AWS Well-Architected Framework

Pilier Sécurité

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

Pilier Sécurité: AWS Well-Architected Framework

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

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

Table of Contents

Résumé et introduction 1
Introduction 1
Bases de la sécurité 3
Principes de conception 3
Définition 4
Responsabilité partagée 4
Gouvernance 7
AWSGestion et séparation des comptes 8
SEC01-BP01 Séparer les charges de travail à l'aide de comptes 10
SEC01-BP02 Sécuriser l'utilisateur racine et les propriétés du compte 13
Gestion sécurisée de votre charge de travail 19
SEC01-BP03 Identifier et valider les objectifs de contrôle 21
SEC01-BP04 Connaître les menaces et recommandations en matière de sécurité 23
SEC01-BP05 Réduire la portée de la gestion de la sécurité 25
SEC01-BP06 Automatiser le déploiement des contrôles de sécurité standard 28
SEC01-BP07 Identifier les menaces et hiérarchiser les atténuations à l'aide d'un modèle de menaces 31
SEC01-BP08 Évaluer et mettre en œuvre régulièrement de nouveaux services et de nouvelles fonctions de sécurité 36
Gestion des identités et des accès 39
Gestion des identités 39
SEC02-BP01 Utiliser de solides mécanismes d'authentification 40
SEC02-BP02 Utiliser des informations d'identification temporaires 44
SEC02-BP03 Stocker et utiliser des secrets en toute sécurité 48
SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé 55
SEC02-BP05 Contrôler et effectuer régulièrement une rotation des informations d'identification 60
SEC02-BP06 Utiliser des groupes d'utilisateurs et des attributs 62
Gestion des autorisations 66
SEC03-BP01 Définir les conditions d'accès 68
SEC03-BP02 Accorder un accès selon le principe du moindre privilège 72
SEC03-BP03 Établir un processus d'accès d'urgence 76
SEC03-BP04 Limiter les autorisations au minimum requis en permanence 85
SEC03-BP05 Définir des barrières de protection des autorisations de votre organisation 87

SEC03-BP06 Gérer l’accès en fonction du cycle de vie 92
SEC03-BP07 Analyser l’accès public et intercompte 94
SEC03-BP08 Partager des ressources en toute sécurité au sein de votre organisation 97
SEC03-BP09 Partager des ressources en toute sécurité avec un tiers 101
Détection 106
SEC04-BP01 Configurer une journalisation de service et d’application 107
Directives d’implémentation 11
Ressources 12
SEC04-BP02 Capturer les journaux, les résultats et les métriques dans des emplacements standardisés 112
Directives d’implémentation 11
Étapes d’implémentation 22
Ressources 12
SEC04-BP03 Corréler et enrichir les alertes de sécurité 116
Directives d’implémentation 11
Ressources 12
SEC04-BP04 Lancer la correction pour les ressources non conformes 119
Directives d’implémentation 11
Ressources 12
Protection de l’infrastructure 124
Protection des réseaux 125
SEC05-BP01 Créer des couches réseau 126
SEC05-BP02 Contrôler le flux de trafic au sein de vos couches réseau 129
SEC05-BP03 Mettre en œuvre une protection basée sur l'inspection 132
SEC05-BP04 Automatiser la protection du réseau 136
Protection du calcul 139
SEC06-BP01 Gérer les vulnérabilités 139
SEC06-BP02 Provisionner des calculs à partir d'images renforcées 143
SEC06-BP03 Réduire la gestion manuelle et l’accès interactif 146
SEC06-BP04 Valider l'intégrité du logiciel 149
SEC06-BP05 Automatiser la protection du calcul 151
Protection des données 155
Classification des données 155
SEC07-BP01 Comprendre votre schéma de classification des données 155
SEC07-BP02 Appliquer des contrôles de protection des données en fonction de la sensibilité des données 158

SEC07-BP03 Automatiser l'identification et la classification 161
SEC07-BP04 Définir la gestion évolutive du cycle de vie des données 164
Protection des données au repos 167
SEC08-BP01 Mise en œuvre de la gestion sécurisée des clés 169
SEC08-BP02 Appliquer le chiffrement au repos 172
SEC08-BP03 Automatiser la protection des données au repos 175
SEC08-BP04 Appliquer le contrôle d'accès 179
Protection des données en transit 183
SEC09-BP01 Implémenter la gestion sécurisée des clés et des certificats 184
SEC09-BP02 Application du chiffrement en transit 188
SEC09-BP03 Authentifier les communications réseau 190
Réponse aux incidents 196
AWSRéponse aux incidents 196
Objectifs de conception de la réponse cloud 197
Préparation 199
SEC10-BP01 Identifier les postes clés internes ainsi que les principales ressources externes 199
SEC10-BP02 Développer des plans de gestion des incidents 203
SEC10-BP03 Préparer les fonctionnalités d'analyse poussée 207
SEC10-BP04 Développer et tester des playbooks de réponse aux incidents de sécurité 211
SEC10-BP05 Préallouer les accès 213
SEC10-BP06 Prédéployer les outils 217
SEC10-BP07 Exécuter des simulations 220
Opérations 222
Activité postérieure à l'incident 223
SEC10-BP08 Établir un cadre pour tirer des enseignements des incidents 224
Sécurité des applications 227
SEC11-BP01 Formation à la sécurité des applications 228
Directives d'implémentation 11
Ressources 12
SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication 232
Directives d'implémentation 11
Ressources 12
SEC11-BP03 Réalisation de tests de pénétration réguliers 236
Directives d'implémentation 11

Ressources 12
SEC11-BP04 Mener des examens de code 239
Directives d'implémentation 11
Ressources 12
SEC11-BP05 Centralisation des services pour les packages et les dépendances 242
Directives d'implémentation 11
Ressources 12
SEC11-BP06 Déploiement programmatique de logiciels 244
Directives d'implémentation 11
Ressources 12
SEC11-BP07 Évaluation régulière des caractéristiques de sécurité des pipelines 248
Directives d'implémentation 11
Ressources 12
SEC11-BP08 Création d'un programme permettant aux équipes responsables de la charge de travail de s'approprier les mécanismes de sécurité 251
Directives d'implémentation 11
Ressources 12
Conclusion 254
Collaborateurs 255
Suggestions de lecture 257
Révisions du document 258
Avis 262
AWS Glossaire 263

Pilier Sécurité - AWS Well-Architected Framework

Date de publication : 6 novembre 2024 (Révisions du document)

Ce document porte sur le pilier Sécurité du cadre 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

Le cadre AWS Well-Architected Framework vous permet de comprendre les avantages et inconvénients des décisions que vous prenez lors de la création de 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 permettra de 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 de la sécurité

Le pilier de sécurité décrit comment tirer parti des technologies cloud pour protéger les données, les systèmes et les actifs de manière à améliorer votre posture 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 :

- Mise en place d'une base identitaire solide : appliquez le principe du moindre privilège et mettez en œuvre la séparation des tâches avec une 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.
- Maintien de la traçabilité : supervisez, alertez et auditez 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 défensive en profondeur 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 de sécurité : les mécanismes de sécurité automatisés basés sur le logiciel améliorent votre capacité à évoluer plus rapidement et de manière plus économique 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, le cas échéant.
- Protéger l'accès aux données : utilisez des mécanismes et des 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 événements de sécurité : préparez-vous à un incident en mettant en place une politique et des processus de gestion et d'investigation en matière d'incidents qui correspondent

aux exigences de votre organisation. 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 de la sécurité
- Gestion des identités et des accès
- Détection
- Protection de l'infrastructure
- Protection des données
- Intervention en cas d'incidents
- Sécurité des applications

Responsabilité partagée

La sécurité et la conformité sont la responsabilité partagée d'AWS et du 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 d'AWS « Sécurité du cloud » : AWS est responsable de la protection de l'infrastructure qui fait fonctionner tous les services offerts dans le Cloud AWS. Cette infrastructure

est composée du matériel, des logiciels, du réseau et des installations exécutant les services cloud AWS.

