
- Envisagez des limites d'autorisations : une limite des autorisations est une fonction qui permet d'utiliser une stratégie gérée définissant les autorisations maximales qu'une entité IAM peut recevoir d'une politique basée sur une identité. La limite des autorisations d'une entité lui permet d'exécuter uniquement les actions autorisées par ses stratégies basées sur l'identité et ses limites d'autorisations.
- Envisagez les balises de ressources pour les autorisations : un modèle de contrôle d'accès basé sur des attributs utilisant des balises de ressources vous permet d'accorder l'accès en fonction de l'objectif de la ressource, du propriétaire, de l'environnement ou d'autres critères. Par exemple, vous pouvez utiliser des balises de ressources pour différencier les environnements de développement et de production. En utilisant ces balises, vous pouvez limiter les développeurs à l'environnement de développement. En combinant les politiques de balisage et d'autorisations, vous pouvez obtenir un accès précis aux ressources sans avoir à définir des politiques compliquées et personnalisées pour chaque fonction professionnelle.
- Utilisez les politiques de contrôle des services pour AWS Organizations. Les politiques de contrôle des services contrôlent de façon centralisée les autorisations disponibles maximum pour les comptes membres de votre organisation. Il est important de noter que les politiques de contrôle des services vous permettent de limiter les autorisations des utilisateurs root dans les comptes

membres. Envisagez également d'utiliser AWS Control Tower, qui fournit des contrôles gérés normatifs permettant d'enrichir AWS Organizations. Vous pouvez également définir vos propres contrôles dans Control Tower.

- Établissez une politique de cycle de vie de l'utilisateur pour votre organisation : les politiques du cycle de vie de l'utilisateur définissent les tâches à effectuer lorsque les utilisateurs sont intégrés à AWS, changent de rôle ou de fonctions, ou qu'ils n'ont plus besoin d'accéder à AWS. Les autorisations doivent être vérifiées à chaque étape du cycle de vie d'un utilisateur pour s'assurer qu'elles sont suffisamment restrictives et éviter les dérives.
- Établissez un calendrier régulier pour passer en revue les autorisations et supprimer les autorisations inutiles : vous devez régulièrement passer en revue les accès utilisateur afin de vérifier que les utilisateurs ne disposent pas d'un accès trop permissif. AWS Config et IAM Access Analyzer peuvent être utiles pour auditer les autorisations utilisateur.
- Établissez une matrice des fonctions : une matrice des fonctions permet de visualiser les différents rôles et les niveaux d'accès requis pour votre empreinte AWS. À l'aide d'une matrice des fonctions, vous pouvez définir et séparer les autorisations en fonction des responsabilités des utilisateurs au sein de votre organisation. Utilisez des groupes au lieu d'appliquer des autorisations directement aux utilisateurs ou rôles individuels.

Ressources

Documents connexes :

- Accorder un accès selon le principe du moindre privilège
- Limites d'autorisations pour les entités IAM
- Techniques for writing least privilege IAM policies
- IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity
- Delegate permission management to developers by using IAM permissions boundaries
- Ajustement des autorisations dans AWS à l'aide des dernières informations consultées
- Politiques et autorisations dans IAM
- Test des politiques IAM avec le simulateur de politiques IAM
- Guardrails in AWS Control Tower
- Zero Trust architectures: An AWS perspective

- How to implement the principle of least privilege with CloudFormation StackSets
- Contrôle d'accès basé sur les attributs (ABAC)
- Réduction de la portée de la politique en affichant l'activité des utilisateurs
- Afficher l'accès du rôle
- Use Tagging to Organize Your Environment and Drive Accountability
- AWS Tagging Strategies
- Tagging AWS resources

Vidéos connexes :

- Next-generation permissions management
- Zero Trust: An AWS perspective
- How can I use permissions boundaries to limit users and roles to prevent privilege escalation?

Exemples connexes :

- Atelier : IAM permissions boundaries delegating role creation
- Atelier : IAM tag based access control for EC2

SEC03-BP03 Établir un processus d'accès d'urgence

Élaborez un processus permettant un accès d'urgence à vos charges de travail dans le cas peu probable où un problème avec votre fournisseur d'identité centralisé surviendrait.

Vous devez concevoir des processus pour les différents modes de défaillance susceptibles de provoquer un événement d'urgence. Par exemple, dans des circonstances normales, les utilisateurs en interne se fédèrent au cloud à l'aide d'un fournisseur d'identité centralisé (SEC02-BP04) pour gérer leur charge de travail. Toutefois, si votre fournisseur d'identité centralisé échoue ou si la configuration de la fédération dans le cloud est modifiée, les utilisateurs en interne risquent de ne pas parvenir à se fédérer dans le cloud. Un processus d'accès d'urgence permet aux administrateurs autorisés d'accéder à vos ressources cloud par d'autres moyens (tels qu'une autre forme de fédération ou un accès utilisateur direct) afin de résoudre les problèmes liés à la configuration de la fédération ou à vos charges de travail. Le processus d'accès d'urgence est utilisé jusqu'à ce que le mécanisme de fédération normal soit rétabli.

Résultat souhaité :

- Vous avez défini et documenté les modes de défaillance considérés comme une urgence : envisagez les circonstances habituelles et les systèmes dont dépendent vos utilisateurs pour gérer leurs charges de travail. Réfléchissez à la façon dont chacune de ces dépendances peut échouer et provoquer une situation d'urgence. Les questions et les bonnes pratiques du pilier Fiabilité vous aideront à identifier les modes de défaillance et à concevoir des systèmes plus résilients afin de minimiser le risque de défaillance.
- Vous avez documenté les étapes à suivre pour confirmer qu'une défaillance est une urgence. Par exemple, vous pouvez demander aux administrateurs d'identité de vérifier l'état des fournisseurs d'identité principal et secondaire et, si les deux ne sont pas disponibles, de déclarer un événement d'urgence pour cause de défaillance du fournisseur d'identité.
- Vous avez défini un processus d'accès d'urgence spécifique à chaque type d'urgence ou de mode de défaillance. En étant aussi précis que possible, vous éviterez que les utilisateurs abusent d'un processus général pour tous les types d'urgence. Vos processus d'accès d'urgence décrivent les circonstances dans lesquelles chaque processus doit être utilisé, et inversement les situations dans lesquelles le processus ne doit pas être utilisé et renvoie à d'autres processus qui peuvent s'appliquer.
- Vos processus sont bien documentés avec des instructions détaillées et des playbooks qui peuvent être suivis rapidement et efficacement. N'oubliez pas qu'un événement d'urgence peut être stressant pour vos utilisateurs et qu'ils peuvent être soumis à des contraintes de temps extrêmes. Concevez donc votre processus de manière à ce qu'il soit aussi simple que possible.

Anti-modèles courants :

- Vous ne disposez pas de processus d'accès d'urgence bien documentés et bien testés. Vos utilisateurs ne sont pas préparés à une situation d'urgence et suivent des processus improvisés lorsqu'une situation d'urgence survient.
- Vos processus d'accès d'urgence dépendent des mêmes systèmes (tels qu'un fournisseur d'identité centralisé) que vos mécanismes d'accès habituels. Autrement dit, la défaillance d'un système de ce type peut avoir un impact à la fois sur vos mécanismes d'accès habituels et sur les mécanismes d'accès d'urgence, et nuire à votre capacité à vous remettre de la panne.
- Vos processus d'accès d'urgence sont utilisés dans des situations non urgentes. Par exemple, vos utilisateurs utilisent fréquemment à mauvais escient les processus d'accès d'urgence, car ils trouvent qu'il est plus facile d'apporter des modifications directement que de les soumettre par le biais d'un pipeline.

- Vos processus d'accès d'urgence ne génèrent pas suffisamment de journaux pour auditer les processus, ou les journaux ne sont pas surveillés pour signaler une éventuelle utilisation inappropriée des processus.

Avantages liés au respect de cette bonne pratique :

- En disposant de processus d'accès d'urgence bien documentés et bien testés, vous réduisez le temps nécessaire à vos utilisateurs pour répondre à un événement d'urgence et le résoudre. Cela peut se traduire par une réduction des temps d'arrêt et une meilleure disponibilité des services que vous offrez à vos clients.
- Vous pouvez suivre chaque demande d'accès d'urgence, détecter les tentatives non autorisées d'utilisation abusive du processus pour des événements non urgents et les signaler.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Cette section fournit des conseils pour créer des processus d'accès d'urgence pour plusieurs modes de défaillance liés aux charges de travail déployées sur AWS, en commençant par des conseils communs applicables à tous les modes de défaillance, suivies de directives spécifiques basées sur le type de mode de défaillance.

Conseils communs pour tous les modes de défaillance

Envisagez les points suivants lorsque vous concevez un processus d'accès d'urgence pour un mode de défaillance :

- Documentez les conditions préalables et les hypothèses du processus : situations dans lesquelles le processus doit être utilisé et situations dans lesquelles il ne doit pas être utilisé. Il est utile de détailler le mode de défaillance et de documenter les hypothèses, telles que l'état d'autres systèmes connexes. Par exemple, le processus du mode de défaillance 2 suppose que le fournisseur d'identité est disponible, mais que la configuration sur AWS est modifiée ou a expiré.
- Créez au préalable les ressources nécessaires au processus d'accès d'urgence (SEC10-BP05). Par exemple, créez au préalable le Compte AWS d'accès d'urgence avec les rôles et IAM users, ainsi que les rôles IAM entre comptes dans tous les comptes de la charge de travail. Vous pourrez ainsi vérifier que ces ressources sont prêtes et disponibles en cas d'urgence. En créant des ressources au préalable, vous n'êtes pas tributaire des API de plan de contrôle AWS (utilisées pour créer et modifier les ressources AWS) qui peuvent ne pas être disponibles en cas d'urgence. De

plus, en créant au préalable des ressources IAM, vous n'avez pas besoin de prendre en compte les retards potentiels dus à la cohérence à terme.

- Incluez les processus d'accès d'urgence dans vos plans de gestion des incidents (SEC10-BP02). Documentez la manière dont les événements d'urgence sont suivis et communiqués aux autres membres de votre organisation (tels que vos pairs et la direction) et, le cas échéant, à vos clients et partenaires commerciaux.
- Définissez le processus de demande d'accès d'urgence dans votre système de flux de travail des demandes de service existant, si vous en avez un. Généralement, ces systèmes de flux de travail vous permettent de créer des formulaires de réception pour collecter des informations sur la demande, de suivre la demande à chaque étape du flux de travail et d'ajouter des étapes d'approbation automatisées et manuelles. Associez chaque demande à un événement d'urgence correspondant suivi dans votre système de gestion des incidents. Le fait de disposer d'un système uniforme pour les accès d'urgence vous permet de suivre ces demandes dans un seul système, d'analyser les tendances d'utilisation et d'améliorer vos processus.
- Vérifiez que vos processus d'accès d'urgence ne peuvent être initiés que par des utilisateurs autorisés et nécessitent l'approbation de pairs ou de la direction de l'utilisateur, le cas échéant. Le processus d'approbation doit fonctionner efficacement pendant les heures de bureau et au-delà. Définissez comment les demandes d'approbation autorisent les approbateurs secondaires si les approbateurs principaux ne sont pas disponibles et comment elles remontent dans la chaîne de gestion jusqu'à ce qu'elles soient approuvées.
- Vérifiez que le processus génère des journaux d'audit et des événements détaillés pour les tentatives d'accès d'urgence qui aboutissent et pour celles qui échouent. Surveillez à la fois le processus de demande et le mécanisme d'accès d'urgence pour détecter les abus ou les accès non autorisés. Corrélez l'activité avec les événements d'urgence en cours depuis votre système de gestion des incidents et signalez les situations où des actions se produisent en dehors des périodes prévues. Par exemple, vous devez surveiller le Compte AWS d'accès d'urgence et signaler toute activité, car il ne doit jamais être utilisé dans le cadre des opérations habituelles.
- Testez régulièrement les processus d'accès d'urgence pour vérifier que les étapes sont claires et accorder le niveau d'accès approprié rapidement et efficacement. Vos processus d'accès d'urgence doivent être testés dans le cadre de simulations de réponse aux incidents (SEC10-BP07) et de tests de reprise après sinistre (REL13-BP03).

Mode de défaillance 1 : le fournisseur d'identité utilisé pour la fédération à AWS n'est pas disponible

Comme décrit dans SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé, nous vous recommandons de faire appel à un fournisseur d'identité centralisé pour fédérer les utilisateurs en

interne et accorder l'accès aux Comptes AWS. Vous pouvez fédérer les utilisateurs à plusieurs Comptes AWS au sein de votre organisation AWS à l'aide de IAM Identity Center, ou vous pouvez les fédérer à des Comptes AWS individuels avec IAM. Dans les deux cas, les utilisateurs en interne s'authentifient auprès de votre fournisseur d'identité centralisé avant d'être redirigés vers un point de terminaison de connexion AWS pour l'authentification unique.

Dans le cas peu probable où votre fournisseur d'identité centralisé ne serait pas disponible, les utilisateurs en interne ne pourraient pas se fédérer aux Comptes AWS ni gérer leurs charges de travail. Dans ce cas d'urgence, vous pouvez fournir un processus d'accès d'urgence permettant à un petit groupe d'administrateurs d'accéder aux Comptes AWS pour effectuer des tâches critiques qui ne peuvent pas attendre que vos fournisseurs d'identité centralisés soient de nouveau disponibles. Par exemple, votre fournisseur d'identité n'est pas disponible pendant 4 heures et, durant cette période, vous devez modifier les limites supérieures d'un groupe Amazon EC2 Auto Scaling dans un compte de production pour faire face à un pic inattendu du trafic client. Vos administrateurs d'urgence doivent suivre le processus d'accès d'urgence pour accéder au Compte AWS de production spécifique et apporter les modifications nécessaires.

Le processus d'accès d'urgence repose sur un Compte AWS d'accès d'urgence créé au préalable, qui est utilisé uniquement pour l'accès d'urgence et dispose de ressources AWS (comme les rôles IAM et les IAM users) pour soutenir le processus d'accès d'urgence. Pendant les opérations normales, personne ne doit accéder au compte d'accès d'urgence et vous devez surveiller et signaler tout cas d'utilisation abusive de ce compte (pour plus de détails, consultez la section précédente consacrée aux conseils communs).

Le compte d'accès d'urgence possède des rôles IAM d'accès d'urgence autorisés à endosser des rôles entre comptes dans les Comptes AWS nécessitant un accès d'urgence. Ces rôles IAM sont créés au préalable et configurés avec des politiques d'approbation qui assurent la validité des rôles IAM du compte d'urgence.

Le processus d'accès d'urgence peut utiliser l'une des approches suivantes :

- Vous pouvez créer au préalable un ensemble d'IAM users pour vos administrateurs d'urgence dans le compte d'accès d'urgence avec des mots de passe forts et des jetons MFA associés. Ces IAM users seront autorisés à endosser les rôles IAM qui autoriseront ensuite l'accès intercompte au Compte AWS où un accès d'urgence est requis. Nous vous recommandons de créer le moins d'utilisateurs possible et d'affecter chaque utilisateur à un seul administrateur d'urgence. En cas d'urgence, un utilisateur administrateur d'urgence se connecte au compte d'accès d'urgence à l'aide de son mot de passe et de son code de jeton MFA, passe au rôle IAM d'accès d'urgence dans le compte d'urgence, puis passe au rôle IAM d'accès d'urgence dans le compte de la charge

de travail pour effectuer l'action de modification d'urgence. L'avantage de cette approche est que chaque IAM user est associé à un seul administrateur d'urgence et que vous pouvez savoir quel utilisateur s'est connecté en consultant les événements CloudTrail. L'inconvénient est que vous devez gérer plusieurs IAM users avec leurs mots de passe de longue durée de vie et leurs jetons MFA associés.

- Vous pouvez utiliser l'utilisateur root du Compte AWS d'accès d'urgence pour vous connecter au compte d'accès d'urgence, endosser le rôle IAM d'accès d'urgence et endosser le rôle entre comptes dans le compte de la charge de travail. Nous recommandons de définir un mot de passe fort et plusieurs jetons MFA pour l'utilisateur root. Nous conseillons également de stocker le mot de passe et les jetons MFA dans un coffre-fort d'informations d'identification d'entreprise sécurisé qui applique des mécanismes solides d'authentification et d'autorisation. Vous devez sécuriser les facteurs de réinitialisation des mots de passe et des jetons MFA : configurez l'adresse e-mail du compte sur une liste de distribution surveillée par vos administrateurs de sécurité cloud, et le numéro de téléphone du compte doit être un numéro partagé également surveillé par ces administrateurs. L'avantage de cette approche est qu'il n'existe qu'un seul ensemble d'informations d'identification d'utilisateur root à gérer. L'inconvénient est qu'étant donné qu'il s'agit d'un utilisateur partagé, plusieurs administrateurs ont la possibilité de se connecter en tant qu'utilisateur root. Vous devez auditer les événements de journal de votre coffre-fort d'entreprise pour identifier quel administrateur a extrait le mot de passe de l'utilisateur root.

Mode de défaillance 2 : la configuration du fournisseur d'identité sur AWS est modifiée ou a expiré

Pour permettre aux utilisateurs en interne de se fédérer aux Comptes AWS, vous pouvez configurer la IAM Identity Center auprès d'un fournisseur d'identité externe ou créer un fournisseur d'identité IAM (SEC02-BP04). Généralement, vous les configurez en important un document XML de métadonnées SAML fourni par votre fournisseur d'identité. Ce document XML de métadonnées inclut un certificat X.509 correspondant à une clé privée que le fournisseur d'identité utilise pour signer ses assertions SAML.

Ces configurations côté AWS peuvent être modifiées ou supprimées par erreur par un administrateur. Dans un autre scénario, le certificat X.509 importé dans AWS peut expirer, et aucun nouveau fichier XML de métadonnées contenant un nouveau certificat n'a encore été importé dans AWS. Ces deux scénarios peuvent désactiver la fédération des utilisateurs en interne à AWS, ce qui peut entraîner une situation d'urgence.

Dans un tel cas d'urgence, vous pouvez fournir à vos administrateurs d'identité un accès à AWS pour résoudre les problèmes de fédération. Par exemple, votre administrateur d'identité utilisera le

processus d'accès d'urgence pour se connecter au Compte AWS d'accès d'urgence, passera à un rôle dans le compte administrateur d'Identity Center et mettra à jour la configuration du fournisseur d'identité externe en important le dernier document XML de métadonnées SAML de votre fournisseur d'identité afin de réactiver la fédération. Une fois la fédération rétablie, les utilisateurs en interne pourront continuer à utiliser le processus d'exploitation habituel pour se fédérer aux comptes de leur charge de travail.

Vous pouvez suivre les approches détaillées dans le précédent mode de défaillance 1 pour créer un processus d'accès d'urgence. Vous pouvez accorder des autorisations de moindre privilège aux administrateurs d'identité pour qu'ils ne puissent accéder qu'au compte administrateur d'Identity Center et effectuer des actions sur Identity Center dans ce compte uniquement.

Mode de défaillance 3 : interruption d'Identity Center

Dans le cas peu probable où une Région AWS ou une connexion IAM Identity Center serait interrompue, nous vous recommandons de créer une configuration que vous pourrez utiliser pour assurer un accès temporaire à la AWS Management Console.

Le processus d'accès d'urgence utilise une fédération directe entre votre fournisseur d'identité et IAM dans un compte d'urgence. Pour plus de détails sur le processus et les considérations de conception, voir Configurer un accès d'urgence à la AWS Management Console.

Étapes d'implémentation

Étapes communes pour tous les modes de défaillance

- Créez un Compte AWS dédié aux processus d'accès d'urgence. Créez au préalable les ressources IAM nécessaires dans le compte, telles que les rôles IAM ou les IAM users et, éventuellement, les fournisseurs d'identité IAM. En outre, créez au préalable des rôles IAM entre comptes dans les Comptes AWS de la charge de travail avec des relations d'approbation avec les rôles IAM correspondants dans le compte d'accès d'urgence. Vous pouvez utiliser AWS CloudFormation StackSets avec AWS Organizations pour créer ces ressources dans les comptes membres de votre organisation.

- Créez des politiques de contrôle des services AWS Organizations (SCP) pour refuser la suppression et la modification des rôles IAM entre comptes dans les Comptes AWS membres.
- Activez CloudTrail pour le Compte AWS d'accès d'urgence et envoyez les événements de suivi vers un compartiment S3 central du Compte AWS de collecte de journaux. Si vous utilisez AWS Control Tower pour configurer et gérer votre environnement AWS multi-comptes, chaque compte

que vous créez avec AWS Control Tower ou que vous inscrivez dans AWS Control Tower est activé pour CloudTrail par défaut et envoyé vers un compartiment S3 dans un Compte AWS d'archive de journal dédié.

- Surveillez l'activité du compte d'accès d'urgence en créant des règles EventBridge qui correspondent lors de la connexion à la console et de l'activité de l'API en fonction des rôles IAM d'urgence. Envoyez des notifications à votre centre des opérations de sécurité lorsque des activités se produisent en dehors d'un événement d'urgence en cours suivi dans votre système de gestion des incidents.

Étapes supplémentaires pour le mode de défaillance 1 : le fournisseur d'identité utilisé pour la fédération à AWS n'est pas disponible et pour le mode de défaillance 2 : la configuration du fournisseur d'identité sur AWS est modifiée ou a expiré

- Créez des ressources au préalable en fonction du mécanisme que vous avez choisi pour l'accès d'urgence :
  - Avec les IAM users: créez au préalable les IAM users avec des mots de passe forts et les dispositifs MFA associés.
  - Avec l'utilisateur root du compte d'urgence : configurez l'utilisateur root avec un mot de passe fort et stockez ce mot de passe dans le coffre-fort d'informations d'identification de votre entreprise. Associez plusieurs appareils MFA physiques à l'utilisateur root et stockez-les à des emplacements auxquels les membres de votre équipe d'administrateurs d'urgence peuvent accéder rapidement.

Étapes supplémentaires pour le mode de défaillance 3 : interruption d'Identity Center

- Comme indiqué dans Configurer un accès d'urgence à la AWS Management Console, dans le Compte AWS d'accès d'urgence, créez un fournisseur d'identité IAM pour activer la fédération SAML directe à partir de votre fournisseur d'identité.
- Créez des groupes d'opérations d'urgence dans votre fournisseur d'identité sans aucun membre.
- Créez des rôles IAM correspondant aux groupes d'opérations d'urgence dans le compte d'accès d'urgence.

Ressources

Bonnes pratiques Well-Architected connexes :

- SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège
- SEC10-BP02 Développer des plans de gestion des incidents
- SEC10-BP07 Organiser des jeux de rôle

Documents connexes :

- Configurer un accès d'urgence à la AWS Management Console
- Permettre aux utilisateurs fédérés SAML 2.0 d'accéder à la AWS Management Console
- Accès en mode « bris de glace »

Vidéos connexes :

- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive

Exemples connexes :

- AWS Break Glass Role
- AWS customer playbook framework
- AWS incident response playbook samples

SEC03-BP04 Limiter les autorisations au minimum requis en permanence

Au fur et à mesure que vos équipes déterminent les accès nécessaires, supprimez les autorisations inutiles et mettez en place des processus de révision afin d'obtenir des autorisations de moindre privilège. Surveillez et supprimez en permanence les identités et autorisations inutilisées pour les accès humains et machine.

Résultat souhaité : les politiques d'autorisation doivent respecter le principe du moindre privilège. Au fur et à mesure que les tâches et les rôles sont mieux définis, vos politiques d'autorisation doivent être revues de façon à supprimer les autorisations inutiles. Cette approche réduit l'impact si les informations d'identification sont exposées par inadvertance ou autrement consultées sans autorisation.

Anti-modèles courants :

- Octroi par défaut des autorisations d'administrateur aux utilisateurs.
- Création de politiques trop permissives, mais sans tous les privilèges d'administrateur.
- Maintien des politiques d'autorisation une fois qu'elles ne sont plus nécessaires.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : moyen

Directives d'implémentation

Lorsque les équipes et les projets ne font que commencer, des politiques d'autorisation permissives peuvent être utilisées pour favoriser l'innovation et l'agilité. Par exemple, dans un environnement de développement ou de test, les développeurs peuvent se voir octroyer un accès à un large éventail de services AWS. Nous vous recommandons d'évaluer l'accès en continu et de restreindre l'accès aux services et aux actions de service nécessaires pour effectuer le travail en cours. Nous recommandons cette évaluation pour les identités humaines et machine. Les identités machine, parfois appelées comptes de système ou de service, donnent un accès AWS aux applications ou aux serveurs. Cet accès est particulièrement important dans un environnement de production, où des autorisations trop permissives peuvent avoir un impact important et exposer les données des clients.

AWS fournit plusieurs méthodes pour identifier les utilisateurs, les rôles, les autorisations et les informations d'identification inutilisés. AWS peut également faciliter l'analyse de l'activité d'accès des utilisateurs et rôles IAM, notamment des clés associées, ainsi que l'accès aux ressources AWS telles que les objets dans les compartiments Amazon S3. La génération de politiques AWS Identity and Access Management Access Analyzer peut vous aider à créer des politiques d'autorisations restrictives basées sur les services et les actions réels avec lesquels un principal interagit. Le contrôle d'accès basé sur les attributs (ABAC) peut permettre de simplifier la gestion des autorisations, car vous pouvez fournir des autorisations aux utilisateurs en utilisant leurs attributs au lieu d'associer des politiques d'autorisations directement à chaque utilisateur.

Étapes d'implémentation

- Utilisez AWS Identity and Access Management Access Analyzer : IAM Access Analyzer permet d'identifier les ressources de votre organisation et des comptes, comme les compartiments Amazon Simple Storage Service (Amazon S3) ou les rôles IAM qui sont partagés avec une entité externe.
- Utilisez la génération de politiques IAM Access Analyzer : la génération de politiques IAM Access Analyzer vous permet de créer des politiques d'autorisation détaillées basées sur l'activité d'accès d'un utilisateur ou d'un rôle IAM.

- Déterminez un calendrier et une politique d'utilisation acceptables pour les utilisateurs et les rôles IAM : utilisez l'horodatage des derniers accès pour identifier les utilisateurs et les rôles inutilisés et les supprimer. Passez en revue les informations relatives aux services et actions consultés en dernier afin d'identifier et de restreindre les autorisations à des utilisateurs et des rôles spécifiques. Par exemple, vous pouvez utiliser les dernières informations consultées pour identifier les actions Amazon S3 spécifiques dont votre rôle d'application a besoin et limiter l'accès du rôle à celles-ci uniquement. Ces fonctionnalités relatives aux informations sur les derniers accès sont disponibles dans la AWS Management Console et par programmation pour vous permettre de les intégrer dans vos flux de travail d'infrastructure et vos outils automatisés.
- Envisagez de consigner les événements de données dans AWS CloudTrail : par défaut, CloudTrail ne consigne pas les événements de données tels que l'activité au niveau des objets Amazon S3 (par exemple, `GetObject` et `DeleteObject`) ou les activités de table Amazon DynamoDB (par exemple, `PutItem` et `DeleteItem`). Envisagez d'autoriser la journalisation de ces événements afin de déterminer quels utilisateurs et rôles ont besoin d'accéder à des objets Amazon S3 ou des éléments de table DynamoDB spécifiques.

Ressources

Documents connexes :

- Grant least privilege
- Remove unnecessary credentials
- Qu'est-ce qu'AWS CloudTrail ?
- Gestion des politiques IAM
- Journalisation et surveillance dans DynamoDB
- Activation de la journalisation des événements CloudTrail pour les compartiments et les objets Amazon S3
- Obtenir des rapports d'informations d'identification pour votre Compte AWS

Vidéos connexes :

- Become an IAM Policy Master in 60 Minutes or Less
- Separation of Duties, Least Privilege, Delegation, and CI/CD
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive

SEC03-BP05 Définir des protections par autorisation pour votre organisation

Établissez des contrôles communs qui limitent l'accès à toutes les identités de votre organisation. Par exemple, vous pouvez restreindre l'accès à des Régions AWS spécifiques ou empêcher vos techniciens de supprimer des ressources communes, telles qu'un rôle IAM utilisé pour votre équipe de sécurité centrale.

Anti-modèles courants :

- Exécution des charges de travail dans votre compte d'administrateur organisationnel.
- Exécution des charges de travail de production et autres dans le même compte.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : Moyen

Directives d'implémentation

Au fur et à mesure que vous développez et gérez des charges de travail supplémentaires dans AWS, vous devez séparer ces charges de travail à l'aide de comptes et gérer ces comptes à l'aide d'AWS Organizations. Nous vous recommandons d'établir des protections par autorisation communes qui limitent l'accès à toutes les identités de votre organisation. Par exemple, vous pouvez restreindre l'accès à des Régions AWS spécifiques ou empêcher votre équipe de supprimer des ressources communes, telles qu'un rôle IAM utilisé par votre équipe de sécurité centrale.

Vous pouvez commencer en implémentant des exemples de politiques de contrôle des services, par exemple en empêchant les utilisateurs de désactiver les services clés. Les SCP utilisent le langage de politique IAM et vous permettent d'établir des contrôles auxquels tous les principaux (utilisateurs et rôles) IAM adhèrent. Vous pouvez restreindre l'accès à des actions de service spécifiques, à des ressources et en fonction de conditions spécifiques pour répondre aux besoins de contrôle d'accès de votre organisation. Si nécessaire, vous pouvez définir des exceptions à vos barrières de protection. Par exemple, vous pouvez restreindre les actions de service pour toutes les entités IAM du compte, à l'exception d'un rôle d'administrateur spécifique.

Nous vous déconseillons l'exécution de vos charges de travail dans votre compte de gestion. Le compte de gestion doit être utilisé afin de gouverner et déployer des barrières de protection en matière de sécurité qui affecteront les comptes des membres. Certains services AWS prennent en charge l'utilisation d'un compte d'administrateur délégué. Lorsqu'il est disponible, nous vous

recommandons d'utiliser ce compte délégué plutôt que le compte de gestion. Vous devez limiter fortement l'accès au compte d'administrateur organisationnel.

La mise en place d'une stratégie multicompte vous permet de bénéficier d'une plus grande flexibilité dans l'application de barrières de protection à vos charges de travail. L'AWS Security Reference Architecture propose des conseils normatifs en ce qui concerne la conception de la structure de votre compte. Les services AWS tels qu'AWS Control Tower offrent des capacités de gestion centralisée des contrôles préventifs et de détection au sein de votre organisation. Définissez un objectif clair pour chaque compte ou unité opérationnelle au sein de votre organisation et limitez les contrôles conformément à cet objectif.

Ressources

Documents connexes :

- AWS Organizations
- Politiques de contrôle de service (SCP)
- Get more out of service control policies in a multi-account environment
- AWS Architecture de référence de sécurité (AWS SRA)

Vidéos connexes :

- Enforce Preventive Guardrails using Service Control Policies
- Building governance at scale with AWS Control Tower
- AWS Identity and Access Management deep dive

SEC03-BP06 Gérer l'accès en fonction du cycle de vie

Intégrez les contrôles d'accès au cycle de vie des opérateurs et des applications et à votre fournisseur de fédération centralisée. Par exemple, supprimez l'accès d'un utilisateur lorsqu'il quitte l'organisation ou change de poste.

Lorsque vous gérez des charges de travail à l'aide de comptes distincts, vous devrez partager des ressources entre ces comptes. Nous vous recommandons de partager des ressources à l'aide d' AWS Resource Access Manager (AWS RAM). Ce service vous permet de partager facilement et en toute sécurité des ressources AWS au sein de votre AWS Organizations et de vos unités d'organisation. Avec AWS RAM, l'accès aux ressources partagées est automatiquement accordé ou

révoqué lorsque les comptes sont déplacés vers et hors de l'organisation ou de l'unité d'organisation avec laquelle ils sont partagés. Cela permet de vous assurer que les ressources sont uniquement partagées avec les comptes que vous souhaitez.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

Cycle de vie de l'accès utilisateur : implémentez une stratégie de cycle de vie d'accès utilisateur pour les nouveaux utilisateurs qui rejoignent l'entreprise, les changements de poste et les utilisateurs qui quittent l'entreprise, afin que seuls les utilisateurs actifs disposent d'un accès approprié.

Ressources

Documents connexes :

- Contrôle d'accès basé sur les attributs (ABAC)
- Accorder le privilège le plus faible
- IAM Access Analyzer
- Suppression des informations d'identification inutiles
- Travailler avec des stratégies

Vidéos connexes :

- Devenir un expert en stratégie IAM en 60 minutes maximum
- Séparation des responsabilités, moindre privilège, délégation et CI/CD

SEC03-BP07 Analyser l'accès public et entre les comptes

Surveillez en continu les résultats qui mettent en évidence l'accès public et intercompte. Limitez l'accès public et intercompte uniquement aux ressources spécifiques qui requièrent ce type d'accès.

Résultat souhaité : savoir quelles ressources AWS sont partagées et avec qui. Surveillez et auditez continuellement vos ressources partagées afin de vérifier qu'elles ne sont partagées qu'avec les principaux autorisés.

Anti-modèles courants :

- Ne pas tenir un inventaire des ressources partagées.

- Ne pas suivre de processus pour régir l'accès intercompte et public aux ressources.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : faible

Directives d'implémentation

Si votre compte est dans AWS Organizations, vous pouvez accorder l'accès aux ressources à l'ensemble de l'organisation, à des unités d'organisation spécifiques ou à des comptes individuels. Si votre compte n'est pas membre d'une organisation, vous pouvez partager des ressources avec des comptes individuels. Vous pouvez accorder un accès direct intercompte à l'aide de politiques axées sur les ressources, par exemple les politiques de compartiment Amazon Simple Storage Service (Amazon S3), ou en autorisant un principal dans un autre compte à assumer un rôle IAM dans votre compte. Lorsque vous utilisez des politiques de ressources, vérifiez que l'accès n'est accordé qu'aux principaux autorisés. Définissez un processus d'approbation de toutes les ressources qui doivent être accessibles au public.

AWS Identity and Access Management Access Analyzer utilise une sécurité prouvable pour identifier tous les chemins d'accès à une ressource depuis l'extérieur de son compte. Il passe en revue les stratégies de ressources en continu et présente les résultats d'accès public et intercompte pour vous permettre d'analyser facilement un accès potentiellement étendu. Envisagez de configurer IAM Access Analyzer avec AWS Organizations afin de vérifier que vous avez une visibilité sur tous vos comptes. IAM Access Analyzer vous permet également de prévisualiser les résultats avant de déployer les autorisations des ressources. Vous pouvez ainsi vérifier que vos modifications de politique n'accordent que l'accès public et intercompte prévu à vos ressources. Lors de la conception pour un accès multicompte, vous pouvez utiliser les politiques d'approbation afin de contrôler dans quels cas un rôle peut être assumé. Par exemple, vous pouvez utiliser la clé de condition `PrincipalOrgId` pour refuser une tentative d'assumer un rôle depuis l'extérieur de votre AWS Organizations.

AWS Config peut signaler les ressources qui sont mal configurées et, via des contrôles de politique AWS Config, il peut détecter les ressources pour lesquelles un accès public est configuré. Des services tels que AWS Control Tower et AWS Security Hub simplifient le déploiement des contrôles de détection et des barrières de protection dans AWS Organizations afin d'identifier et de résoudre les problèmes des ressources exposées au public. Par exemple, AWS Control Tower a une barrière de protection gérée qui peut détecter si des instantanés Amazon EBS peuvent être restaurés par des Comptes AWS.

Étapes d'implémentation

- Envisagez d'activer AWS Config pour AWS Organizations : AWS Config vous permet de regrouper les résultats de plusieurs comptes d'un AWS Organizations dans un compte d'administrateur délégué. Cela fournit une vue d'ensemble et vous permet de déployer AWS Config Rules sur plusieurs comptes afin de détecter les ressources accessibles publiquement.
- Configurez AWS Identity and Access Management Access Analyzer IAM Access Analyzer vous permet d'identifier les ressources de votre organisation et les comptes, par exemple les compartiments Amazon S3 ou les rôles IAM qui sont partagés avec une entité externe.
- Utilisez l'atténuation automatique dans AWS Config pour répondre aux changements apportés à la configuration de l'accès public des compartiments Amazon S3 : Vous pouvez réactiver automatiquement les paramètres d'accès public du bloc pour les compartiments Amazon S3.
- Implémentez la surveillance et les alertes afin de déterminer si les compartiments Amazon S3 sont devenus publics : vous devez mettre en place la surveillance et les alertes pour identifier si le Blocage de l'accès public Amazon S3 est désactivé et si les compartiments Amazon S3 deviennent publics. De plus, si vous utilisez AWS Organizations, vous pouvez créer une politique de contrôle des services qui empêche les modifications des politiques d'accès public Amazon S3. AWS Trusted Advisor vérifie les compartiments Amazon S3 qui ont des autorisations d'accès ouvert. Les autorisations de compartiment qui accordent à tous un accès au chargement ou à la suppression créent des problèmes de sécurité potentiels, en permettant à quiconque d'ajouter, de modifier ou de supprimer les éléments d'un compartiment. La vérification Trusted Advisor examine les autorisations explicites de compartiment et les politiques associées de compartiment susceptibles de remplacer les autorisations du compartiment. Vous pouvez également utiliser AWS Config pour surveiller l'accès public de vos compartiments Amazon S3. Pour plus d'informations, consultez How to Use AWS Config to Monitor for and Respond to Amazon S3 Buckets Allowing Public Access. Lors de l'examen de l'accès, il est important de tenir compte des types de données contenus dans les compartiments Amazon S3. Amazon Macie permet de découvrir et de protéger les données sensibles, comme les PII, les PHI et les informations d'identification, dont les clés privées ou AWS.

Ressources

Documents connexes :

- Utiliser AWS Identity and Access Management Access Analyzer
- Bibliothèque des contrôles AWS Control Tower
- AWS Foundational Security Best Practices standard (Normes concernant les bonnes pratiques de sécurité de base AWS)
- AWS Config Managed Rules (Règles gérées AWS Config)

- Référence de la vérification AWS Trusted Advisor
- Surveillance des résultats de vérification AWS Trusted Advisor avec Amazon EventBridge
- Managing AWS Config Rules Across All Accounts in Your Organization (Gestion des règles AWS Config pour tous les comptes de votre organisation)
- AWS Config et AWS Organizations

Vidéos connexes :

- Best Practices for securing your multi-account environment
- Dive Deep into IAM Access Analyzer

SEC03-BP08 Partager des ressources en toute sécurité au sein de votre organisation

À mesure que le nombre de charges de travail augmente, vous devrez peut-être partager l'accès aux ressources de ces charges de travail ou fournir les ressources plusieurs fois pour plusieurs comptes. Vous pouvez utiliser des constructions pour compartimenter votre environnement, par exemple des environnements de développement, de test et de production. Cependant, le fait d'avoir des constructions distinctes ne vous empêche pas de partager en toute sécurité. En partageant des composants qui se chevauchent, vous pouvez réduire les frais d'exploitation et offrir une expérience cohérente sans avoir à deviner ce que vous avez pu manquer en créant la même ressource plusieurs fois.

Résultat souhaité : limiter autant que possible les accès involontaires en utilisant des méthodes sécurisées pour partager des ressources au sein de votre organisation, et vous aider dans le cadre de votre initiative de prévention de la perte de données. Réduisez vos frais généraux opérationnels par rapport à la gestion de composants individuels, réduisez les erreurs liées à la création manuelle du même composant plusieurs fois et augmentez la capacité de mise à l'échelle de vos charges de travail. Vous pouvez bénéficier d'une réduction du délai de résolution dans les scénarios de défaillance multipoints et augmenter votre confiance dans l'évaluation du moment où un composant n'est plus nécessaire. Pour des conseils normatifs sur l'analyse des ressources partagées en externe, consultez SEC03-BP07 Analyser l'accès public et entre les comptes.

Anti-modèles courants :

- Manque de processus pour surveiller continuellement et alerter automatiquement sur un partage externe inattendu.
- Manque de référence sur ce qui doit être partagé et ce qui ne doit pas l'être.
- Adoption par défaut d'une politique largement ouverte au lieu de la partager explicitement lorsque c'est nécessaire.
- Création manuelle des ressources de base qui se chevauchent si nécessaire.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : moyen

Directives d'implémentation

Concevez vos contrôles et modèles d'accès de façon à régir la consommation de ressources partagées en toute sécurité et uniquement avec des entités approuvées. Surveillez les ressources partagées et examinez l'accès aux ressources partagées en permanence, et soyez alerté sur les partages inappropriés ou inattendus. Consultez Analyser l'accès public et intercompte pour vous aider à établir une gouvernance afin de réduire l'accès externe aux seules ressources qui en ont besoin, et d'établir un processus de surveillance continue et d'alerte automatique.

Le partage intercompte dans AWS Organizations est pris en charge par un certain nombre de services AWS, comme AWS Security Hub, Amazon GuardDuty et AWS Backup. Ces services permettent de partager les données vers un compte central, de rendre les données accessibles à partir d'un compte central ou de gérer les ressources et les données à partir d'un compte central. Par exemple, AWS Security Hub peut transférer les découvertes des comptes individuels vers un compte central où vous pouvez voir toutes ces informations. AWS Backup peut prendre une sauvegarde pour une ressource et la partager entre les comptes. Vous pouvez utiliser AWS Resource Access Manager (AWS RAM) afin de partager d'autres ressources communes, telles que les sous-réseaux VPC et les pièces jointes Transit Gateway, AWS Network Firewall ou les pipelines Amazon SageMaker.

Pour limiter votre compte au partage de ressources au sein de votre organisation, utilisez les politiques de contrôle des services (SCP) afin d'empêcher l'accès aux principaux externes. Lorsque vous partagez des ressources, combinez les contrôles basés sur l'identité et les contrôles réseau afin de créer un périmètre de données pour votre organisation dans le but de contribuer à la protection contre les accès involontaires. Un périmètre de données est un ensemble de barrières de protection préventives qui vous permettent de vous assurer que seules les identités approuvées accèdent aux ressources approuvées à partir des réseaux attendus. Ces contrôles doivent placer des limites appropriées pour les ressources susceptibles d'être partagées et empêcher le partage ou l'exposition de ressources qui ne doivent pas être autorisées. Par exemple, dans le cadre de votre

périmètre de données, vous pouvez utiliser les politiques de point de terminaison VPC et la condition `AWS:PrincipalOrgId` afin de vous assurer que les identités qui accèdent aux compartiments Amazon S3 appartiennent à votre organisation. Il est important de noter que les SCP ne s'appliquent pas aux rôles liés aux services (LSR) ni aux principaux de services AWS.

Lorsque vous utilisez Amazon S3, désactivez les listes de contrôle d'accès pour votre compartiment Amazon S3 et utilisez les politiques IAM pour définir le contrôle des accès. Pour limiter l'accès à une origine Amazon S3 depuis Amazon CloudFront, migrez depuis l'identité d'accès d'origine (OAI) vers le contrôle d'accès d'origine (OAC) qui prend en charge des fonctionnalités supplémentaires, y compris le chiffrement côté serveur avec AWS Key Management Service.

Dans certains cas, vous pouvez autoriser le partage des ressources à l'extérieur de votre organisation ou accorder à un tiers l'accès à vos ressources. Pour des conseils normatifs sur la gestion des autorisations de partage des ressources à l'externe, consultez Gestion des autorisations.

Étapes d'implémentation

1. Utilisez AWS Organizations.

   AWS Organizations est un service de gestion des comptes qui vous permet de regrouper plusieurs Comptes AWS dans une organisation que vous créez et gérez de façon centralisée. Vous pouvez regrouper vos comptes en unités d'organisation (UO) et joindre différentes politiques à chacune d'entre elles afin de vous aider à répondre à vos besoins en matière de budget, de sécurité et de conformité. Vous pouvez également contrôler la façon dont l'intelligence artificielle (IA) et le machine learning (ML) d'AWS peuvent collecter et stocker des données, et utiliser la gestion multicompte des services AWS intégrés à Organizations.
2. Intégrez AWS Organizations aux services AWS.

   Lorsque vous permettez à un service AWS d'effectuer des tâches en votre nom dans les comptes membres de votre organisation, AWS Organizations crée un rôle IAM lié à ce service dans chaque compte membre. Gérez l'accès approuvé à l'aide de la AWS Management Console, des API AWS ou d'AWS CLI. Pour obtenir des conseils normatifs sur la mise en place d'un accès approuvé, consultez Utilisation d'AWS Organizations avec d'autres services AWS et Services AWS que vous pouvez utiliser avec Organizations.
3. Établissez un périmètre de données.

   Le périmètre AWS est généralement représenté comme une organisation gérée par AWS Organizations. Avec les réseaux et les systèmes sur site, l'accès aux ressources AWS est ce que beaucoup considèrent comme le périmètre de mon AWS. L'objectif du périmètre est de vérifier

que l'accès est autorisé si l'identité est approuvée, si la ressource est approuvée et si le réseau est attendu.

a. Définissez et implémentez les périmètres.

   Suivez les étapes décrites dans Perimeter implementation (Implémentation du périmètre) dans le livre blanc Building a Perimeter on AWS (Créer un périmètre sur AWS) pour chaque condition d'autorisation. Pour des conseils normatifs sur la protection de la couche réseau, consultez Protection des réseaux.

b. Surveillez et alertez en continu.

   AWS Identity and Access Management Access Analyzer vous permet d'identifier les ressources de votre organisation et les comptes qui sont partagés avec des entités externes. Vous pouvez intégrer IAM Access Analyzer à AWS Security Hub pour envoyer et regrouper les découvertes d'une ressource d'IAM Access Analyzer vers Security Hub afin de contribuer à l'analyse de la situation de sécurité de votre environnement. Pour mettre en place l'intégration, activez IAM Access Analyzer et Security Hub dans chaque région de chaque compte. Vous pouvez utiliser AWS Config Rules pour auditer la configuration et alerter la partie appropriée à l'aide d'AWS Chatbot avec AWS Security Hub. Vous pouvez ensuite utiliser les documents AWS Systems Manager Automation pour résoudre les problèmes des ressources non conformes.

c. Pour des conseils normatifs sur la surveillance et les alertes en continu relatives aux ressources partagées en externe, consultez Analyser l'accès public et entre les comptes.

4. Utilisez le partage des ressources dans les services AWS et limitez l'accès en conséquence.

   De nombreux services AWS vous permettent de partager des ressources avec un autre compte ou de cibler une ressource dans un autre compte, par exemple Amazon Machine Images (AMI) et AWS Resource Access Manager (AWS RAM). Limitez l'API `ModifyImageAttribute` à la spécification des comptes approuvés pour partager l'AMI. Spécifiez la condition `ram:RequestedAllowsExternalPrincipals` lorsque vous utilisez AWS RAM pour limiter le partage à votre organisation seulement, pour empêcher l'accès à des identités non approuvées. Pour des conseils et des considérations normatifs, consultez Partage des ressources et cibles externes.

5. Utilisez AWS RAM pour partager en toute sécurité dans un compte ou avec d'autres Comptes AWS.

   AWS RAM vous aide à partager en toute sécurité les ressources que vous avez créées avec les rôles et les utilisateurs de votre compte et avec d'autres Comptes AWS. Dans un environnement multicompte, AWS RAM vous permet de créer une ressource une fois et de la partager avec

d'autres comptes. Cette approche permet de réduire vos frais généraux opérationnels tout en assurant la cohérence, la visibilité et l'auditabilité grâce à des intégrations avec Amazon CloudWatch et AWS CloudTrail, que vous ne recevez pas lorsque vous utilisez l'accès intercompte.

Si vous avez déjà partagé des ressources à l'aide d'une politique basée sur les ressources, vous pouvez utiliser l'API `PromoteResourceShareCreatedFromPolicy` ou un équivalent pour faire passer le partage des ressources vers un partage AWS RAM complet.

Dans certains cas, vous devrez peut-être prendre des mesures supplémentaires pour partager les ressources. Par exemple, pour partager un instantané chiffré, vous devez partager une clé AWS KMS.

Ressources

Bonnes pratiques associées :

- SEC03-BP07 Analyser l'accès public et entre les comptes
- SEC03-BP09 Partager des ressources en toute sécurité avec un tiers
- SEC05-BP01 Créer des couches réseau

Documents connexes :

- Propriétaire d'un compartiment accordant des autorisations entre comptes à des objets qu'il ne possède pas
- How to use Trust Policies with IAM
- Building Data Perimeter on AWS
- Procédure d'utilisation d'un ID externe lorsque vous accordez l'accès à vos ressources AWS à un tiers
- Services AWS que vous pouvez utiliser avec AWS Organizations
- Establishing a data perimeter on AWS: Allow only trusted identities to access company data

Vidéos connexes :

- Granular Access with AWS Resource Access Manager
- Securing your data perimeter with VPC endpoints

- Establishing a data perimeter on AWS

Outils associés :

- Exemples de politiques de périmètre de données

SEC03-BP09 Partager des ressources en toute sécurité avec un tiers

La sécurité de votre environnement cloud ne s'arrête pas à votre organisation. Votre organisation peut faire appel à un tiers pour gérer une partie de vos données. La gestion des autorisations pour le système géré par un tiers doit suivre la pratique de l'accès juste à temps en utilisant le principe du moindre privilège avec des informations d'identification temporaires. En travaillant en étroite collaboration avec un tiers, vous pouvez réduire ensemble l'étendue de l'impact et le risque d'accès involontaire.

Résultat souhaité : des informations d'identification AWS Identity and Access Management (IAM) à long terme, des clés d'accès IAM et des clés secrètes qui sont associées à un utilisateur peuvent être utilisées par n'importe qui tant que les informations d'identification sont valides et actives. L'utilisation d'un rôle IAM et d'informations d'identification temporaires vous permettent d'améliorer votre situation globale en matière de sécurité en réduisant l'effort de gestion des informations d'identification à long terme, y compris la gestion et les frais généraux opérationnels de ces détails sensibles. En utilisant un identifiant unique universel (UUID) pour l'ID externe dans la politique d'approbation IAM et en veillant à ce que les politiques IAM restent attachées au rôle IAM sous votre contrôle, vous pouvez auditer et vérifier que l'accès accordé au tiers n'est pas trop permissif. Pour des conseils normatifs sur l'analyse des ressources partagées en externe, consultez SEC03-BP07 Analyser l'accès public et entre les comptes.

Anti-modèles courants :

- Utilisation de la politique d'approbation IAM sans aucune condition.
- Utilisation d'informations d'identification IAM et de clés d'accès à long terme.
- Réutilisation des ID externes.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : moyen

Directives d'implémentation

Vous pouvez autoriser le partage des ressources en dehors d'AWS Organizations ou accorder un accès tiers à votre compte. Par exemple, un tiers peut fournir une solution de surveillance qui doit accéder aux ressources de votre compte. Dans ces cas de figure, vous devez créer un rôle intercompte IAM en lui attribuant uniquement les privilèges requis par le tiers. De plus, vous devez définir une politique d'approbation à l'aide de la condition d'ID externe. Lorsque vous utilisez un identifiant externe, vous pouvez (ou le tiers peut) générer un identifiant unique pour chaque client, tiers ou location. L'ID unique ne doit être contrôlé que par vous après sa création. Le tiers doit implémenter un processus pour relier l'ID externe au client de manière sécurisée, auditable et reproductible.

Vous pouvez également utiliser IAM Roles Anywhere afin de gérer les rôles IAM pour les applications en dehors d'AWS qui utilisent les API AWS.

Si le tiers n'a plus besoin d'accéder à votre environnement, supprimez le rôle. Évitez de fournir à des tiers des informations d'identification à long terme. Gardez un œil sur les autres services AWS qui prennent en charge le partage. Par exemple, AWS Well-Architected Tool autorise le partage d'une charge de travail avec d'autres Comptes AWS et AWS Resource Access Manager vous aide à partager en toute sécurité une ressource AWS que vous possédez avec d'autres comptes.

Étapes d'implémentation

1. Utilisez des rôles intercomptes pour donner accès aux comptes externes.

   Les rôles intercomptes réduisent la quantité d'informations sensibles stockées par des comptes externes et des tiers pour servir leurs clients. Les rôles intercomptes vous permettent d'octroyer l'accès aux ressources AWS de votre compte en toute sécurité à un tiers, par exemple aux AWS Partner ou à d'autres comptes de votre organisation, tout en préservant la capacité de gérer et de vérifier cet accès.

   Il se peut que le tiers vous fournisse des services à partir d'une infrastructure hybride ou qu'il extraie des données hors site pour les transférer dans un emplacement hors site. IAM Roles Anywhere permet aux charges de travail tierces d'interagir en toute sécurité avec vos charges de travail AWS et réduit davantage la nécessité d'utiliser des informations d'identification à long terme.

   Vous ne devez pas utiliser d'informations d'identification à long terme ni de clés d'accès associées aux utilisateurs pour fournir un accès à un compte externe. Utilisez plutôt les rôles intercomptes pour fournir l'accès intercompte.

2. Utilisez un ID externe avec des tiers.

   L'utilisation d'un ID externe vous permet de désigner qui peut assumer un rôle dans une politique d'approbation IAM. La politique d'approbation peut exiger que l'utilisateur qui assume le rôle fasse valoir la condition et la cible dans lesquelles il opère. Elle permet également au propriétaire du compte d'accepter que le rôle soit endossé uniquement dans des circonstances spécifiques. La fonction principale de l'ID externe est de traiter et de prévenir le problème de confusion de principal.

   Utilisez un ID externe si vous êtes propriétaire d'un Compte AWS et vous avez configuré un rôle pour un tiers qui accède à d'autres Comptes AWS en plus des vôtres, ou lorsque vous assumez des rôles au nom de différents clients. Collaborez avec votre tiers ou AWS Partner pour établir une condition d'identification externe à inclure dans la politique d'approbation IAM.

3. Utilisez des ID externes universellement uniques.

   Implémentez un processus qui génère une valeur unique aléatoire pour un ID externe, comme un identifiant unique universel (UUID). Un tiers qui réutilise des ID externes entre différents clients ne règle pas le problème de confusion du principal, car le client A pourrait être en mesure de consulter les données du client B en utilisant le rôle ARN du client B avec l'ID externe dupliqué. Dans un environnement multilocataire, où un tiers prend en charge plusieurs clients avec différents Comptes AWS, le tiers doit utiliser un ID unique différent comme ID externe pour chaque Compte AWS. Le tiers est responsable de la détection des ID externes dupliqués et de la correspondance sécurisée entre chaque client et son ID externe respectif. Le tiers doit vérifier qu'il peut uniquement assumer ce rôle lorsqu'il indique l'ID externe. Le tiers doit s'abstenir de stocker le rôle du client ARN et l'ID externe jusqu'à ce que l'ID externe soit requis.

   L'ID externe n'est pas traité comme un secret, mais il ne doit pas être facile à deviner, comme un numéro de téléphone, un nom ou un numéro de compte. Faites de l'ID externe un champ en lecture seule afin qu'il ne puisse pas être modifié dans le but de se faire passer pour la configuration.

   Le tiers ou vous-même pouvez générer l'ID externe. Définissez un processus pour déterminer qui est responsable de la génération de l'ID. Quelle que soit l'entité qui crée l'ID externe, le tiers applique l'unicité et les formats de façon uniforme parmi les clients.

4. Rendez obsolètes les informations d'identification à long terme fournis par le client.

   Rendez obsolète l'utilisation d'informations d'identification à long terme et utilisez des rôles intercomptes ou IAM Roles Anywhere. Si vous devez utiliser des informations d'identification

à long terme, établissez un plan pour migrer vers un accès basé sur les rôles. Pour plus d'informations sur la gestion des clés, consultez Gestion des identités. Collaborez également avec votre équipe Compte AWS et le tiers pour établir un runbook d'atténuation des risques. Pour obtenir des conseils normatifs sur la façon d'intervenir et d'atténuer les répercussions potentielles d'un incident de sécurité, consultez Réponse aux incidents.

5. Vérifiez que la configuration est conforme aux conseils normatifs ou qu'elle est automatisée.

   La politique créée pour l'accès intercompte doit suivre le principe du moindre privilège. Le tiers doit fournir un document de politique de rôle ou un mécanisme de configuration automatisé qui utilise un modèle AWS CloudFormation ou un équivalent pour vous. Cela réduit le risque d'erreurs associées à la création manuelle de politiques et offre une piste auditable. Pour plus d'informations sur l'utilisation d'un modèle AWS CloudFormation afin de créer des rôles intercomptes, consultez Rôles intercomptes.

   Le tiers doit fournir un mécanisme de configuration automatisé et auditable. Cependant, si vous utilisez le document de politique de rôle décrivant l'accès nécessaire, vous devez automatiser la configuration du rôle. Si vous utilisez un modèle AWS CloudFormation ou un équivalent, vous devrez surveiller les changements liés à la détection des dérives dans le cadre de la pratique d'audit.

6. Planifiez les modifications.

   Votre structure de compte, la nécessité de faire appel à un tiers, ou son offre de service peuvent changer. Vous devez anticiper les changements et les défaillances, et planifier en conséquence avec les personnes, processus et technologies appropriés. Auditez régulièrement le niveau d'accès que vous fournissez et implémentez des méthodes de détection pour vous avertir des changements imprévus. Surveillez et auditez l'utilisation du rôle et de l'entrepôt de données des ID externes. Vous devez être prêt à révoquer l'accès tiers, de façon temporaire ou permanente, en raison de changements ou de tendances d'accès imprévus. De plus, mesurez l'impact sur votre opération de révocation, y compris le temps nécessaire pour l'exécution, les personnes impliquées, le coût et l'impact sur d'autres ressources.

   Pour des conseils normatifs sur les méthodes de détection, consultez Bonnes pratiques de détection.

Ressources

Bonnes pratiques associées :

- SEC02-BP02 Utiliser des informations d'identification temporaires
- SEC03-BP05 Définir des protections par autorisation pour votre organisation
- SEC03-BP06 Gérer l'accès en fonction du cycle de vie
- SEC03-BP07 Analyser l'accès public et entre les comptes
- SEC04 Détection

Documents connexes :

- Propriétaire d'un compartiment accordant des autorisations entre comptes à des objets qu'il ne possède pas
- How to use trust policies with IAM roles
- Déléguer l'accès entre les Comptes AWS à l'aide des rôles IAM
- How do I access resources in another Compte AWS using IAM?
- Bonnes pratiques de sécurité dans IAM
- Logique d'évaluation de politiques intercomptes
- Procédure d'utilisation d'un ID externe lorsque vous accordez l'accès à vos ressources AWS à un tiers
- Collecting Information from AWS CloudFormation Resources Created in External Accounts with Custom Resources
- Securely Using External ID for Accessing AWS Accounts Owned by Others
- Extend IAM roles to workloads outside of IAM with IAM Roles Anywhere

Vidéos connexes :

- How do I allow users or roles in a separate Compte AWS access to my Compte AWS?
- AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less
- AWS Knowledge Center Live: IAM Best Practices and Design Decisions

Exemples connexes :

- Atelier Well-Architected – Lambda cross account IAM role assumption (Level 300)
- Configure cross-account access to Amazon DynamoDB (Configuration de l'accès intercompte à Amazon DynamoDB)

- AWS STS Network Query Tool

Détection

La détection se compose de deux parties : la détection des modifications de configuration inattendues ou indésirables et la détection des comportements inattendus. La première peut avoir lieu à plusieurs endroits dans un cycle de vie de livraison d'application. À l'aide d'une infrastructure en tant que code (par exemple, un modèle CloudFormation), vous pouvez rechercher les configurations indésirables avant le déploiement d'une charge de travail en mettant en œuvre des vérifications dans les pipelines CI/CD ou le contrôle de la source. Ensuite, lorsque vous déployez une charge de travail dans des environnements de non-production et de production, vous pouvez vérifier la configuration à l'aide d'outils AWS, d'outils open source ou d'outils de partenaires AWS natifs. Ces vérifications peuvent concerner une configuration qui ne respecte pas les principes de sécurité ou les bonnes pratiques, ou des modifications apportées entre une configuration testée et déployée. Pour une application en cours d'exécution, vous pouvez vérifier si la configuration a été modifiée de manière inattendue, y compris en dehors d'un déploiement connu ou d'un événement de mise à l'échelle automatique.

Pour la deuxième partie de la détection (comportement inattendu), vous pouvez utiliser des outils ou configurer des alertes en cas d'augmentation d'un type particulier d'appel d'API. Grâce à Amazon GuardDuty, vous pouvez être alerté lorsqu'une activité inattendue et potentiellement non autorisée ou malveillante se produit dans vos comptes AWS. Vous devez également surveiller explicitement les appels d'API en mutation que vous ne vous attendez pas à utiliser dans votre charge de travail, et les appels d'API qui modifient le niveau de sécurité.

La détection permet d'identifier une erreur potentielle dans la configuration des mesures de sécurité, une menace ou un comportement inattendu. Il s'agit d'une partie essentielle de la sécurité et elle peut être utilisée pour soutenir un processus de qualité, une obligation légale ou de conformité, ainsi que pour identifier les menaces et les efforts de réponse. Il existe différents types de mécanismes de détection. Par exemple, les journaux de votre charge de travail peuvent être analysés pour détecter les failles de sécurité exploitées. Vous devez vérifier régulièrement les mécanismes de détection liés à votre charge de travail afin de vous assurer que vous respectez les politiques et les exigences internes et externes. Les alertes et notifications automatisées doivent être basées sur des conditions définies pour permettre à vos équipes ou outils d'enquêter. Ces mécanismes sont des facteurs réactifs importants qui peuvent aider votre organisation à identifier et à comprendre la portée d'une activité anormale.

Dans AWS, il existe plusieurs approches que vous pouvez utiliser pour aborder les mécanismes de détection. Les sections suivantes décrivent comment utiliser ces approches :

Bonnes pratiques

SEC04-BP01 Configurer une journalisation de service et d'application

Conservez les journaux d'événements de sécurité des services et des applications. Il s'agit d'un principe de sécurité fondamental pour les cas d'audit, d'enquête et d'utilisation opérationnelle, et d'une exigence de sécurité commune dictée par les normes, politiques et procédures de gouvernance, de risque et de conformité (GRC).

Résultat souhaité : une organisation doit être en mesure de récupérer de façon fiable et cohérente les journaux d'événements de sécurité à partir de services et d'applications AWS rapidement lorsqu'il est nécessaire de réaliser un processus ou une obligation interne, par exemple une intervention en cas d'incident de sécurité. Envisagez de centraliser les journaux pour obtenir de meilleurs résultats opérationnels.

Anti-modèles courants :

- Les journaux sont stockés à perpétuité ou supprimés trop tôt.
- Tout le monde peut accéder aux journaux.
- Se fier entièrement aux processus manuels pour la gouvernance et l'utilisation des journaux.
- Stocker chaque type de journal au cas où il serait nécessaire.
- Vérifier l'intégrité des journaux uniquement lorsque cela s'avère nécessaire.

Avantages liés à l'instauration de cette bonne pratique : implémentation d'un mécanisme d'analyse des causes fondamentales (RCA) pour les incidents de sécurité et une source de preuve pour vos obligations en matière de gouvernance, de risque et de conformité.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Au cours d'une enquête de sécurité ou d'autres cas d'utilisation en fonction de vos besoins, vous devez être en mesure d'examiner les journaux pertinents pour consigner et comprendre la portée et la chronologie complètes de l'incident. Des journaux sont également requis pour la génération d'alertes, indiquant que certaines actions intéressantes ont eu lieu. Il est essentiel de sélectionner, d'activer, de stocker et de configurer les mécanismes d'interrogation et de récupération ainsi que les alertes.

Étapes d'implémentation

- Sélectionnez et activez les sources du journal. Avant une enquête de sécurité, vous devez saisir les journaux pertinents pour reconstruire rétroactivement l'activité dans un Compte AWS. Sélectionnez et activez les sources de journaux pertinentes pour vos charges de travail.

  Les critères de sélection des sources de journalisation doivent être fondés sur les cas d'utilisation requis par votre entreprise. Établissez une piste pour chaque Compte AWS en utilisant AWS CloudTrail ou une piste AWS Organizations, puis configurez un compartiment Amazon S3 pour cette piste.

  AWS CloudTrail est un service de journalisation qui suit les appels API sur un Compte AWS pour capturer l'activité de service AWS. Il est activé par défaut avec une conservation de 90 jours des événements de gestion qui peuvent être extraits via l'historique des événements CloudTrail à l'aide de la AWS Management Console, de l'AWS CLI ou d'un kit AWS SDK. Pour une conservation et une visibilité plus longues des données, créez une piste CloudTrail et associez-la à un compartiment Amazon S3, ainsi qu'à un groupe de journaux Amazon CloudWatch si nécessaire. Vous pouvez également créer un CloudTrail Lake, qui conserve les journaux CloudTrail jusqu'à sept ans et fournit une fonction de requête SQL.

  AWS recommande aux clients qui utilisent un VPC d'activer les journaux réseau trafic et DNS en utilisant les journaux de flux VPC et les journaux de requête du résolveur de requêtes Amazon Route 53, respectivement, et de les diffuser en continu dans un compartiment Amazon S3 ou un groupe de journaux CloudWatch. Vous pouvez créer un journal de flux VPC pour un VPC, un sous-réseau ou une interface réseau. Pour les journaux de flux VPC, vous pouvez choisir la façon dont et l'endroit où vous les utilisez pour réduire les coûts.

  Les journaux AWS CloudTrail, les journaux de flux VPC et les journaux de requêtes du résolveur Route 53 sont les sources de journalisation de base qui soutiennent les enquêtes de sécurité dans AWS. Vous pouvez également utiliser Amazon Security Lake pour collecter, normaliser

et stocker ces données de journaux au format Apache Parquet et Open Cybersecurity Schema Framework (OCSF), qui est prêt pour l'interrogation. Security Lake prend également en charge d'autres journaux AWS et des journaux de sources tierces.

Les services AWS peuvent générer des journaux non capturés par les sources de journaux de base, comme les journaux Elastic Load Balancing, les journaux AWS WAF, les journaux de l'enregistreur AWS Config, les découvertes Amazon GuardDuty, les journaux d'audit Amazon Elastic Kubernetes Service (Amazon EKS) et les journaux d'application et de système d'exploitation des instances Amazon EC2. Pour une liste complète des options de journalisation et de surveillance, consultez Annexe A : Définitions de la capacité cloud – Journalisation et événements dans le Guide de réponse aux incidents de sécurité AWS.

- Recherchez les capacités de journalisation pour chaque service et application AWS : chaque service et application AWS vous offre des options de stockage des journaux, chacune avec ses propres capacités de conservation et de cycle de vie. Les deux services de stockage de journaux les plus courants sont Amazon Simple Storage Service (Amazon S3) et Amazon CloudWatch. Pour de longues périodes de conservation, il est recommandé d'utiliser Amazon S3 pour sa rentabilité et ses capacités de cycle de vie flexibles. Si l'option de journalisation principale est Journaux Amazon CloudWatch, en tant qu'option, vous devez envisager d'archiver les journaux les moins consultés dans Amazon S3.
- Sélectionnez le stockage des journaux : le choix du stockage des journaux est généralement lié à l'outil d'interrogation que vous utilisez, aux capacités de conservation, à la familiarité et au coût. Les options principales du stockage de journaux sont un compartiment Amazon S3 ou un groupe de journaux CloudWatch.

  Un compartiment Amazon S3 offre un stockage durable et rentable avec une politique de cycle de vie facultative. Les journaux stockés dans des compartiments Amazon S3 peuvent être interrogés à l'aide de services tels que Amazon Athena.

  Un groupe de journaux CloudWatch offre un stockage durable et une installation de requête intégrée via CloudWatch Logs Insights.
- Identifiez la conservation appropriée des journaux : lorsque vous utilisez un compartiment Amazon S3 ou un groupe de journaux CloudWatch pour stocker des journaux, vous devez établir des cycles de vie adéquats pour chaque source de journaux afin d'optimiser les coûts de stockage et de récupération. Les clients ont généralement entre trois mois et un an de journaux facilement disponibles pour la recherche, avec une conservation de sept ans maximum. Le choix de la disponibilité et de la conservation doit correspondre à vos exigences en matière de sécurité et à un ensemble d'obligations statutaires, réglementaires et opérationnelles.

- Activez la journalisation pour chaque service et application AWS avec des politiques de conservation et de cycle de vie appropriées : pour chaque service ou application AWS dans votre organisation, recherchez les conseils de configuration de journalisation spécifiques :
  - Configurer AWS CloudTrail Trail
  - Configurer des journaux de flux VPC
  - Configurer l'exportation des découvertes Amazon GuardDuty
  - Configurer l'enregistrement AWS Config
  - Configurer le trafic d'ACL web AWS WAF
  - Configurer les journaux de trafic réseau AWS Network Firewall
  - Configurer les journaux d'accès Elastic Load Balancing
  - Configurer les journaux de requêtes du résolveur Amazon Route 53
  - Configurer les journaux Amazon RDS
  - Configurer les journaux de plan de contrôle Amazon EKS
  - Configurer l'agent Amazon CloudWatch pour les instances Amazon EC2 et les serveurs sur site
- Sélectionnez et implémentez des mécanismes d'interrogation pour les journaux : pour les interrogations de journaux, vous pouvez utiliser CloudWatch Logs Insights pour les données stockées dans les groupes de journaux CloudWatch, et Amazon Athena et Amazon OpenSearch Service pour les données stockées dans Amazon S3. Vous pouvez également utiliser des outils d'interrogation tiers tels qu'un service de gestion des informations de sécurité et des événements (SIEM).

  Le processus de sélection d'un outil d'interrogation de journaux doit tenir compte des aspects humains, technologiques et de processus de vos opérations de sécurité. Choisissez un outil qui répond aux exigences opérationnelles, métier et de sécurité, tout en étant accessible et gérable à long terme. Gardez à l'esprit que les outils d'interrogation de journaux fonctionnent de manière optimale lorsque le nombre de journaux à analyser est maintenu dans les limites de l'outil. Il n'est pas rare d'avoir plusieurs outils d'interrogation en raison de contraintes de coût ou techniques.

  Par exemple, vous pouvez utiliser un outil de gestion des événements et des informations de sécurité tiers pour effectuer des requêtes sur les 90 derniers jours de données, mais utiliser Athena pour effectuer des requêtes au-delà de 90 jours en raison du coût d'ingestion du journal d'un SIEM. Quelle que soit l'implémentation choisie, assurez-vous que votre approche réduit au minimum le nombre d'outils requis pour maximiser l'efficacité opérationnelle, en particulier pendant une enquête sur un événement de sécurité.

- Utilisez des journaux pour les alertes : AWS fournit des alertes par l'intermédiaire de plusieurs services de sécurité :
  - AWS Config surveille et enregistre vos configurations de ressources AWS et vous permet d'automatiser l'évaluation et la correction par rapport aux configurations souhaitées.
  - Amazon GuardDuty est un service de détection des menaces qui surveille continuellement les activités malveillantes et les comportements non autorisés pour protéger votre Comptes AWS et vos charges de travail. GuardDuty ingère, regroupe et analyse les informations provenant de sources telles que la gestion et les événements de données AWS CloudTrail, les journaux DNS, les flux de journaux VPC et les journaux d'audit Amazon EKS. GuardDuty extrait des flux de données indépendants directement depuis CloudTrail, les journaux de flux VPC, les journaux de requêtes DNS et Amazon EKS. Vous n'avez pas besoin de gérer les politiques de compartiment Amazon S3 ni de modifier la façon dont vous collectez et stockez les journaux. Il est toujours recommandé de conserver ces journaux à des fins d'enquête et de conformité.
  - AWS Security Hub fournit un emplacement unique qui regroupe, organise et priorise vos alertes de sécurité ou vos résultats provenant de plusieurs services AWS et de produits tiers en option pour vous donner une vue complète des alertes de sécurité et du statut de conformité.

  Vous pouvez également utiliser des moteurs de génération d'alertes personnalisés pour les alertes de sécurité non couvertes par ces services ou pour les alertes spécifiques pertinentes à votre environnement. Pour plus d'informations sur la création de ces alertes, consultez Détection dans le guide des réponses aux incidents de sécurité AWS.

Ressources

Bonnes pratiques associées :

- SEC04-BP02 Analyse centralisée des journaux, des résultats et des métriques
- SEC07-BP04 Définir la gestion du cycle de vie des données
- SEC10-BP06 Prédéployer les outils

Documents connexes :

- AWS Security Incident Response Guide
- Démarrer avec Amazon Security Lake
- Mise en route avec Amazon CloudWatch Logs

- Security Partner Solutions: Logging and Monitoring (Solutions partenaires de sécurité : journalisation et surveillance)

Vidéos connexes :

- AWS re:Invent 2022 - Introducing Amazon Security Lake

Exemples connexes :

- Assisted Log Enabler for AWS
- AWS Security Hub Findings Historical Export

Outils associés :

- Snowflake pour la cybersécurité

SEC04-BP02 Analyse centralisée des journaux, des résultats et des métriques

les équipes responsables des opérations de sécurité s'appuient sur la collecte de journaux et l'utilisation d'outils de recherche pour découvrir les événements d'intérêt potentiels, susceptibles d'indiquer une activité non autorisée ou une modification non intentionnelle. Cependant, la simple analyse des données collectées et le traitement manuel des informations ne suffisent pas pour faire face au volume d'informations provenant d'architectures complexes. L'analyse et les rapports ne facilitent pas l'affectation des ressources appropriées pour traiter un événement dans les délais impartis.