Responsabilité du client « Sécurité dans le cloud » : la responsabilité du client sera déterminée par les services AWS Cloud qu'il choisit. 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.

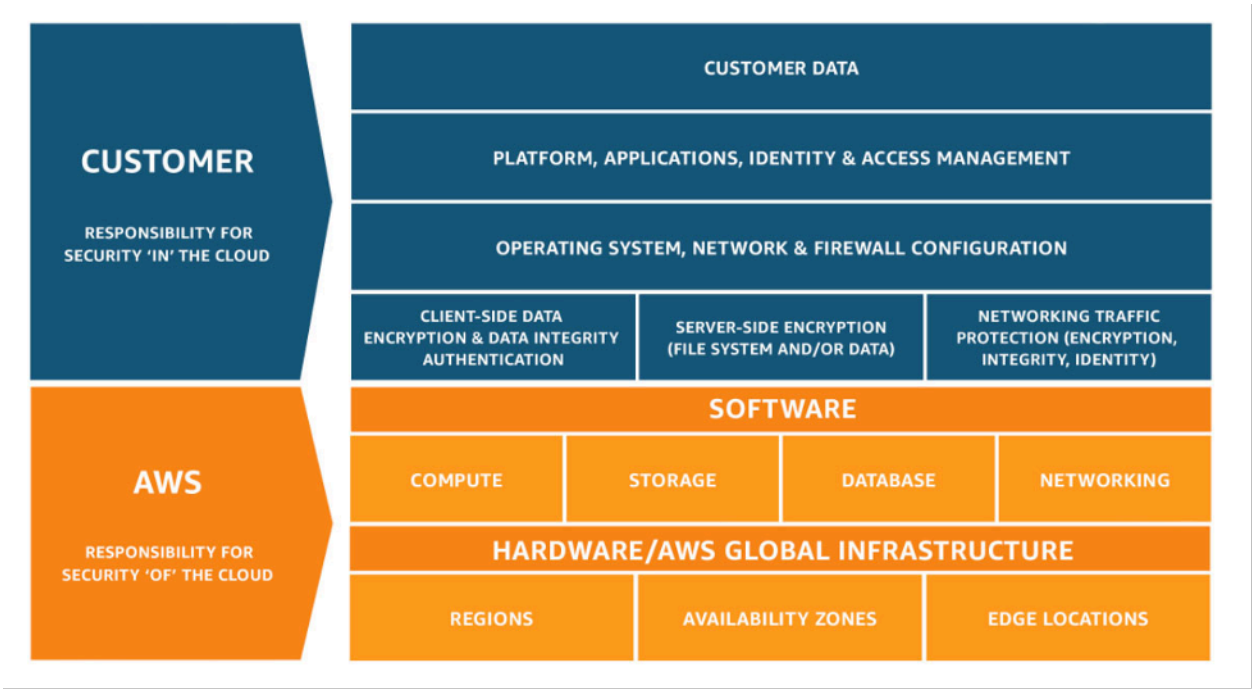


Figure 1 : Modèle de responsabilité partagée AWS

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 dont 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.
  - Pour les services AWS gérés fonctionnant sur des architectures à locataire unique (comme Amazon ElastiCache, Amazon RDS et Amazon OpenSearch Service), la responsabilité de la gestion des correctifs est partagée comme suit :
    - Responsabilité d'AWS : identifier les vulnérabilités, développer et valider les correctifs, publier les correctifs dans le respect du SLA de l'application de correctifs du service et informer les clients des mises à jour disponibles via le mécanisme de notification documenté du service.
    - Responsabilité du client : passer en revue les mises à jour disponibles et faciliter l'application de correctifs en sélectionnant les fenêtres de maintenance, en appliquant les mises à jour du service ou en planifiant les redémarrages requis dans les délais communiqués par AWS.
  - Pour les services gérés par AWS fonctionnant sur des architectures à locataires multiples (comme Amazon ElastiCache sans serveur, Amazon DynamoDB et Amazon S3), la responsabilité de la gestion des correctifs est partagée comme suit :
    - Responsabilité d'AWS : appliquer les correctifs sans que le client n'ait à intervenir.

    - Responsabilité du client : consulter la documentation relative aux correctifs et à la maintenance de chaque service utilisé géré par AWS, pour comprendre les mécanismes de notification spécifiques, les options de fenêtre de maintenance et mettre à jour les processus d'application mis à leur disposition.
- Gestion de la configuration : AWS gère la configuration de ses appareils 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.

Spécifique 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. AWS Artifact est une ressource utile, 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. Il s'agit du 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 matière d'argent, de réputation et de durée.

Likelihood	Risk Level				
Very Likely	Low	Medium	High	Critical	Critical
Likely	Low	Medium	Medium	High	Critical
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Very unlikely	Low	Low		Medium	High
Consequence	Minimal	Low	Medium	High	Severe

Figure 2 : matrice de probabilité du niveau de risque

AWSGestion et séparation des comptes

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. Les organisations vous permettent de regrouper des comptes en unités d'organisation (OU), 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 Gestion des identités et des accès AWS (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, automatise la mise en service, applique des guardrails (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 CloudTrail et 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 racine 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 escompté : une structure de compte qui isole les opérations cloud, les charges de travail indépendantes et les environnements dans des comptes distincts, renforçant ainsi la sécurité de 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 au respect 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 d’exposition au risque si cette bonne pratique n’est pas respectée : 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 la mise en œuvre d'une stratégie multi-comptes sur AWS, consultez 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.

AWS Organizations et AWS Control Tower sont deux services que vous pouvez utiliser pour mettre en œuvre et gérer cette structure multi-comptes dans votre environnement AWS. AWS Organizations vous permet d'organiser les comptes selon une hiérarchie définie par une ou plusieurs couches d'unités d'organisation, chaque unité d'organisation 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 précis sur les comptes des membres et AWS Config peut être utilisé pour établir des contrôles proactifs et détectifs sur les comptes des membres. De nombreux services AWS s'intègrent à AWS Organizations pour fournir des contrôles administratifs délégués et effectuer des tâches spécifiques aux services sur tous les comptes membres de l'organisation.