Une bonne pratique pour constituer une équipe d'opérations de sécurité mature consiste à intégrer profondément le flux d'événements et de résultats de sécurité dans un système de notification et de flux de travail, tel qu'un système de tickets, un système de gestion des bogues et problèmes ou un autre système de gestion des informations et des événements de sécurité (SIEM). Ainsi, le flux de travail n'est plus intégré aux rapports par e-mail et statiques, ce qui permet d'acheminer, de transférer et de gérer les événements ou les résultats. De nombreuses organisations intègrent également des alertes de sécurité dans leurs plateformes de discussion instantanée et collaborative et de productivité des développeurs. Pour les organisations qui se lancent dans l'automatisation, un

système de tickets à faible latence axé sur les API, offre une flexibilité considérable pour planifier ce qu'il faut automatiser en premier.

Cette bonne pratique s'applique non seulement aux événements de sécurité générés par les messages du journal décrivant l'activité des utilisateurs ou les événements du réseau, mais aussi aux changements détectés dans l'infrastructure elle-même. La capacité à détecter les changements, à déterminer si un changement était approprié, puis à acheminer ces informations vers le processus de correction approprié est essentielle pour gérer et valider une architecture sécurisée, dans le contexte de changements dont la nature indésirable est suffisamment subtile pour que leur exécution ne puisse être actuellement empêchée par une combinaison de configuration AWS Identity and Access Management(IAM) et AWS Organizations.

Amazon GuardDuty et AWS Security Hub fournissent des mécanismes d'agrégation, de déduplication et d'analyse pour les enregistrements de journaux qui sont également mis à votre disposition via d'autres services AWS. GuardDuty ingère, agrège et analyse les informations provenant de sources telles que les événements de gestion et de données AWS CloudTrail, les journaux DNS VPC et les journaux de flux VPC. Security Hub peut ingérer, agréger et analyser les résultats provenant de GuardDuty, AWS Config, Amazon Inspector, Amazon Macie, AWS Firewall Manager et d'un nombre important de produits de sécurité tiers disponibles dans AWS Marketplace et, s'il a été conçu en conséquence, votre propre code. GuardDuty et Security Hub ont tous les deux un modèle Administrateur/Maître qui peut agréger les résultats et les informations sur plusieurs comptes. Security Hub est souvent utilisé par les clients qui ont un système de gestion des informations et des événements de sécurité (SIEM) sur site comme préprocesseur et agrégateur de journaux et d'alertes côté AWS à partir duquel ils peuvent ensuite ingérer Amazon EventBridge via un processeur et un redirecteur basé sur AWS Lambda.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Débit

Directives d'implémentation

- Évaluer les fonctionnalités de traitement des journaux : évaluez les options disponibles pour le traitement des journaux.
  - Utilisez Amazon OpenSearch Service pour enregistrer et surveiller (presque) tout.
  - Trouvez un partenaire spécialisé dans les solutions de journalisation et de surveillance.
- Pour commencer à analyser les journaux CloudTrail, testez Amazon Athena.
  - Configuration d'Athena pour analyser les journaux CloudTrail

- Implémenter la journalisation centralisée dans AWS : consultez l'exemple de solution AWS suivant pour centraliser la journalisation à partir de plusieurs sources.
  - Centraliser la solution de journalisation
- Implémenter la journalisation centralisée avec le partenaire : les partenaires APN disposent de solutions pour vous aider à analyser les journaux de manière centralisée.
  - Journalisation et surveillance

Ressources

Documents connexes :

- AWS Answers : journalisation centralisée
- AWS Security Hub
- Amazon CloudWatch
- Amazon EventBridge
- Premiers pas : Amazon CloudWatch Logs
- Solutions partenaires de sécurité : journalisation et surveillance

Vidéos connexes :

- Surveillance centralisée de la configuration et de la conformité des ressources
- Résolution des problèmes identifiés par Amazon GuardDuty et AWS Security Hub
- Gestion des menaces dans le cloud : Amazon GuardDuty et AWS Security Hub

SEC04-BP03 Automatiser la réponse aux événements

L'utilisation de l'automatisation pour enquêter et corriger les événements réduit les efforts humains et les erreurs. Elle vous permet aussi de mettre à l'échelle les capacités d'investigation. Les vérifications régulières vous aideront à ajuster les outils d'automatisation et à itérer en continu.

Dans AWS, l'analyse des événements d'intérêt et des informations utiles sur des changements potentiellement inattendus dans un flux de travail automatisé peut être réalisée avec Amazon EventBridge. Ce service fournit un moteur de règles évolutif conçu pour négocier les formats d'événements AWS natifs (tels que les événements AWS CloudTrail) ainsi que les événements personnalisés que vous pouvez générer vous-même. Amazon GuardDuty vous permet également

d'acheminer les événements vers un système de flux de travail pour ceux qui mettent en place des systèmes de réponse aux incidents (AWS Step Functions), vers un compte de sécurité central ou encore vers un compartiment pour une analyse plus approfondie.

La détection des changements et l'acheminement de ces informations vers le flux de travail approprié peuvent également être réalisés via AWS Config Rules et les packs de conformité. AWS Config détecte les modifications apportées aux services concernés (bien que sa latence soit supérieure à celle d'EventBridge) et génère des événements qui peuvent être analysés avec AWS Config Rules pour la restauration, l'application de la politique de conformité et le transfert d'informations aux systèmes, tels que les plateformes de gestion des modifications et les systèmes de tickets opérationnels. En plus d'écrire vos propres fonctions Lambda pour répondre aux événements AWS Config, vous pouvez tirer parti du kit de développement AWS Config Ruleset d'une bibliothèque de règles open source AWS Config Rules. Les packs de conformité sont une collection d'actions correctives et de règles AWS Config Rules que vous déployez en tant qu'entité unique créée en tant que modèle YAML. A exemple de modèle de pack de conformité est disponible pour le pilier Sécurité Well-Architected.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

- Implémenter des alertes automatisées avec GuardDuty : GuardDuty est un service de détection des menaces qui surveille en permanence les activités malveillantes et les comportements non autorisés afin de protéger vos Comptes AWS et vos charges de travail. Activez GuardDuty et configurez des alertes automatiques.
- Automatiser les processus d'investigation : développez des processus automatisés qui enquêtent sur un événement et rapportent les informations à un administrateur pour gagner du temps.
  - Atelier : Amazon GuardDuty dans la pratique

Ressources

Documents connexes :

- AWS Answers : journalisation centralisée
- AWS Security Hub
- Amazon CloudWatch
- Amazon EventBridge

- Premiers pas : Amazon CloudWatch Logs
- Solutions partenaires de sécurité : journalisation et surveillance
- Configuration d'Amazon GuardDuty

Vidéos connexes :

- Surveillance centralisée de la configuration et de la conformité des ressources
- Résolution des problèmes identifiés par Amazon GuardDuty et AWS Security Hub
- Gestion des menaces dans le cloud : Amazon GuardDuty et AWS Security Hub

Exemples connexes :

- Atelier : Déploiement automatisé des contrôles de détection

SEC04-BP04 Implémenter des événements de sécurité exploitables

Créez des alertes qui sont envoyées à votre équipe et qui peuvent être exécutées par celle-ci. Assurez-vous que les alertes incluent des informations pertinentes pour que l'équipe agisse en conséquence. pour chaque mécanisme de détection dont vous disposez, vous devez également disposer d'un processus, sous la forme d'un runbook ou d'un playbookpour enquêter. Par exemple, lorsque vous activez Amazon GuardDuty, il génère des résultats différents. Vous devez avoir une entrée de runbook pour chaque type de résultat. Par exemple, si un cheval de Troie est détecté, votre runbook comporte des instructions simples qui demandent à quelqu'un d'enquêter et de corriger.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Découvrir les métriques disponibles pour les services AWS : découvrez les métriques disponibles via Amazon CloudWatch pour les services que vous utilisez.
  - Documentation des services AWS
  - Utilisation des métriques Amazon CloudWatch
- Configurez des alarmes Amazon CloudWatch.
  - Utilisation des alarmes Amazon CloudWatch

Ressources

Documents connexes :

- Amazon CloudWatch
- Amazon EventBridge
- Solutions partenaires de sécurité : journalisation et surveillance

Vidéos connexes :

- Surveillance centralisée de la configuration et de la conformité des ressources
- Résolution des problèmes identifiés par Amazon GuardDuty et AWS Security Hub
- Gestion des menaces dans le cloud : Amazon GuardDuty et AWS Security Hub

Protection de l'infrastructure

La protection des infrastructures englobe les méthodes de contrôle, telles que la défense en profondeur, qui sont nécessaires pour répondre aux bonnes pratiques et aux obligations organisationnelles ou réglementaires. L'utilisation de ces méthodologies est essentielle au succès des opérations en cours, que ce soit dans le cloud ou sur site.

La protection de l'infrastructure est un aspect essentiel du programme de sécurité des informations. Elle garantit que les systèmes et les services de votre charge de travail sont protégés contre les accès involontaires et non autorisés, et les failles potentielles. Par exemple, vous définirez des frontières de confiance (par exemple, limites de réseau et de comptes), la configuration et la maintenance de la sécurité du système (par exemple, renforcement, minimisation et correction), l'authentification et les autorisations du système d'exploitation (par exemple, utilisateurs, clés et niveaux d'accès) et d'autres points d'application de stratégie appropriés (par exemple, pare-feu d'applications Web et/ou passerelles API).

Régions, zones de disponibilité, AWS Local Zones et AWS Outposts

Assurez-vous de bien connaître les régions, les zones de disponibilité, AWS Local Zoneset AWS Outposts, qui sont des composants de l'infrastructure mondiale AWS sécurisée.

AWS utilise le concept de région, qui est un emplacement physique dans le monde où nous regroupons des centres de données. Nous appelons chaque groupe de centres de données logiques une zone de disponibilité (AZ). Chaque région AWS se compose de plusieurs AZ isolées et physiquement séparées au sein d'une zone géographique. Si vous devez respecter des exigences en matière de situation géographique des données, vous pouvez choisir la région AWS la plus proche de l'emplacement souhaité. Vous conservez le contrôle total et la propriété de la région dans laquelle vos données se trouvent physiquement, ce qui facilite le respect des exigences locales de conformité et de localisation des données. Chaque AZ dispose de systèmes d'électricité, de climatisation et de sécurité physique indépendants. Si une application est partitionnée sur plusieurs AZ, vous êtes mieux isolé et protégé contre les problèmes tels que les pannes de courant, la foudre, les tornades, les tremblements de terre, etc. Les AZ sont physiquement séparées par une distance de plusieurs kilomètres des autres AZ, mais elles se trouvent toutes à 100 km de distance les unes des autres. Toutes les AZ d'une régionAWS sont interconnectées avec un réseau à large bande passante et à faible latence, qui utilise une fibre métropolitaine dédiée entièrement redondante fournissant un réseau à haut débit et à faible latence entre les AZ. Tout le trafic entre les AZ est chiffré. Les clients AWS axés sur la haute disponibilité peuvent concevoir leurs applications pour qu'elles s'exécutent dans plusieurs zones de disponibilité afin d'obtenir une tolérance aux pannes encore plus grande.

Les régions AWS répondent aux niveaux les plus élevés de sécurité, de conformité et de protection des données.

AWS Local Zones placent le calcul, le stockage, la base de données et d'autres services AWS spécifiques plus près des utilisateurs finaux. Avec AWS Local Zones, vous pouvez facilement exécuter des applications très exigeantes qui nécessitent des latences de quelques millisecondes pour vos utilisateurs finaux, telles que la création de contenu multimédia et de divertissement, les jeux en temps réel, les simulations de réservoir, l'automatisation de la conception électronique et le machine learning. Chaque emplacement AWS Local Zone est une extension d'une région AWS dans laquelle vous pouvez exécuter vos applications sensibles à la latence, à l'aide de services AWS tels qu'Amazon EC2, Amazon VPC, Amazon EBS, Amazon File Storage et Elastic Load Balancing à proximité géographique des utilisateurs finaux. Les emplacements AWS Local Zones fournissent une connexion sécurisée à haut débit entre les charges de travail locales et celles qui s'exécutent dans la région AWS, vous permettant de vous connecter de manière transparente à la gamme complète de services dans la région via les mêmes API et ensembles d'outils.

AWS Outposts apporte des services, une infrastructure et des modèles d'exploitation AWS natifs à pratiquement n'importe quel centre de données, espace de colocation ou installation sur site. Vous pouvez utiliser les mêmes API, outils et infrastructures AWS dans les installations sur site et dans le cloud AWS pour offrir une expérience hybride vraiment cohérente. AWS Outposts est conçu pour les environnements connectés et permet de prendre en charge les charges de travail qui doivent rester sur site en raison d'une faible latence ou de besoins de traitement de données locaux.

Dans AWS, il existe un certain nombre d'approches pour protéger l'infrastructure. Les sections suivantes décrivent comment utiliser ces approches.

Rubriques

Protection des réseaux

Les utilisateurs, tant au sein de votre personnel que de vos clients, peuvent être situés n'importe où. Vous devez vous éloigner des modèles traditionnels visant à accepter tout le monde et tout ce qui a accès à votre réseau. Lorsque vous suivez le principe d'application de la sécurité à toutes les couches, vous adoptez une approche zéro confiance . La sécurité zéro confiance est un modèle dans

lequel les composants d'application ou les microservices sont considérés comme distincts les uns des autres. Aucun composant ou microservice ne fait confiance à un autre.

La planification et la gestion minutieuses de la conception de votre réseau constituent la base même de votre action pour isoler les ressources dans le cadre de votre charge de travail. Comme de nombreuses ressources de votre charge de travail opèrent dans un VPC et héritent des propriétés de sécurité, il est essentiel que la conception soit soutenue par des mécanismes d'inspection et de protection basés sur l'automatisation. De même, pour les charges de travail qui fonctionnent en dehors d'un VPC, en utilisant des services purement périphériques et/ou sans serveur, les bonnes pratiques s'appliquent dans une approche plus simple. Reportez-vous à AWS Well-Architected Serverless Applications Lens (Présentation à la loupe des applications sans serveur - AWS Well-Architected Framework) pour obtenir des conseils sur la sécurité serverless.

Bonnes pratiques

- SEC05-BP01 Créer des couches réseau
- SEC05-BP02 Contrôler le trafic sur toutes les couches
- SEC05-BP03 Automatiser la protection du réseau
- SEC05-BP04 Mettre en œuvre l'inspection et la protection

SEC05-BP01 Créer des couches réseau

Créez des groupes multicouches pour les composants qui partagent des exigences en matière de sensibilité afin de réduire au minimum la portée potentielle des répercussions d'un accès non autorisé. Par exemple, un cluster de bases de données dans un cloud privé virtuel (VPC) n'ayant pas besoin d'accès à Internet doit être placé dans des sous-réseaux sans routage vers ou depuis Internet. Le trafic ne doit provenir que de la ressource adjacente suivante la moins sensible. Réfléchissez au cas d'une application web se trouvant derrière un équilibreur de charge. Votre base de données ne doit pas être accessible directement depuis l'équilibreur de charge. La logique métier ou le serveur web doivent être les seuls à avoir un accès direct à votre base de données.

Résultat souhaité : créer un réseau multicouche. Les réseaux multicouches permettent de regrouper logiquement des composants de réseau similaires. Ils réduisent également la portée potentielle de l'impact de l'accès non autorisé au réseau. Un réseau multicouche approprié complique les choses pour les utilisateurs non autorisés qui souhaitent accéder à des ressources supplémentaires au sein de votre environnement AWS. En plus de sécuriser les chemins réseau internes, vous devez également protéger votre périphérie de réseau, comme les applications web et les points de terminaison d'API.

Anti-modèles courants :

- Créer toutes les ressources dans un seul VPC ou sous-réseau.
- Utiliser des groupes de sécurité trop permissifs.
- Ne pas utiliser de sous-réseaux.
- Autoriser un accès direct aux stockages de données tels que les bases de données.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Les composants, tels que les instances Amazon Elastic Compute Cloud (Amazon EC2), les clusters de bases de données Amazon Relational Database Service (Amazon RDS) et les fonctions AWS Lambda qui partagent les exigences d'accessibilité, peuvent être segmentés en couches formées par des sous-réseaux. Envisagez de déployer des charges de travail sans serveur, comme les fonctions Lambda dans un VPC ou derrière un Amazon API Gateway. Les tâches AWS Fargate (Fargate) qui n'ont pas besoin d'accès à Internet doivent être placées dans des sous-réseaux sans routage vers ou depuis Internet. Cette approche multicouche réduit l'impact d'une mauvaise configuration de couche unique, ce qui pourrait autoriser un accès involontaire. Pour AWS Lambda, vous pouvez exécuter vos fonctions dans votre VPC pour anticiper les contrôles basés sur un VPC.

Pour une connectivité réseau pouvant inclure des milliers de VCP, des Comptes AWS et des réseaux sur site, vous devez utiliser AWS Transit Gateway. Transit Gateway agit comme un hub qui contrôle la façon dont le trafic est acheminé entre tous les réseaux connectés, qui agissent comme des rayons. Le trafic entre Amazon Virtual Private Cloud (Amazon VPC) et Transit Gateway reste sur le réseau privé AWS, ce qui réduit l'exposition externe aux utilisateurs non autorisés et les problèmes de sécurité potentiels. L'appairage inter-région Transit Gateway chiffre également le trafic inter-région sans point unique de défaillance ni goulot d'étranglement sur la bande passante.

Étapes d'implémentation

- Utilisez Reachability Analyzer pour analyser le chemin entre une source et une destination en fonction de la configuration : Reachability Analyzer vous permet d'automatiser la vérification de la connectivité vers et depuis les ressources connectées VPC. Notez que cette analyse se fait en examinant la configuration (aucun paquet réseau n'est envoyé lors de l'analyse).
- Utilisez l'analyseur d'accès réseau Amazon VPC pour identifier l'accès involontaire aux ressources du réseau : l'analyseur d'accès réseau Amazon VPC vous permet de spécifier vos besoins d'accès réseau et d'identifier les chemins réseau potentiels.

- Déterminez si les ressources doivent être dans un sous-réseau public : ne placez pas les ressources dans les sous-réseaux publics de votre VPC à moins qu'elles doivent absolument recevoir du trafic réseau entrant de sources publiques.
- Créez des sous-réseaux dans vos VPC : créez des sous-réseaux pour chaque couche réseau (dans les groupes qui comprennent plusieurs zones de disponibilité) pour améliorer la micro-segmentation. Vérifiez également que vous avez associé les tables de routage appropriées à vos sous-réseaux pour contrôler le routage et la connectivité Internet.
- Utilisez AWS Firewall Manager pour gérer vos groupes de sécurité VPC : AWS Firewall Manager permet d'alléger la complexité de gestion liée à l'utilisation de plusieurs groupes de sécurité.
- Utilisez AWS WAF pour vous protéger contre les vulnérabilités web courantes : AWS WAF peut permettre d'améliorer la sécurité de la périphérie en inspectant le trafic à la recherche des vulnérabilités web courantes, telles que l'injection de SQL. Il vous permet également de limiter le trafic des adresses IP provenant de certains pays ou emplacements géographiques.
- Utilisez Amazon CloudFront comme réseau de distribution de contenu (CDN) : Amazon CloudFront peut vous aider à accélérer votre application web en stockant les données plus près de vos utilisateurs. Il peut également améliorer la sécurité de la périphérie en appliquant HTTPS, en limitant l'accès aux zones géographiques et en veillant à ce que le trafic réseau ne puisse accéder aux ressources que lorsqu'il est acheminé via CloudFront.
- Utilisez Amazon API Gateway lors de la création d'interfaces de programmation d'applications (API) : Amazon API Gateway permet de publier, surveiller et sécuriser les API REST, HTTPS et WebSocket.

Ressources

Documents connexes :

- AWS Firewall Manager
- Amazon Inspector
- Sécurité dans Amazon VPC
- Reachability Analyzer
- Amazon VPC Network Access Analyzer (Analyseur d'accès réseau VPC)

Vidéos connexes :

- AWS Transit Gateway reference architectures for many VPCs

- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield
- AWS re:Inforce 2022 - Validate effective network access controls on AWS
- AWS re:Inforce 2022 - Advanced protections against bots using AWS WAF

Exemples connexes :

- Atelier Well-Architected – Automated Deployment of VPC
- Atelier : Amazon VPC Network Access Analyzer

SEC05-BP02 Contrôler le trafic sur toutes les couches

lorsque vous créez l'architecture de votre topologie réseau, vous devez examiner les exigences de connectivité de chaque composant. Par exemple, si un composant nécessite d'accéder à Internet (en entrée et en sortie), une connectivité aux VPC, aux services périphériques et aux centres de données externes.

Un VPC vous permet de définir votre topologie de réseau qui s'étend sur une Région AWS avec une plage d'adresses IPv4 privée que vous définissez, ou une plage d'adresses IPv6 que sélectionne AWS. Vous devez appliquer des contrôles multiples avec une approche de défense en profondeur pour le trafic entrant et sortant, y compris l'utilisation de groupes de sécurité (pare-feu à inspection permanente), de listes de contrôle d'accès (ACL) réseau, de sous-réseaux et de tables de routage. Au sein d'un VPC, vous pouvez créer des sous-réseaux dans une zone de disponibilité. Chaque sous-réseau peut avoir une table de routage associée qui définit les règles de routage pour gérer les chemins que le trafic emprunte au sein du sous-réseau. Vous pouvez définir un sous-réseau routable Internet en ayant une route qui accède à une passerelle Internet ou NAT connectée au VPC, ou passant par un autre VPC.

Lorsqu'une instance, une base de données Amazon Relational Database Service(Amazon RDS) ou un autre service sont lancés au sein d'un VPC, ils disposent de leur propre groupe de sécurité sur chaque interface réseau. Ce pare-feu se situe en dehors de la couche du système d'exploitation et peut être utilisé pour définir des règles pour le trafic entrant et sortant autorisé. Vous pouvez également définir les relations entre les groupes de sécurité. Par exemple, les instances d'un groupe de sécurité de la couche base de données n'acceptent que le trafic des instances de la couche application, par référence aux groupes de sécurité appliqués aux instances concernées. Si vous utilisez des protocoles non-TCP, il n'est pas nécessaire de laisser une instance Amazon Elastic Compute Cloud(Amazon EC2) directement accessible par Internet (même avec des ports restreints par des groupes de sécurité) sans utiliser d'équilibreur de charge ou CloudFront. Cela permet de la

protéger contre un accès involontaire en cas de problème de système d'exploitation ou d'application. Un sous-réseau peut également avoir une liste ACL réseau qui fait office de pare-feu sans état. Vous devez configurer la liste de contrôle d'accès(ACL) au réseau de manière à réduire l'étendue du trafic autorisé entre les couches. Notez que vous devez définir des règles à la fois pour les flux entrants et sortants.

Certains services AWS nécessitent que des composants accèdent à Internet pour effectuer des appels d'API, là où les points de terminaison d'API AWS sont situés. D'autres services AWS utilisent les Points de terminaison d'un VPC dans vos Amazon VPC. De nombreux services AWS, notamment Amazon S3 et Amazon DynamoDB, prennent en charge les points de terminaison d'un VPC, et cette technologie a été généralisée dans . AWS PrivateLink. Nous vous recommandons d'utiliser cette approche pour accéder en toute sécurité aux services AWS, aux services tiers et à vos propres services hébergés dans d'autres VPC. Tout le trafic réseau sur AWS PrivateLink reste sur la dorsale mondiale AWS et ne traverse jamais Internet. La connectivité ne peut être initiée que par le consommateur du service, et non par le fournisseur du service. Utiliser AWS PrivateLink pour l'accès au service externe vous permet de créer des VPC isolés sans accès à Internet et contribue à protéger vos VPC contre les vecteurs de menace externes. Les services tiers peuvent utiliser AWS PrivateLink pour permettre à leurs clients de se connecter aux services à partir de leurs VPC via des adresses IP privées. Pour les ressources VPC qui ont besoin d'établir des connexions sortantes à Internet, celles-ci peuvent être établies en mode sortant uniquement (unidirectionnel) via une passerelle NAT gérée par AWS, une passerelle Internet en mode sortant uniquement ou des proxys Web que vous créez et gérez.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Débit

Directives d'implémentation

- Contrôler le trafic réseau dans un VPC : mettez en œuvre les bonnes pratiques liées aux VPC pour contrôler le trafic.
  - Sécurité des Amazon VPC
  - Points de terminaison d'un VPC
  - Groupe de sécurité de Amazon VPC
  - ACL réseau
- Contrôler le trafic en périphérie : implémentez des services périphériques comme Amazon CloudFront pour fournir une couche supplémentaire de protection et d'autres fonctions.
  - Cas d'utilisation d'Amazon CloudFront
  - AWS Global Accelerator

  - AWS Web Application Firewall (AWS WAF)
  - Amazon Route 53
  - Amazon VPC Ingress Routing
- Contrôler le trafic réseau privé : implémentez des services qui protègent le trafic privé pour votre charge de travail.
  - Appairage des Amazon VPC
  - Amazon VPC Endpoint Services (AWS PrivateLink)
  - Amazon VPC Transit Gateway
  - AWS Direct Connect
  - AWS Site-to-Site VPN
  - AWS Client VPN
  - Points d'accès Amazon S3

Ressources

Documents connexes :

- AWS Firewall Manager
- Amazon Inspector
- Démarrer avec AWS WAF

Vidéos connexes :

- AWS Transit Gateway reference architectures for many VPCs
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield

Exemples connexes :

- Atelier : Déploiement automatisé d'un VPC

SEC05-BP03 Automatiser la protection du réseau

Automatisez les mécanismes de protection pour disposer d'un réseau capable de se défendre lui-même grâce à l'intelligence des menaces et à la détection des anomalies. Par exemple, des outils de

détection et de prévention des intrusions capables de s'adapter aux menaces actuelles et de réduire leur impact. Un pare-feu d'application web est un scénario dans lequel vous pouvez automatiser la protection du réseau, par exemple, en utilisant la solution AWS WAF Security Automations (https://github.com/awslabs/aws-waf-security-automations) pour bloquer automatiquement les requêtes provenant d'adresses IP associées à des acteurs de menaces connus.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

- Automatiser la protection du trafic web : AWS propose une solution qui utilise AWS CloudFormation pour déployer automatiquement un ensemble de règles AWS WAF conçues pour filtrer les attaques courantes sur le web. Les utilisateurs peuvent choisir parmi des fonctions de protection préconfigurées qui définissent les règles incluses dans une liste de contrôle d'accès (ACL web) AWS WAF.
  - Automatisations de sécurité AWS WAF
- Envisager les solutions AWS Partner : les partenaires AWS proposent des centaines de produits leaders du secteur qui sont équivalents, identiques ou s'intègrent aux 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.
  - Sécurité de l'infrastructure

Ressources

Documents connexes :

- AWS Firewall Manager
- Amazon Inspector
- Sécurité des VPC Amazon
- Démarrer avec AWS WAF

Vidéos connexes :

- AWS Transit Gateway reference architectures for many VPCs
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield

Exemples connexes :

- Atelier : Déploiement automatisé d'un VPC

SEC05-BP04 Mettre en œuvre l'inspection et la protection

Inspectez et filtrez votre trafic au niveau de chaque couche. Vous pouvez inspecter les configurations de vos VPC pour détecter tout accès involontaire potentiel à l'aide de VPC Network Access Analyzer. Vous pouvez spécifier vos exigences d'accès au réseau et identifier les chemins réseau potentiels qui ne les satisfont pas. Pour les composants effectuant des transactions via des protocoles basés sur HTTP, un pare-feu d'application Web peut protéger contre les attaques courantes. AWS WAF est un pare-feu d'application Web qui permet de surveiller et de bloquer les requêtes HTTP correspondant à vos règles configurables qui sont transmises à une API Amazon API Gateway, à Amazon CloudFront ou à un Application Load Balancer. Pour commencer à utiliser AWS WAF, vous pouvez utiliser des AWS Managed Rules en combinaison avec les vôtres ou utiliser des intégrations de partenaires existantes.

Pour gérer AWS WAF, les protections AWS Shield Advanced et les groupes de sécurité Amazon VPC dans AWS Organizations, vous pouvez utiliser AWS Firewall Manager. Il vous permet de configurer et de gérer de manière centralisée les règles de pare-feu de l'ensemble de vos comptes et applications, ce qui facilite l'application à grande échelle des règles communes. Il permet également de répondre rapidement aux attaques, à l'aide d' AWS Shield Advancedou de solutions qui peuvent bloquer automatiquement les demandes indésirables adressées à vos applications Web. Firewall Manager fonctionne également avec AWS Network Firewall. AWS Network Firewall est un service géré qui utilise un moteur de règles pour vous donner un contrôle précis sur le trafic réseau avec et sans état. Il prend en charge les spécifications du système de prévention des intrusions (IPS) open source compatible avec Suricata pour les règles afin de protéger plus efficacement votre charge de travail.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Configurer Amazon GuardDuty : GuardDuty est un service de détection des menaces qui surveille en permanence les activités malveillantes et les comportements non autorisés afin de protéger vos Comptes AWS et vos charges de travail. Activez GuardDuty et configurez des alertes automatiques.
  - Amazon GuardDuty

    - Atelier : Déploiement automatisé des contrôles de détection
- Configurer des flux de journaux de cloud privé virtuel (VPC) : les journaux de flux de VPC sont une fonction qui vous permet de capturer des informations sur le trafic IP allant et venant des interfaces réseau de votre VPC. Les données des journaux de flux peuvent être publiées sur Amazon CloudWatch Logs et Amazon Simple Storage Service (Amazon S3). Une fois que vous avez créé un journal de flux, vous pouvez extraire et afficher ses données dans la destination de votre choix.
- Envisager la mise en miroir du trafic VPC : la mise en miroir du trafic est une fonction Amazon VPC que vous pouvez utiliser pour copier le trafic réseau à partir d'une interface réseau Elastic d'instances Amazon Elastic Compute Cloud (Amazon EC2), puis l'envoyer à des appareils de sécurité et de surveillance hors bande pour l'inspection du contenu, la surveillance des menaces et le dépannage.
    - Mise en miroir du trafic VPC

Ressources

Documents connexes :

- AWS Firewall Manager
- Amazon Inspector
- Sécurité du Amazon VPC
- Démarrer avec AWS WAF

Vidéos connexes :

- AWS Transit Gateway reference architectures for many VPCs
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield

Exemples connexes :

- Atelier : Déploiement automatisé d'un VPC

Protection du calcul

Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, et plus encore. Chacun de ces types de ressources de calcul nécessite des approches de sécurisation différentes. Cependant, ils partagent des stratégies communes que vous devez prendre en compte : défense en profondeur, gestion des vulnérabilités, réduction de la surface d'attaque, automatisation de la configuration et de l'exploitation et réalisation d'actions à distance. Dans cette section, vous découvrirez des conseils généraux permettant de protéger les ressources de calcul pour les services clés. Pour chaque service AWS utilisé, il est important de vérifier les recommandations de sécurité correspondantes dans la documentation du service.

Bonnes pratiques

- SEC06-BP01 Gérer les failles
- SEC06-BP02 Réduire la surface d'attaque
- SEC06-BP03 Mettre en œuvre des services gérés
- SEC06-BP04 Automatiser la protection du calcul
- SEC06-BP05 Permettre aux utilisateurs d'effectuer des actions à distance
- SEC06-BP06 Valider l'intégrité des logiciels

SEC06-BP01 Gérer les failles

Analysez et éliminez fréquemment les failles de sécurité dans votre code, vos dépendances et votre infrastructure afin de vous protéger contre les nouvelles menaces.

Résultat souhaité : créer et gérer un programme de gestion des failles. Analysez et corrigez régulièrement les ressources telles que les instances Amazon EC2, les conteneurs Amazon Elastic Container Service (Amazon ECS) et les charges de travail Amazon Elastic Kubernetes Service (Amazon EKS). Configurez des fenêtres de maintenance pour les ressources gérées par AWS, par exemple les bases de données Amazon Relational Database Service (Amazon RDS). Utilisez l'analyse de code statique pour rechercher des problèmes courants dans le code source de l'application. Envisagez de tester la pénétration des applications web si votre organisation possède les compétences requises ou peut recruter de l'aide externe.

Anti-modèles courants :

- L'absence de programme de gestion des failles.

- L'application de correctifs système sans tenir compte de la gravité ni de l'évitement des risques.
- Utilisation d'un logiciel dont la date de fin de vie (EOL) a été dépassée.
- Déploiement du code en production avant de l'analyser afin de détecter tout problème de sécurité.

Avantages liés à l'instauration de cette bonne pratique :

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Un programme de gestion des failles comprend l'évaluation de la sécurité, l'identification des problèmes, l'établissement des priorités et la mise en œuvre des correctifs dans le cadre de la résolution des problèmes. L'automatisation est la clé pour analyser continuellement les charges de travail afin de détecter les problèmes, l'exposition involontaire du réseau et la mise en œuvre de mesures correctives. L'automatisation de la création et de la mise à jour des ressources permet de gagner du temps et de réduire le risque d'erreurs de configuration, ce qui crée d'autres problèmes. Un programme de gestion des failles bien conçu doit également tenir compte des tests de vulnérabilité pendant les étapes de développement et de déploiement du cycle de vie du logiciel. L'implémentation de la gestion des failles pendant le développement et le déploiement réduit les risques d'avoir une vulnérabilité dans votre environnement de production.

L'implémentation d'un programme de gestion des failles nécessite une bonne compréhension du modèle de responsabilité partagée AWS et de la façon dont cela affecte vos charges de travail spécifiques. Dans le cadre du modèle de responsabilité partagée, AWS est responsable de la protection de l'infrastructure du AWS Cloud. Cette infrastructure se compose de matériels, de logiciels, de réseaux et d'installations exécutant les services du AWS Cloud. Vous êtes responsable de la sécurité dans le cloud, par exemple des données réelles, de la configuration de la sécurité et des tâches de gestion des instances Amazon EC2. Vous devez également vérifier que les objets Amazon S3 sont classés et configurés correctement. Votre approche en matière de gestion des failles peut également varier selon les services que vous utilisez. Par exemple, AWS gère l'application des correctifs pour notre service de base de données relationnelle gérée, Amazon RDS, mais vous êtes responsable de l'application des correctifs dans les bases de données auto-hébergées.

AWS offre une gamme de services pour vous aider dans le cadre de votre programme de gestion des failles. Amazon Inspector analyse continuellement les charges de travail AWS afin d'identifier les problèmes de logiciels et les accès réseau involontaires. Le Gestionnaire de correctifs d'AWS Systems Manager permet de gérer l'application des correctifs sur vos instances Amazon EC2.

Amazon Inspector et Systems Manager peuvent être consultés dans AWS Security Hub, un service de gestion de la situation de sécurité dans le cloud qui aide à automatiser les contrôles de sécurité AWS et à centraliser les alertes de sécurité.

Amazon CodeGuru permet d'identifier les problèmes potentiels dans les applications Java et Python en utilisant l'analyse de code statique.

Étapes d'implémentation

- Configurez Amazon Inspector : Amazon Inspector détecte automatiquement les instances Amazon EC2 qui viennent d'être lancées, les fonctions Lambda et les images de conteneur éligibles envoyées dans Amazon ECR, et il les analyse immédiatement afin d'identifier les problèmes de logiciels, les défauts potentiels et tout exposition involontaire du réseau.
- Analysez le code source : rechercher les problèmes et les défauts dans les bibliothèques et les dépendances. Amazon CodeGuru peut analyser et recommander des mesures correctives pour les problèmes de sécurité courants dans les applications Java et Python. La Fondation OWASP publie une liste des outils d'analyse de code source (également appelés outils SAST).
- Implémentez un mécanisme permettant d'analyser et de corriger votre environnement existant, ainsi qu'une analyse dans le cadre d'un processus de création de pipeline CI/CD : implémentez un mécanisme pour analyser et corriger les problèmes dans vos dépendances et systèmes d'exploitation afin de garantir votre protection contre les nouvelles menaces. Exécutez ce mécanisme régulièrement. La gestion des failles logicielles est essentielle pour comprendre où vous devez appliquer les correctifs ou résoudre les problèmes logiciels. Privilégiez la correction des problèmes de sécurité potentiels en intégrant rapidement les évaluations des vulnérabilités à votre pipeline d'intégration continue et de livraison continue (CI/CD). Votre approche peut varier en fonction des services AWS que vous utilisez. Pour vérifier l'absence de problèmes potentiels dans le logiciel exécuté dans les instances Amazon EC2, ajoutez Amazon Inspector à votre pipeline pour vous alerter et arrêter le processus de construction si des problèmes ou des défauts potentiels sont détectés. Amazon Inspector surveille les ressources en continu. Vous pouvez également utiliser des produits open source tels que OWASP Dependency-Check, Snyk, OpenVAS, des gestionnaires de packages et des outils AWS Partner pour la gestion des failles.
- Utilisez AWS Systems Manager : vous êtes responsable de la gestion des correctifs pour vos ressources AWS, notamment les instances Amazon Elastic Compute Cloud (Amazon EC2), les Amazon Machine Images (AMI) et d'autres ressources de calcul. Le Gestionnaire de correctifs AWS Systems Manager automatise le processus d'application de correctifs aux instances gérées avec des mises à jour liées à la sécurité et d'autres types de mises à jour. Le Gestionnaire de correctifs peut être utilisé pour appliquer des correctifs sur les instances Amazon EC2 pour les

systèmes d'exploitation et les applications, dont les applications Microsoft, les packs de service Windows et les mises à niveau mineures pour les instances basées sur Linux. Outre Amazon EC2, le Gestionnaire de correctifs peut également être utilisé pour corriger les serveurs sur site.

Pour obtenir la liste des systèmes d'exploitation compatibles, consultez Systèmes d'exploitation compatibles dans le guide utilisateur Systems Manager. Vous pouvez analyser les instances pour afficher uniquement un rapport sur les correctifs manquants, ou vous pouvez analyser et installer automatiquement tous les correctifs manquants.

- Utilisez AWS Security Hub : Security Hub fournit une vue complète de votre situation de sécurité dans AWS. Il collecte des données de sécurité dans plusieurs services AWS et communique ces découvertes dans un format normalisé, ce qui vous permet d'établir l'ordre de priorité des découvertes en matière de sécurité dans les services AWS.
- Utilisez AWS CloudFormation : AWS CloudFormation est un service d'infrastructure en tant que code (IaC) qui permet la gestion des failles en automatisant le déploiement des ressources et en normalisant l'architecture des ressources sur plusieurs comptes et environnements.

Ressources

Documents connexes :

- AWS Systems Manager
- Security Overview of AWS Lambda
- Amazon CodeGuru
- Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector
- Automate vulnerability management and remediation in AWS using Amazon Inspector and AWS Systems Manager – Part 1

Vidéos connexes :

- Securing Serverless and Container Services
- Security best practices for the Amazon EC2 instance metadata service

SEC06-BP02 Réduire la surface d'attaque

Réduisez votre exposition aux accès imprévus en renforçant les systèmes d'exploitation et en limitant au minimum l'utilisation des composants, des bibliothèques et des services consommables en externe. Commencez par réduire les composants inutilisés, qu'il s'agisse de packages de système d'exploitation ou d'applications pour les charges de travail basées sur Amazon Elastic Compute Cloud (Amazon EC2), ou de modules logiciels externes dans votre code (pour toutes les charges de travail). Il existe de nombreux guides sur le renforcement et la configuration de la sécurité pour les systèmes d'exploitation et les logiciels serveur courants. Par exemple, vous pouvez commencer par le Center for Internet Security et partir de là.

Dans Amazon EC2, vous pouvez créer vos propres Amazon Machine Images (AMI), auxquelles vous avez appliqué des correctifs et dont vous avez renforcé la sécurité, pour vous aider à répondre aux exigences de sécurité spécifiques de votre organisation. Les correctifs et autres contrôles de sécurité que vous appliquez sur l'AMI sont effectifs au moment où ils ont été créés. Ils ne sont pas dynamiques, sauf si vous les modifiez après le lancement, par exemple, avec AWS Systems Manager.

Vous pouvez simplifier le processus de création d'AMI sécurisées avec EC2 Image Builder. EC2 Image Builder réduit considérablement l'effort requis pour créer et préserver des images de référence sans avoir à écrire ni à gérer l'automatisation. Lorsque des mises à jour logicielles sont disponibles, Image Builder génère automatiquement une nouvelle image sans obliger les utilisateurs à lancer manuellement les créations d'image. EC2 Image Builder vous permet de valider facilement la fonctionnalité et la sécurité de vos images avant de les utiliser en production avec les tests fournis par AWS et vos propres tests. Vous pouvez également appliquer les paramètres de sécurité fournis par AWS pour sécuriser davantage vos images afin de répondre aux critères de sécurité internes. Par exemple, vous pouvez créer des images conformes à la norme Security Technical Implementation Guide (STIG) à l'aide de modèles fournis par AWS.

Grâce à des outils d'analyse de code statique tiers, vous pouvez identifier les problèmes de sécurité courants tels que les limites d'entrée de fonction non contrôlées, ainsi que les vulnérabilités et expositions courantes applicables. Vous pouvez utiliser Amazon CodeGuru pour les langues prises en charge. Les outils de vérification des dépendances peuvent également être utilisés pour déterminer si les bibliothèques avec lesquelles votre code est lié sont les dernières versions, sont elles-mêmes exemptes de vulnérabilités et d'expositions courantes et ont des conditions de licence qui répondent aux exigences de votre politique logicielle.

À l'aide d'Amazon Inspector, vous pouvez effectuer des évaluations de configuration de vos instances pour identifier les vulnérabilités et expositions communes connues, les évaluer par rapport à des points de référence en matière de sécurité et automatiser la notification des défauts. Amazon Inspector s'exécute sur des instances de production ou dans un pipeline de conception et notifie les développeurs et ingénieurs lorsque les résultats sont prêts. Vous pouvez accéder aux résultats par programmation et diriger votre équipe vers les systèmes de suivi des bugs et des retards. EC2 Image Builder peut être utilisé pour gérer les images de serveur (AMI) avec l'application de correctifs automatisée, l'application de politiques de sécurité fournies par AWS et d'autres personnalisations. Lorsque vous utilisez des conteneurs, mettez en œuvre l' analyse d'image ECR dans votre pipeline de génération et régulièrement par rapport à votre référentiel d'images pour rechercher les failles CVE dans vos conteneurs.

Si Amazon Inspector et d'autres outils sont efficaces pour identifier les configurations et les failles CVE présentes, d'autres méthodes sont nécessaires pour tester votre charge de travail au niveau de l'application. Le fuzzing est une méthode bien connue pour trouver des bugs en utilisant l'automatisation pour injecter des données malformées dans les champs de saisie et d'autres parties de votre application.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Débit

Directives d'implémentation

- Renforcer la sécurité du système d'exploitation : configurez les systèmes d'exploitation de manière à respecter les bonnes pratiques.
  - Sécurisation d'Amazon Linux
  - Sécurisation de Microsoft Windows Server
- Renforcer la sécurité des ressources conteneurisées : configurez les ressources conteneurisées de manière à respecter les bonnes pratiques en matière de sécurité.
- Implémentez les bonnes pratiques AWS Lambda.
  - Bonnes pratiques AWS Lambda

Ressources

Documents connexes :

- AWS Systems Manager
- Remplacement d'un hôte bastion par Amazon EC2 Systems Manager

- Présentation de la sécurité d'AWS Lambda

Vidéos connexes :

- Exécution de charges de travail à haute sécurité sur Amazon EKS
- Sécurisation des services sans serveur et de conteneur
- Bonnes pratiques de sécurité pour le service des métadonnées d'instance Amazon EC2

Exemples connexes :

- Atelier : Déploiement automatisé d'un pare-feu d'application Web

SEC06-BP03 Mettre en œuvre des services gérés

Mettez en œuvre des services qui gèrent les ressources, comme Amazon Relational Database Service (Amazon RDS), AWS Lambda, and Amazon Elastic Container Service (Amazon ECS), afin de réduire vos tâches de maintenance de la sécurité dans le cadre du modèle de responsabilité partagée. Par exemple, Amazon RDS vous aide à configurer, exploiter et dimensionner une base de données relationnelle, automatise les tâches d'administration telles que la mise en service du matériel, la configuration de base de données, l'application de correctifs et les sauvegardes. Cela signifie que vous pouvez consacrer plus de temps à la sécurisation de votre application selon les autres méthodes décrites dans le cadre AWS Well-Architected Framework. Lambda vous permet d'exécuter le code sans avoir à mettre en service ni à gérer des serveurs. Par conséquent, vous pouvez vous concentrer uniquement sur la connectivité, les appels et la sécurité au niveau du code, et non pas sur l'infrastructure ou le système d'exploitation.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

- Explorer les services disponibles : explorez, testez et implémentez des services qui gèrent des ressources, notamment Amazon RDS, AWS Lambda et Amazon ECS.

Ressources

Documents connexes :

- Site web AWS
- AWS Systems Manager
- Remplacement d'un hôte bastion par Amazon EC2 Systems Manager
- Présentation de la sécurité d'AWS Lambda

Vidéos connexes :

- Exécution de charges de travail à haute sécurité sur Amazon EKS
- Sécurisation des services sans serveur et de conteneur
- Bonnes pratiques de sécurité pour le service des métadonnées d'instance Amazon EC2

Exemples connexes :

- Atelier : Demander un certificat public avec AWS Certificate Manager

SEC06-BP04 Automatiser la protection du calcul

Automatisez vos mécanismes de protection du calcul, en particulier la gestion des failles, la réduction de la surface d'attaque et la gestion des ressources. L'automatisation vous aide à investir du temps pour sécuriser d'autres aspects de votre charge de travail, et à réduire le risque d'erreur humaine.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

- Automatiser la gestion de la configuration : appliquez et validez des configurations sécurisées automatiquement à l'aide d'un service ou d'un outil de gestion de la configuration.
  - AWS Systems Manager
  - AWS CloudFormation
  - Atelier : Déploiement automatisé d'un VPC
  - Atelier : Déploiement automatisé d'une application Web avec EC2

- Automatiser l'application de correctifs aux instances Amazon Elastic Compute Cloud (Amazon EC2) : AWS Systems Manager Patch Manager automatise le processus de correction des instances gérées avec des mises à jour liées à la sécurité et d'autres types de mises à jour.

Vous pouvez utiliser le gestionnaire de correctifs pour appliquer des correctifs aux systèmes d'exploitation et aux applications.

- le gestionnaire de correctifs AWS Systems Manager
- Application centralisée de correctifs multicomptes et multirégions avec AWS Systems Manager Automation

- Mettre en place une détection et une prévention des intrusions : mettez en place un outil de détection et de prévention des intrusions pour surveiller et arrêter les opérations malveillantes au niveau des instances.
- Envisager les solutions AWS Partner : les partenaires AWS proposent des centaines de produits leaders du secteur qui sont équivalents, identiques ou s'intègrent aux 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.
  - Sécurité de l'infrastructure

Ressources

Documents connexes :

- AWS CloudFormation
- AWS Systems Manager
- le gestionnaire de correctifs AWS Systems Manager
- Application centralisée de correctifs multicomptes et multirégions avec AWS Systems Manager Automation
- Sécurité de l'infrastructure
- Remplacement d'un hôte bastion par Amazon EC2 Systems Manager
- Présentation de la sécurité d'AWS Lambda

Vidéos connexes :

- Exécution de charges de travail à haute sécurité sur Amazon EKS
- Sécurisation des services sans serveur et de conteneur
- Bonnes pratiques de sécurité pour le service des métadonnées d'instance Amazon EC2

Exemples connexes :

- Atelier : Déploiement automatisé d'un pare-feu d'application Web
- Atelier : Déploiement automatisé d'une application Web avec EC2

SEC06-BP05 Permettre aux utilisateurs d'effectuer des actions à distance

La suppression de la possibilité d'accès interactif réduit le risque d'erreur humaine et le potentiel de configuration ou de gestion manuelle. Par exemple, utilisez un flux de travail de gestion des modifications pour déployer des instances Amazon Elastic Compute Cloud (Amazon EC2) à l'aide d'une infrastructure en tant que code, puis gérez les instances Amazon EC2 avec des outils tels qu'AWS Systems Manager au lieu d'autoriser un accès direct ou via un hôte bastion. AWS Systems Manager automatise diverses tâches de maintenance et de déploiement à l'aide de fonctionnalités telles que l' automatisation (flux de travail), les documents (playbooks) et la Run Command. Les piles AWS CloudFormation sont construites à partir de pipelines et peuvent automatiser les tâches de déploiement et de gestion de votre infrastructure sans utiliser directement AWS Management Console ni les API.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Remplacer l'accès à la console : remplacez l'accès (protocole SSH ou RDP) aux instances depuis la console par AWS Systems Manager Run Command pour automatiser les tâches de gestion.

- AWS Systems Manager Run Command

Ressources

Documents connexes :

- AWS Systems Manager
- AWS Systems Manager Run Command
- Remplacement d'un hôte bastion par Amazon EC2 Systems Manager
- Présentation de la sécurité d'AWS Lambda

Vidéos connexes :

- Exécution de charges de travail à haute sécurité sur Amazon EKS
- Sécurisation des services sans serveur et de conteneur
- Bonnes pratiques de sécurité pour le service des métadonnées d'instance Amazon EC2

Exemples connexes :

- Atelier : Déploiement automatisé d'un pare-feu d'application Web

SEC06-BP06 Valider l'intégrité des logiciels

Mettez en place des mécanismes (signature de code) pour confirmer que les logiciels, le code et les bibliothèques utilisés dans la charge de travail proviennent de sources fiables et n'ont pas été altérés. Par exemple, vous devez vérifier le certificat de signature de code des fichiers binaires et des scripts pour vérifier l'auteur, et vous assurer qu'il n'a pas été altéré depuis sa création par l'auteur. AWS Signer contribue à garantir la confiance et l'intégrité de votre code en gérant de manière centralisée le cycle de vie de la signature de code, y compris la certification de la signature et les clés publiques et privées. Vous pouvez apprendre à utiliser des modèles avancés et les bonnes pratiques en matière de signature de code avec AWS Lambda. En outre, un total de contrôle du logiciel que vous téléchargez, comparé à celui du fournisseur, peut garantir qu'il n'a pas été altéré.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Étudier les mécanismes : la signature de code est un mécanisme qui peut être utilisé pour valider l'intégrité des logiciels.
  - NIST : considérations de sécurité pour la signature de code

Ressources

Documents connexes :

- AWS Signer
- Nouveau : la signature de code, un contrôle de confiance et d'intégrité pour AWS Lambda

Protection des données

Avant de concevoir l'architecture d'une charge de travail, il convient de mettre en place des pratiques fondamentales qui influencent la sécurité. Par exemple, la classification des données permet de classer les données en fonction de leur niveau de sensibilité, et le chiffrement protège les données en les rendant inintelligibles à un accès non autorisé. Ces méthodes sont importantes, car elles sous-tendent des objectifs tels que la prévention des erreurs de manipulation ou le respect des obligations réglementaires.

Dans AWS, il existe un certain nombre d'approches différentes à prendre en compte en matière de protection des données. La section suivante décrit comment utiliser ces approches.

Rubriques

Classification des données

La classification des données fournit un moyen de classer les données organisationnelles en fonction de leur criticité et de leur sensibilité afin de vous aider à déterminer les contrôles de protection et de conservation appropriés.

Bonnes pratiques

SEC07-BP01 Identifier les données au sein de votre charge de travail

Il est essentiel de comprendre le type et la classification des données que votre charge de travail traite, les processus d'entreprise associés, l'endroit où les données sont stockées et qui est le propriétaire des données. Vous devez également connaître les exigences légales et de conformité

applicables à votre charge de travail, et savoir quels contrôles de données doivent être appliqués. L'identification des données est la première étape du processus de classification des données.

Avantages liés à l'instauration de cette bonne pratique :

La classification des données permet aux responsables de la charge de travail d'identifier les emplacements qui stockent des données sensibles et de déterminer comment ces données doivent être consultées et partagées.

La classification des données vise à répondre aux questions suivantes :

- De quel type de données disposez-vous ?

  Il peut s'agir de données telles que :

  - Propriété intellectuelle, comme les secrets commerciaux, les brevets ou les contrats.
  - Informations de santé protégées (PH), comme les dossiers médicaux qui contiennent des informations sur les antécédents médicaux d'une personne.
  - Données d'identification personnelle (PII), comme le nom, l'adresse, la date de naissance et le numéro d'identification ou d'enregistrement national.
  - Données de carte bancaire, comme le numéro de compte principal (PAN), le nom du titulaire de la carte, la date d'expiration et le numéro de code de service.
  - Où les données sensibles sont-elles stockées ?
  - Qui peut consulter, modifier et supprimer des données ?
  - Il est essentiel de comprendre les autorisations des utilisateurs pour éviter toute manipulation inappropriée des données.
- Qui peut effectuer des opérations de création, de lecture, de mise à jour et de suppression (CRUD) ?
  - Tenez compte de l'escalade potentielle des privilèges en comprenant qui peut gérer les autorisations d'accès aux données.
- Quelles sont les répercussions sur les activités si les données sont divulguées involontairement, modifiées ou supprimées ?
  - Comprenez les conséquences du risque si des données sont modifiées, supprimées ou divulguées par inadvertance.

En connaissant les réponses à ces questions, vous pouvez prendre les mesures suivantes :

- Réduire la portée des données sensibles (comme le nombre d'emplacements de données sensibles) et limiter l'accès aux données sensibles aux utilisateurs approuvés uniquement.
- Comprendre les différents types de données afin de pouvoir implémenter des mécanismes et des techniques de protection des données appropriés, tels que le chiffrement, la prévention de la perte de données et la gestion des identités et des accès.
- Optimiser les coûts en fournissant les bons objectifs de contrôle pour les données.
- Répondre en toute confiance aux questions des organismes de réglementation et des vérificateurs concernant les types et la quantité de données, et la façon dont les données de sensibilités différentes sont isolées les unes des autres.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

La classification des données consiste à déterminer la sensibilité des données. Il peut s'agir de baliser les données pour les rendre facilement interrogeables et traçables. La classification des données réduit également la duplication des données, ce qui peut permettre de réduire les coûts de stockage et de sauvegarde, tout en accélérant le processus de recherche.

Utilisez des services tels que Amazon Macie pour automatiser à grande échelle la découverte et la classification des données sensibles. D'autres services, comme Amazon EventBridge et AWS Config, peuvent être utilisés pour automatiser la correction des problèmes de sécurité des données, comme les compartiments Amazon Simple Storage Service (Amazon S3) non chiffrés et les volumes EBS Amazon EC2 ou les ressources de données non balisées. Pour obtenir une liste complètes des intégrations de service AWS, consultez la documentation EventBridge.

La détection des PII dans les données non structurées, comme les e-mails des clients, les tickets de support, les examens de produits et les réseaux sociaux, peut être effectuée en utilisant Amazon Comprehend, qui est un service de traitement du langage naturel (NLP) qui utilise le machine learning (ML) pour trouver des idées et des relations, comme les personnes, les lieux, les sentiments et les sujets dans un texte non structuré. Pour une liste des services AWS qui peuvent faciliter l'identification des données, consultez Techniques courantes pour détecter les données PHI et PII à l'aide des services AWS.

Une autre méthode qui prend en charge la classification et la protection des données est le balisage des ressources AWS. Le balisage vous permet d'attribuer des métadonnées à vos ressources AWS pour vous aider à gérer, identifier, organiser, rechercher et filtrer ces dernières.

Dans certains cas, vous pouvez choisir de baliser des ressources entières (comme un compartiment S3), surtout lorsqu'une charge de travail ou un service particulier est censé stocker des processus ou des transmissions d'une classification de données déjà connue.

Le cas échéant, vous pouvez baliser un compartiment S3 au lieu d'objets individuels pour faciliter l'administration et la maintenance de la sécurité.

Étapes d'implémentation

Détectez les données sensibles dans Amazon S3 :

1. Avant de commencer, assurez-vous de disposer des autorisations appropriées pour accéder à la console Amazon Macie et aux opérations d'API. Pour plus d'informations, consultez Mise en route de Amazon Macie.
2. Utilisez Amazon Macie pour effectuer la découverte automatisée des données lorsque vos données sensibles résident dans Amazon S3.
   - Utilisez le guide Mise en route de Amazon Macie afin de configurer un référentiel pour les résultats de découverte de données sensibles et de créer une tâche de découverte des données sensibles.
   - Comment utiliser Amazon Macie pour prévisualiser les données sensibles dans les compartiments S3.

     Par défaut, Macie analyse les objets en utilisant l'ensemble d'identifiants de données gérés que nous recommandons pour la découverte automatisée de données sensibles. Vous pouvez personnaliser l'analyse en configurant Macie de façon à utiliser des identifiants de données gérés spécifiques, des identifiants de données personnalisés et des listes d'autorisations lorsqu'il effectue la découverte automatisée des données sensibles pour votre compte ou votre organisation. Vous pouvez ajuster la portée de l'analyse en excluant des compartiments spécifiques (par exemple, les compartiments S3 qui stockent généralement les données de journalisation AWS).
3. Pour configurer et utiliser la découverte automatisée de données sensibles, consultez Effectuer la découverte automatisée des données sensibles avec Amazon Macie.
4. Consultez également Découverte automatisée des données pour Amazon Macie.

Détectez les données sensibles dans Amazon RDS :

pour plus d'informations sur la découverte des données dans les bases de données Amazon Relational Database Service (Amazon RDS), consultez Classification des données pour la base de données Amazon RDS avec Macie.

Détectez les données sensibles dans DynamoDB :

- la section Détection des données sensibles dans DynamoDB avec Macie explique comment utiliser Amazon Macie pour détecter les données sensibles dans les tables Amazon DynamoDB en exportant les données dans Amazon S3 en vue de leur analyse.

Solutions de partenaires AWS :

- Envisagez d'utiliser notre AWS Partner Network étendu. Les partenaires AWS disposent d'outils complets et de frameworks de conformité qui s'intègrent directement aux services AWS. Les partenaires peuvent vous fournir une solution de gouvernance et de conformité adaptée à vos besoins organisationnels.
- Pour plus d'informations sur les solutions personnalisées de classification des données, consultez Gouvernance des données à l'ère de la réglementation et exigences de conformité.

Vous pouvez appliquer automatiquement les normes de balisage que votre organisation adopte en créant et en déployant des politiques avec AWS Organizations. Les politiques de balises vous permettent de spécifier les règles qui définissent les noms de clés valides et les valeurs valides pour chaque clé. Vous pouvez choisir de surveiller uniquement, ce qui vous donne la possibilité d'évaluer et de nettoyer vos balises existantes. Une fois que vos balises sont conformes aux normes que vous avez choisies, vous pouvez activer l'application des politiques relatives aux balises pour empêcher la création de balises non conformes. Pour plus d'informations, consultez Sécurisation des balises de ressources utilisées pour l'autorisation à l'aide d'une politique de contrôle des services dans AWS Organizations et l'exemple de politique sur les solutions pour éviter la modification des balises, sauf par les principaux autorisés..

- Pour commencer à utiliser des politiques de balises dans AWS Organizations, il est vivement recommandé de suivre le workflow dans Mise en route des politiques de balises avant de passer à des politiques de balises plus avancées. Comprendre les effets d'une simple politique de balise sur un seul compte avant de l'étendre à toute une unité d'organisation (UO) ou une organisation vous permet de voir les effets d'une politique de balise avant d'appliquer la politique de balise. Mise en route des politiques de balises fournit des liens vers des instructions relatives à des tâches plus avancées en matière de politiques.

- Envisagez d'évaluer d'autres services et fonctionnalités AWS qui prennent en charge la classification des données, comme indiqué dans le livre blanc sur la classification des données.

Ressources

Documents connexes :

- Getting started with Amazon Macie (Mise en route de Amazon Macie)
- Automated data discovery with Amazon Macie
- Mise en route des politiques de balises
- Detecting PII entities (Détecter les entités PII)

Blogs connexes :

- Comment utiliser Amazon Macie pour prévisualiser les données sensibles dans les compartiments S3.
- Performing automated sensitive data discovery with Amazon Macie.
- Common techniques to detect PHI and PII data using AWS Services
- Detecting and redacting PII using Amazon Comprehend
- Securing resource tags used for authorization using a service control policy in AWS Organizations
- Enabling data classification for Amazon RDS database with Macie
- Detecting sensitive data in DynamoDB with Macie
-

Vidéos connexes :

- Event-driven data security using Amazon Macie
- Amazon Macie for data protection and governance
- Fine-tune sensitive data findings with allow lists

SEC07-BP02 Définir les contrôles de protection des données

Protégez les données en fonction de leur niveau de classification. Par exemple, sécurisez les données classées comme publiques à l'aide des recommandations pertinentes tout en protégeant les données sensibles grâce à des contrôles supplémentaires.

En utilisant des balises de ressource, des comptes AWS séparés par sensibilité (et éventuellement aussi pour chaque mise en garde, isolement ou communauté d'intérêt), les politiques IAM, les politiques de contrôle des services (SCP) AWS Organizations, AWS Key Management Service (AWS KMS) et AWS CloudHSM, vous pouvez définir et mettre en œuvre vos politiques de classification et de protection des données avec chiffrement. Par exemple, si vous disposez d'un projet avec des compartiments S3 qui contiennent des données hautement critiques ou des instances Amazon Elastic Compute Cloud (Amazon EC2) qui traitent des données confidentielles, ils peuvent être marqués avec une balise `Project=ABC` . Seule votre équipe immédiate sait ce que le code du projet signifie, et cela permet d'utiliser un contrôle d'accès basé sur les attributs. Vous pouvez définir des niveaux d'accès aux clés de chiffrement AWS KMS par le biais de politiques de clés et d'autorisations afin de garantir que seuls les services appropriés ont accès au contenu sensible par un mécanisme sécurisé. Si vous prenez des décisions d'autorisation basées sur des balises, vous devez vous assurer que les autorisations sur les balises sont définies de manière appropriée en utilisant des politiques de balises dans AWS Organizations.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Débit

Directives d'implémentation

- Définir votre schéma d'identification et de classification des données : l'identification et la classification de vos données sont faites pour évaluer l'impact potentiel et le type de données que vous stockez et qui peut y accéder.
  - Documentation AWS
- Découvrir les contrôles AWS disponibles : découvrez les contrôles de sécurité pour les services AWS que vous utilisez ou prévoyez d'utiliser. De nombreux services disposent d'une section relative à la sécurité dans leur documentation.
  - Documentation AWS
- Identifier les ressources de conformité AWS : identifiez les ressources que propose AWS pour vous aider.
  - https://aws.amazon.com/compliance/

Ressources

Documents connexes :

- Documentation AWS
- Livre blanc sur la classification des données
- Démarrer avec Amazon Macie
- Texte manquant

Vidéos connexes :

- Introducing the New Amazon Macie

SEC07-BP03 Automatiser l'identification et la classification

l'automatisation de l'identification et de la classification des données peut vous aider à mettre en œuvre les contrôles appropriés. Le recours à l'automatisation en la circonstance plutôt qu'à l'accès direct d'une personne réduit le risque d'erreur humaine et d'exposition. Vous devez évaluer, en utilisant un outil tel qu' Amazon Macie, qui utilise le machine learning pour découvrir, catégoriser et protéger les données sensibles dans AWS. Amazon Macie reconnaît les données sensibles en tant que données d'identification personnelle (PII) ou propriété intellectuelle, et génère des tableaux de bord et des alertes pour vous offrir de la visibilité sur les méthodes de déplacement ou d'accès à ces données.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

- Utiliser l'inventaire Amazon Simple Storage Service (Amazon S3) : l'inventaire Amazon S3 est l'un des outils que vous pouvez utiliser pour auditer et signaler le statut de réplication et de chiffrement de vos objets.
  - Inventaire Amazon S3
- Envisager Amazon Macie : Amazon Macie utilise le machine learning pour détecter et classer automatiquement les données stockées dans Amazon S3.
  - Amazon Macie

Ressources

Documents connexes :

- Amazon Macie
- Inventaire Amazon S3
- Livre blanc sur la classification des données
- Mise en route avec Amazon Macie

Vidéos connexes :

- Introducing the New Amazon Macie

SEC07-BP04 Définir la gestion du cycle de vie des données

votre stratégie de cycle de vie définie doit être basée sur le niveau de sensibilité, ainsi que sur les exigences légales et organisationnelles. Des aspects, tels que la durée de conservation des données, les processus de destruction des données, la gestion de l'accès aux données, la transformation des données et le partage des données, doivent être pris en compte. Lorsque vous choisissez une méthodologie de classification des données, équilibrez l'utilisabilité par rapport à l'accès. Vous devez également tenir compte des multiples niveaux d'accès et des nuances pour mettre en œuvre une approche sécurisée, mais toujours utilisable, pour chaque niveau. Utilisez toujours une approche de défense en profondeur et réduisez l'accès humain aux données et aux mécanismes de transformation, de suppression ou de copie des données. Par exemple, exigez que les utilisateurs s'authentifient d'une manière forte auprès d'une application, et donnez à l'application, plutôt qu'aux utilisateurs, l'autorisation d'accès requise pour effectuer une « action à distance ». En outre, veillez à ce que les utilisateurs proviennent d'un chemin de réseau approuvé et aient besoin d'un accès aux clés de déchiffrement. Utiliser des outils, tels que des tableaux de bord et des rapports automatisés, pour donner aux utilisateurs des informations à partir des données plutôt que de leur fournir un accès direct aux données.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Identifier les types de données : identifiez les types de données que vous stockez ou traitez dans votre charge de travail. Ces données peuvent être du texte, des images, des bases de données binaires, etc.

Ressources

Documents connexes :

- Livre blanc sur la classification des données
- Mise en route avec Amazon Macie

Vidéos connexes :

- Introducing the New Amazon Macie

Protection des données au repos

Données au repos représentent toutes les données que vous conservez dans un stockage non volatil pendant toute la durée de votre charge de travail. Cela comprend le stockage par bloc, le stockage d'objets, les bases de données, les archives, les appareils IoT et tout autre support de stockage sur lequel les données sont conservées. La protection de vos données inactives permet de réduire le risque d'accès non autorisé, lorsque le chiffrement et les contrôles d'accès appropriés sont mis en place.

Le chiffrement et la création de jetons sont deux programmes de protection des données distincts mais importants.

La création de jetons est un processus qui vous permet de définir un jeton pour représenter une information sensible (par exemple, un jeton pour représenter le numéro de carte de crédit d'un client). Un jeton doit être vide de sens en soi et ne doit pas être dérivé des données qu'il contient. Par conséquent, un algorithme de chiffrement n'est pas utilisable comme jeton. En planifiant soigneusement votre approche de création de jetons, vous pouvez renforcer la protection de votre contenu et vous assurer que vous répondez à vos exigences de conformité. Par exemple, vous pouvez réduire le champ de conformité d'un système de traitement des cartes de crédit si vous utilisez un jeton au lieu d'un numéro de carte de crédit.

Chiffrement est un moyen de transformer un contenu de manière à le rendre illisible sans clé secrète, nécessaire pour le déchiffrer. La création de jetons et le chiffrement peuvent être utilisés pour sécuriser et protéger des informations, le cas échéant. En outre, le masquage est une technique qui permet d'expurger une partie d'une donnée jusqu'à ce que le reste de la donnée ne soit plus considéré comme sensible. Par exemple, la norme PCI-DSS permet de conserver les quatre derniers chiffres d'un numéro de carte en dehors du périmètre de conformité pour l'indexation.

Auditer l'utilisation des clés de chiffrement : vous devez comprendre et contrôler l'utilisation des clés de chiffrement afin de vérifier que les mécanismes de contrôle d'accès sur les clés sont correctement mis en œuvre. Par exemple, un service AWS utilisant une clé AWS KMS enregistre chaque utilisation dans AWS CloudTrail. Vous pouvez ensuite interroger AWS CloudTrail à l'aide d'un outil tel qu'Amazon CloudWatch Insights pour vous assurer que toutes les utilisations de vos clés sont valides.

Bonnes pratiques

- SEC08-BP01 Mise en œuvre de la gestion sécurisée des clés
- SEC08-BP02 Appliquer le chiffrement au repos
- SEC08-BP03 Automatiser la protection des données au repos
- SEC08-BP04 Appliquer le contrôle d'accès
- SEC08-BP05 Utiliser des mécanismes pour protéger l'accès aux données

SEC08-BP01 Mise en œuvre de la gestion sécurisée des clés

La gestion sécurisée des clés inclut le stockage, la rotation, le contrôle d'accès et la surveillance des informations sur les clés nécessaires pour sécuriser les données inactives adaptées à votre charge de travail.

Résultat souhaité : Un mécanisme de gestion des clés évolutif, reproductible et automatisé. Ce mécanisme devrait permettre de faire respecter le principe du moindre privilège d'accès aux informations sur les clés et de trouver le juste équilibre entre la disponibilité des clés, la confidentialité et l'intégrité. L'accès aux clés doit être surveillé et les informations sur les clés doivent être alternées par le biais d'un processus automatisé. Les clés ne doivent jamais être accessibles aux identités humaines.

Anti-modèles courants :

- Accès humain à des informations sur les clés non chiffrées.

- Création d'algorithmes cryptographiques personnalisés.
- Autorisations trop larges pour accéder aux informations sur les clés.

Avantages liés au respect de cette bonne pratique : En établissant un mécanisme sécurisé de gestion des clés pour votre charge de travail, vous contribuez à protéger votre contenu contre tout accès non autorisé. En outre, vous pouvez être soumis à des exigences réglementaires en matière de chiffrement de vos données. Une solution efficace de gestion des clés peut fournir des mécanismes techniques conformes à ces réglementations afin de protéger les informations sur les clés.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : Élevé

Directives d'implémentation

De nombreuses exigences réglementaires et bonnes pratiques incluent le chiffrement des données au repos en tant que contrôle de sécurité fondamental. Afin de respecter ce contrôle, votre charge de travail a besoin d'un mécanisme permettant de stocker et de gérer en toute sécurité les informations sur les clés utilisées pour chiffrer vos données au repos.

AWS propose AWS Key Management Service (AWS KMS) pour fournir un stockage durable, sécurisé et redondant pour les clés AWS KMS. De nombreux services AWS s'intègrent à AWS KMS pour prendre en charge le chiffrement de vos données. AWS KMS utilise des modules de sécurité matériels validés FIPS 140-2 niveau 3 pour protéger vos clés. Il n'existe aucun mécanisme permettant d'exporter les clés AWS KMS en texte brut.

Lors du déploiement de charges de travail à l'aide d'une stratégie multi-comptes, il est conseillé de conserver les clés AWS KMS dans le même compte que la charge de travail qui les utilise. Dans ce modèle distribué, la responsabilité de la gestion des clés AWS KMS incombe à l'équipe chargée de l'application. Dans d'autres cas d'utilisation, les entreprises peuvent choisir de stocker les clés AWS KMS dans un compte centralisé. Cette structure centralisée nécessite des politiques supplémentaires pour permettre l'accès intercompte requis afin que le compte de la charge de travail puisse accéder aux clés stockées dans le compte centralisé, mais elle s'applique peut-être plus aux cas d'utilisation où une seule clé est partagée entre plusieurs Comptes AWS.

Quel que soit l'endroit où les informations sur les clés sont stockées, l'accès à la clé doit être étroitement contrôlé grâce à l'utilisation de politiques de clés et de stratégies IAM. Les politiques de clés constituent le principal moyen de contrôler l'accès à une clé AWS KMS. En outre, les octrois de clés AWS KMS peuvent donner accès à des services AWS permettant de chiffrer et de déchiffrer les données en votre nom. Prenez le temps de consulter les bonnes pratiques en matière de contrôle d'accès à vos clés AWS KMS.

Il est recommandé de surveiller l'utilisation des clés de chiffrement afin de détecter les modèles d'accès inhabituels. Les opérations effectuées à l'aide de clés gérées par AWS et de clés gérées par le client stockées dans AWS KMS peuvent être journalisées dans AWS CloudTrail et doivent être examinées périodiquement. Une attention particulière doit être accordée à la surveillance des événements de destruction des clés. Pour limiter la destruction accidentelle ou malveillante des informations sur les clés, les événements de destruction des clés ne suppriment pas immédiatement ces informations. Les tentatives de suppression de clés AWS KMS sont soumises à une période d'attente dont la durée par défaut est de 30 jours, ce qui laisse aux administrateurs le temps de vérifier ces actions et d'annuler la requête si nécessaire.