Situé au-dessus d'AWS Organizations, AWS Control Tower fournit une configuration des bonnes pratiques en un clic pour un environnement AWS multicomptes 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 contrôles de sécurité obligatoires intégrés qui sont automatiquement appliquées aux comptes admis dans l'organisation.

- Des contrôles facultatifs qui peuvent être activés ou désactivés pour un ensemble donné d'unités d'organisation.
- AWS Control Tower Account Factory permet le déploiement automatique de comptes contenant des lignes de base et des options de configuration préapprouvées au sein de votre organisation.

Étapes d'implémentation

1. Conception d'une structure d'unité organisationnelle : une structure d'unité organisationnelle correctement conçue réduit la charge de gestion requise pour créer et maintenir des politiques de contrôle des services et d'autres contrôles de sécurité. La structure de votre unité organisationnelle doit être alignée sur les besoins de votre entreprise, la sensibilité des données et la structure de la charge de travail.
2. Créez une zone de destination pour votre environnement multicomptes : une zone de destination fournit une base de sécurité et d'infrastructure cohérente 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 : mettez en place des barrières de protection de sécurité cohérentes pour votre environnement dans toute 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. Restreindre l'accès aux régions nouvellement ajoutées : pour les nouvelles Régions AWS, les ressources IAM comme les utilisateurs et les rôles sont uniquement propagées vers les régions que vous activez. Cette action peut être effectuée via la console lorsque vous utilisez Control Tower ou en ajustant les politiques d'autorisation IAM dans AWS Organizations.
5. Envisager AWS StackSets : StackSets peut être utilisé pour déployer des ressources, y compris 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 Consignes pour les audits de sécurité
- Bonnes pratiques IAM
- Utiliser StackSets CloudFormation pour allouer des ressources sur plusieurs Comptes AWS et régions
- Organisations FAQ
- AWS Organizations Terminologie et concepts relatifs à
- Best Practices for Service Control Policies in an AWS Organizations Multi-Account Environment
- AWS Guide de référence sur la gestion des comptes
- Organisation de votre environnement AWS à l'aide de comptes multiple

Vidéos connexes:

- Permettre l'adoption d'AWS à grande échelle grâce à l'automatisation et à la gouvernance
- Bonnes pratiques de sécurité : une approche Well-Architected
- Building and Governing Multiple Accounts using AWS Control Tower
- Activer Control Tower pour les organisations existantes

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

L'utilisateur racine 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 racine, établissez des contrôles appropriés pour l'utilisateur racine et évitez l'utilisation de routine de l'utilisateur racine, vous réduirez le risque d'exposition accidentelle des informations d'identification racine et de compromission ultérieure de l'environnement cloud.

Résultat escompté : la sécurisation de l'utilisateur racine permet de réduire les risques de dommages accidentels ou intentionnels dus à une mauvaise utilisation des informations d'identification de l'utilisateur racine. 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 racine.

Anti-modèles courants:

- Se servir de l'utilisateur racine pour des tâches autres que celles nécessitant des informations d'identification de l'utilisateur racine.
- 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 du respect de cette bonne pratique : la sécurisation de l'accès à l'utilisateur racine permet de s'assurer que les actions de votre compte sont contrôlées et auditées.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : 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 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 racine du Compte AWS. Vous pouvez vous connecter en tant qu'utilisateur racine avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. En raison de l'accès élevé accordé à l'utilisateur racine AWS, vous devez limiter l'utilisation de l'utilisateur racine AWS aux seules tâches qui l'exigent spécifiquement. Les informations d'identification de l'utilisateur racine doivent être étroitement protégées et l'authentification multifactorielle (MFA) doit toujours être activée pour l'utilisateur racine du Compte AWS.

Outre le flux d'authentification normal pour vous connecter à votre utilisateur racine 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 racine 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 racine 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 racine 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 racine. 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 racine de votre compte de gestion, puis occupez-vous des utilisateurs racine des comptes membres. La stratégie de sécurisation de l'utilisateur racine de votre compte de gestion peut différer de celle des utilisateurs racine des comptes membres et vous pouvez placer des contrôles de sécurité préventifs sur les utilisateurs racine des comptes membres.

Étapes d'implémentation

Les étapes d'implémentation suivantes sont recommandées afin d'établir des contrôles pour l'utilisateur racine. Le cas échéant, les recommandations sont recoupées avec la version de référence 1.4.0 de CIS AWS Foundations. Outre ces étapes, consultez les directives relatives aux bonnes pratiques AWS pour sécuriser votre Compte AWS et vos ressources.

Contrôles préventifs

1. Configurez des informations de contact précises 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 racine. 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 racine 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 racine. 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 racine.

   b. Si des clés d'accès de l'utilisateur racine existent déjà, vous devez transférer les processus utilisant ces clés pour utiliser les clés d'accès temporaires d'un rôle Gestion des identités et des accès AWS (IAM), puis supprimer les clés d'accès de l'utilisateur racine.

3. Déterminez si vous devez stocker les informations d'identification de l'utilisateur racine.
   a. Si vous utilisez AWS Organizations pour créer de nouveaux comptes membres, le mot de passe initial pour l'utilisateur racine 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 de votre compte de gestion AWS Organization pour obtenir l'accès 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 racine. Utilisez l'authentification multifactorielle pour l'utilisateur racine.
4. Utilisez les contrôles préventifs pour les utilisateurs racine des comptes membres dans les environnements AWS multicomptes.
   a. Envisagez d'utiliser la barrière de sécurité préventive Interdire la création de clés d'accès racine pour l'utilisateur racine pour les comptes des membres.
   b. Envisagez d'utiliser la barrière de sécurité préventive Désactiver les actions en tant qu'utilisateur racine pour les comptes des membres.
5. Si vous avez besoin d'informations d'identification pour l'utilisateur racine :
   a. Utilisez un mot de passe complexe.
   b. Activez l'authentification multifactorielle (MFA) pour l'utilisateur racine, 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)
      - Pour configurer l'authentification multifactorielle pour l'utilisateur racine, suivez les instructions de création d'un appareil d'authentification multifactorielle virtuel ou d'un appareil d'authentification multifactoriel matériel.
   d. Envisagez d'inscrire plusieurs appareils d'authentification multifactorielle à des fins de 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 racine désactive automatiquement le processus de récupération de votre compte en cas de perte de l'appareil d'authentification multifactorielle.

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 racine.
   - Les bonnes pratiques relatives à la gestion des informations d'identification dépendent de vos exigences en matière de réglementation et de politiques. Les utilisateurs racine 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 racine réduit le risque d'utilisation abusive d'un mot de passe exposé par inadvertance.

Contrôles de détection

- Créez des alarmes pour détecter l'utilisation des informations d'identification racine (CIS 1.7). Amazon GuardDuty peut surveiller l'utilisation des informations d'identification de l'API de l'utilisateur racine et émettre des alertes à ce sujet par le biais du résultat RootCredentialUsage.
- Évaluez et implémentez les contrôles de détection inclus dans le Pack de conformité AWS Well-Architected Security Pillar pour AWS Config ou, si vous utilisez AWS Control Tower, les Contrôles fortement recommandés disponibles dans Control Tower.