La plupart des services AWS utilisent AWS KMS de manière transparente pour vous. Vous n'avez qu'à décider si vous souhaitez utiliser une clé gérée par AWS ou une clé gérée par le client. Si votre charge de travail nécessite l'utilisation directe de AWS KMS pour chiffrer ou déchiffrer des données, il est conseillé de recourir au chiffrement d'enveloppe pour protéger vos données. Le kit SDK AWS Encryption peut fournir à vos applications des primitives de chiffrement côté client pour implémenter le chiffrement d'enveloppe et l'intégrer à AWS KMS.

Étapes d'implémentation

1. Déterminez les options appropriées de gestion des clés (gérées par AWS ou par le client).
    - Pour faciliter l'utilisation, AWS propose des clés AWS qui appartiennent au client et des clés gérées par AWS pour la plupart des services. Elles fournissent une fonctionnalité de chiffrement au repos sans qu'il soit nécessaire de gérer les informations sur les clés ou les politiques les concernant.
    - Lorsque vous utilisez des clés gérées par le client, pensez au key store par défaut afin de trouver le meilleur équilibre entre agilité, sécurité, souveraineté des données et disponibilité. D'autres cas d'utilisation peuvent nécessiter l'utilisation de key stores personnalisés avec AWS CloudHSM ou le key store externe.
2. Consultez la liste des services que vous utilisez pour votre charge de travail afin de comprendre comment AWS KMS s'y intègre. Par exemple, les instances EC2 peuvent utiliser des volumes EBS chiffrés. Elles vérifient ainsi que les instantanés Amazon EBS créés à partir de ces volumes sont également chiffrés à l'aide d'une clé gérée par le client et limitent la divulgation accidentelle des données instantanées non chiffrées.
    - Comment les services AWS utilisent AWS KMS
    - Pour obtenir des informations détaillées sur les options de chiffrement proposées par un service AWS, consultez la rubrique Chiffrement au repos du guide de l'utilisateur ou du guide du développeur du service.

3. Mettez en œuvre AWS KMS : AWS KMS simplifie la création et la gestion des clés et le contrôle de l'utilisation du chiffrement dans un large éventail de services AWS et dans vos applications.
   - Premiers pas : AWS Key Management Service (AWS KMS)
   - Consultez les bonnes pratiques en matière de contrôle d'accès à vos clés AWS KMS.
4. Envisagez AWS Encryption SDK : utilisez le kit AWS Encryption SDK avec l'intégration AWS KMS lorsque votre application doit chiffrer des données côté client.
   - AWS Encryption SDK
5. Activez IAM Access Analyzer pour examiner et envoyer automatiquement des notifications si les politiques des clés AWS KMS sont trop génériques.
6. Activez Security Hub pour recevoir des notifications en cas de mauvaise configuration des politiques relatives aux clés, de clés dont la suppression est prévue ou de clés dont la rotation automatique est activée.
7. Déterminez le niveau de journalisation approprié pour vos clés AWS KMS. Étant donné que les appels à AWS KMS, y compris les événements en lecture seule, sont journalisés, les journaux CloudTrail associés à AWS KMS peuvent devenir volumineux.
   - Certaines organisations préfèrent séparer les activités de journalisation AWS KMS à un emplacement distinct. Pour en savoir plus, consultez la section Journalisation des appels d'API AWS KMS avec CloudTrail dans le guide du développeur AWS KMS.

Ressources

Documents connexes :

- AWS Key Management Service
- Services et outils cryptographiques AWS
- Protection des données Amazon S3 à l'aide du chiffrement
- Chiffrement d'enveloppe
- L'engagement de souveraineté numérique
- Démystifier les opérations de clés AWS KMS, apporter votre propre clé, key store personnalisé et portabilité du texte chiffré
- Informations cryptographiques AWS Key Management Service

Vidéos connexes :

- How Encryption Works in AWS
- Securing Your Block Storage on AWS
- AWS data protection: Using locks, keys, signatures, and certificates

Exemples connexes :

- Mettre en œuvre des mécanismes de contrôle d'accès avancés avec AWS KMS

SEC08-BP02 Appliquer le chiffrement au repos

Vous devez appliquer l'utilisation du chiffrement pour les données au repos. Le chiffrement permet de préserver la confidentialité des données sensibles en cas d'accès non autorisé ou de divulgation accidentelle.

Résultat souhaité : les données privées doivent être chiffrées par défaut au repos. Le chiffrement permet de préserver la confidentialité des données et offre une protection supplémentaire contre la divulgation ou l'exfiltration intentionnelle ou involontaire des données. Les données chiffrées ne peuvent pas être lues ni consultées si elles n'ont pas été déchiffrées au préalable. Toutes les données stockées non chiffrées doivent être inventoriées et contrôlées.

Anti-modèles courants :

- Ne pas utiliser les configurations chiffrées par défaut.
- Fournir un accès trop permissif aux clés de déchiffrement.
- Ne pas surveiller l'utilisation des clés de chiffrement et de déchiffrement.
- Stocker des données non chiffrées.
- Utiliser la même clé de chiffrement pour toutes les données, quels que soient l'utilisation, le type et la classification des données.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Mappez les clés de chiffrement aux classifications de données dans vos charges de travail. Cette approche offre une protection contre les accès trop permissifs lors de l'utilisation d'une seule, ou d'un très petit nombre de clés de chiffrement pour vos données (consultez SEC07-BP01 Identifier les données au sein de votre charge de travail).

AWS Key Management Service (AWS KMS) s'intègre à de nombreux services AWS afin de faciliter le chiffrement des données au repos. Par exemple, dans Amazon Simple Storage Service (Amazon S3), vous pouvez définir un chiffrement par défaut sur un compartiment pour que tous les nouveaux objets soient chiffrés automatiquement. Lorsque vous utilisez AWS KMS, tenez compte du degré de restriction des données. Les clés AWS KMS par défaut et contrôlées par le service sont gérées et utilisées en votre nom par AWS. Pour les données sensibles qui nécessitent un accès précis à la clé de chiffrement sous-jacente, envisagez les clés gérées par le client (CMK). Vous disposez d'un contrôle total sur les CMK, y compris la rotation et la gestion des accès grâce à l'utilisation de politiques de clés.

De plus, Amazon Elastic Compute Cloud (Amazon EC2) et Amazon S3 prennent en charge la mise en application du chiffrement en définissant le chiffrement par défaut. Vous pouvez utiliser AWS Config Rules pour vérifier automatiquement que vous utilisez le chiffrement, par exemple, pour les volumes Amazon Elastic Block Store (Amazon EBS), les instances Amazon Relational Database Service (Amazon RDS) et les compartiments Amazon S3.

AWS fournit également des options de chiffrement côté client, ce qui vous permet de chiffrer les données avant de les télécharger dans le cloud. Le AWS Encryption SDK fournit une solution pour chiffrer vos données à l'aide du chiffrement d'enveloppe. Vous fournissez la clé de wrapping et le AWS Encryption SDK génère une clé de données unique pour chaque objet de données qu'il chiffre. Envisagez AWS CloudHSM si vous avez besoin d'un module de sécurité du matériel géré à un seul locataire (HSM). AWS CloudHSM vous permet de générer, d'importer et de gérer des clés de chiffrement sur un HSM validé FIPS 140-2 de niveau 3. Certains cas d'utilisation pour AWS CloudHSM incluent la protection des clés privées pour l'émission d'une autorité de certification (CA) et le chiffrement transparent des données (TDE) pour les bases de données Oracle. Le kit SDK client AWS CloudHSM fournit un logiciel qui vous permet de chiffrer des données côté client à l'aide de clés stockées dans AWS CloudHSM avant de télécharger vos données dans AWS. Amazon DynamoDB Encryption Client vous permet également de chiffrer et de signer les éléments avant de les télécharger dans une table DynamoDB.

Étapes d'implémentation

- Imposez le chiffrement au report pour Amazon S3 : implémentez le chiffrement par défaut des compartiments Amazon S3.

  Configurez le chiffrement par défaut pour les nouveaux volumes Amazon EBS : indiquez que vous souhaitez que tous les nouveaux volumes Amazon EBS soient chiffrés, avec la possibilité d'utiliser la clé par défaut fournie par AWS ou une clé que vous créez.

Configurez des Amazon Machine Images (AMI) chiffrées : la copie d'une AMI existante avec le chiffrement activé chiffrera automatiquement les volumes racine et les instantanés.

Configurez le chiffrement Amazon RDS : configurez le chiffrement de vos clusters de bases de données Amazon RDS et de vos instantanés au repos en utilisant l'option de chiffrement.

Créez et configurez des clés AWS KMS avec des politiques qui limitent l'accès aux principaux appropriés pour chaque classification des données : par exemple, créez une clé AWS KMS pour chiffrer les données de production et une clé différente pour chiffrer les données de développement ou de test. Vous pouvez également fournir un accès de clé à d'autres Comptes AWS. Envisagez d'avoir différents comptes pour vos environnements de développement et de production. Si votre environnement de production a besoin de déchiffrer des artefacts dans le compte de développement, vous pouvez modifier la politique de CMK utilisée pour chiffrer les artefacts de développement afin de permettre au compte de production de déchiffrer ces artefacts. L'environnement de production peut ensuite ingérer les données déchiffrées afin de les utiliser en production.

Configurez le chiffrement dans des services AWS supplémentaires : pour les autres services AWS que vous utilisez, consultez la documentation sur la sécurité associée aux services concernés afin de déterminer vos options de chiffrement.

Ressources

Documents connexes :

- Documentation sur AWS Crypto Tools
- Documentation sur AWS
- AWS Encryption SDK
- Livre blanc Présentation des détails cryptographiques de AWS KMS
- AWS Key Management Service
- AWS cryptographic services and tools (Services et outils de chiffrement AWS)
- Chiffrement Amazon EBS
- Default encryption for Amazon EBS volumes
- Chiffrement des ressources Amazon RDS
- How do I enable default encryption for an Amazon S3 bucket?

- Protection des données Amazon S3 à l'aide du chiffrement

Vidéos connexes :

- How Encryption Works in AWS
- Securing Your Block Storage on AWS

SEC08-BP03 Automatiser la protection des données au repos

utilisez des outils automatisés pour valider et faire respecter en permanence les contrôles des données au repos, par exemple en vérifiant qu'il n'y a que des ressources de stockage chiffrées. Vous pouvez automatiser la validation du chiffrement de tous les volumes de données EBS en utilisant AWS Config Rules. AWS Security Hub peut également vérifier plusieurs contrôles différents via des vérifications automatisées par rapport aux normes de sécurité. De plus, AWS Config Rules peut corriger les ressources non conformes automatiquement.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

Données au repos représentent toutes les données que vous conservez dans un stockage non volatil pendant toute la durée de votre charge de travail. Cela comprend le stockage par bloc, le stockage d'objets, les bases de données, les archives, les appareils IoT et tout autre support de stockage sur lequel les données sont conservées. La protection de vos données inactives permet de réduire le risque d'accès non autorisé, lorsque le chiffrement et les contrôles d'accès appropriés sont mis en place.

Appliquer le chiffrement au repos : vous devez faire en sorte que le seul moyen de stocker des données est de les chiffrer. AWS KMS s'intègre en toute transparence à de nombreux services AWS pour vous permettre de chiffrer plus facilement toutes vos données au repos. Par exemple, dans Amazon Simple Storage Service (Amazon S3), vous pouvez définir un chiffrement par défaut sur un compartiment pour que tous les nouveaux objets soient chiffrés automatiquement. En outre, Amazon EC2 et Amazon S3 prennent en charge la mise en application du chiffrement en définissant le chiffrement par défaut. Vous pouvez utiliser des règles de configuration gérées AWS pour vérifier automatiquement que vous utilisez le chiffrement, par exemple, pour les volumes EBS, les instances Amazon Relational Database Service (Amazon RDS)et des compartiments Amazon S3.

Ressources

Documents connexes :

- Outils de chiffrement AWS
- Kit SDK AWS

Vidéos connexes :

- How Encryption Works in AWS
- Securing Your Block Storage on AWS

SEC08-BP04 Appliquer le contrôle d'accès

Pour vous aider à protéger vos données au repos, appliquez le contrôle d'accès à l'aide de mécanismes tels que l'isolement et la gestion des versions, et appliquez le principe du moindre privilège. Empêchez l'octroi d'un accès public à vos données.

Résultat souhaité : vérifiez que seuls les utilisateurs autorisés peuvent accéder aux données en fonction de la nécessité de les connaître. Protégez vos données avec des sauvegardes et des versions régulières pour éviter toute modification ou suppression intentionnelle ou involontaire des données. Isolez les données critiques des autres données afin de protéger leur confidentialité et leur intégrité.

Anti-modèles courants :

- Stocker ensemble des données ayant différentes exigences en termes de sensibilité ou de classification.
- Utiliser des autorisations trop permissives sur les clés de déchiffrement.
- Classer les données de façon incorrecte.
- Ne pas conserver les sauvegardes détaillées des données importantes.
- Fournir un accès permanent aux données de production.
- Ne pas auditer l'accès aux données ni examiner régulièrement les autorisations

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : faible

Directives d'implémentation

L'utilisation de plusieurs contrôles permet de protéger vos données au repos, y compris l'accès (en utilisant le moindre privilèges), l'isolement et la gestion des versions. L'accès à vos données doit être vérifié à l'aide des mécanismes de détection, notamment AWS CloudTrail, et le journal des niveaux de service, comme les journaux d'accès Amazon Simple Storage Service (Amazon S3). Vous devez faire l'inventaire des données accessibles au public et créer un plan permettant de réduire la quantité de données disponibles publiquement au fil du temps.

Amazon S3 Glacier Vault Lock et Amazon S3 Object Lock sont des fonctionnalités qui fournissent un contrôle d'accès obligatoire pour les objets dans Amazon S3. Lorsqu'une politique de coffre est verrouillée avec l'option de conformité, même l'utilisateur root ne peut pas la modifier avant l'expiration du verrouillage.

Étapes d'implémentation

- Appliquez le contrôle d'accès : appliquez le contrôle d'accès avec le principe du moindre privilège, y compris l'accès aux clés de chiffrement.
- Séparez les données selon différents niveaux de classification : utilisez différents Comptes AWS pour les niveaux de classification des données et gérez ces comptes en utilisant AWS Organizations.
- Vérifiez les politiques AWS Key Management Service (AWS KMS) : vérifiez le niveau d'accès octroyé dans les politiques AWS KMS.
- Examinez les autorisations de compartiment et d'objet Amazon S3 : examinez régulièrement le niveau d'accès octroyé dans les politiques de compartiment S3. Une bonne pratique consiste à éviter d'utiliser des compartiments publiquement accessibles en lecture ou en écriture. Envisagez d'utiliser AWS Config pour détecter les compartiments publiquement disponibles et Amazon CloudFront pour diffuser du contenu depuis Amazon S3. Vérifiez que les compartiments qui ne doivent pas permettre l'accès public sont configurés correctement pour empêcher l'accès public. Par défaut, tous les compartiments S3 sont privés et ne sont accessibles qu'aux utilisateurs auxquels l'accès a été explicitement accordé.
- Activez l'Analyseur d'accèsAWS IAM : l'Analyseur d'accès IAM analyse les compartiments Amazon S3 et génère une découverte quand une politique S3 octroie un accès à une entité externe.
- Activez la gestion des versions Amazon S3 et le le verrouillage des objets lorsque c'est nécessaire.
- Utilisez l'inventaire Amazon S3 : l'inventaire Amazon S3 peut être utilisé pour auditer et rendre compte du statut de réplication et de chiffrement de vos objets S3.

- Passez en revue les autorisations de partage Amazon EBS et AMI : le partage des autorisations peut permettre le partage des images et des volumes avec des Comptes AWS externes à votre charge de travail.
- Vérifiez régulièrement les partages du Gestionnaire des accès aux ressources AWS afin de déterminer si des ressources doivent encore être partagées. Le Gestionnaire des accès aux ressources vous permet de partager des ressources, telles que les politiques AWS Network Firewall, les règles du résolveur Amazon Route 53 et les sous-réseaux avec vos Amazon VPC. Auditez régulièrement les ressources partagées et cessez de partager les ressources qui n'ont plus besoin de l'être.

Ressources

Bonnes pratiques associées :

- SEC03-BP01 Définir les conditions d'accès
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège

Documents connexes :

- Livre blanc Présentation des détails cryptographiques de AWS KMS
- Introduction to Managing Access Permissions to Your Amazon S3 Resources (Introduction à la gestion des autorisations d'accès à vos ressources Amazon S3)
- Overview of managing access to your AWS KMS resources (Aperçu de la gestion de l'accès à vos ressources KMS AWS)
- AWS Config Rules
- Amazon S3 + Amazon CloudFront: A Match Made in the Cloud
- Utilisation de la gestion des versions
- Utilisation du verrouillage des objets Amazon S3
- Partager un instantané Amazon EBS
- AMI partagées
- Hosting a single-page application on Amazon S3 (Hébergement d'une application à une page sur Amazon S3)

Vidéos connexes :

- Securing Your Block Storage on AWS

SEC08-BP05 Utiliser des mécanismes pour protéger l'accès aux données

Empêchez tous les utilisateurs d'accéder directement aux données et systèmes sensibles dans des circonstances opérationnelles normales. Par exemple, utilisez un flux de travail de gestion des changements pour gérer les instances Amazon Elastic Compute Cloud (Amazon EC2) avec des outils au lieu d'autoriser un accès direct ou un hôte bastion. Pour ce faire, recourez à AWS Systems Manager Automation, qui utilise des documents d'automatisation contenant les étapes nécessaires pour effectuer les tâches. Ces documents peuvent être stockés dans un système de contrôle de source, être examinés par des pairs avant l'exécution et être testés minutieusement pour minimiser les risques par rapport à un accès shell. Les utilisateurs de l'entreprise peuvent disposer d'un tableau de bord au lieu d'un accès direct à un magasin de données afin d'effectuer des requêtes. Lorsque des pipelines CI/CD ne sont pas utilisés, identifiez les contrôles et processus nécessaires pour fournir de manière adéquate un mécanisme alternatif normalement désactivé.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Faible

Directives d'implémentation

- Implémenter des mécanismes pour protéger l'accès aux données : ces mécanismes incluent l'utilisation de tableaux de bord comme Amazon QuickSight pour présenter les données aux utilisateurs au lieu d'envoyer des requêtes directement.
  - Amazon QuickSight
- Automatisez la gestion de la configuration : effectuez des actions à distance, appliquez et validez automatiquement des configurations sécurisées en utilisant un service ou un outil de gestion de configuration. Évitez d'utiliser des hôtes bastion ou d'accéder directement aux instances EC2.
  - AWS Systems Manager
  - AWS CloudFormation
  - Pipeline CI/CD pour les modèles AWS CloudFormation sur AWS

Ressources

Documents connexes :

- Livre blanc sur les informations cryptographiques AWS KMS

Vidéos connexes :

- How Encryption Works in AWS
- Securing Your Block Storage on AWS

Protection des données en transit

Données en transit sont toutes les données envoyées d'un système à un autre. Cela inclut la communication entre les ressources dans votre charge de travail, ainsi que la communication entre d'autres services et vos utilisateurs finaux. En fournissant le niveau de protection approprié pour vos données en transit, vous protégez la confidentialité et l'intégrité des données de votre charge de travail.

Sécuriser les données entre les VPC ou les emplacements sur site : Vous pouvez utiliser AWS PrivateLink pour créer une connexion réseau sécurisée et privée entre Amazon Virtual Private Cloud (Amazon VPC) ou une connectivité sur site aux services hébergés dans AWS. Vous pouvez accéder aux services AWS, aux services tiers et aux services d'autres Comptes AWS comme s'ils se trouvaient sur votre réseau privé. Avec AWS PrivateLink, vous pouvez accéder aux services sur plusieurs comptes avec des blocs CIDR d'adresses IP qui se chevauchent sans avoir besoin d'une passerelle Internet ou d'un NAT. Vous n'avez pas non plus besoin de configurer des règles de pare-feu, des définitions de chemin ou des tables de routage. Le trafic reste sur le backbone d'Amazon et ne traverse pas Internet. Vos données sont donc protégées. Vous pouvez rester conforme aux réglementations de conformité sectorielles, telles que les lois HIPAA et EU/US Privacy Shield. AWS PrivateLink fonctionne de manière transparente avec des solutions tierces pour créer un réseau mondial simplifié, vous permettant d'accélérer la migration vers le cloud et de profiter des services AWS disponibles.

Bonnes pratiques

- SEC09-BP01 Implémenter la gestion sécurisée des clés et des certificats
- SEC09-BP02 Appliquer le chiffrement en transit
- SEC09-BP03 Automatiser la détection des accès involontaires aux données
- SEC09-BP04 Authentifier les communications réseau

SEC09-BP01 Implémenter la gestion sécurisée des clés et des certificats

Les certificats du protocole TLS (Transport Layer Security) permettent de sécuriser les communications réseau et établir l'identité des sites web, des ressources et des charges de travail sur Internet, ainsi que sur les réseaux privés.

Résultat souhaité : Un système de gestion des certificats sécurisé qui peut provisionner, déployer, stocker et renouveler des certificats dans une infrastructure à clé publique (PKI). Un mécanisme sécurisé de gestion des clés et des certificats empêche la divulgation de la clé privée du certificat et renouvelle automatiquement et périodiquement le certificat. Il s'intègre également à d'autres services pour fournir des communications réseau et une identité sécurisées pour les ressources de la machine au sein de votre charge de travail. Les clés ne doivent jamais être accessibles aux identités humaines.

Anti-modèles courants :

- Exécuter des étapes manuelles au cours des processus de déploiement ou de renouvellement des certificats.
- Ne pas accorder suffisamment d'attention à la hiérarchie de l'autorité de certification (AC) lors de la conception d'une AC privée.
- Utiliser des certificats auto-signés pour les ressources publiques.

Avantages liés au respect de cette bonne pratique :

- Simplifiez la gestion des certificats en automatisant leur déploiement et leur renouvellement
- Encouragez le chiffrage des données en transit à l'aide de certificats TLS
- Amélioration de la sécurité et de l'auditabilité des actions de certification entreprises par l'autorité de certification
- Organisation des tâches de gestion à différents niveaux de la hiérarchie de l'AC

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Élevé

Directives d'implémentation

Les charges de travail modernes font un usage intensif des communications réseau chiffrées à l'aide de protocoles PKI tels que le protocole TLS. La gestion des certificats PKI peut être complexe, mais

le provisionnement, le déploiement et le renouvellement automatisés des certificats peuvent réduire les inconvénients liés à la gestion des certificats.

AWS fournit deux services pour gérer les certificats PKI à usage général : AWS Certificate Manager et AWS Private Certificate Authority (AWS Private CA). ACM est le principal service que les clients utilisent pour provisionner, gérer et déployer des certificats destinés à être utilisés dans des charges de travail AWS publiques et privées. ACM émet des certificats en utilisant AWS Private CA et intègre avec de nombreux autres services gérés AWS pour fournir des certificats TLS sécurisés pour les charges de travail.

AWS Private CA vous permet d'établir votre propre autorité de certification racine ou subordonnée et d'émettre des certificats TLS par l'intermédiaire d'une API. Vous pouvez utiliser ce type de certificats dans des scénarios où vous contrôlez et gérez la chaîne de confiance du côté client de la connexion TLS. En plus des cas d'utilisation TLS, AWS Private CA peut émettre des certificats à des pods Kubernetes, des attestations produits pour appareils Matter, une signature de code et d'autres cas d'utilisation avec un modèle personnalisé. » Vous pouvez également utiliser IAM Roles Anywhere pour fournir des informations d'identification IAM temporaires aux charges de travail sur site qui ont reçu des certificats X.509 signés par votre autorité de certification privée.

En plus de ACM et AWS Private CA, AWS IoT Core fournit un support spécialisé pour provisionner, gérer et déployer des certificats PKI sur des appareils de l'Internet des objets. AWS IoT Core fournit des mécanismes spécialisés pour l'intégration des appareils IoT dans votre infrastructure de clés publiques à grande échelle.

Considérations relatives à l'établissement d'une hiérarchie d'autorités de certification privées

Lorsque vous devez établir une autorité de certification privée, il est important de prendre soin de concevoir correctement la hiérarchie de l'autorité de certification dès le départ. La bonne pratique consiste à déployer chaque niveau de votre hiérarchie d'autorité de certification dans des Comptes AWS distincts lorsque vous créez une hiérarchie d'autorité de certification privée. Cette étape intentionnelle réduit la surface de chaque niveau de la hiérarchie de l'autorité de certification, ce qui facilite la découverte d'anomalies dans les données de journalisation CloudTrail et réduit l'étendue de l'accès ou l'impact en cas d'accès non autorisé à l'un des comptes. L'autorité de certification racine doit résider dans son propre compte et ne doit être utilisée que pour émettre un ou plusieurs certificats d'autorité de certification intermédiaire.

Créez ensuite une ou plusieurs autorités de certification intermédiaires dans des comptes distincts du compte de l'autorité de certification racine afin d'émettre des certificats pour les utilisateurs finaux, les appareils ou d'autres charges de travail. Enfin, émettez des certificats à partir de votre autorité

de certification racine vers les autorités de certification intermédiaires, qui émettront à leur tour des certificats vers vos utilisateurs finaux ou vos appareils. Pour plus d'informations sur la planification du déploiement des AC et la conception de la hiérarchie des AC, y compris la planification de la résilience, la réplication interrégionale, le partage des AC au sein de votre organisation et plus encore, voir Planification de votre déploiement AWS Private CA. »

Étapes d'implémentation

1. Déterminez les services AWS pertinents requis pour votre cas d'utilisation :
    - De nombreux cas d'utilisation peuvent s'appuyer sur l'infrastructure de clés publiques existante d'AWS à l'aide de AWS Certificate Manager. ACM peut déployer des certificats TLS pour les serveurs web, les équilibreurs de charge ou d'autres utilisations pour des certificats publiquement approuvés.
    - Envisagez AWS Private CA si vous devez établir votre propre hiérarchie d'autorité de certification privée ou si vous avez besoin d'accéder à des certificats exportables. ACM peut ensuite émettre de nombreux types de certificats d'entités finales à l'aide de AWS Private CA.
    - Pour les cas d'utilisation où les certificats doivent être provisionnés à grande échelle pour les appareils de l'Internet des objets (IoT) embarqués, envisagez AWS IoT Core. »
2. Mettez en œuvre le renouvellement automatisé des certificats dans la mesure du possible :
    - Utilisez le renouvellement géré de ACM pour les certificats émis par ACM, ainsi que les services intégrés gérés par AWS.
3. Établissez des journaux et des pistes d'audit :
    - Activez les journaux CloudTrail pour suivre l'accès aux comptes détenant des autorités de certification. Envisagez de configurer la validation de l'intégrité des fichiers journaux dans CloudTrail pour vérifier l'authenticité des données du journal.
    - Générez et révisez périodiquement des rapports d'audit répertoriant les certificats émis ou révoqués par votre autorité de certification privée. Ces rapports peuvent être exportés vers un compartiment S3.
    - Lors du déploiement d'une autorité de certification privée, vous devrez également créer un compartiment S3 pour stocker la liste de révocation des certificats (CRL). Pour obtenir des conseils sur la configuration de ce compartiment S3 en fonction des exigences de votre charge de travail, voir Planification d’une liste de révocation de certifications (CRL). »

Ressources

Bonnes pratiques associées :

- SEC02-BP02 Utiliser des informations d'identification temporaires
- SEC08-BP01 Mise en œuvre de la gestion sécurisée des clés
- SEC09-BP04 Authentifier les communications réseau

Documents connexes :

- Comment héberger et gérer une infrastructure complète de certificats privés dans AWS
- Comment garantir une hiérarchie d'autorités de certification privées ACM à l'échelle de l'entreprise pour l'automobile et la fabrication
- Private CA best practices
- Comment utiliser AWS RAM pour partager votre compte croisé Private CA ACM

Vidéos connexes :

- Activer Private CA AWS Certificate Manager (atelier)

Exemples connexes :

- Atelier sur Private CA
- Atelier sur IOT Device Management (y compris l'allocation des appareils)

Outils associés :

- Plugin pour Kubernetes cert-manager à utiliser AWS Private CA

SEC09-BP02 Appliquer le chiffrement en transit

Appliquez vos exigences de chiffrement définies en fonction des politiques, des obligations réglementaires et des normes de votre entreprise afin de répondre aux exigences organisationnelles, juridiques et de conformité. Utilisez uniquement les protocoles avec chiffrement lors de la transmission de données sensibles en dehors de votre cloud privé virtuel (VPC). Le chiffrement

permet de préserver la confidentialité des données, même lorsque celles-ci transitent par des réseaux non fiables.

Résultat souhaité : toutes les données doivent être chiffrées en transit à l'aide de protocoles TLS sécurisés et de suites de chiffrement. Le trafic réseau entre vos ressources et Internet doit être chiffré pour limiter l'accès non autorisé aux données. Le trafic réseau uniquement au sein de votre environnement AWS doit être chiffré à l'aide de TLS dès que possible. Le réseau interne AWS est chiffré par défaut et le trafic réseau au sein d'un VPC ne peut pas être falsifié ni reniflé à moins qu'une partie non autorisée n'ait accès à quelque ressource que ce soit qui génère du trafic (comme les instances Amazon EC2 et les conteneurs Amazon ECS). Envisagez de protéger le trafic réseau à réseau avec un réseau privé virtuel (VPN) IPsec.

Anti-modèles courants :

- Utiliser des versions obsolètes de composants SSL, TLS et de suite de chiffrement (par exemple, SSL v3.0, clés RSA 1024 bits et chiffrement RC4).
- Autoriser le trafic non chiffré (HTTP) vers ou depuis des ressources publiques.
- Ne pas surveiller et ne pas remplacer les certificats X.509 avant leur expiration.
- Utiliser des certificats X.509 auto-signés pour TLS.

Niveau de risque exposé si cette bonne pratique n'est pas instaurée : élevé

Directives d'implémentation

Les services AWS fournissent des points de terminaison HTTPS utilisant TLS pour la communication, ce qui assure le chiffrement en transit lors de la communication avec les API AWS. Les protocoles non sécurisés comme HTTP peuvent être contrôlés et bloqués dans un VPC à l'aide de groupes de sécurité. Les requêtes HTTP peuvent également être redirigées automatiquement vers HTTPS dans Amazon CloudFront ou sur un Application Load Balancer. Vous disposez d'un contrôle total sur vos ressources de calcul pour mettre en œuvre le chiffrement en transit dans l'ensemble de vos services. De plus, vous pouvez utiliser la connectivité VPN dans votre VPC à partir d'un réseau externe ou d'AWS Direct Connect pour faciliter le chiffrement du trafic. Vérifiez que vos clients effectuent des appels vers des API AWS en utilisant au moins TLS 1.2, car AWS cessera d'utiliser TLS 1.0 et 1.1 en juin 2023. Des solutions tierces sont disponibles sur AWS Marketplace si vous avez des exigences particulières.

Étapes d'implémentation

- Appliquez le chiffrement en transit : vos exigences en matière de chiffrement doivent être définies selon les dernières normes et bonnes pratiques en matière de sécurité, et doivent autoriser uniquement des protocoles sécurisés. Par exemple, configurez un groupe de sécurité afin d'autoriser uniquement le protocole HTTPS pour un Application Load Balancer ou une instance Amazon EC2.
- Configurez des protocoles sécurisés dans les services périphériques : configurez HTTPS avec Amazon CloudFront et utilisez un profil de sécurité approprié pour votre situation de sécurité et votre cas d'utilisation.
- Utilisez un VPN pour la connectivité externe : envisagez d'utiliser un VPN IPsec pour sécuriser les connexions point à point ou réseau à réseau afin d'assurer à la fois la confidentialité et l'intégrité des données.
- Configurez les protocoles de sécurité dans les équilibreurs de charge : sélectionnez une politique de sécurité qui fournit les suites de chiffrement les plus solides prises en charge par les clients qui se connecteront à l'écouteur. Créez un écouteur HTTPS pour votre Application Load Balancer.
- Configurez des protocoles sécurisés dans Amazon Redshift : configurez votre cluster de façon à exiger une connexion SSL ou TLS.
- Configurez des protocoles de sécurité : consultez la documentation des services AWS afin de déterminer les capacités de chiffrement en transit.
- Configurez un accès sécurisé lors du téléchargement vers les compartiments Amazon S3 : utilisez les contrôles des politiques de compartiments Amazon S3 pour appliquer un accès sécurisé aux données.
- Envisagez d'utiliser AWS Certificate Manager : ACM vous permet de mettre en service, de gérer et de déployer des certificats TLS publics en vue de leur utilisation avec des services AWS.
- Envisagez d'utiliser AWS Private Certificate Authority pour les besoins PKI privés : AWS Private CA vous permet de créer des hiérarchies d'autorités de certification privées afin d'émettre des certificats X.509 d'entité finale qui peuvent être utilisés afin de créer des canaux TLS chiffrés.

Ressources

Documents connexes :

- Documentation sur AWS
- Utilisation du protocole HTTP avec CloudFront
- Connexion de votre VPC à des réseaux distants utilisant AWS Virtual Private Network

- Create an HTTPS listener for your Application Load Balancer (Créer un écouteur HTTPS pour votre Application Load Balancer)
- Didacticiel : Configurer SSL/TLS sur Amazon Linux 2
- Using SSL/TLS to encrypt a connection to a DB instance (Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données)
- Configuration des options de sécurité des connexions

SEC09-BP03 Automatiser la détection des accès involontaires aux données

Utilisez des outils comme Amazon GuardDuty pour détecter automatiquement les activités suspectes ou les tentatives de déplacement de données en dehors des limites définies. Par exemple, GuardDuty peut détecter une activité de lecture Amazon Simple Storage Service (Amazon S3) inhabituelle avec le résultat Exfiltration:S3/AnomalousBehavior. Outre GuardDuty, les journaux de flux Amazon VPC, qui capture des informations sur le trafic réseau, peuvent être utilisés avec Amazon EventBridge pour déclencher la détection des connexions anormales, qu'elles aboutissent ou non. Amazon S3 Access Analyzer peut vous aider à déterminer les données accessibles aux utilisateurs de vos compartiments Amazon S3.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyenne entreprise

Directives d'implémentation

- Automatiser la détection de l'accès involontaire aux données : utilisez un outil ou un mécanisme de détection pour identifier automatiquement les tentatives de déplacement des données en dehors des limites définies, par exemple, pour détecter un système de base de données qui copie des données vers un hôte non reconnu.
  - Journaux de flux VPC
- Envisager Amazon Macie : Amazon Macie est un service de sécurité et de confidentialité des données entièrement géré qui utilise le machine learning et la comparaison de modèles pour découvrir et protéger vos données sensibles dans AWS.
  - Amazon Macie

Ressources

Documents connexes :

- Journaux de flux VPC
- Amazon Macie

SEC09-BP04 Authentifier les communications réseau

Vérifiez l'identité des communications à l'aide de protocoles comme TLS (Transport Layer Security) ou IPsec qui prennent en charge l'authentification.

Concevez votre charge de travail de manière à utiliser des protocoles réseau sécurisés et authentifiés lors de la communication entre les services, les applications ou avec les utilisateurs. L'utilisation de protocoles réseau qui prennent en charge l'authentification et l'autorisation permet de mieux contrôler les flux du réseau et de réduire l'impact des accès non autorisés.

Résultat souhaité : une charge de travail avec des flux de trafic bien définis entre les services au niveau du plan de données et du plan de contrôle. Les flux de trafic utilisent des protocoles réseau authentifiés et chiffrés lorsque cela est techniquement possible.

Anti-modèles courants :

- Flux de trafic non chiffrés ou non authentifiés au sein de votre charge de travail.
- Réutilisation des informations d'authentification par plusieurs utilisateurs ou entités.
- S'appuyer uniquement sur les contrôles réseau pour contrôler les accès.
- Créer un mécanisme d'authentification personnalisé au lieu d'utiliser des mécanismes d'authentification standard.
- Flux de trafic trop permissifs entre les composants des services ou d'autres ressources dans le VPC.

Avantages liés à l'instauration de cette bonne pratique :

- Limite l'impact des accès non autorisés à une partie de la charge de travail.
- Offre la garantie que les actions ne sont effectuées que par des entités authentifiées.
- Améliore le découplage des services en définissant clairement et en appliquant les interfaces de transfert de données prévues.
- Améliore la surveillance, la journalisation et la réponse aux incidents grâce à l'attribution des demandes et à des interfaces de communication bien définies.