Conseils opérationnels

- Déterminez qui, au sein de l'organisation, doit avoir accès aux informations d'identification de l'utilisateur racine.
  - 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 racine.
  - 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 racine uniquement de façon exceptionnelle (CIS 1.7).
  - L'utilisateur racine AWS ne doit pas être employé pour des tâches quotidiennes, même les tâches d'administration. Connectez-vous uniquement en tant qu'utilisateur racine pour effectuer

des tâches AWS nécessitant un utilisateur racine. Toutes les autres actions doivent être effectuées par d'autres utilisateurs assumant les rôles appropriés.

- Vérifiez régulièrement que l'accès à l'utilisateur racine fonctionne afin que les procédures soient testées avant une situation d'urgence nécessitant l'utilisation des informations d'identification de l'utilisateur racine.
- Vérifiez régulièrement que l'adresse e-mail associée au compte et celles répertoriées sous Contacts alternatifs 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 racine. Consultez le guide de réponse aux incidents de sécurité AWS et les bonnes pratiques décrites dans la section Réponse aux incidents du livre blanc sur le pilier Sécurité pour plus d'informations sur l'élaboration d'une stratégie de réponse aux incidents adaptée à 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 Consignes pour les audits de sécurité
- Bonnes pratiques IAM
- Amazon GuardDuty — alerte d'utilisation des informations d'identification racine
- Conseils détaillés sur la surveillance de l'utilisation des informations d'identification racine via CloudTrail
- Jetons MFA approuvés pour une utilisation avec AWS

- Mise en œuvre de l'accès au mode « bris de glace » sur AWS
- Les 10 meilleurs éléments de sécurité à améliorer dans votre Compte AWS
- Que faire si je remarque une activité non autorisée dans mon Compte AWS?

Vidéos connexes:

- Permettre l'adoption d'AWS à grande échelle grâce à l'automatisation et à la gouvernance
- Bonnes pratiques de sécurité : une approche Well-Architected
- Limiting use of AWS root credentials from AWS re:inforce 2022 – Security best practices with AWS IAM

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.

Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opérationnelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. En restant informé des recommandations AWS et du secteur, ainsi que des renseignements sur les menaces, vous pouvez 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 Connaître les menaces et recommandations en matière de sécurité
- SEC01-BP05 Réduire la portée de la gestion de la sécurité
- SEC01-BP06 Automatiser le déploiement des contrôles de sécurité standard
- 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.

Résultat escompté : les objectifs de contrôle de sécurité de votre entreprise sont bien définis et conformes à vos exigences de conformité. Des contrôles sont mis en œuvre et appliqués par le biais de l'automatisation et des politiques. Leur efficacité dans le cadre de la réalisation de vos objectifs est évaluée en continu. Les preuves de l'efficacité à un moment donné et au cours d'une période spécifique peuvent être facilement transmises aux auditeurs.

Anti-modèles courants:

- Les exigences réglementaires, les attentes du marché et les normes du secteur en matière de sécurité assurable ne sont pas bien comprises pour votre entreprise
- Vos cadres de cybersécurité et vos objectifs de contrôle ne sont pas adaptés aux exigences de votre entreprise
- La mise en œuvre des contrôles n'est pas étroitement liée à vos objectifs de contrôle de manière mesurable
- Vous n'utilisez pas l'automatisation pour rendre compte de l'efficacité de vos contrôles

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

Directives d'implémentation

De nombreux cadres de cybersécurité courants peuvent constituer la base de vos objectifs en matière de contrôle de sécurité. Tenez compte des exigences réglementaires, des attentes du marché et des normes du secteur pour votre entreprise afin de déterminer les cadres les plus adaptés à vos besoins. Les exemples incluent AICPA SOC 2, HITRUST, PCI-DSS, ISO 27001 et NIST SP 800-53.

En ce qui concerne les objectifs de contrôle que vous identifiez, comprenez comment les services AWS que vous consommez vous aident à atteindre ces objectifs. Utilisez AWS Artifact pour trouver de la documentation et des rapports conformes à vos cadres cibles qui décrivent l'étendue des responsabilités couvertes par AWS et des conseils pour le champ d'application restant sous votre responsabilité. Pour obtenir des conseils supplémentaires spécifiques aux services, dans la mesure

où ils s'alignent sur les différentes déclarations de contrôle du cadre, consultez les guides de conformité destinés aux clients AWS.

Lorsque vous définissez les contrôles destinés à vous permettre d'atteindre vos objectifs, codifiez l'application à l'aide de contrôles préventifs et automatisez les mesures d'atténuation à l'aide de contrôles de détection. Aidez à prévenir les configurations de ressources et les actions non conformes dans l'ensemble de vos AWS Organizations à l'aide de politiques de contrôle des services (SCP). Mettez en œuvre des règles dans AWS Config pour surveiller et signaler les ressources non conformes, puis basculez les règles vers un modèle d'application une fois que vous êtes sûr de leur comportement. Pour déployer des ensembles de règles prédéfinies et gérées qui s'alignent sur vos cadres de cybersécurité, évaluez l'utilisation des normes AWS Security Hub CSPM comme première option. La norme des pratiques exemplaires en matière de sécurité de base AWS (FSBP) et la référence CIS AWS Foundations Benchmark constituent de bons points de départ avec des contrôles qui s'alignent sur de nombreux objectifs partagés par plusieurs cadres standard. Lorsque Security Hub CSPM ne dispose pas intrinsèquement des détections de contrôle souhaitées, il peut être complété par des packs de conformité AWS Config.

Utilisez les groupes de partenaires APN recommandés par l'équipe AWS Global Security and Compliance Acceleration (GSCA) pour obtenir l'assistance de conseillers en sécurité, d'agences de conseil, de systèmes de collecte de preuves et d'information, d'auditeurs et d'autres services complémentaires en cas de besoin.

Étapes d'implémentation

1. Évaluez les cadres de cybersécurité courants et alignez vos objectifs de contrôle sur ceux que vous aurez choisis.
2. Obtenez la documentation pertinente sur les directives et les responsabilités relatives à votre cadre en utilisant AWS Artifact. Déterminez quels aspects de la conformité relèvent de la partie AWS du modèle de responsabilité partagée et quels éléments relèvent de votre responsabilité.
3. Utilisez les SCP, les politiques de ressources, les politiques d'approbation des rôles et d'autres barrières de protection pour empêcher les configurations de ressources et les actions non conformes.
4. Évaluez le déploiement des normes Security Hub CSPM et des packs de conformité AWS Config qui correspondent à vos objectifs de contrôle.

Ressources

Bonnes pratiques associées:

- SEC03-BP01 Définir les conditions d’accès
- SEC04-BP01 Configurer une journalisation de service et d’application
- SEC07-BP01 Comprendre votre schéma de classification des données
- OPS01-BP03 Évaluer les exigences de gouvernance
- OPS01-BP04 Évaluer les exigences de conformité
- PERF01-BP05 Utiliser des stratégies et des architectures de référence
- COST02-BP01 Développer des stratégies en fonction des exigences de votre organisation

Documents connexes:

- AWS Guides de conformité pour les clients

Outils associés:

- AWS Artifact

SEC01-BP04 Connaître les menaces et recommandations en matière de sécurité

Restez au fait des dernières menaces et mesures d’atténuation en surveillant les publications et les flux de données sur les menaces dans le secteur afin de connaître les données les plus à jour. Évaluez les offres de services gérés qui sont automatiquement mises à jour en fonction des données les plus récentes sur les menaces.