- Assure une défense approfondie de vos charges de travail en combinant des contrôles réseau avec des contrôles d'authentification et d'autorisation.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : faible

Directives d'implémentation

Les modèles de trafic réseau de votre charge de travail peuvent être classés en deux catégories :

- Le trafic est-ouest représente le trafic entre les services qui constituent une charge de travail.
- Le trafic nord-sud représente le trafic entre votre charge de travail et les consommateurs.

Le chiffrement du trafic nord-sud est courant, mais la sécurisation du trafic est-ouest à l'aide de protocoles authentifiés l'est moins. Les pratiques modernes de sécurité recommandent que la conception du réseau ne permette pas à elle seule d'établir une relation de confiance entre deux entités. Lorsque deux services peuvent résider dans les limites d'un réseau commun, il est toujours recommandé de chiffrer, d'authentifier et d'autoriser les communications entre ces services.

Par exemple, les API des services AWS utilisent le protocole de signature des demandes d'API AWS Version 4 (SigV4) pour authentifier l'appelant, quel que soit le réseau d'origine de la demande. Cette authentification garantit que les API AWS peuvent vérifier l'identité de la personne qui a demandé l'action, et cette identité peut ensuite être combinée avec des stratégies pour décider si l'action doit être autorisée ou non.

Des services comme Amazon VPC Lattice et Amazon API Gateway vous permettent d'utiliser le même protocole de signature SigV4 pour ajouter une authentification et une autorisation au trafic est-ouest dans vos propres charges de travail. Si des ressources extérieures à votre environnement AWS ont besoin de communiquer avec des services qui nécessitent une authentification et une autorisation basées sur SigV4, vous pouvez utiliser AWS Identity and Access Management (IAM) Roles Anywhere sur la ressource non AWS pour obtenir des informations d'identification AWS temporaires. Ces informations d'identification peuvent être utilisées pour signer les demandes de services utilisant SigV4 pour autoriser l'accès.

L'authentification mutuelle TLS (mTLS) est un autre mécanisme courant pour authentifier le trafic est-ouest. De nombreuses applications IoT (Internet des objets) et B2B, ainsi que des microservices utilisent mTLS pour valider l'identité des deux côtés d'une communication TLS à l'aide de certificats X.509 côté client et côté serveur. Ces certificats peuvent être émis par AWS Private Certificate Authority (AWS Private CA). Vous pouvez utiliser des services comme Amazon API

Gateway et AWS App Mesh pour fournir une authentification mTLS pour les communications entre les charges de travail ou à l'intérieur de celles-ci. mTLS fournit des informations d'authentification pour les deux côtés d'une communication TLS, mais elle ne fournit pas de mécanisme d'autorisation.

Enfin, OAuth 2.0 et OpenID Connect (OIDC) sont deux protocoles généralement utilisés pour contrôler l'accès aux services par les utilisateurs, mais ils sont également de plus en plus populaires pour le trafic de service à service. API Gateway fournit un mécanisme d'autorisation JSON Web Token (JWT), permettant aux charges de travail de restreindre l'accès aux routes API à l'aide de JWT émis par les fournisseurs d'identité OIDC et OAuth 2.0. Les champs d'application OAuth2 peuvent être utilisés comme source pour les décisions d'autorisation de base, mais les contrôles d'autorisation doivent encore être mis en œuvre dans la couche applicative, et les champs d'application OAuth2 ne peuvent pas à eux seuls répondre à des besoins d'autorisation plus complexes.

Étapes d'implémentation

- Définir et documenter les flux de réseau de votre charge de travail : la première étape de la mise en œuvre d'une stratégie de défense en profondeur consiste à définir les flux de trafic de votre charge de travail.
  - Créez un diagramme de flux de données qui définit clairement la transmission des données entre les différents services qui constituent votre charge de travail. Ce schéma constitue la première étape de l'application de ces flux par le biais de réseaux authentifiés.
  - Instrumentez votre charge de travail lors des phases de développement et de test pour vérifier que le diagramme de flux de données reflète avec précision le comportement de la charge de travail lors de l'exécution.
  - Un diagramme de flux de données peut également être utile lors d'un exercice de modélisation des menaces, comme décrit dans SEC01-BP07 Identifier les menaces et hiérarchiser les atténuations à l'aide d'un modèle de menaces.
- Mettre en place des contrôles de réseau : tenez compte de capacités d'AWS pour mettre en place des contrôles réseau alignés sur vos flux de données. Les limites du réseau ne doivent pas représenter le seul contrôle de sécurité, mais elles constituent une couche de la stratégie de défense en profondeur visant à protéger votre charge de travail.
  - Utilisez des groupes de sécurité pour établir, définir et restreindre les flux de données entre les ressources.
  - Envisagez d'utiliser AWS PrivateLink pour communiquer avec les services d'assistance AWS et tiers qui prennent en charge AWS PrivateLink. Les données envoyées via un point de terminaison d'interface AWS PrivateLink restent dans le réseau AWS et ne transitent pas par l'Internet public.

- Mettre en œuvre un système d'authentification et d'autorisation pour tous les services de votre charge de travail : choisissez l'ensemble de services AWS le plus approprié pour authentifier et chiffrer les flux de trafic de votre charge de travail.
  - Envisagez d'utiliser Amazon VPC Lattice pour sécuriser les communications de service à service. VPC Lattice peut utiliser l'authentification SigV4 et des stratégies d'authentification pour contrôler les accès de service à service.
  - Pour la communication de service à service à l'aide de mTLS, envisagez d'utiliser API Gateway ou App Mesh. AWS Private CA peut être utilisé pour établir une hiérarchie des autorités de certification privées capables d'émettre des certificats à utiliser avec mTLS.
  - Pour l'intégration à des services utilisant OAuth 2.0 ou OIDC, envisagez d'utiliser API Gateway avec les mécanismes d'autorisation JWT.
  - Pour les communications entre votre charge de travail et des appareils IoT, AWS IoT Core propose plusieurs options de chiffrement et d'authentification du trafic réseau.
- Surveiller les accès non autorisés : surveillez en permanence les canaux de communication involontaires, les personnes non autorisées qui tentent d'accéder à des ressources protégées et autres schémas d'accès inappropriés.
  - Si vous utilisez VPC Lattice pour gérer l'accès à vos services, envisagez d'activer et de surveiller les journaux d'accès VPC Lattice. Ces journaux contiennent des informations sur le demandeur et le réseau, notamment le VPC source et de destination, et les métadonnées des demandes.
  - Envisagez d'activer les journaux de flux VPC pour capturer des métadonnées sur les flux du réseau et passer régulièrement en revue les anomalies.
  - Consultez le guide de réponse aux incidents de sécurité AWS et la section Réponse aux incidents du livre blanc Pilier de sécurité - AWS Well-Architected Framework pour plus de conseils sur la planification et la simulation des incidents de sécurité, ainsi que la réponse qui y est apportée.

Ressources

Bonnes pratiques associées :

- SEC03-BP07 Analyser l'accès public et entre les comptes
- SEC02-BP02 Utiliser des informations d'identification temporaires
- SEC01-BP07 Identifier les menaces et hiérarchiser les atténuations à l'aide d'un modèle de menaces

Documents connexes :

- Evaluating access control methods to secure Amazon API Gateway APIs
- Configuration de l'authentification TLS mutuelle pour une API REST
- How to secure API Gateway HTTP endpoints with JWT authorizer
- Authorizing direct calls to AWS services using AWS IoT Core credential provider
- AWS Security Incident Response Guide

Vidéos connexes :

- AWS re:invent 2022: Introducing VPC Lattice
- AWS re:invent 2020: Serverless API authentication for HTTP APIs on AWS

Exemples connexes :

- Amazon VPC Lattice Workshop
- Zero-Trust Episode 1 – The Phantom Service Perimeter workshop

Réponse aux incidents

Même avec des contrôles préventifs et de détection matures, votre organisation doit mettre en place des mécanismes pour répondre aux incidents de sécurité et en atténuer l'impact potentiel. Votre préparation affectera fortement la capacité de vos équipes à opérer efficacement lors d'un incident, à analyser, isoler et contenir les problèmes, et à rétablir les opérations à un état de fonctionnement correct. La mise en place des outils et des accès avant un incident de sécurité, puis la pratique régulière de la réponse aux incidents pendant des exercices de simulation, vous permettent de rétablir les opérations tout en minimisant les interruptions d'activité.

Rubriques

Aspects de la réponse aux incidents AWS

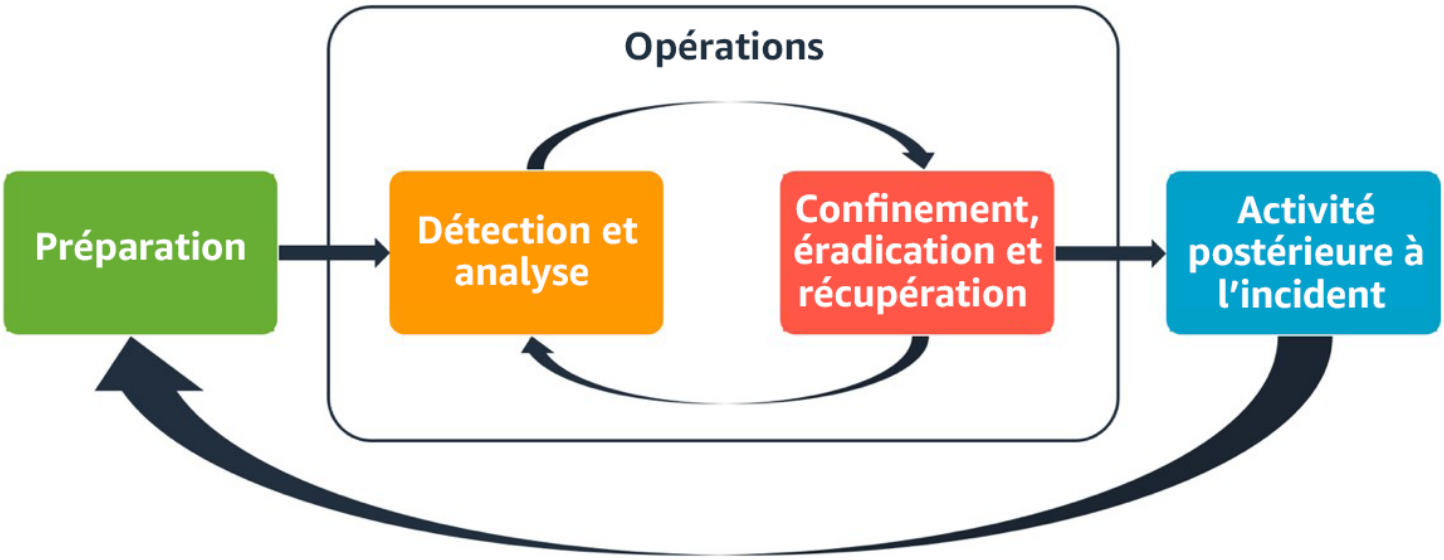
Tous les utilisateurs AWS d'une organisation doivent avoir une connaissance de base des processus de réponse aux incidents de sécurité. Le personnel de sécurité doit, quant à lui, savoir comment répondre aux problèmes de sécurité. L'éducation, la formation et l'expérience sont essentielles à la réussite d'un programme de réponse aux incidents dans le cloud et sont idéalement mises en œuvre bien avant de devoir gérer un éventuel incident de sécurité. La réussite d'un programme de réponse aux incidents dans le cloud repose sur plusieurs aspects : Préparation, Opérationset Activité postérieure à l'incident.

Pour comprendre chacun de ces aspects, tenez compte des descriptions suivantes :

- Préparation : préparez votre équipe de réponse aux incidents à détecter les incidents et à y répondre dans AWS en activant des contrôles de détection et en vérifiant l'accès approprié aux outils et services cloud nécessaires. De plus, préparez les playbooks nécessaires (manuels et automatisés) pour garantir des réponses fiables et cohérentes.
- Opérations : gérez les événements de sécurité et les incidents potentiels en suivant les phases de réponse aux incidents du NIST : détecter, analyser, contenir, éradiquer et récupérer.

- Activité postérieure à l'incident : réitérez les résultats de vos événements de sécurité et de vos simulations pour améliorer l'efficacité de la réponse, accroître la valeur dérivée de la réponse et de l'enquête, et réduire davantage les risques. Vous devez tirer les leçons des incidents et vous impliquer pleinement dans les activités d'amélioration.

Le schéma suivant présente le déroulement de ces différents aspects, en s'alignant sur le cycle de vie de réponse aux incidents du NIST mentionné précédemment, mais avec des opérations comprenant la détection et l'analyse avec la maîtrise, l'éradication et la récupération.



Aspects de la réponse aux incidents AWS

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 Guiderestent valables, nous vous encourageons à évaluer 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, les conseillers juridiques et les responsables de votre organisation pour déterminer l'objectif de la réponse à un incident. Parmi les objectifs communs, citons la maîtrise et l'atténuation du problème, le rétablissement des ressources affectées, la préservation des données à des fins d'investigation, le retour à un fonctionnement sûr et connu, puis les leçons à tirer des incidents.
- Répondre à l'aide du cloud : mettez en œuvre des modèles de réponse dans le cloud, là où se trouvent l'événement et les données.

- Savoir ce dont vous disposez et ce dont vous avez besoin : préservez les journaux, les ressources, les instantanés et les autres preuves en les copiant et en les stockant dans un compte cloud centralisé dédié à la réponse. Utilisez des balises, des métadonnées et des mécanismes qui appliquent des stratégies de conservation. Vous devrez comprendre quels services vous utilisez, puis identifier les exigences relatives à l'investigation de ces services. Pour mieux comprendre votre environnement, vous pouvez également utiliser le balisage.
- Utiliser les 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. Si une faille possible est identifiée, vérifiez que votre redéploiement inclut des mesures d'atténuation fructueuses et validées des causes profondes.
- Automatiser autant que possible : lorsque des problèmes surviennent ou que les incidents se répètent, mettez en place des mécanismes pour trier les événements courants et y répondre de manière programmatique. La réponse à des incidents uniques, complexes ou sensibles pour lesquels les automatisations sont insuffisantes doit être gérée par les équipes compétentes.
- Choisir des solutions évolutives : essayez d'ajuster la capacité de mise à l'échelle de votre organisation en matière de cloud computing. Mettez en œuvre des mécanismes de détection et de réponse qui s'adaptent à l'ensemble de vos environnements afin de réduire efficacement le délai entre la détection et la réponse.
- Apprendre et améliorer votre processus : soyez proactif en identifiant les lacunes dans vos processus, vos outils ou votre personnel, et mettez en œuvre une stratégie pour y remédier. Les simulations sont des méthodes sûres permettant d'identifier les lacunes et d'améliorer les processus.

Ces objectifs de conception vous rappellent que vous devez examiner la mise en œuvre de votre architecture afin de déterminer si elle est capable de répondre aux incidents et de détecter les menaces. Lorsque vous planifiez vos mises en œuvre dans le cloud, pensez à la réponse aux incidents, idéalement avec une méthodologie de réponse rigoureuse. Dans certains cas, cela signifie que vous pouvez avoir plusieurs organisations, comptes et outils spécifiquement configurés pour ces tâches de réponse. Ces outils et fonctions doivent être mis à la disposition du gestionnaire de l'incident par le biais d'un pipeline de déploiement. Ils ne doivent pas être statiques, car cela peut entraîner un risque plus important.

Préparation

Pour une réponse rapide et efficace aux incidents, la préparation est essentielle. La préparation couvre trois domaines :

- Les collaborateurs : pour préparer votre personnel à un incident de sécurité, vous devez identifier les parties prenantes et les former à la réponse aux incidents et aux technologies cloud.
- Les processus : la préparation de vos processus en cas d'incident de sécurité implique de documenter les architectures, d'élaborer des stratégies de réponse complètes aux incidents et de créer des guides pour un gestion cohérente des événements de sécurité.
- La technologie : pour préparer votre technologie à un incident de sécurité, vous devez configurer l'accès, agréger et surveiller les journaux nécessaires, mettre en œuvre des mécanismes d'alerte efficaces et développer des fonctionnalités de réponse et d'investigation.

Chacun de ces domaines joue un rôle tout aussi important pour une réponse efficace aux incidents. Aucun programme de réponse aux incidents n'est complet ou efficace sans ces trois aspects. Au cours de la préparation, vous devez intégrer étroitement le personnel, les processus et la technologie afin de pouvoir faire face aux incidents.

Bonnes pratiques

- SEC10-BP01 Identifier les postes clés internes ainsi que les principales ressources externes
- SEC10-BP02 Développer des plans de gestion des incidents
- SEC10-BP03 Préparer les fonctionnalités d'analyse poussée
- SEC10-BP04 Développer et tester des playbooks de réponse aux incidents de sécurité
- SEC10-BP05 Préallouer les accès
- SEC10-BP06 Prédéployer les outils
- SEC10-BP07 Exécuter des simulations

SEC10-BP01 Identifier les postes clés internes ainsi que les principales ressources externes

Identifiez les postes clés internes et externes, les ressources et les obligations légales qui aideront votre organisation à réagir en cas d'incident.

Lorsque vous définissez votre approche de la réponse aux incidents dans le cloud, à l'unisson avec d'autres équipes (telles que votre conseiller juridique, vos dirigeants, les parties prenantes de l'entreprise, les services AWS Support, etc.), vous devez identifier le personnel clé, les parties prenantes et les contacts pertinents. Pour réduire la dépendance et le temps de réponse, veillez à ce que votre équipe, les équipes de sécurité spécialisées et les intervenants soient formés aux services que vous utilisez et aient la possibilité d'effectuer des exercices pratiques.

Nous vous encourageons à identifier des partenaires de sécurité AWS externes qui peuvent vous fournir une expertise extérieure et une perspective différente pour augmenter 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.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Élevé

Directives d'implémentation

- Identifier les postes clés de votre organisation : Tenez à jour une liste des employés au sein de votre organisation que vous devez impliquer pour réagir et récupérer après un incident.
- Identifier les partenaires externes : Collaborez le cas échéant avec des partenaires externes qui pourront vous aider à réagir et à reprendre après un incident.

Ressources

Documents connexes :

- Guide de réponse aux incidents AWS

Vidéos connexes :

- Prepare for and respond to security incidents in your AWS environment

Exemples connexes :

SEC10-BP02 Développer des plans de gestion des incidents

Le premier document à élaborer pour la réponse aux incidents est le plan de réponse aux incidents. Le plan de réponse aux incidents est conçu pour servir de base à votre programme et à votre stratégie de réponse aux incidents.

Avantages liés au respect de cette bonne pratique : Le développement de processus de réponse aux incidents complets et clairement définis est essentiel à la réussite d'un programme de réponse aux incidents évolutif. Lorsqu'un incident de sécurité se produit, des étapes et des flux de travail clairs peuvent vous aider à réagir rapidement. Vous disposez peut-être déjà de processus de réponse aux incidents. Quel que soit votre état actuel, il est important de mettre à jour, d'itérer et de tester régulièrement vos processus de réponse aux incidents.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Élevé

Directives d'implémentation

Un plan de gestion des incidents est essentiel pour réagir, atténuer et se remettre des répercussions potentielles des incidents de sécurité. Un plan de gestion des incidents est un processus structuré qui permet d'identifier les incidents de sécurité, d'y remédier et d'y répondre rapidement.

Le cloud comporte un grand nombre de rôles et exigences opérationnels identiques à ceux d'un environnement sur site. Lorsque vous créez un plan de gestion des incidents, il est important de tenir compte des stratégies d'intervention et de récupération qui correspondent le mieux aux résultats opérationnels et aux exigences de conformité. Par exemple, si vous exécutez des charges de travail dans AWS qui sont conformes à FedRAMP aux États-Unis, il est utile de respecter NIST SP 800-61 Computer Security Handling Guide. De la même manière, lorsque vous exécutez des charges de travail avec des données européennes personnellement identifiables, envisagez des scénarios tels que la façon dont vous pourriez protéger les données et résoudre des problèmes liés à la résidence des données, comme l'exige le Règlement Général sur la Protection des Données (RGPD). »

Lorsque vous élaborez un plan de gestion des incidents pour vos charges de travail dans AWS, commencez par le Modèle de responsabilité partagée AWS, afin de créer une approche de défense en profondeur en matière de réponse aux incidents. Dans le cadre de ce modèle, AWS gère la sécurité du cloud et vous êtes responsable de la sécurité dans le cloud. Cela signifie que vous conservez le contrôle et que vous êtes responsable des contrôles de sécurité que vous choisissez d'implémenter. L' AWS Security Incident Response Guide détaille les concepts clés et les conseils de base pour l'élaboration d'un plan de gestion des incidents axé sur le cloud.

Un plan de gestion des incidents efficace doit être répété constamment, tout en poursuivant votre objectif d'opérations dans le cloud. Envisagez d'utiliser les plans d'implémentation décrits ci-dessous pour créer et faire évoluer votre plan de gestion des incidents.

Étapes d'implémentation

Définissez les rôles et les responsabilités

La gestion des événements de sécurité exige une discipline interorganisationnelle et une volonté d'action. Au sein de votre structure organisationnelle, de nombreuses personnes doivent être responsables, tenues de rendre des comptes, consultées ou tenues informées lors d'un incident. Il peut notamment s'agir de représentants des ressources humaines (RH), de l'équipe de direction et du service juridique. Tenez compte de ces rôles et responsabilités et déterminez si des tiers doivent être impliqués. Notez que de nombreuses zones géographiques ont des lois locales qui régissent ce

qui doit et ne doit pas être fait. Bien qu'il puisse sembler bureaucratique de créer un tableau RACI (réalisateur, approbateur, consulté et informé) pour vos plans de réponse en matière de sécurité, cela facilite une communication rapide et directe et définit clairement le leadership à chaque étape de l'événement.

Lors d'un incident, il est essentiel d'inclure les propriétaires et les développeurs des applications et des ressources concernées, car ce sont des experts en la matière (SME) qui peuvent fournir des informations et un contexte afin d'aider à mesurer l'impact. Assurez-vous d'établir et de maintenir des relations avec les développeurs et les propriétaires d'applications avant de vous fier à leur expertise pour répondre aux incidents. Les propriétaires d'applications ou SME, tels que vos administrateurs ou ingénieurs cloud, peuvent avoir besoin d'agir dans des situations où l'environnement est inconnu ou complexe, ou lorsque les intervenants n'y ont pas accès.

Enfin, des partenaires de confiance peuvent être impliqués dans l'enquête ou la réponse car ils peuvent apporter une expertise supplémentaire et un examen minutieux. Si vous ne possédez pas ces compétences au sein de votre propre équipe, vous pouvez faire appel à un tiers pour obtenir de l'aide.

Comprenez les équipes d'intervention et le support AWS

- AWS Support
  - AWS Support propose une gamme de plans qui donnent accès à des outils et à une expertise qui contribuent à la réussite et à l'intégrité opérationnelle de vos solutions AWS. Si vous avez besoin d'un support technique et de ressources supplémentaires pour planifier, déployer et optimiser votre environnement AWS, vous pouvez sélectionner le plan de support le plus adapté à votre cas d'utilisation AWS.
  - Envisagez le Centre de support dans AWS Management Console (connexion requise) en tant que point de contact central pour obtenir de l'aide en cas de problèmes affectant vos ressources AWS. L'accès à AWS Support est contrôlé par AWS Identity and Access Management. Pour plus d'informations sur l'accès aux fonctionnalités AWS Support, consultez Mise en route avec AWS Support.
- Équipe de réponse aux incidents clients (CIRT) AWS
  - L'équipe de réponse aux incidents clients (CIRT) AWS est une équipe AWS internationale spécialisée et disponible 24 heures sur 24, 7 jours sur 7, qui fournit une assistance aux clients lors d'événements de sécurité actifs côté client du Modèle de responsabilité partagée AWS.
  - Lorsque la CIRT AWS vous accompagne, elle fournit une assistance en matière de triage et de récupération en cas d'événement de sécurité actif sur AWS. Elle peut vous aider à analyser les

causes profondes à l'aide des journaux de service AWS et vous fournir des recommandations pour la récupération. Elle peut également fournir des recommandations de sécurité et des bonnes pratiques pour vous aider à éviter des incidents de sécurité à l'avenir.
    - Les clients AWS peuvent contacter la CIRT AWS par le biais d'un cas AWS Support.
- Support de réponse aux attaques DDoS
    - Offres AWS AWS Shield, qui fournit un service géré de protection contre le déni de service distribué (DDoS) protégeant les applications Web exécutées sur AWS. Shield fournit une détection permanente et des mesures d'atténuation automatiques en ligne capables de minimiser les temps d'arrêt et la latence des applications, de sorte qu'il n'est pas nécessaire d'engager AWS Support pour bénéficier de la protection DDoS. Il existe deux niveaux de Shield : AWS Shield Standard et AWS Shield Advanced. Pour en savoir plus sur les différences entre ces deux niveaux, consultez la documentation sur les fonctionnalités Shield.
- AWS Managed Services (AMS)
    - AWS Managed Services (AMS) fournit une gestion continue de votre infrastructure AWS afin que vous puissiez vous concentrer sur vos applications. En mettant en œuvre les meilleures pratiques pour gérer votre infrastructure, AMS permet de réduire vos frais généraux et vos risques opérationnels. 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 de cycle de vie complets pour provisionner, exécuter et prendre en charge votre infrastructure.
    - AMS prend la responsabilité de déployer une suite de contrôles de sécurité et fournit une réponse de première ligne 24 heures sur 24, 7 jours sur 7 aux alertes. Lorsqu'une alerte est déclenchée, AMS suit un ensemble standard de playbooks automatisés et manuels pour vérifier une réponse cohérente. Ces playbooks sont partagés avec les clients AMS lors de l'intégration afin qu'ils puissent développer et coordonner une réponse avec AMS.

Élaborez le plan de réponse aux incidents

Le plan de réponse aux incidents est conçu pour servir de base à votre programme et à votre stratégie de réponse aux incidents. Le plan de réponse aux incidents doit figurer dans un document formel. Un plan de réponse aux incidents comprend généralement les sections suivantes :

- Présentation de l'équipe de réponse aux incidents : décrit les objectifs et les fonctions de l'équipe de réponse aux incidents.
- Rôles et responsabilités : répertorie les parties prenantes de la réponse aux incidents et détaille leurs rôles en cas d'incident.

- Un plan de communication : détaille les coordonnées et la manière dont vous communiquez lors d'un incident.
- Méthodes de communication de secours : il est recommandé d'utiliser une communication hors bande comme solution de secours pour les communications en cas d'incident. Un exemple d'application qui fournit un canal de communication hors bande sécurisé est AWS Wickr.
- Phases de la réponse aux incidents et mesures à prendre : énumère les phases de la réponse aux incidents (par exemple, détection, analyse, éradication, maîtrise et récupération), y compris les mesures de haut niveau à prendre au cours de ces phases.
- Définitions de la gravité et de la hiérarchisation des incidents : décrit en détail comment classer la gravité d'un incident, comment hiérarchiser l'incident, puis comment les définitions de gravité affectent les procédures de remontée.

Bien que ces sections soient communes à des entreprises de tailles et de secteurs différents, le plan de réponse aux incidents de chaque organisation est unique. Vous devez élaborer un plan de réponse aux incidents qui convient le mieux à votre organisation.

Ressources

Bonnes pratiques connexes :

- SEC04 (Comment détecter et enquêter sur les événements de sécurité ?)

Documents connexes :

- AWS Security Incident Response Guide
- NIST: Computer Security Incident Handling Guide

SEC10-BP03 Préparer les fonctionnalités d'analyse poussée

Pour anticiper un incident de sécurité, envisagez de développer des fonctionnalités d'analyse poussée pour faciliter les enquêtes sur les événements de sécurité.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyen

Les concepts issus de l'analyse poussée traditionnelle sur site s'appliquent à AWS. Pour obtenir des informations clés sur la manière de commencer à renforcer les capacités d'analyse poussée dans

le AWS Cloud, consultez Stratégies d'environnement d'enquête pour les analyses poussées dans le AWS Cloud (langue française non garantie). »

Une fois que vous avez configuré la structure de votre environnement et de votre compte Compte AWS en vue de l'analyse poussée, définissez les technologies requises pour appliquer efficacement les méthodologies d'analyse poussée en quatre phases :

- Collecte : Collectez des journaux AWS pertinents, tels que AWS CloudTrail, AWS Config, les journaux de flux VPC et les journaux au niveau de l'hôte. Collectez des instantanés, des sauvegardes et des fichiers de vidage de mémoire des ressources AWS concernées, le cas échéant.
- Examen : Examinez les données collectées en extrayant et en évaluant les informations pertinentes.
- Analyse : Analysez les données collectées afin de comprendre l'incident et d'en tirer des conclusions.
- Reporting : Présentez les informations issues de la phase d'analyse.

Étapes d'implémentation

Préparation de votre environnement d'analyse poussée

AWS Organizations vous permet de gérer et de gouverner de manière centralisée un environnement AWS à mesure que vous vous développez et que vous mettez à l'échelle vos ressources AWS. Une organisation AWS consolide vos Comptes AWS pour que vous puissiez les administrer en tant qu'unité unique. Vous pouvez utiliser des unités d'organisation (UO) pour regrouper des comptes afin de les administrer en tant qu'unité unique.

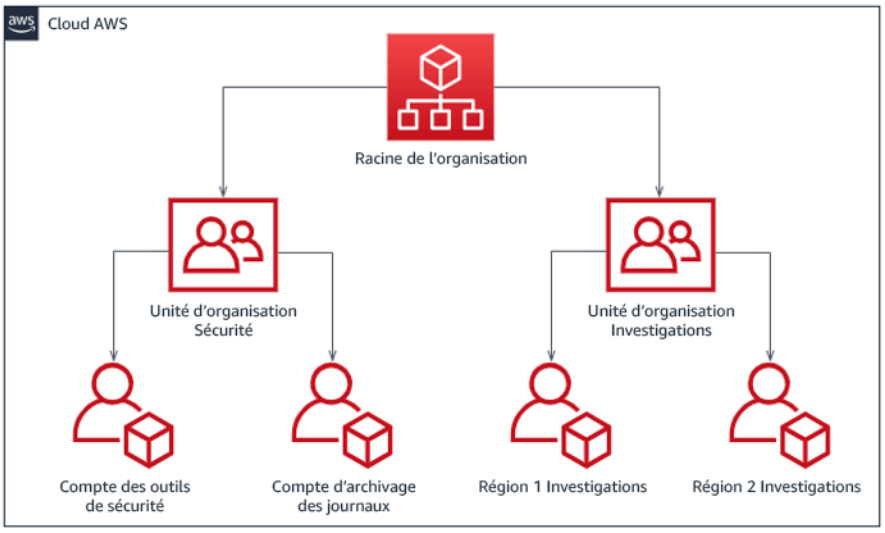
Pour réagir face aux incidents, il est utile de disposer d'une structure de Compte AWS prenant en charge les fonctions de réponse aux incidents, qui comprend une unité d'organisation de sécurité et une unité d'organisation d'analyse poussée.. » Au sein de l'unité d'organisation de sécurité, vous devez disposer de comptes pour :

- Archivage des journaux : Regroupez les journaux dans un Compte AWS d'archivage de journaux avec des autorisations limitées.
- Outils de sécurité : Centralisez les services de sécurité dans un Compte AWS d'outil de sécurité. Ce compte joue le rôle d'administrateur délégué pour les services de sécurité.

Au sein de l'unité d'organisation d'analyse poussée, vous avez la possibilité de mettre en place un ou plusieurs comptes d'analyse poussée pour chaque région dans laquelle vous opérez, selon ce qui convient le mieux à votre entreprise et à votre modèle opérationnel. Si vous créez un compte d'analyse poussée par région, vous pouvez bloquer la création des ressources AWS en dehors de cette région et réduire le risque que les ressources soient copiées vers une région non prévue. Par exemple, si vous opérez uniquement dans US East (N. Virginia) Region (`us-east-1`) et US West (Oregon) (`us-west-2`), vous auriez alors deux comptes dans l'unité d'organisation d'analyse poussée : une pour `us-east-1` et une pour `us-west-2`. »

Vous pouvez créer un Compte AWS d'analyse poussée pour plusieurs régions. Soyez prudent lorsque vous copiez des ressources AWS sur ce compte afin de vérifier que vous respectez vos exigences en matière de souveraineté des données. Étant donné que la mise en place de nouveaux comptes prend du temps, il est impératif de créer et d'instrumenter les comptes d'analyse poussée bien avant un incident afin que les intervenants puissent être prêts à les utiliser efficacement pour intervenir.

Le diagramme suivant présente un exemple de structure de compte, y compris une unité d'organisation d'analyse poussée avec des comptes d'analyse poussée par région :



Structure de compte par région pour la réponse aux incidents

Capture de sauvegardes et d'instantanés

La configuration de sauvegardes des systèmes et des bases de données clés s'avère essentielle pour récupérer d'un incident de sécurité et à des fins d'analyse poussée. Une fois les sauvegardes en place, vous pouvez restaurer vos systèmes à leur état stable antérieur. Sur AWS, vous pouvez

prendre des instantanés de différentes ressources. Les instantanés fournissent des sauvegardes ponctuelles de ces ressources. De nombreux services AWS peuvent vous aider en matière de sauvegarde et de restauration. Pour plus de détails sur ces services et approches en matière de sauvegarde et de restauration, consultez Conseils normatifs sur la sauvegarde et la restauration et Utilisez des sauvegardes pour restaurer après des incidents de sécurité. »

Il est essentiel que vos sauvegardes soient bien protégées, en particulier dans le cas de rançongiciels. Pour obtenir des conseils sur la sécurisation de vos sauvegardes, consultez Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS. » Outre la sécurisation de vos sauvegardes, vous devez régulièrement tester vos processus de sauvegarde et de restauration pour vérifier que la technologie et les processus que vous avez mis en place fonctionnent comme prévu.

Automatisation de l'analyse poussée

Lors d'un événement de sécurité, votre équipe de réponse aux incidents doit être en mesure de collecter et d'analyser rapidement les preuves tout en préservant l'exactitude de la période pendant laquelle s'est produit l'événement (par exemple, en capturant les journaux relatifs à un événement ou à une ressource spécifique ou en collectant les fichiers de vidage de mémoire d'une instance Amazon EC2). Il est à la fois difficile et fastidieux pour l'équipe de réponse aux incidents de collecter manuellement les preuves pertinentes, en particulier sur un grand nombre d'instances et de comptes. De plus, la collecte manuelle peut faire l'objet d'erreurs humaines. Pour ces raisons, vous devez développer et mettre en œuvre autant que possible l'automatisation de l'analyse poussée.

AWS propose un certain nombre de ressources d'automatisation pour l'analyse poussée, qui sont répertoriées dans la section Ressources suivante. Ces ressources sont des exemples de modèles d'analyse poussée que nous avons développés et que les clients ont mis en œuvre. Bien qu'elles puissent constituer une architecture de référence utile au départ, envisagez de les modifier ou de créer de nouveaux modèles d'automatisation de l'analyse poussée en fonction de votre environnement, de vos exigences, de vos outils et de vos processus d'analyse poussée.

Ressources

Documents connexes :

- Guide AWS de réponse aux incidents de sécurité - Développement des fonctionnalités d'analyse poussée (langue française non garantie)
- Guide AWS de réponse aux incidents de sécurité - Ressources d'analyse poussée (langue française non garantie)

- Stratégies d'environnement d'enquête pour les analyses poussées dans le AWS Cloud (langue française non garantie)
- Comment automatiser la collecte de disques d'analyse dans AWS
- Recommandations AWS - Automatiser la réponse aux incidents et l'analyse poussée (langue française non garantie)

Vidéos connexes :

- Automatisation de la réponse aux incidents et investigations

Exemples connexes :

- Cadre d'automatisation de la réponse aux incidents et de l'analyse poussée (langue française non garantie)
- Orchestrateur d'analyse poussée automatisée pour Amazon EC2 (langue française non garantie)

SEC10-BP04 Développer et tester des playbooks de réponse aux incidents de sécurité

L'élaboration de playbooks est une étape clé de la préparation de vos processus de réponse aux incidents. Les playbooks de réponse aux incidents fournissent une série de recommandations et d'étapes à suivre en cas d'événement de sécurité. Le fait de disposer d'une structure et d'étapes claires simplifie la réponse et réduit le risque d'erreur humaine.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyen

Directives d'implémentation

Il est recommandé de créer des playbooks dans les scénarios d'incidents suivants :

- Incidents attendus: créez des playbooks pour les incidents que vous anticipez. Cela inclut des menaces telles que le déni de service (DoS), les rançongiciels et la mise en péril des informations d'identification.
- Résultats ou alertes de sécurité connus: créez des playbooks pour vos résultats et alertes de sécurité connus, tels que les résultats GuardDuty. Vous pourriez recevoir un résultat GuardDuty et vous demander ce que vous devez en faire. Pour éviter de mal gérer ou d'ignorer un résultat GuardDuty, créez un playbook pour chaque résultat GuardDuty potentiel. Certains détails et

conseils de résolution sont disponibles dans la documentation GuardDuty. » Il convient de noter que GuardDuty n'est pas activé par défaut et que son activation n'entraîne aucun frais. Pour plus de détails sur GuardDuty, consultez Annexe A : Définition de la capacité du cloud - Visibilité et alertes (langue française non garantie). »

Les playbooks doivent contenir les étapes techniques qu'un analyste de sécurité doit suivre afin d'enquêter de manière adéquate et de répondre à un éventuel incident de sécurité.