Résultat escompté : vous restez informé au fur et à mesure que les publications du secteur sont mises à jour avec les dernières menaces et recommandations. Vous utilisez l’automatisation pour détecter les vulnérabilités et les expositions potentielles au fur et à mesure que vous identifiez de nouvelles menaces. Vous prenez des mesures pour atténuer ces menaces. Vous adoptez des services AWS qui sont automatiquement mis à jour avec les dernières informations sur les menaces.

Anti-modèles courants:

- Ne pas disposer d’un mécanisme fiable et reproductible pour connaître les informations les plus récentes sur les menaces.

- Gérer un inventaire manuel de votre portefeuille technologique, de vos charges de travail et de vos dépendances qui nécessitent un examen humain pour détecter les vulnérabilités et les expositions potentielles.
- Ne pas avoir mis en place de mécanismes pour mettre à jour vos charges de travail et vos dépendances avec les dernières versions disponibles qui fournissent des mesures d'atténuation des menaces connues.

Avantages du respect de cette bonne pratique : l'utilisation de sources d'information sur les menaces pour rester à jour réduit le risque de passer à côté de changements importants du paysage des menaces susceptibles d'avoir un impact sur votre entreprise. La mise en place d'une automatisation pour analyser, détecter et corriger les vulnérabilités ou les expositions potentielles présentes dans vos charges de travail et leurs dépendances peut vous aider à atténuer les risques de manière rapide et prévisible, par rapport à des solutions manuelles. Cela permet de contrôler le temps et les coûts liés à l'atténuation des vulnérabilités.

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

Directives d'implémentation

Consultez des publications fiables comportant des informations sur les menaces pour rester au fait de l'évolution de ces dernières. Consultez la base de connaissances MITRE ATT&CK pour obtenir de la documentation sur les tactiques, techniques et procédures antagonistes (TTP) connues. Consultez la liste des vulnérabilités et expositions courantes (CVE) de MITRE pour rester informé des vulnérabilités connues des produits sur lesquels vous comptez. Comprenez les risques critiques auxquels sont exposées les applications Web grâce au célèbre projet OWASP Top 10 de l'Open Worldwide Application Security Project (OWASP).

Tenez-vous au courant des événements de sécurité AWS et des mesures correctives recommandées grâce aux bulletins de sécurité AWS pour les CVE.

Afin de réduire les efforts et les frais généraux liés au maintien de connaissances à jour, envisagez l'utilisation de services AWS qui intègrent automatiquement les nouvelles informations sur les menaces au fil du temps. Par exemple, Amazon GuardDuty reste à jour en ce qui concerne les informations sur les menaces du secteur pour détecter les comportements anormaux et les signatures de menaces au sein de vos comptes. Amazon Inspector met automatiquement à jour une base de données des CVE qu'il utilise pour ses fonctionnalités de numérisation continue. AWS WAF et AWS Shield Advanced fournissent tous deux des groupes de règles gérés qui sont mis à jour automatiquement à mesure que de nouvelles menaces apparaissent.

Passez en revue le pilier Excellence opérationnelle Well-Architected pour la gestion automatisée des flottes et l'application de correctifs.

Étapes d'implémentation

- Abonnez-vous aux mises à jour des publications comportant des informations sur les menaces pertinentes pour votre entreprise et votre secteur d'activité. Abonnez-vous aux bulletins de sécurité AWS.
- Envisagez d'adopter des services qui intègrent automatiquement les nouvelles informations sur les menaces, comme Amazon GuardDuty et Amazon Inspector.
- Déployez une stratégie de gestion de flotte et de correctifs conforme aux bonnes pratiques du pilier Excellence opérationnelle Well-Architected.

Ressources

Bonnes pratiques associées:

- SEC01-BP07 Identifier les menaces et hiérarchiser les atténuations à l'aide d'un modèle de menaces
- OPS01-BP05 Évaluer les menaces existantes
- OPS11-BP01 Définir un processus d'amélioration continue

SEC01-BP05 Réduire la portée de la gestion de la sécurité

Déterminez si vous pouvez réduire votre périmètre de sécurité en utilisant des services AWS qui transfèrent la gestion de certains contrôles vers AWS (services gérés). Ces services peuvent vous aider à réduire vos tâches de maintenance de sécurité, telles que le provisionnement de l'infrastructure, la configuration logicielle, l'application de correctifs ou les sauvegardes.

Résultat escompté : vous tenez compte de l'étendue de votre gestion de la sécurité lorsque vous sélectionnez les services AWS adaptés à votre charge de travail. Le coût des frais de gestion et des tâches de maintenance (le coût total de possession, ou TCO) est évalué par rapport au coût des services que vous sélectionnez, outre les autres considérations liées à Well-Architected. Vous intégrez la documentation de contrôle et de conformité AWS dans vos procédures d'évaluation et de vérification des contrôles.

Anti-modèles courants:

- Déployer des charges de travail sans bien comprendre le modèle de responsabilité partagée pour les services que vous sélectionnez.
- Héberger des bases de données et d'autres technologies sur des machines virtuelles sans avoir évalué un équivalent de service géré.
- Ne pas inclure les tâches de gestion de la sécurité dans le coût total de possession des technologies d'hébergement sur les machines virtuelles par rapport aux options de services gérés.

Avantages du respect de cette bonne pratique : l'utilisation de services gérés peut réduire la charge globale que représente la gestion des contrôles de sécurité opérationnels, ce qui peut réduire les risques de sécurité et le coût total de possession. Le temps qui serait autrement consacré à certaines tâches de sécurité peut être réinvesti dans des tâches qui apportent plus de valeur à votre entreprise. Les services gérés peuvent également réduire la portée de vos exigences de conformité en transférant certaines exigences de contrôle à AWS.

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

Directives d'implémentation

Vous pouvez intégrer les composants de votre charge de travail sur de plusieurs manières AWS. L'installation et l'exécution de technologies sur des instances Amazon EC2 vous obligent souvent à assumer la plus grande part de la responsabilité globale en matière de sécurité. Pour réduire la charge liée à l'utilisation de certains contrôles, identifiez les services gérés par AWS qui réduisent la portée de votre côté du modèle de responsabilité partagée et comprenez comment vous pouvez les utiliser dans votre architecture existante. Les exemples incluent l'utilisation d'Amazon Relational Database Service (Amazon RDS) pour le déploiement de bases de données, d'Amazon Elastic Kubernetes Service (Amazon EKS) ou d'Amazon Elastic Container Service (Amazon ECS) pour l'orchestration de conteneurs ou l'utilisation d'options sans serveur. Lorsque vous créez de nouvelles applications, réfléchissez aux services qui peuvent vous aider à réduire les délais et les coûts liés à la mise en œuvre et à la gestion des contrôles de sécurité.