Étapes d'implémentation

Les éléments à inclure dans un playbook incluent :

- Présentation du playbook: quel scénario de risque ou d'incident ce playbook aborde-t-il ? Quel est l'objectif du playbook ?
- Conditions préalables: quels journaux, mécanismes de détection et outils automatisés sont requis pour ce scénario d'incident ? Quelle est la notification attendue ?
- Informations sur la communication et les remontées: qui sont les personnes impliquées et quelles sont leurs coordonnées ? Quelles sont les responsabilités de chacune des parties prenantes ?
- Étapes de réponse: quelles sont les mesures tactiques à prendre au cours des différentes phases de la réponse à un incident ? Quelles requêtes un analyste doit-il exécuter ? Quel code doit être exécuté pour obtenir le résultat souhaité ?
  - Détecter: comment l'incident sera-t-il détecté ?
  - Analyser: comment l'étendue de l'impact sera-t-elle déterminée ?
  - Contenir: comment l'incident sera-t-il isolé pour en limiter la portée ?
  - Éradiquer: comment éliminer la menace de l'environnement ?
  - Récupérer: comment le système ou la ressource concernés seront-ils remis en production ?
- Résultats attendus: une fois les requêtes et le code exécutés, quel est le résultat attendu du playbook ?

Ressources

Bonnes pratiques Well-Architected connexes :

- SEC10-BP02 - Développer des plans de gestion des incidents

Documents connexes :

- Cadre des playbooks de réponse aux incidents (langue française non garantie)
- Développer vos propres playbooks de réponse aux incidents (langue française non garantie)
- Exemples de playbooks de réponse aux incidents (langue française non garantie)
- Création d'un runbook de réponse aux incidents AWS à l'aide de playbooks Jupyter et CloudTrail Lake (langue française non garantie)

SEC10-BP05 Préallouer les accès

Vérifiez que les intervenants en cas d'incident disposent du bon accès préalablement alloué dans AWS afin de réduire le temps d'investigation jusqu'à la reprise.

Anti-modèles courants :

- Utilisation du compte racine pour la réponse aux incidents.
- Modification des comptes utilisateur existants.
- Manipulation des autorisations IAM directement lors de la fourniture d'une élévation de privilèges juste-à-temps.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : Moyen

Directives d'implémentation

AWS recommande de réduire ou de supprimer l'utilisation des informations d'identification durables dans la mesure du possible et de privilégier les informations d'identification temporaire à la place, ainsi que les mécanismes d'élévation des privilèges juste-à-temps. Les informations d'identification durables sont sujettes aux risques de sécurité et augmentent les frais généraux opérationnels. Pour la plupart des tâches de gestion et de réponse aux incidents, nous vous recommandons de mettre en œuvre la fédération d'identité parallèlement à l'élévation temporaire pour l'accès administratif. Dans le cadre de ce modèle, un utilisateur demande une élévation à un niveau de privilège plus élevé (par exemple un rôle de réponse aux incidents) et, si l'utilisateur est admissible à cette élévation, une demande est envoyée à un approbateur. Si la demande est approuvée, l'utilisateur reçoit un ensemble d'informations d'identification AWS temporaires qui peuvent être utilisées afin d'exécuter les tâches. Une fois que ces informations d'identification ont expiré, l'utilisateur doit soumettre une nouvelle demande d'élévation.

Nous vous recommandons d'utiliser une élévation temporaire des privilèges dans la plupart des cas de réponse aux incidents. Dans cette optique, la meilleure solution consiste à utiliser AWS Security Token Service et les politiques de session afin de délimiter l'accès.

Dans certains cas, les identités fédérées ne sont pas disponibles, par exemple :

- Panne liée à la compromission d'un fournisseur d'identité (IdP).
- Mauvaise configuration ou erreur humaine entraînant la panne d'un système de gestion d'accès fédéré.
- Activité malveillante, par exemple un déni de service distribué (DDoS) ou une indisponibilité du système.

Dans les cas précédents, il doit y avoir un accès d'urgence de type Break Glass configuré afin de permettre l'analyse et la correction rapide des incidents. Nous vous recommandons également d'utiliser un utilisateur IAM disposant des autorisations appropriées pour effectuer des tâches et accéder aux ressources AWS. Utilisez des informations d'identification racine uniquement pour les tâches qui requièrent un accès en tant qu'utilisateur root. Pour vérifier que les intervenants en cas d'incident disposent d'un niveau d'accès approprié à AWS et aux autres systèmes pertinents, nous vous recommandons de pré-allouer des comptes utilisateur dédiés. Les comptes utilisateur requièrent un accès privilégié et doivent être étroitement contrôlés et surveillés. Les comptes doivent être créés avec le moins de privilèges requis pour effectuer les tâches nécessaires et le niveau d'accès doit être basé sur les playbooks créés dans le cadre du plan de gestion des incidents.

Utilisez des utilisateurs et des rôles spécialement conçus et dédiés au titre de bonne pratique. L'élévation temporaire de l'accès des utilisateurs ou des rôles via l'ajout de politiques IAM ne permet pas de savoir clairement de quel type d'accès bénéficiaient les utilisateurs pendant l'incident et peut empêcher la révocation des privilèges élevés au niveau supérieur.

Il est important de supprimer autant de dépendances que possible afin de vérifier que l'accès peut être obtenu dans le plus grand nombre possible de scénarios de défaillance. Afin de vous faciliter la tâche, créez un playbook permettant de vérifier que les utilisateurs chargés des réponses en cas d'incident ont été créés en tant qu'utilisateurs AWS Identity and Access Management dans un compte de sécurité dédié et qu'ils ne sont pas gérés via une solution d'authentification unique ou de fédération existante. Chaque intervenant en cas d'incident doit avoir son propre compte nommé. La configuration du compte doit appliquer une politique stricte de gestion des mots de passe et une authentification multifactorielle (MFA). Si les playbooks de réponse aux incidents ne nécessitent qu'un accès à la AWS Management Console, l'utilisateur ne doit pas avoir de clés

d'accès configurées et il doit lui être explicitement interdit de créer des clés d'accès. Cela peut être configuré avec des politiquesIAM ou des politiques de contrôle de service (SCP), comme mentionné dans les bonnes pratiques de sécurité AWS pour les SCP AWS Organizations. Les utilisateurs ne doivent pas avoir d'autres privilèges que la capacité d'assumer des rôles de réponse aux incidents dans d'autres comptes.

Pendant un incident, il peut être nécessaire d'accorder l'accès à d'autres personnes internes ou externes afin de prendre en charge les activités d'analyse, de correction ou de reprise. Dans ce cas, utilisez le mécanisme de playbook mentionné précédemment. Celui-ci doit comporter un processus permettant de s'assurer que tout accès supplémentaire est révoqué immédiatement après l'incident.

Pour s'assurer que l'utilisation des rôles de réponse aux incidents peut être correctement surveillée et vérifiée, il est essentiel que les comptes utilisateur IAM créés à cette fin ne soient pas partagés entre les personnes et que l'utilisateur root Compte AWS ne soit pas utilisé, sauf si cela s'avère nécessaire pour une tâche spécifique. Si l'utilisateur root est requis (par exemple, l'accès IAM à un compte spécifique n'est pas disponible), utilisez un processus distinct avec un playbook disponible afin de vérifier la disponibilité du mot de passe utilisateur root et du jeton d'authentification multifactorielle.

Pour configurer les politiques IAM des rôles de réponse aux incidents, pensez à utiliser IAM Access Analyzer pour générer des politiques basées sur les journaux AWS CloudTrail. Pour cela, accordez à l'administrateur l'accès au rôle de réponse aux incidents sur un compte hors production et exécutez vos playbooks. Une fois que vous aurez terminé, vous pourrez créer une politique autorisant uniquement les mesures prises. Cette politique peut ensuite être appliquée à tous les rôles de réponse aux incidents dans tous les comptes. Vous pouvez éventuellement créer une politique IAM distincte pour chaque playbook afin de faciliter la gestion et la vérification. Les exemples de playbooks peuvent comprendre des plans d'intervention pour les rançongiciels, les atteintes à la protection des données, la perte d'accès à la production et d'autres scénarios.

Utilisez les comptes utilisateur de réponse aux incidents pour assumer les rôles IAM dédiés de réponse aux incidents dans d'autres Comptes AWS. Ces rôles doivent être configurés de façon à pouvoir être assumés uniquement par les utilisateurs du compte de sécurité et la relation de confiance doit exiger que le principal appelant ait été authentifié au moyen de l'authentification multifactorielle. Les rôles doivent utiliser des politiques IAM à portée limitée afin de contrôler l'accès. Assurez-vous que toutes les demandes `AssumeRole` pour ces rôles sont consignées dans CloudTrail et font l'objet d'une alerte, et que toutes les mesures prises en utilisant ces rôles sont consignées.

Il est vivement recommandé de nommer les comptes utilisateur IAM et les rôles IAM afin d'en faciliter la recherche dans les journaux CloudTrail. Par exemple, les comptes IAM pourraient être nommés *<USER_ID>*-BREAK-GLASS et les rôles IAM pourraient être nommés BREAK-GLASS-ROLE.

CloudTrail est utilisé pour consigner l'activité de l'API dans vos comptes AWS et doit être utilisé pour configurer les alertes sur l'utilisation des rôles de réponse aux incidents. Consultez la publication de blog sur la configuration des alertes lorsque les clés racine sont utilisées. Les instructions peuvent être modifiées de façon à configurer la métrique Amazon CloudWatch de filtre à filtre sur les événements AssumeRole liés au rôle IAM de réponse aux incidents :