Les exigences de conformité peuvent également entrer en ligne de compte lors de la sélection des services. Les services gérés peuvent transférer la conformité de certaines exigences vers AWS. Discutez avec votre équipe de conformité de son degré d'aisance avec l'audit des aspects des services que vous utilisez et gérez, et avec l'acceptation des déclarations de contrôle dans les rapports d'audit AWS pertinents. Vous pouvez fournir les artefacts d'audit trouvés dans AWS Artifact à vos auditeurs ou régulateurs comme preuve des contrôles de sécurité AWS. Vous pouvez également utiliser les conseils en matière de responsabilité fournis par certains artefacts d'audit AWS

pour concevoir votre architecture, ainsi que les guides de conformité destinés aux clients AWS. Ces conseils aident à déterminer les contrôles de sécurité supplémentaires à mettre en place afin de prendre en charge les cas d'utilisation spécifiques de votre système.

Lorsque vous utilisez des services gérés, familiarisez-vous avec le processus de mise à jour de leurs ressources vers les nouvelles versions (par exemple, mise à jour de la version d'une base de données gérée par Amazon RDS ou d'un langage de programmation exécutable pour une fonction AWS Lambda). Bien que le service géré puisse effectuer cette opération pour vous, il vous incombe de configurer le calendrier de la mise à jour et de comprendre son impact sur vos opérations. Des outils comme AWS Health peuvent vous aider à suivre et à gérer ces mises à jour dans l'ensemble de vos environnements.

Étapes d'implémentation

1. Évaluez les composants de votre charge de travail qui peuvent être remplacés par un service géré.
    a. Si vous migrez une charge de travail vers AWS, tenez compte de la réduction de la gestion (temps et dépenses) et de la réduction des risques lorsque vous déterminez si vous devez réhéberger, refactoriser, replateformer, reconstruire ou remplacer votre charge de travail. Dans certains cas, des investissements supplémentaires au début d'une migration peuvent permettre de réaliser des économies importantes à long terme.
2. Envisagez de mettre en œuvre des services gérés, comme Amazon RDS, au lieu d'installer et de gérer vos propres déploiements technologiques.
3. Utilisez les conseils de responsabilité dans AWS Artifact afin de vous aider à déterminer quels contrôles de sécurité doivent être mis en place pour votre charge de travail.
4. Tenez un inventaire des ressources utilisées et restez au courant des nouveaux services et approches afin d'identifier de nouvelles opportunités de réduction de la portée.

Ressources

Bonnes pratiques associées:

- PERF02-BP01 Sélectionner les meilleures options de calcul pour votre charge de travail
- PERF03-BP01 Utiliser un magasin de données dédié le mieux adapté à vos besoins en matière de stockage des données et d'accès aux données
- SUS05-BP03 Utiliser des services gérés

Documents connexes:

- Événements du cycle de vie planifiés pour AWS Health

Outils associés:

- AWS Health
- AWS Artifact
- AWS Guides de conformité pour les clients

Vidéos connexes:

- Comment effectuer une migration vers une instance de base de données MySQL Amazon RDS ou Aurora à l'aide d'AWS DMS ?
- AWS re:Invent 2023 - Manage resource lifecycle events at scale with AWS Health

SEC01-BP06 Automatiser le déploiement des contrôles de sécurité standard

Appliquez les pratiques DevOps modernes lorsque vous développez et déployez des contrôles de sécurité standard dans tous vos environnements AWS. Définissez des contrôles et des configurations de sécurité standard à l'aide de modèles d'infrastructure en tant que code (IaC), capturez les modifications dans un système de contrôle de version, testez les modifications dans le cadre d'un pipeline CI/CD et automatisez le déploiement des modifications dans vos environnements AWS.

Résultat escompté : les modèles IaC capturent des contrôles de sécurité standardisés et les transmettent à un système de contrôle de version. Les pipelines CI/CD sont situés à des endroits qui détectent les changements et automatisent les tests et le déploiement de vos environnements AWS. Des barrières de protection sont en place pour détecter et signaler les erreurs de configuration des modèles avant de procéder au déploiement. Les charges de travail sont déployées dans des environnements où des contrôles standard sont en place. Les équipes peuvent déployer des configurations de service approuvées via un mécanisme en libre-service. Des stratégies de sauvegarde et de restauration sécurisées sont en place pour contrôler les configurations, les scripts et les données associées.

Anti-modèles courants:

- Apporter des modifications à vos contrôles de sécurité standard manuellement, via une console Web ou une interface de ligne de commande.
- S'appuyer sur des équipes chargées de la charge de travail individuelles pour mettre en œuvre manuellement les contrôles définis par une équipe centrale.
- S'appuyer sur une équipe de sécurité centrale pour déployer des contrôles au niveau de la charge de travail à la demande d'une équipe responsable d'une charge de travail.
- Permettre aux mêmes personnes ou équipes de développer, de tester et de déployer des scripts d'automatisation des contrôles de sécurité sans séparation appropriée des tâches ni freins et contrepoids.

Avantages du respect de cette bonne pratique : l'utilisation de modèles pour définir vos contrôles de sécurité standard vous permet de suivre et de comparer les modifications au fil du temps à l'aide d'un système de contrôle de version. L'utilisation de l'automatisation pour tester et déployer les modifications crée de la standardisation et de la prévisibilité, ce qui augmente les chances de réussite du déploiement et réduit les tâches manuelles répétitives. La fourniture d'un mécanisme en libre-service permettant aux équipes responsables de la charge de travail de déployer des services et des configurations approuvés réduit le risque d'erreurs et de mauvaise utilisation de la configuration. Cela leur permet également d'intégrer des contrôles plus tôt dans le processus de développement.

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

Directives d'implémentation

Si vous suivez les pratiques décrites dans SEC01-BP01 Séparer les charges de travail à l'aide de comptes, vous vous retrouverez avec plusieurs Comptes AWS pour différents environnements que vous gérez à l'aide d'AWS Organizations. Bien que ces environnements et charges de travail puissent nécessiter des contrôles de sécurité distincts, vous pouvez standardiser certains contrôles de sécurité au sein de votre organisation. Cela concerne notamment l'intégration de fournisseurs d'identité centralisés, la définition de réseaux et de pares-feux, et la configuration d'emplacements standard pour le stockage et l'analyse des journaux. De la même manière que vous pouvez utiliser l'infrastructure en tant que code (IaC) pour appliquer la même rigueur de développement de code d'application au provisionnement de l'infrastructure, vous pouvez également utiliser l'IaC pour définir et déployer vos contrôles de sécurité standard.

Dans la mesure du possible, définissez vos contrôles de sécurité de manière déclarative, par exemple dans AWS CloudFormation, et stockez-les dans un système de contrôle source. Utilisez les pratiques DevOps pour automatiser le déploiement de vos contrôles afin de rendre les versions

plus prévisibles, les tests automatisés à l'aide d'outils tels que AWS CloudFormation Guard et la détection des écarts entre les contrôles déployés et la configuration souhaitée. Vous pouvez construire un pipeline CI/CD à l'aide de services tels que AWS CodePipeline, AWS CodeBuild et AWS CodeDeploy. Consultez les instructions de la section Organisation de votre environnement AWS à l'aide de plusieurs comptes pour configurer ces services dans leurs propres comptes, distincts des autres pipelines de déploiement.