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !
= "AwsServiceEvent" }
```

Dans la mesure où les rôles de réponse aux incidents sont susceptibles d'avoir un niveau d'accès élevé, il est important que ces alertes soient transmises à un vaste groupe et qui y donnera suite rapidement.

Lors d'un incident, il est possible qu'un intervenant ait besoin d'accéder à des systèmes qui ne sont pas sécurisés directement par IAM. Il peut notamment s'agir d'instances Amazon Elastic Compute Cloud, de bases de données Amazon Relational Database Service ou de plateformes de logiciel en tant que service (SaaS). Il est vivement recommandé d'utiliser AWS Systems Manager Session Manager plutôt que des protocoles natifs tels que SSH ou RDP pour tous les accès administratifs aux instances Amazon EC2. Cet accès peut être contrôlé à l'aide d'IAM, qui est sécurisé et vérifié. Il est également possible d'automatiser certaines parties de vos playbooks en utilisant des documents AWS Systems Manager,qui permettent de réduire les erreurs utilisateur et d'améliorer le temps de récupération. Pour accéder aux bases de données et aux outils tiers, nous recommandons de stocker les informations d'identification dans AWS Secrets Manager et d'accorder l'accès aux rôles des intervenants en cas d'incident.

En dernier lieu, la gestion des comptes utilisateur IAM de réponse aux incidents doit être ajoutée à vos processus d'entrées, de changements et de sorties. Elle doit également être vérifiée et testée régulièrement afin de vous assurer que seul l'accès prévu est autorisé.

Ressources

Documents connexes :

- Managing temporary elevated access to your AWS environment

- AWS Security Incident Response Guide
- AWS Elastic Disaster Recovery
- AWS Systems Manager Incident Manager
- Définition d'une politique de mot de passe du compte pour les utilisateurs IAM
- Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS
- Configuring Cross-Account Access with MFA
- Using IAM Access Analyzer to generate IAM policies
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment
- How to Receive Notifications When Your AWS Account's Root Access Keys Are Used
- Create fine-grained session permissions using IAM managed policies

Vidéos connexes :

- Automating Incident Response and Forensics in AWS
- DIY guide to runbooks, incident reports, and incident response
- Prepare for and respond to security incidents in your AWS environment

Exemples connexes :

- Atelier : AWS Account Setup and Root User
- Atelier : Incident Response with AWS Console and CLI

SEC10-BP06 Prédéployer les outils

Vérifiez que le personnel de sécurité dispose des outils appropriés préalablement déployés pour accélérer l'enquête jusqu'à la récupération.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyen

Directives d'implémentation

Pour automatiser les fonctions de réponse et d'exploitation de la sécurité, vous pouvez utiliser un ensemble complet d'API et d'outils d'AWS. Vous pouvez automatiser entièrement la gestion des identités, la sécurité des réseaux, la protection des données et les fonctionnalités de surveillance, et

les mettre en œuvre en utilisant les méthodes de développement de logiciel les plus courantes que vous avez déjà mises en place. Lorsque vous automatisez la sécurité, votre système peut surveiller, examiner et déclencher une réponse, plutôt que d'avoir à demander à des personnes de surveiller votre niveau 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. L'intégration de systèmes de détection d'anomalies, comme Amazon GuardDuty, AWS CloudTrail Insights et Amazon CloudWatch Anomaly Detection, peut alléger les alertes courantes basées sur des seuils.

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 cette 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.

Au cours d'une enquête de sécurité, vous devez être en mesure d'examiner les journaux pertinents pour consigner et comprendre la portée et la chronologie complètes de l'incident. Des journaux sont également requis pour la génération d'alertes, indiquant que certaines actions intéressantes ont eu lieu. Il est essentiel de sélectionner, d'activer, de stocker et de configurer les mécanismes d'interrogation et de récupération et de configurer les alertes. En outre, une solution efficace qui fournit des outils de recherche dans les données des journaux est Amazon Detective. »

AWS propose plus de 200 services cloud et des milliers de fonctionnalités. Nous vous recommandons de passer en revue les services susceptibles de prendre en charge et de simplifier votre stratégie de réponse aux incidents.

Outre la journalisation, vous devez développer et mettre en œuvre une cohérente. » Le balisage peut aider à mettre en contexte l'objectif d'une ressource AWS. Le balisage peut également être utilisé à des fins d'automatisation.

Étapes d'implémentation

Sélection et configuration de journaux à des fins d'analyse et d'alerte

Consultez la documentation suivante relative à la configuration de la journalisation pour la réponse aux incidents :

- Stratégies de journalisation pour la réponse aux incidents de sécurité (langue française non garantie)
- SEC04-BP01 Configurer une journalisation de service et d'application

Activation de la prise en charge de la détection et de la réponse pour les services de sécurité

AWS fournit des fonctionnalités natives de détection, de prévention et de réponse et d'autres services peuvent être utilisés pour concevoir des solutions de sécurité personnalisées. Pour obtenir la liste des services les plus pertinents en matière de réponse aux incidents de sécurité, consultez Définition de la capacité du cloud (langue française non garantie). »

Élaboration et mise en œuvre d'une stratégie de balisage

Il peut être difficile d'obtenir des informations contextuelles sur le cas d'utilisation métier et les parties prenantes internes pertinentes concernant une ressource AWS. Pour ce faire, vous pouvez utiliser des balises qui attribuent des métadonnées à vos ressources AWS. Ces balises comprennent une clé et une valeur définies par l'utilisateur. Vous pouvez créer des balises pour classer les ressources par objectif, propriétaire, environnement, type de données traitées et d'autres critères de votre choix.

Le fait de disposer d'une stratégie de balisage cohérente peut accélérer les temps de réponse et réduire le temps consacré au contexte organisationnel en vous permettant d'identifier et de discerner rapidement les informations contextuelles relatives à une ressource AWS. Les balises peuvent également servir de mécanisme pour initier l'automatisation des réponses. Pour plus de détails sur les éléments à étiqueter, consultez Balisage de vos ressources AWS. » Vous devez d'abord définir les balises que vous souhaitez implémenter dans votre organisation. Ensuite, vous mettez en œuvre et appliquez cette stratégie de balisage. Pour plus de détails sur la mise en œuvre et l'application, consultez Mise en œuvre d'une stratégie de balisage des ressources AWS à l'aide de politiques de balisage AWS et de politiques de contrôle des services (SCP) (langue française non garantie).. »

Ressources

Bonnes pratiques Well-Architected connexes :

- SEC04-BP01 Configurer une journalisation de service et d'application
- SEC04-BP02 Analyse centralisée des journaux, des résultats et des métriques

Documents connexes :

- Stratégies de journalisation pour la réponse aux incidents de sécurité (langue française non garantie)
- Définition de la capacité du cloud pour la réponse aux incidents (langue française non garantie)

Exemples connexes :

- Détection et réponse aux menaces avec Amazon GuardDuty et Amazon Detective (langue française non garantie)
- Atelier Security Hub (langue française non garantie)
- Gestion des vulnérabilités avec Amazon Inspector (langue française non garantie)

SEC10-BP07 Exécuter des simulations

À mesure que les organisations se développent et évoluent au fil du temps, le paysage des menaces change. Il est donc important de revoir en permanence vos capacités de réponse aux incidents. L'organisation de simulations (également appelées « journées de jeu ») est une méthode qui peut être utilisée pour effectuer cette évaluation. Les simulations utilisent des scénarios d'événements de sécurité réels conçus pour imiter les tactiques, techniques et procédures (TTP) d'un acteur de la menace et permettre à une organisation d'exercer et d'évaluer ses capacités de réponse aux incidents en réagissant à ces cyberévénements fictifs tels qu'ils peuvent se produire dans la réalité.

Avantages liés au respect de cette bonne pratique : les simulations présentent de nombreux avantages :

- Validation de l'état de préparation à la cybersécurité et renforcement de la confiance de vos intervenants en cas d'incident.
- Test de la précision et de l'efficacité des outils et des flux de travail.
- Amélioration des méthodes de communication et de remontées en fonction de votre plan de réponse aux incidents.
- Possibilité de répondre à des vecteurs moins courants.

Niveau de risque exposé si cette bonne pratique n'est pas établie: moyen

Directives d'implémentation

Il existe trois principaux types de simulations :

- Exercices de simulation : l'approche théorique des simulations est une session basée sur des discussions auxquelles participent les différentes parties prenantes de la réponse aux incidents afin de mettre en pratique leurs rôles et leurs responsabilités et d'utiliser des outils de communication et des manuels établis. L'animation d'exercices peut généralement être réalisée en une journée complète dans un lieu virtuel, un lieu physique ou une combinaison des deux. Dans la mesure où il repose sur la discussion, l'exercice théorique met l'accent sur les processus, les personnes et la collaboration. La technologie fait partie intégrante de la discussion, mais l'utilisation effective d'outils ou de scripts de réponse aux incidents ne fait généralement pas partie de l'exercice théorique.
- Exercices de l'équipe violette : les exercices de l'équipe violette augmentent le niveau de collaboration entre les intervenants en cas d'incident (équipe bleue) et les acteurs de menaces simulées (équipe rouge). L'équipe bleue est composée de membres du centre des opérations de sécurité (SOC), mais peut également inclure d'autres parties prenantes qui seraient impliquées lors d'un véritable cyberévénement. L'équipe rouge est composée d'une équipe de tests de pénétration ou de parties prenantes clés formées à la sécurité offensive. L'équipe rouge travaille en collaboration avec les animateurs de l'exercice lors de la conception d'un scénario afin que celui-ci soit précis et réalisable. Lors des exercices de l'équipe violette, l'accent est principalement mis sur les mécanismes de détection, les outils et les procédures opérationnelles standard (SOP) qui soutiennent les efforts de réponse aux incidents.
- Exercices de l'équipe rouge : au cours d'un exercice de l'équipe rouge, l'attaque (l'équipe rouge) effectue une simulation pour atteindre un objectif donné ou un ensemble d'objectifs à partir d'une portée prédéterminée. Les défenseurs (équipe bleue) ne seront pas nécessairement au courant de la portée ni de la durée de l'exercice, ce qui permet d'évaluer de manière plus réaliste la manière dont ils réagiraient en cas d'incident réel. Étant donné que les exercices de l'équipe rouge peuvent être des tests invasifs, soyez prudent et mettez en œuvre des contrôles pour vérifier que l'exercice ne cause pas de dommages réels à votre environnement.

Envisagez d'animer des simulations cybernétiques à intervalles réguliers. Chaque type d'exercice peut apporter des avantages uniques aux participants et à l'organisation dans son ensemble. Vous pouvez donc choisir de commencer par des types de simulation moins complexes (tels que des exercices théoriques) et de passer ensuite à des types de simulation plus complexes (exercices de l'équipe rouge). Vous devez sélectionner un type de simulation en fonction de la maturité de votre

sécurité, de vos ressources et des résultats souhaités. Certains clients peuvent décider de ne pas effectuer les exercices de l'équipe rouge en raison de leur complexité et de leur coût.

Étapes d'implémentation

Quel que soit le type de simulation que vous choisissez, les simulations suivent généralement les étapes de mise en œuvre suivantes :

1. Définissez les principaux éléments de l'exercice : définissez le scénario de simulation et les objectifs de la simulation. Les deux doivent être acceptés par les dirigeants.
2. Identifiez les principales parties prenantes : un exercice nécessite au minimum des animateurs et des participants. Selon le scénario, d'autres parties prenantes telles que les services juridiques, l'équipe de communication ou la direction, peuvent être impliquées.
3. Créez et testez le scénario : le scénario devra peut-être être redéfini au fur et à mesure de sa création si des éléments spécifiques ne sont pas réalisables. Un scénario finalisé est attendu à l'issue de cette étape.
4. Animez la simulation : le type de simulation détermine l'animation utilisée (un scénario papier par rapport à un scénario simulé hautement technique). Les animateurs doivent adapter leurs tactiques d'animation aux objectifs de l'exercice et impliquer tous les participants dans l'exercice dans la mesure du possible afin d'en tirer le meilleur parti.
5. Effectuez un rapport après action (AAR) : identifiez les domaines qui se sont bien déroulés, ceux qui peuvent être améliorés et les lacunes potentielles. L'AAR doit mesurer l'efficacité de la simulation ainsi que la réponse de l'équipe à l'événement simulé afin que les progrès puissent être suivis au fil du temps lors de futures simulations.

Ressources

Documents connexes :

- Guide AWS de réponse aux incidents (langue française non garantie)

Vidéos connexes :

- AWS GameDay - Security Edition

Opérations

Les opérations sont au cœur de la réponse aux incidents. C'est à ce niveau que se déroulent les actions de réponse et de résolution des incidents de sécurité. Les opérations comprennent les cinq phases suivantes : détection, analyse, maîtrise, éradicationet récupération. Vous trouverez la description de ces phases et des objectifs dans le tableau suivant.

Phase	Objectif
Détection	Identifiez un événement de sécurité potentiel.
Analyse	Déterminez si l'événement de sécurité est un incident et évaluez son ampleur.
Maîtrise	Minimisez et limitez la portée de l'événement de sécurité.
Éradication	Éliminez les ressources ou artefacts non autorisés liés à l'événement de sécurité. Mettez en œuvre les mesures d'atténuation à l'origine de l'incident de sécurité.
Récupération	Restaurez les systèmes dans un état sûr connu et surveillez-les pour vérifier que la menace ne se reproduit pas.

Utilisez ces phases à titre de référence pour réagir de manière efficace et robuste aux incidents. Les actions que vous effectuerez varieront en fonction de l'incident lui-même. Un incident impliquant un rançongiciel, par exemple, nécessite un ensemble d'étapes de réponse différent de celui d'un incident impliquant un compartiment Amazon S3 public. De plus, ces phases ne se déroulent pas nécessairement de manière séquentielle. Après la maîtrise et l'éradication, vous devrez peut-être revenir à l'analyse pour déterminer si vos actions ont été efficaces.

Une préparation minutieuse de votre personnel, de vos processus et de la technologie est essentielle à l'efficacité des opérations. Suivez donc les bonnes pratiques de la section Préparation pour répondre efficacement à un événement de sécurité actif.

Pour en savoir plus, reportez-vous à la section Opérations du guide des réponses aux incidents de sécurité AWS.

Activité postérieure à l'incident

Les menaces existantes sont en constante évolution. La capacité de votre organisation à protéger efficacement vos environnements doit suivre le rythme. La clé de l'amélioration continue consiste à réitérer les résultats de vos incidents et de vos simulations afin d'améliorer vos capacités à détecter, à gérer et à analyser efficacement les incidents de sécurité potentiels, en réduisant les vulnérabilités éventuelles, les délais de réponse et le retour à des opérations sûres. Les mécanismes suivants peuvent vous aider à vérifier que votre organisation dispose de toutes les capacités et les connaissances les plus récentes nécessaires pour réagir efficacement, quelle que soit la situation.

Bonnes pratiques

- SEC10-BP08 Établir un cadre pour tirer des enseignements des incidents

SEC10-BP08 Établir un cadre pour tirer des enseignements des incidents

La mise en œuvre d'un cadre d'enseignements tirés et d'une capacité d'analyse des causes profondes peut non seulement contribuer à améliorer les capacités de réponse aux incidents, mais également à empêcher que l'incident ne se reproduise. En tirant les leçons de chaque incident, vous pouvez éviter de répéter les mêmes erreurs, expositions ou erreurs de configuration, non seulement en améliorant votre posture de sécurité, mais également en réduisant le temps perdu dans des situations évitables.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : Moyen

Directives d'implémentation

Il est important de mettre en œuvre un cadre d'enseignements tirés qui établit et atteint, à un niveau élevé, les points suivants :

- Quand se déroule un processus des enseignements tirés ?
- En quoi consiste le processus des enseignements tirés ?
- Comment se déroule un processus des enseignements tirés ?
- Qui est impliqué dans le processus et comment ?
- Comment les domaines à améliorer seront-ils identifiés ?

- Comment allez-vous vérifier que les améliorations sont suivies et mises en œuvre de manière efficace ?

Le cadre ne doit pas se concentrer sur les individus ni les blâmer, mais doit plutôt se concentrer sur l'amélioration des outils et des processus.

Étapes d'implémentation

Outre les résultats de haut niveau énumérés ci-dessus, il est important de poser les bonnes questions afin de tirer le meilleur parti (informations menant à des améliorations réalisables) du processus. Posez-vous les questions suivantes pour commencer à développer vos discussions sur les enseignements tirés :

- Quel a été l'incident ?
- Quand l'incident a-t-il été identifié pour la première fois ?
- Comment a-t-il été identifié ?
- Quels systèmes ont alerté sur l'activité ?
- Quels systèmes, services et données étaient concernés ?
- Que s'est-il passé précisément ?
- Qu'est-ce qui a bien fonctionné ?
- Qu'est-ce qui n'a pas bien fonctionné ?
- Quels processus ou procédures ont échoué ou n'ont pas pu être mis à l'échelle pour répondre à l'incident ?
- Qu'est-ce qui peut être amélioré dans les domaines suivants :
  - Les collaborateurs
    - Les personnes à contacter étaient-elles réellement disponibles et la liste de contacts était-elle à jour ?
    - Les personnes manquaient-elles de formation ou n'avaient-elles pas les capacités nécessaires pour intervenir et enquêter efficacement sur l'incident ?
    - Les ressources appropriées étaient-elles prêtes et disponibles ?
  - Les processus
    - Les processus et procédures ont-ils été suivis ?
    - Les processus et procédures étaient-ils documentés et disponibles pour cet incident ou ce type d'incident ?

    - Les processus et procédures requis étaient-ils absents ?
    - Les intervenants ont-ils pu accéder en temps opportun aux informations requises pour répondre au problème ?
- La technologie
    - Les systèmes d'alerte existants ont-ils identifié l'activité et ont-ils envoyé des alertes efficaces ?
    - Comment aurions-nous pu réduire le délai de détection de 50 % ?
    - Les alertes existantes doivent-elles être améliorées ou de nouvelles alertes doivent-elles être créées pour cet incident ou ce type d'incident ?
    - Les outils existants ont-ils permis d'enquêter efficacement (recherche/analyse) sur l'incident ?
    - Que peut-on faire pour identifier cet incident ou ce type d'incident plus rapidement ?
    - Que peut-on faire pour éviter que cet incident ou ce type d'incident ne se reproduise ?
    - À qui appartient le plan d'amélioration et comment allez-vous vérifier qu'il a été mis en œuvre ?
    - Quel est le calendrier des contrôles et processus de surveillance ou de prévention supplémentaires à mettre en œuvre et à tester ?

Cette liste n'est pas exhaustive, mais vise à servir de point de départ pour identifier les besoins de l'organisation et de l'entreprise et la manière dont vous pouvez les analyser afin de tirer les meilleurs enseignements des incidents et d'améliorer en permanence votre posture de sécurité. Le plus important est de commencer par intégrer les enseignements tirés dans le cadre standard de votre processus de réponse aux incidents, de la documentation et des attentes des parties prenantes.

Ressources

Documents connexes :

- Guide de réponse aux incidents de sécurité AWS - Établir un cadre pour tirer des enseignements des incidents (langue française non garantie)
- Recommandations CAF du NCSC - Enseignements tirés (langue française non garantie)

Sécurité des applications

La sécurité des applications (AppSec) décrit le processus global de conception, d'élaboration et de test des propriétés de sécurité des charges de travail que vous développez. Vous devez disposer de personnes correctement formées dans votre organisation, comprendre les propriétés de sécurité de votre infrastructure de création et de diffusion, et utiliser l'automatisation pour identifier les problèmes de sécurité.

L'adoption de tests de sécurité des applications dans le cadre du cycle de développement des logiciels (SDLC) et des processus de validation permet de s'assurer que vous disposez d'un mécanisme structuré pour identifier, corriger et prévenir les problèmes de sécurité des applications dans votre environnement de production.

Votre méthodologie de développement d'applications doit inclure des contrôles de sécurité lors de la conception, de l'élaboration, du déploiement et de l'exploitation de vos charges de travail. Ce faisant, alignez le processus afin de limiter les défauts en continu et de minimiser la dette technique. Par exemple, l'utilisation de la modélisation des menaces au cours de la phase de conception permet de découvrir rapidement les défauts de conception, ce qui les rend plus faciles et moins coûteux à corriger que d'attendre et de les atténuer plus tard.

Généralement, plus vous avancez dans le cycle de vie du développement logiciel, plus le coût et la complexité de la résolution des failles augmentent. Le moyen le plus simple de résoudre les problèmes est de ne pas en avoir. C'est pourquoi le fait de commencer par élaborer un modèle de menace permet de se concentrer sur les bons résultats dès la phase de conception. À mesure que votre programme AppSec gagne en maturité, vous pouvez augmenter la quantité de tests effectués à l'aide de l'automatisation, améliorer la pertinence des commentaires aux concepteurs et réduire le temps nécessaire pour les examens de sécurité. Toutes ces actions améliorent la qualité du logiciel que vous créez et accélèrent la mise en production des fonctionnalités.

Ces lignes directrices pour l'implémentation se concentrent sur quatre domaines : l'organisation et la culture, la sécurité du pipeline, la sécurité dans le pipeline et la gestion des dépendances. Chaque domaine fournit un ensemble de principes que vous pouvez implémenter ainsi qu'une vue d'ensemble de la manière dont vous concevez, développez, construisez, déployez et exploitez les charges de travail.

Au sein d'AWS, il existe un certain nombre d'approches que vous pouvez utiliser lorsque vous abordez votre programme de sécurité des applications. Certaines de ces approches reposent sur la

technologie, tandis que d'autres se concentrent sur les aspects humains et organisationnels de votre programme de sécurité des applications.

Bonnes pratiques

- SEC11-BP01 Formation à la sécurité des applications
- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication
- SEC11-BP03 Réalisation de tests de pénétration réguliers
- SEC11-BP04 Révisions de code manuelles
- SEC11-BP05 Centralisation des services pour les packages et les dépendances
- SEC11-BP06 Déploiement programmatique de logiciels
- SEC11-BP07 Évaluation régulière des caractéristiques de sécurité des pipelines
- SEC11-BP08 Création d'un programme permettant aux équipes responsables de la charge de travail de s'approprier les mécanismes de sécurité

SEC11-BP01 Formation à la sécurité des applications

Formez les concepteurs de votre organisation aux pratiques courantes de développement et d'exploitation sécurisés des applications. L'adoption de pratiques de développement axées sur la sécurité permet de réduire la probabilité d'apparition de problèmes décelés uniquement au stade de l'examen de la sécurité.

Résultat souhaité : les logiciels doivent être conçus et construits en tenant compte de la sécurité. Lorsque les concepteurs d'une organisation sont formés à des pratiques de développement sécurisées qui commencent par un modèle de menace, la qualité et la sécurité globales des logiciels produits s'en trouvent améliorées. Cette approche peut réduire le délai de livraison des logiciels ou des fonctionnalités, car moins de retouches sont nécessaires après la phase d'examen de la sécurité.

Aux fins de cette bonne pratique, le développement sécurisé désigne le logiciel conçu et les outils ou systèmes qui soutiennent le cycle du développement logiciel (SDLC).

Anti-modèles courants :

- Attendre un examen de la sécurité, puis réfléchir aux propriétés de sécurité d'un système.
- Laisser toutes les décisions en matière de sécurité à l'équipe de sécurité.

- Ne pas communiquer sur la manière dont les décisions prises au cours du cycle de développement du logiciel sont liées aux attentes ou aux politiques générales de l'organisation en matière de sécurité.
- S'impliquer trop tard dans le processus d'examen de la sécurité.

Avantages liés au respect de cette bonne pratique :

- Meilleure connaissance des exigences organisationnelles en matière de sécurité dès le début du cycle de développement.
- Possibilité d'identifier les problèmes de sécurité potentiels et d'y remédier plus rapidement, ce qui se traduit par une mise à disposition plus rapide des fonctionnalités.
- Amélioration de la qualité des logiciels et des systèmes.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Formez les concepteurs de votre organisation. Une formation à la modélisation des menaces constitue une bonne base pour se former à la sécurité. Idéalement, les concepteurs devraient pouvoir accéder en libre-service aux informations pertinentes pour leur charge de travail. Cet accès leur permet de prendre des décisions éclairées sur les propriétés de sécurité des systèmes qu'ils construisent, sans avoir à solliciter une autre équipe. Le processus de participation de l'équipe de sécurité aux révisions doit être clairement défini et simple à suivre. Les étapes du processus de révision doivent être ajoutées à la formation à la sécurité. Lorsque des modèles d'implémentation connus sont disponibles, ils doivent être faciles à trouver et à relier aux exigences de sécurité globales. Envisagez d'utiliser AWS CloudFormation, AWS Cloud Development Kit (AWS CDK) Constructs, Service Catalog, ou d'autres outils de modélisation pour réduire la nécessité d'une configuration personnalisée.

Étapes d'implémentation

- Commencez par donner aux concepteurs un cours sur la modélisation des menaces afin de leur donner une bonne base et de les aider à penser à la sécurité.
- Fournissez un accès aux formations AWS Training and Certification, de l'industrie ou des partenaires AWS.

- Dispensez une formation sur le processus d'examen de la sécurité de votre organisation, qui clarifie la répartition des responsabilités entre l'équipe chargée de la sécurité, les équipes responsables de la charge de travail et les autres parties prenantes.
- Publiez des conseils en libre-service sur la manière de répondre à vos exigences en matière de sécurité, y compris des exemples de code et des modèles, s'ils sont disponibles.
- Recueillez régulièrement les commentaires des équipes de concepteurs sur leur expérience du processus d'examen de la sécurité et de la formation, et utilisez ces commentaires pour vous améliorer.
- Utilisez des tests de simulation de pannes ou des campagnes de chasse aux bogues pour réduire le nombre de problèmes et améliorer les compétences de vos concepteurs.

Ressources

Bonnes pratiques associées :

- SEC11-BP08 Création d'un programme permettant aux équipes responsables de la charge de travail de s'approprier les mécanismes de sécurité

Documents connexes :

- AWS Training and Certification
- How to think about cloud security governance
- How to approach threat modeling
- Accelerating training – The AWS Skills Guild (Accélérer la formation – AWS Skills Guild)

Vidéos connexes :

- Proactive security: Considerations and approaches

Exemples connexes :

- Atelier sur la modélisation des menaces
- Sensibilisation des développeurs à l'industrie

Services associés :

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) Constructs
- Service Catalog
- AWS BugBust

SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication

Automatisez les tests des propriétés de sécurité tout au long du cycle de développement et de publication. L'automatisation facilite l'identification systématique et répétée des problèmes potentiels dans les logiciels avant leur diffusion, ce qui réduit le risque de problèmes de sécurité dans les logiciels fournis.

Résultat souhaité : l'objectif des tests automatisés est de fournir un moyen programmatique de détecter les problèmes potentiels de manière précoce et fréquente tout au long du cycle de développement. Lorsque vous automatisez les tests de régression, vous pouvez exécuter à nouveau les tests fonctionnels et non fonctionnels pour vérifier que le logiciel testé précédemment fonctionne toujours comme prévu après une modification. Lorsque vous définissez des tests d'unités de sécurité pour vérifier les erreurs de configuration courantes, telles qu'une authentification défaillante ou manquante, vous pouvez identifier et résoudre ces problèmes dès le début du processus de développement.

L'automatisation des tests utilise des cas de test spécifiques pour la validation de l'application, sur la base des exigences de l'application et de la fonctionnalité souhaitée. Le résultat du test automatisé est basé sur la comparaison entre le résultat du test généré et le résultat attendu, ce qui accélère le cycle de vie global du test. Les méthodologies de test telles que les tests de régression et les suites de tests d'unités sont les mieux adaptées à l'automatisation. L'automatisation des tests des propriétés de sécurité permet aux concepteurs de recevoir des commentaires automatisés sans avoir à attendre un examen de sécurité. Les tests automatisés sous forme d'analyse statique ou dynamique du code peuvent améliorer la qualité du code et aider à détecter les problèmes logiciels potentiels dès le début du cycle de développement.

Anti-modèles courants :

- Ne pas communiquer les cas de test et les résultats des tests automatisés.
- Effectuer uniquement les tests automatisés juste avant la mise en production.

- Automatiser les cas de test avec des exigences qui changent fréquemment.
- Ne pas fournir de recommandations sur la manière de traiter les résultats des tests de sécurité.

Avantages liés au respect de cette bonne pratique :

- Réduction de la dépendance à l'égard des personnes qui évaluent les propriétés de sécurité des systèmes.
- Le fait de disposer de résultats cohérents dans plusieurs domaines de travail améliore la cohérence.
- Réduction de la probabilité d'introduire des problèmes de sécurité dans les logiciels de production.
- Un délai plus court entre la détection et la remédiation grâce à une détection plus précoce des problèmes logiciels.
- Visibilité accrue des comportements systémiques ou répétés dans plusieurs domaines de travail, ce qui peut être utilisé pour apporter des améliorations à l'échelle de l'organisation.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Au fur et à mesure du développement de votre logiciel, adoptez divers mécanismes de test pour vous assurer que vous testez votre application à la fois pour les exigences fonctionnelles, basées sur la logique commerciale de votre application, et pour les exigences non fonctionnelles, qui sont axées sur la fiabilité, la performance et la sécurité de l'application.

Les tests statiques de sécurité des applications (SAST) analysent votre code source à la recherche de schémas de sécurité anormaux et fournissent des indications sur le code sujet aux défauts. Les tests SAST s'appuient sur des données statiques, telles que la documentation (spécifications des exigences, documentation de conception et spécifications de conception) et le code source de l'application, pour tester une série de problèmes de sécurité connus. Les analyseurs de code statique permettent d'accélérer l'analyse de gros volumes de code. Le groupe de qualité NIST propose une comparaison des analyseurs de sécurité du code source, qui comprend des outils open source pour les lecteurs de codes à octets et les lecteurs de code binaire.

Complétez vos tests statiques par des méthodes de sécurité des applications (DAST), qui consistent à effectuer des tests sur l'application en cours d'exécution afin d'identifier les comportements potentiellement inattendus. Les tests dynamiques peuvent détecter des problèmes potentiels qui ne

sont pas détectables par l'analyse statique. Les tests effectués aux stades du référentiel de code, de la build et du pipeline vous permettent de vérifier différents types de problèmes potentiels avant qu'ils ne s'introduisent dans votre code. Amazon CodeWhisperer fournit des recommandations sur le code, y compris l'analyse de la sécurité, dans l'IDE du créateur. Amazon CodeGuru Reviewer peut identifier les problèmes critiques, les problèmes de sécurité et les bogues difficiles à trouver pendant le développement de l'application, et fournit des recommandations pour améliorer la qualité du code.

L'atelier sur la sécurité pour les développeurs utilise des outils de développement AWS, tels que AWS CodeBuild, AWS CodeCommit, et AWS CodePipeline, pour l'automatisation de la chaîne de production qui comprend les méthodologies de test SAST et DAST.

Au fur et à mesure que vous progressez dans votre cycle de développement du logiciel, mettez en place un processus itératif qui comprend des révisions périodiques des applications avec votre équipe de sécurité. Les commentaires recueillis lors de ces examens de sécurité doivent être traités et validés dans le cadre de l'examen de l'état de préparation à la mise en production. Ces examens permettent de définir un solide niveau de sécurité des applications et fournissent aux concepteurs des commentaires exploitables pour résoudre les problèmes potentiels.

Étapes d'implémentation

- Implémentez des outils cohérents d'IDE, de révision du code et de CI/CD qui incluent des tests de sécurité.
- Réfléchissez à l'étape du cycle de développement du logiciel où il convient de bloquer les pipelines au lieu de simplement avertir les concepteurs que des problèmes doivent être résolus.
- L'atelier sur la sécurité pour les développeurs fournit un exemple d'intégration des tests statiques et dynamiques dans un pipeline de publication.
- La réalisation de tests ou d'analyses de code à l'aide d'outils automatisés, tels que Amazon CodeWhisperer intégré aux IDE des développeurs et Amazon CodeGuru Reviewer pour l'analyse du code lors de la validation, aide les concepteurs à obtenir des commentaires au bon moment.
- Lorsque vous utilisez AWS Lambda pour votre conception, vous pouvez utiliser Amazon Inspector pour analyser le code de l'application dans vos fonctions.
- L'Atelier CI/CD AWS fournit un point de départ pour construire des pipelines CI/CD sur AWS.
- Lorsque les tests automatisés sont inclus dans les pipelines CI/CD, vous devez utiliser un système de tickets pour suivre la notification et la résolution des problèmes logiciels.
- Pour les tests de sécurité susceptibles de donner lieu à des conclusions, un lien vers des conseils pour remédier à la situation aide les concepteurs à améliorer la qualité du code.

- Analysez régulièrement les résultats des outils automatisés afin de donner la priorité à la prochaine automatisation, à la formation des concepteurs ou à la campagne de sensibilisation.

Ressources

Documents connexes :

- Livraison et déploiement continus

- Partenaires de compétence AWS DevOps
- Partenaires de compétence en matière de sécurité d'AWS pour la sécurité des applications
- Choosing a Well-Architected CI/CD approach
- Monitoring CodeCommit events in Amazon EventBridge and Amazon CloudWatch Events (Surveillance des événements CodeCommit sur Amazon EventBridge et Amazon CloudWatch Events)
- Secrets detection in Amazon CodeGuru Review
- Accelerate deployments on AWS with effective governance
- Comment AWS aborde l'automatisation de déploiement sans intervention et en toute sécurité

Vidéos connexes :

- Hands-off: Automating continuous delivery pipelines at Amazon
- Automating cross-account CI/CD pipelines

Exemples connexes :

- Sensibilisation des développeurs au secteur
- Gouvernance AWS CodePipeline (GitHub)
- Atelier sur la sécurité pour les développeurs
- Atelier CI/CD AWS

SEC11-BP03 Réalisation de tests de pénétration réguliers

Effectuez régulièrement des tests de pénétration de votre logiciel. Ce mécanisme permet d'identifier les problèmes logiciels potentiels impossibles à détecter par des tests automatisés ou une révision manuelle du code. Il peut également vous aider à comprendre l'efficacité de vos contrôles de détection. Les tests de pénétration doivent tenter de déterminer si le logiciel peut être amené à fonctionner de manière inattendue, par exemple en exposant des données qui devraient être protégées ou en accordant des autorisations plus étendues que prévu.

Résultat souhaité : les tests de pénétration permettent de détecter, de remédier et de valider les propriétés de sécurité de votre application. Des tests de pénétration réguliers et programmés doivent être effectués dans le cadre du cycle de développement des logiciels (SDLC). Les résultats des tests de pénétration doivent être pris en compte avant le lancement du logiciel. Vous devez analyser les résultats des tests de pénétration pour déterminer s'il existe des problèmes qui pourraient être détectés grâce à l'automatisation. Le fait de disposer d'un processus de test de pénétration régulier et reproductible, qui comprend un mécanisme de commentaires actif, permet d'éclairer les conseils donnés aux concepteurs et d'améliorer la qualité des logiciels.

Anti-modèles courants :

- Les tests de pénétration ne concernent que les problèmes de sécurité connus ou répandus.
- Tests de pénétration d'applications sans outils et bibliothèques tiers dépendants.
- Uniquement des tests de pénétration pour les problèmes de sécurité des packages, et non l'évaluation de la logique métier implémentée.

Avantages liés au respect de cette bonne pratique :

- Confiance accrue dans les propriétés de sécurité du logiciel avant sa diffusion.
- Possibilité d'identifier des modèles d'application privilégiés, ce qui permet d'améliorer la qualité des logiciels.
- Une boucle de rétroaction permettant d'identifier plus tôt dans le cycle de développement où l'automatisation ou une formation supplémentaire peuvent améliorer les propriétés de sécurité des logiciels.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Le test de pénétration est un exercice de test de sécurité structuré dans lequel vous exécutez des scénarios de faille de sécurité planifiés afin de détecter des problèmes, d'y remédier et de valider les contrôles de sécurité. Les tests de pénétration commencent par une reconnaissance, au cours de laquelle des données sont recueillies sur la base de la conception actuelle de l'application et de ses dépendances. Une liste de scénarios de test spécifiques à la sécurité est élaborée et exécutée. L'objectif principal de ces tests est de découvrir les problèmes de sécurité de votre application, qui pourraient être exploités pour obtenir un accès involontaire à votre environnement ou un accès non autorisé aux données. Vous devez effectuer des tests de pénétration lorsque vous lancez de nouvelles fonctionnalités, ou chaque fois que votre application a subi des changements majeurs en matière de fonction ou d'implémentation technique.

Vous devez identifier l'étape la plus appropriée du cycle de développement pour effectuer des tests de pénétration. Ces tests doivent avoir lieu suffisamment tard pour que la fonctionnalité du système soit proche de l'état final prévu, mais avec suffisamment de temps pour remédier aux éventuels problèmes.

Étapes d'implémentation

- Prévoyez un processus structuré pour l'étendue des tests de pénétration. Le fait de baser ce processus sur le modèle de menace est un bon moyen de maintenir le contexte.
- Identifiez l'endroit approprié dans le cycle de développement pour effectuer des tests de pénétration. Ce délai doit être respecté lorsque les changements attendus dans l'application sont minimes, mais qu'il reste suffisamment de temps pour mettre en œuvre des mesures correctives.
- Formez vos créateurs sur ce qu'il faut attendre des résultats des tests de pénétration et sur la manière d'obtenir des informations sur les mesures correctives.
- Utilisez des outils pour accélérer le processus de test de pénétration en automatisant les tests courants ou reproductibles.
- Analysez les résultats des tests de pénétration afin d'identifier les problèmes de sécurité systémiques et utilisez ces données pour effectuer des tests automatisés supplémentaires et former en permanence les créateurs.

Ressources

Bonnes pratiques associées :

- SEC11-BP01 Formation à la sécurité des applications
- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication

Documents connexes :

- Le test de pénétration AWS fournit des conseils détaillés pour les tests de pénétration sur AWS
- Accelerate deployments on AWS with effective governance
- Partenaires AWS disposant de la compétence Sécurité
- Modernize your penetration testing architecture on AWS Fargate
- AWS Fault Injection Simulator

Exemples connexes :

- Automate API testing with AWS CodePipeline (GitHub)
- Automated security helper (GitHub)

SEC11-BP04 Révisions de code manuelles

Procédez à une révision manuelle du code des logiciels que vous produisez. Ce processus permet de vérifier que la personne qui a écrit le code n'est pas la seule à en contrôler la qualité.

Résultat souhaité : l'inclusion d'une étape de révision manuelle du code au cours du développement permet d'améliorer la qualité du logiciel conçu, de renforcer les compétences des membres les moins expérimentés de l'équipe et d'identifier les domaines dans lesquels l'automatisation peut être utilisée. Les révisions de code manuelles peuvent être soutenues par des outils et des tests automatisés.

Anti-modèles courants :

- Ne pas effectuer de révision de code avant le déploiement.
- Faire rédiger et réviser le code par la même personne.
- Ne pas utiliser l'automatisation pour assister ou orchestrer les révisions de code.
- Ne pas former les créateurs à la sécurité des applications avant qu'ils ne procèdent à la révision du code.

Avantages liés au respect de cette bonne pratique :

- Amélioration de la qualité du code.
- Amélioration de la cohérence de développement du code grâce à la réutilisation d'approches communes.
- Réduction du nombre de problèmes découverts lors des tests de pénétration et des étapes ultérieures.
- Amélioration du transfert de connaissances au sein de l'équipe.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

L'étape de révision doit être implémentée dans le cadre du flux global de gestion du code. Les spécificités dépendent de l'approche utilisée pour les branches, les demandes d'extraction et la fusion. Vous utilisez peut-être AWS CodeCommit ou des solutions tierces telles que GitHub, GitLab ou Bitbucket. Quelle que soit la méthode utilisée, il est important de vérifier que vos processus exigent la révision du code avant qu'il ne soit déployé dans un environnement de production. L'utilisation d'outils tels que Amazon CodeGuru Reviewer peut faciliter l'orchestration du processus de révision de code.

Étapes d'implémentation

- Implémentez une étape de révision manuelle dans le cadre de votre flux de gestion du code et procédez à cette révision avant de poursuivre.
- Envisagez Amazon CodeGuru Reviewer pour gérer et vous aider dans les révisions de code.
- Implémentez un flux d'approbation qui exige qu'une révision de code soit achevée avant que le code puisse passer à l'étape suivante.
- Vérifiez qu'il existe un processus permettant d'identifier les problèmes découverts lors des révisions manuelles du code et qui pourraient être détectés automatiquement.
- Intégrez l'étape de révision manuelle du code d'une manière qui s'aligne sur vos pratiques de développement du code.

Ressources

Bonnes pratiques associées :

- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication

Documents connexes :

- Utilisation des demandes d'extraction dans les référentiels AWS CodeCommit
- Utilisation des modèles de règles d'approbation dans AWS CodeCommit
- À propos des demandes de tirage (pull requests)
- Automate code reviews with Amazon CodeGuru Reviewer
- Automating detection of security vulnerabilities and bugs in CI/CD pipelines using Amazon CodeGuru Reviewer CLI

Vidéos connexes :

- Continuous improvement of code quality with Amazon CodeGuru

Exemples connexes :

- Atelier sur la sécurité pour les développeurs

SEC11-BP05 Centralisation des services pour les packages et les dépendances

Fournissez des services centralisés aux équipes de créateurs pour l'obtention de packages logiciels et d'autres dépendances. Cela permet de valider les packages avant qu'ils ne soient incorporés au logiciel que vous écrivez, et fournit une source de données pour l'analyse du logiciel utilisé dans votre entreprise.

Résultat souhaité : un logiciel est composé d'un ensemble d'autres packages logiciels en plus du code qui est en train d'être écrit. Cela simplifie la consommation des implémentations de fonctionnalités utilisées de manière répétée, telles qu'un analyseur JSON ou une bibliothèque de chiffrement. La centralisation logique des sources de ces packages et dépendances offre aux équipes de sécurité un mécanisme de validation des propriétés des packages avant leur utilisation. Cette approche réduit également le risque qu'un problème inattendu soit causé par une modification d'un package existant, ou par des équipes de créateurs incluant des packages arbitraires provenant directement d'Internet. Utilisez cette approche en conjonction avec les flux de tests manuels et automatisés pour accroître la confiance dans la qualité du logiciel en cours de développement.

Anti-modèles courants :

- Extraction de packages à partir de référentiels arbitraires sur Internet.
- Ne pas tester les nouveaux packages avant de les mettre à la disposition des créateurs.

Avantages liés au respect de cette bonne pratique :

- Meilleure compréhension des packages utilisés dans le logiciel en cours de création
- Possibilité d'informer les équipes responsables de la charge de travail lorsqu'un package doit être mis à jour en fonction de la compréhension de qui utilise quoi.
- Réduire le risque qu'un package présentant des problèmes soit inclus dans votre logiciel.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Fournissez des services centralisés pour les packages et les dépendances d'une manière simple à utiliser pour les créateurs. Les services centralisés sont logiquement centraux plutôt que d'être implémentés sous la forme d'un système monolithique. Cette approche vous permet de fournir des services de manière à répondre aux besoins de vos concepteurs. Vous devez implémenter une méthode efficace pour ajouter des packages au référentiel lorsque des mises à jour sont effectuées ou que de nouvelles exigences apparaissent. Des services AWS tels que AWS CodeArtifact ou des solutions de partenaires AWS similaires permettent de fournir cette capacité.

Étapes d'implémentation :

- Implémentez un service de référentiel centralisé et logique, disponible dans tous les environnements où des logiciels sont développés.
- Prévoir l'accès au référentiel dans le cadre de la procédure d'attribution du Compte AWS.
- Concevez une automatisation pour tester les packages avant qu'ils ne soient publiés dans un référentiel.
- Conservez des métriques concernant les packages, les langages et les équipes les plus couramment utilisés et ayant subi le plus grand nombre de changements.
- Prévoyez un mécanisme automatisé permettant aux équipes de créateurs de demander de nouveaux packages et de fournir des commentaires.
- Analysez régulièrement les packages de votre référentiel afin d'identifier l'impact potentiel des problèmes récemment découverts.

Ressources

Bonnes pratiques associées :

- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication

Documents connexes :

- Accelerate deployments on AWS with effective governance
- Tighten your package security with CodeArtifact Package Origin Control toolkit
- Detecting security issues in logging with Amazon CodeGuru Reviewer
- Supply chain Levels for Software Artifacts (SLSA)

Vidéos connexes :

- Proactive security: Considerations and approaches
- The AWS Philosophy of Security (re:Invent 2017)
- When security, safety, and urgency all matter: Handling Log4Shell

Exemples connexes :

- Pipeline de publication de packages multirégionaux (GitHub)
- Publication de modules Node.js sur AWS CodeArtifact à l'aide de AWS CodePipeline (GitHub)
- Publication de packages AWS CDK Java CodeArtifact (GitHub)
- Distribuer des packages .NET NuGet privés avec AWS CodeArtifact (GitHub)

SEC11-BP06 Déploiement programmatique de logiciels

Dans la mesure du possible, procédez à des déploiements de logiciels par programme. Cette approche réduit la probabilité qu'un déploiement échoue ou qu'une erreur humaine entraîne un problème inattendu.

Résultat souhaité : éloigner les personnes des données est un principe clé pour construire en toute sécurité dans le AWS Cloud. Ce principe s'applique également à la manière dont vous déployez votre logiciel.

Ne pas dépendre d'individus pour déployer un logiciel vous permet d'être certain que ce que vous déployez correspond à ce que vous avez testé, et que le déploiement est effectué de manière cohérente à chaque fois. Il ne doit pas être nécessaire de modifier un logiciel afin qu'il fonctionne dans différents environnements. L'utilisation des principes du développement d'applications à douze facteurs, en particulier l'externalisation de la configuration, vous permet de déployer le même code dans plusieurs environnements sans avoir à le modifier. Le chiffrement de la signature des packages logiciels permet de vérifier que rien n'a changé d'un environnement à l'autre. Le résultat global de cette approche est de réduire les risques dans votre processus de changement et d'améliorer la cohérence des versions du logiciel.

Anti-modèles courants :

- Déploiement manuel d'un logiciel en production.
- Modification manuelle d'un logiciel pour l'adapter à des environnements différents.

Avantages liés au respect de cette bonne pratique :

- Confiance accrue dans le processus de lancement des logiciels.
- Réduction du risque que l'échec d'une modification affecte l'entreprise.
- Augmentation de la cadence de lancement en raison de la diminution du risque de changement.
- Capacité de restauration automatique en cas d'événements inattendus au cours du déploiement.
- Capacité à prouver par chiffrement que le logiciel testé est celui qui est déployé.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Créez la structure de votre Compte AWS de manière à supprimer la récurrence de l'accès de personnes à partir d'environnements et utilisez des outils CI/CD pour effectuer des déploiements. Concevez vos applications de manière à ce que les données de configuration spécifiques à l'environnement soient obtenues à partir d'une source externe, telle que AWS Systems Manager Parameter Store. Signez les packages après les avoir testés et validez ces signatures lors du déploiement. Configurez vos pipelines CI/CD pour transmettre le code de l'application et utilisez des tests Canary pour confirmer le succès du déploiement. Utilisez des outils tels que AWS CloudFormation ou AWS CDK pour définir votre infrastructure, puis utilisez AWS CodeBuild et AWS CodePipeline pour effectuer des opérations CI/CD.

Étapes d'implémentation

- Créez des pipelines CI/CD bien définis pour rationaliser le processus de déploiement.
- Utilisez AWS CodeBuild et AWS Code Pipeline pour fournir une capacité CI/CD afin de faciliter l'intégration des tests de sécurité dans vos pipelines.
- Suivez les conseils sur la séparation des environnements dans le livre blanc Organisation de votre environnement AWS à l'aide de plusieurs comptes.
- Vérifiez que personne n'a accès aux environnements dans lesquels des charges de travail de production sont en cours d'exécution.
- Architecturez vos applications de manière à prendre en charge l'externalisation des données de configuration.
- Envisagez un modèle de déploiement bleu/vert.
- Implémentez des tests Canary pour valider la réussite du déploiement du logiciel.
- Utilisez des outils cryptographiques tels AWS Signer ou AWS Key Management Service (AWS KMS) pour signer et vérifier les packages logiciels que vous déployez.

Ressources

Bonnes pratiques associées :

- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication

Documents connexes :

- Atelier CI/CD AWS
- Accelerate deployments on AWS with effective governance
- Automatisation de déploiements sécurisés sans intervention
- Code signing using AWS Certificate Manager Private CA and AWS Key Management Service asymmetric keys
- Code Signing, a Trust and Integrity Control for AWS Lambda

Vidéos connexes :

- Hands-off: Automating continuous delivery pipelines at Amazon

Exemples connexes :

- Déploiements bleu/vert avec AWS Fargate

SEC11-BP07 Évaluation régulière des caractéristiques de sécurité des pipelines

Appliquez les principes du pilier Sécurité Well-Architected à vos pipelines, en accordant une attention particulière à la séparation des autorisations. Évaluez régulièrement les caractéristiques de sécurité de votre infrastructure de pipelines. Une gestion efficace de la sécurité des pipelines vous permet d'assurer la sécurité des logiciels qui transitent par ces pipelines.

Résultat souhaité : les pipelines utilisés pour construire et déployer votre logiciel doivent suivre les mêmes pratiques recommandées que toute autre charge de travail dans votre environnement. Les tests implémentés dans les pipelines ne doivent pas être modifiables par les créateurs qui les utilisent. Les pipelines ne doivent disposer que des autorisations nécessaires aux déploiements qu'ils effectuent et doivent implémenter des protections pour éviter de déployer dans les mauvais environnements. Les pipelines ne devraient pas s'appuyer sur des informations d'identification à long terme et devraient être configurés pour émettre un état afin que l'intégrité des environnements de création puisse être validée.

Anti-modèles courants :

- Tests de sécurité qui peuvent être contournés par les créateurs.
- Des autorisations trop larges pour les pipelines de déploiement.
- Les pipelines ne sont pas configurés pour valider les entrées.
- Ne pas passer régulièrement en revue les autorisations associées à votre infrastructure CI/CD.
- Utilisation d'informations d'identification à long terme ou codées en dur.

Avantages liés au respect de cette bonne pratique :

- Une plus grande confiance dans l'intégrité du logiciel conçu et déployé par le biais des pipelines.
- Possibilité d'interrompre un déploiement en cas d'activité suspecte.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Le fait de débuter avec des services CI/CD gérés qui prennent en charge les rôles IAM réduit le risque de fuite d'informations d'identification. L'application des principes de Pilier Sécurité à l'infrastructure de votre pipeline CI/CD peut vous aider à déterminer les améliorations à apporter en matière de sécurité. Suivre les recommandations de l'Architecture de référence des pipelines de déploiement d'AWS constitue un bon point de départ pour construire vos environnements CI/CD. L'examen régulier de l'implémentation des pipelines et l'analyse des journaux à la recherche de comportements inattendus peuvent vous aider à comprendre les schémas d'utilisation des pipelines utilisés pour déployer des logiciels.

Étapes d'implémentation

- Commencez par suivre les recommandations de l'Architecture de référence des pipelines de déploiement d'AWS.
- Envisagez d'utiliser AWS IAM Access Analyzer pour générer de manière programmatique des politiques IAM de moindre privilège pour les pipelines.
- Intégrez des fonctions de surveillance et d'alerte à vos pipelines afin d'être informé des activités inattendues ou anormales, car les services Amazon EventBridge gérés AWS vous permettent d'acheminer les données vers des cibles telles que AWS Lambda ou Amazon Simple Notification Service (Amazon SNS).

Ressources

Documents connexes :

- Architecture de référence des pipelines de déploiement d'AWS
- Surveillance d'AWS CodePipeline
- Bonnes pratiques de sécurité pour AWS CodePipeline

Exemples connexes :

- DevOps monitoring dashboard (GitHub)

SEC11-BP08 Création d'un programme permettant aux équipes responsables de la charge de travail de s'approprier les mécanismes de sécurité

Créez un programme ou un mécanisme qui permette aux équipes de créateurs de prendre des décisions en matière de sécurité pour les logiciels qu'ils créent. Votre équipe de sécurité doit bien sûr procéder à un examen de ces décisions afin de les valider. Mais le fait de rendre les équipes de créateurs responsables de la sécurité permet d'élaborer des charges de travail plus rapides et plus sûres. Ce mécanisme favorise également une culture de responsabilisation qui a un impact positif sur le fonctionnement des systèmes que vous construisez.

Résultat souhaité : pour rendre les équipes de créateurs responsables de la sécurité et décisionnaires, vous pouvez soit former les créateurs aux implications de la sécurité, soit compléter leur formation par des personnes chargées de la sécurité, intégrées ou associées aux équipes de créateurs. Les deux approches sont pertinentes et permettent à l'équipe de prendre des décisions de meilleure qualité en matière de sécurité plus tôt dans le cycle de développement. Ce modèle de responsabilité repose sur la formation à la sécurité des applications. En commençant par le modèle de menace correspondant à une charge de travail donnée, il est possible d'axer le design thinking sur le contexte approprié. Disposer d'une communauté de créateurs axés sur la sécurité ou d'un groupe d'ingénieurs en sécurité travaillant avec des équipes de créateurs présente un autre avantage : la possibilité de comprendre plus en profondeur comment les logiciels sont écrits. Cette compréhension vous aide à déterminer les prochains domaines d'amélioration de votre capacité d'automatisation.

Anti-modèles courants :

- Laisser à une équipe de sécurité le soin de prendre toutes les décisions relatives à la conception de la sécurité.
- Ne pas tenir compte des exigences de sécurité suffisamment tôt dans le processus de développement.
- Ne pas recueillir de commentaires des créateurs et des responsables de la sécurité sur le fonctionnement du programme.

Avantages liés au respect de cette bonne pratique :

- Réduction du temps nécessaire à la réalisation des examens de sécurité.
- Réduction des problèmes de sécurité qui ne sont détectés qu'au stade de l'examen de la sécurité.

- Amélioration de la qualité globale du logiciel en cours d'écriture.
- Possibilité d'identifier et de comprendre les problèmes systémiques ou les domaines d'amélioration à forte valeur ajoutée.
- Réduction de la quantité de travail à refaire en raison des conclusions de l'examen de sécurité.
- Amélioration de la perception de la fonction de sécurité.

Niveau de risque exposé si cette bonne pratique n'est pas respectée : faible

Directives d'implémentation

Commencez par suivre les conseils de SEC11-BP01 Formation à la sécurité des applications. Identifiez ensuite le modèle opérationnel du programme qui vous semble le plus adapté à votre organisation. Les deux principaux modèles consistent à former les créateurs ou à intégrer les responsables de la sécurité dans les équipes de créateurs. Une fois que vous avez décidé de l'approche initiale, vous devez mener un projet pilote avec une seule équipe ou un petit groupe d'équipes de charge de travail afin de prouver que le modèle fonctionne pour votre organisation. Le soutien de la direction de l'organisation en matière de construction et de sécurité contribue à la mise en œuvre et à la réussite du programme. Lors de la création de ce programme, il est important de choisir des métriques qui peuvent être utilisées pour montrer la valeur du programme. Apprendre de la manière dont AWS les autres ont abordé ce problème est une bonne expérience d'apprentissage. Cette bonne pratique est très axée sur le changement organisationnel et la culture. Les outils que vous utilisez doivent favoriser la collaboration entre les créateurs et les responsables de la sécurité.

Étapes d'implémentation

- Commencez par former vos créateurs à la cybersécurité des applications.
- Créer une communauté et un programme d'intégration pour former les créateurs.
- Choisissez un nom pour le programme. Les termes « tuteur », « champion » ou « défenseur » sont couramment utilisés.
- Identifier le modèle à utiliser : former des créateurs, intégrer des ingénieurs en sécurité ou avoir des rôles de sécurité connexes.
- Identifier les sponsors du projet parmi les responsables de la sécurité, les créateurs et éventuellement d'autres groupes concernés.
- Suivez les métriques concernant le nombre de personnes impliquées dans le programme, le temps nécessaire aux examens et les commentaires des créateurs et des responsables de la sécurité. Utilisez ces métriques pour apporter des améliorations.

Ressources

Bonnes pratiques associées :

- SEC11-BP01 Formation à la sécurité des applications
- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication

Documents connexes :

- How to approach threat modeling
- How to think about cloud security governance

Vidéos connexes :

- Proactive security: Considerations and approaches

Conclusion

La sécurité est un effort permanent. Lorsque des incidents surviennent, ils doivent être traités comme des occasions d'améliorer la sécurité de l'architecture. De solides contrôles d'authentification et d'autorisation, l'automatisation des réponses aux événements de sécurité, la protection de l'infrastructure sur plusieurs niveaux, ainsi que le chiffrement des données correctement catégorisées permettent de disposer d'une défense solide et étendue que chaque entreprise doit mettre en œuvre. Cet effort est facilité par les fonctions accessibles par programmation et les fonctions et services AWS présentés dans ce document.

AWS s'efforce de vous aider à concevoir et à exploiter des architectures qui protègent les informations, les systèmes et les ressources tout en apportant de la valeur ajoutée.

Participants

Les personnes et organisations suivantes ont participé à la préparation du présent document :

- Sarita Dharankar, responsable du pilier Sécurité, Well-Architected, Amazon Web Services
- Adam Cerini, architecte principal de solution, Amazon Web Services
- Bill Shinn, mandataire, Bureau du RSSI, Amazon Web Services
- Brigid Johnson, responsable senior du développement logiciel, AWS Identity, Amazon Web Services
- Byron Pogson, architecte principal de solution, Amazon Web Services
- Charlie Hammell, architecte d'entreprise principal, Amazon Web Services
- Darran Boyd, architecte principal de solutions de sécurité, Services financiers, Amazon Web Services
- Dave Walker, architecte de solutions spécialiste principal, sécurité et conformité, Amazon Web Services
- John Formento, architecte principal de solution, Amazon Web Services
- Paul Hawkins, mandataire, Bureau du RSSI, Amazon Web Services
- Sam Elmalak, responsable technologique principal, Amazon Web Services
- Pat Gaw, consultant mandataire en sécurité, Amazon Web Services
- Daniel Begimher, consultant principal, sécurité, Amazon Web Services
- Danny Cortegaca, architecte principal de solutions de sécurité, Amazon Web Services
- Ana Malhotra, architecte de solutions de sécurité, Amazon Web Services
- Debashis Das, mandataire, Bureau du RSSI, Amazon Web Services
- Reef Dsouza, architecte principal de solutions, Amazon Web Services
- Brad Burnett, architecte de solutions de sécurité, identités, Amazon Web Services
- Anna McAbee, architecte senior des solutions de sécurité, détection des menaces et réponse aux incidents, Amazon Web Services
- Jason Garman, architecte principal des solutions de sécurité, Amazon Web Services

Autres lectures

Pour obtenir de l'aide, consultez les ressources suivantes :

- Livre blanc AWS Well-Architected Framework
- Centre d'architecture AWS

Révisions du document

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

Modification	Description	Date
Mises à jour des conseils sur les bonnes pratiques	Les bonnes pratiques ont été mises à jour pour inclure de nouveaux conseils dans les domaines suivants : Gestion sécurisée de votre charge de travail et Protection des données en transit.	December 6, 2023
Mises à jour des conseils sur les bonnes pratiques	Mises à jour majeures des conseils et bonnes pratiques en matière de réponse aux incidents. De nombreuses bonnes pratiques en matière de préparation ont été mises à jour. Deux nouveaux domaines ont été ajoutés à la réponse aux incidents : Opérations et Activité postérieure à l'incident. Ajout d'une nouvelle bonne pratique SEC10-BP08 Établir un cadre pour tirer des enseignements des incidents.	October 3, 2023
Mises à jour des conseils sur les bonnes pratiques	Les bonnes pratiques ont été mises à jour pour inclure de nouveaux conseils dans les domaines suivants : Prepare et Simulate.	July 13, 2023

Mises à jour du nouveau cadre.	Les bonnes pratiques ont été mises à jour avec des recommandations et de nouvelles bonnes pratiques. Ajout d'un nouveau domaine de bonnes pratiques en matière de sécurité des applications (AppSec).	April 10, 2023
Livre blanc mis à jour	Les bonnes pratiques ont été mises à jour avec de nouvelles recommandations en matière d'implémentation.	December 15, 2022
Livre blanc mis à jour	Développement des bonnes pratiques et ajout de plans d'amélioration.	October 20, 2022
Mise à jour mineure	Mise à jour des informations IAM pour refléter les bonnes pratiques actuelles.	June 28, 2022
Mise à jour mineure	Ajout d'informations AWS PrivateLink supplémentaires et correction des liens corrompus .	May 19, 2022
Mise à jour mineure	Ajout de AWS PrivateLink.	May 6, 2022
Mise à jour mineure	Suppression du langage non inclusif.	April 22, 2022
Mise à jour mineure	Ajout d'informations sur VPC Network Access Analyzer.	February 2, 2022
Mise à jour mineure	Ajout du pilier Durabilité dans l'introduction.	December 2, 2021
Mise à jour mineure	Correction d'un lien rompu.	May 27, 2021

Mise à jour mineure	Modifications rédactionnelles dans tout le document.	May 17, 2021
Mise à jour majeure	Ajout d'une section sur la gouvernance, ajout de détails à diverses sections, ajout de nouvelles fonctionnalités et services dans tout le document.	May 7, 2021
Mise à jour mineure	Mise à jour des liens.	March 10, 2021
Mise à jour mineure	Correction d'un lien rompu.	July 15, 2020
Mises à jour pour le nouveau cadre	Mise à jour des conseils sur la gestion des comptes, des identités et des autorisations.	July 8, 2020
Mises à jour pour le nouveau cadre	Mise à jour pour élargir les conseils dans tous les domaines, ainsi que les nouvelles bonnes pratiques , les services et les fonctionn alités.	April 30, 2020
Livre blanc mis à jour	Mises à jour destinées à refléter les nouveaux services et fonctionnalités AWS et les mises à jour des références.	July 1, 2018
Livre blanc mis à jour	Mise à jour de la section Configuration et maintenance de la sécurité du système pour refléter les nouveaux services et les nouvelles fonctionnalités AWS.	May 1, 2017

Publication initiale	Pilier Sécurité - AWS Well-Architected Framework publié.	November 1, 2016

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'AWSet 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'AWSenvers ses clients sont déterminées par les contrats AWS. Le présent document ne fait pas partie d'un contrat entre AWS et ses clients, et ne le modifie pas.