Vous pouvez également définir des modèles pour standardiser la définition et le déploiement de Comptes AWS, des services et des configurations. Cette technique permet à une équipe de sécurité centrale de gérer ces définitions et de les fournir aux équipes responsables de la charge de travail via une approche en libre-service. L'un des moyens d'y parvenir consiste à utiliser Service Catalog, dans lequel vous pouvez publier des modèles sous forme de produits que les équipes chargées des charges de travail peuvent intégrer dans leurs propres déploiements de pipeline. Si vous en utilisez AWS Control Tower, certains modèles et contrôles sont disponibles comme point de départ. Control Tower fournit également la fonctionnalité Account Factory, qui permet aux équipes chargées de la charge de travail de créer de nouveaux Comptes AWS en utilisant les normes que vous définissez. Cette fonctionnalité permet de supprimer les dépendances vis-à-vis d'une équipe centrale chargée d'approuver et de créer de nouveaux comptes lorsqu'ils sont identifiés comme nécessaires par vos équipes responsables des charges de travail. Vous pouvez avoir besoin de ces comptes pour isoler les différents composants de la charge de travail en fonction de raisons telles que la fonction qu'ils remplissent, la sensibilité des données traitées ou leur comportement.

Étapes d'implémentation

1. Déterminez comment vous allez stocker et gérer vos modèles dans un système de contrôle de version.
2. Créez des pipelines CI/CD pour tester et déployer vos modèles. Définissez des tests pour vérifier les erreurs de configuration et vérifier que les modèles sont conformes aux normes de votre entreprise.
3. Créez un catalogue de modèles standardisés pour permettre aux équipes responsables des charges de travail de déployer des services et des Comptes AWS en fonction de vos besoins.
4. Mettez en œuvre des stratégies de sauvegarde et de restauration sécurisées pour vos configurations de contrôle, vos scripts et les données associées.

Ressources

Bonnes pratiques associées:

- OPS05-BP01 Utilisation du contrôle de version
- OPS05-BP04 Utiliser des systèmes de gestion du développement et du déploiement
- REL08-BP05 Déployer les modifications avec l'automatisation
- SUS06-BP01 Adopter des méthodes qui peuvent rapidement présenter des améliorations en matière de durabilité

Documents connexes:

- Organisation de votre environnement AWS à l'aide de comptes multiple

Exemples connexes:

- Automatiser la création de comptes et le provisionnement des ressources à l'aide de Service Catalog, AWS Organizations et AWS Lambda
- Renforcer le pipeline DevOps et protéger les données avec AWS Secrets Manager, AWS KMS et AWS Certificate Manager

Outils associés:

- AWS CloudFormation Guard
- Accélérateur de zone de destination sur AWS

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 d'exposition au risque si cette bonne pratique n'est pas respectée : 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 mesures d'atténuation dans le contexte de la protection de quelque chose de valeur. » – Modélisation des menaces liées aux applications dans le cadre de l'Open Web Application Security Project (OWASP

Pourquoi devriez-vous modéliser les 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 industriel de la sécurité basée sur le décalage à gauche. 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 faut-il modéliser les menaces?

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. Réexaminez vos modèles de menaces au fil du temps, notamment en cas de changement majeur, d'évolution du paysage des menaces ou d'adoption d'une nouvelle fonctionnalité ou d'un nouveau service.

Étapes d'implémentation

Comment 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. L'une des approches consiste à commencer par le cadre à 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 le moyen le plus courant de répondre à cette question, car elle vous permet de visualiser ce que vous construisez, par exemple à l'aide d'un diagramme de flux de 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 pouvons-nous 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 personnes concernées impliquées dans l'exercice de modélisation des menaces. Vous pouvez faciliter votre brainstorming en utilisant un modèle d'identification des menaces, tel que STRIDE, qui suggère différentes catégories à évaluer : usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service et élévation de privilèges. En outre, vous pouvez faciliter le brainstorming en consultant les listes existantes et les recherches pour vous inspirer, notamment le Top 10 de l'OWASP, le catalogue des menaces HiTrust et 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 la responsabilité partagée d'AWS et de vous. 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.

En ce qui concerne 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 par les clients AWS sur AWS Artifact.

Quels que soient les services AWS que vous utilisez, il y a toujours un élément de responsabilité du client, et les mesures d'atténuation correspondant à ces responsabilités doivent être incluses dans votre modèle de menace. 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 considérer comme des mesures 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 être des éléments tels que la validation des entrées, la gestion des sessions et la 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 aller plus loin et vous familiariser avec le sujet, il est recommandé que vous et votre

équipe suiviez le cours sur la bonne modélisation des menaces pour les constructeurs ou l'atelier sur ce sujet. En outre, si vous recherchez des conseils sur la manière d'intégrer la modélisation des menaces dans le cycle de développement des applications de votre entreprise, consultez l'article Comment aborder la modélisation des menaces sur le blog de sécurité 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 rentabilisation lors de la modélisation des menaces. L'outil vous permet d'effectuer les opérations suivantes :

- Rédiger des déclarations de menace utiles, alignées sur la grammaire des menaces, qui fonctionnent dans un flux de travail naturel 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 de plus amples informations, rendez-vous sur Threat Composer et passez à 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 Connaître les menaces et recommandations en matière de sécurité
- SEC01-BP05 Réduire la portée de la gestion de la sécurité
- SEC01-BP08 Évaluer et mettre en œuvre régulièrement de nouveaux services et de nouvelles fonctions de sécurité

Documents connexes:

- Comment aborder la modélisation des menaces (blog sur la sécurité AWS)
- NIST : Guide de modélisation des menaces système centrées sur les données

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:

- Modéliser les menaces de la bonne manière pour les constructeurs : formation virtuelle à suivre à leur rythme avec AWS Skill Builder
- Modéliser les menaces de la bonne manière pour les constructeurs — Atelier AWS

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.

Résultat escompté : vous avez mis en place une pratique standard qui vous informe des nouvelles fonctionnalités et des nouveaux services publiés par AWS et par les partenaires AWS. Vous évaluez l'influence de ces nouvelles fonctionnalités sur la conception des contrôles actuels et nouveaux pour vos environnements et vos charges de travail.

Anti-modèles courants:

- Vous ne vous abonnez pas à des blogs AWS ni à des flux RSS pour découvrir rapidement les nouvelles fonctionnalités et services pertinents.
- Vous vous fiez aux actualités et aux mises à jour concernant les services et fonctionnalités de sécurité provenant de sources secondaires.
- Vous n'encouragez pas les utilisateurs AWS de votre organisation à rester informés des dernières mises à jour.

Avantages liés au respect de cette bonne pratique : lorsque vous restez au fait des nouveaux services et fonctionnalités de sécurité, vous pouvez prendre des décisions éclairées concernant la mise en œuvre des contrôles dans vos environnements cloud et vos charges de travail. Ces sources contribuent à sensibiliser à l'évolution du paysage de la sécurité et à la manière dont les services AWS peuvent être utilisés pour se protéger contre les menaces nouvelles et émergentes.

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

Directives d'implémentation

AWS informe les clients des nouveaux services et fonctionnalités de sécurité par le biais de plusieurs canaux :

- AWS Nouveautés
- AWS Blog d'actualités
- AWS Blog de sécurité
- AWS Bulletins de sécurité
- AWS Aperçu de la documentation

Vous pouvez vous abonner à une rubrique consacrée aux mises à jour quotidiennes des fonctionnalités AWS à l'aide d'Amazon Simple Notification Service (Amazon SNS) pour obtenir un résumé quotidien complet des mises à jour. Certains services de sécurité, tels qu'Amazon GuardDuty et AWS Security Hub CSPM, proposent leurs propres rubriques SNS pour rester informé des nouvelles normes, des résultats et des autres mises à jour relatives à ces services en particulier.

Les nouveaux services et fonctionnalités sont également annoncés et décrits en détail lors de conférences, d'événements et de webinaires organisés chaque année dans le monde entier. Il convient de noter en particulier la conférence annuelle sur la sécurité AWS re:Inforce et la conférence plus générale AWS re:Invent. Les chaînes d'informations AWS mentionnées précédemment partagent les annonces de ces conférences sur la sécurité et d'autres services, et vous pouvez suivre des séances de formation approfondies en petits groupes en ligne sur la chaîne YouTube AWS Events.

Vous pouvez également demander à votre équipe Compte AWS les dernières mises à jour et recommandations des services de sécurité. Vous pouvez contacter votre équipe via le formulaire de Support commercial si vous ne disposez pas de ses coordonnées directes. De même, si vous êtes abonné au Support aux entreprises AWS,vous recevrez des mises à jour hebdomadaires de la

part de votre gestionnaire de compte technique (TAM) et pourrez planifier une réunion de révision régulière avec lui.

Étapes d'implémentation

1. Abonnez-vous aux différents blogs et bulletins à l'aide de votre lecteur RSS préféré ou à la rubrique SNS des mises à jour quotidiennes des fonctionnalités.
2. Évaluez les événements AWS auxquels vous devez participer pour être parmi les premiers à connaître les nouvelles fonctionnalités et les nouveaux services.
3. Organisez des réunions avec votre équipe Compte AWS pour toute question concernant la mise à jour des services et fonctionnalités de sécurité.
4. Envisagez de vous abonner à Enterprise Support pour discuter régulièrement avec un gestionnaire de compte technique (TAM).

Ressources

Bonnes pratiques associées:

- PERF01-BP01 Découvrir et se familiariser avec les services et fonctionnalités cloud disponibles
- COST01-BP07 Suivre les nouvelles versions des services

Gestion des identités et des accès

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
- Gestion des autorisations

Gestion des identités

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

- Identités humaines : les identités humaines qui nécessitent l'accès à vos environnements et applications AWS peuvent être classées en trois groupes : employés, tiers et utilisateurs.

  Le groupe des employés comprend les administrateurs, les développeurs et les opérateurs qui font partie de votre organisation. Ils ont besoin d'un accès pour gérer, créer et exploiter vos ressources AWS.

  Les tiers sont les collaborateurs externes, tels que les sous-traitants, les fournisseurs et les partenaires. Ils interagissent avec vos ressources AWS dans le cadre de leur engagement auprès de votre organisation.

  Les utilisateurs sont les consommateurs de vos applications. Ils accèdent à vos ressources AWS via des navigateurs Web, des applications client, des applications mobiles ou des outils de ligne de commande interactifs.
- Identités des machines : les applications, les outils opérationnels et les composants de votre charge de travail ont besoin d'une identité pour adresser des demandes aux services AWS, telles que la lecture de données. Ces identités incluent également les machines qui s'exécutent dans votre environnement AWS, comme les instances Amazon EC2 ou les fonctions AWS Lambda.

Vous pouvez également gérer les identités des machines pour des parties externes ou des machines en dehors d'AWS, qui ont besoin d'accéder à votre environnement AWS.

Bonnes pratiques

- SEC02-BP01 Utiliser de solides mécanismes d'authentification
- SEC02-BP02 Utiliser des informations d'identification temporaires
- 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 Utiliser 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 escompté : réduisez les risques d'accès involontaire aux informations d'identification dans AWS en utilisant des mécanismes de connexion robustes pour les utilisateurs Gestion des identités et des accès AWS (IAM), l'utilisateur racine du Compte AWS, AWS IAM Identity Center et les fournisseurs d'identité tiers. Cela signifie que vous devez exiger une authentification multifactorielle (MFA), 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 de mots de passe pour vos identités, notamment des mots de passe complexes et l'authentification multifactorielle (MFA).
- Utilisation des mêmes informations d'identification pour différents utilisateurs.
- Ne pas utiliser de contrôles de détection pour les connexions suspectes.

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

Directives d'implémentation

Les identités humaines peuvent se connecter à AWS de plusieurs façons. Une bonne pratique AWS consiste à s'appuyer sur un fournisseur d'identité centralisé en utilisant la fédération (fédération SAML 2.0 directe entre AWS IAM et le fournisseur d'identité centralisé ou utilisant AWS IAM Identity Center) lors de l'authentification auprès d'AWS. Dans ce cas, établissez un processus de 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 racine du Compte AWS. Vous ne devez utiliser l'utilisateur racine du compte que pour configurer l'accès de vos utilisateurs (et pour les tâches nécessitant l'utilisateur racine). Il est important d'activer l'authentification multifactorielle (MFA) pour l'utilisateur racine du compte immédiatement après l'ouverture de votre Compte AWS et de sécuriser l'utilisateur racine à l'aide du guide des bonnes pratiques AWS.

AWS IAM Identity Center est conçu pour les utilisateurs en interne et vous pouvez créer et gérer des identités utilisateur au sein du service et sécuriser le processus d'authentification avec la MFA. AWS Cognito, quant à lui, est conçu pour la gestion de l'identité et de l'accès des clients (CIAM), qui fournit des groupes d'utilisateurs et des fournisseurs d'identité pour les identités des utilisateurs externes dans vos applications.

Si vous créez des utilisateurs dans AWS IAM Identity Center, sécurisez le processus d'authentification dans ce service et activez la MFA. Pour les identités des utilisateurs externes dans vos applications, vous pouvez utiliser les groupes d'utilisateurs Amazon Cognito et sécuriser le processus d'authentification dans ce service ou utiliser l'un des fournisseurs d'identité pris en charge dans les groupes d'utilisateurs Amazon Cognito.

En outre, pour les utilisateurs dans AWS IAM Identity Center, vous pouvez utiliser Accès vérifié par AWS pour fournir un niveau de sécurité supplémentaire en vérifiant l'identité de l'utilisateur et la position de l'appareil avant d'accorder l'accès aux ressources AWS.

Si vous utilisez des utilisateurs Gestion des identités et des accès AWS (IAM), sécurisez le processus d'authentification à l'aide d'IAM.

Vous pouvez utiliser AWS IAM Identity Center et la fédération IAM directe simultanément pour gérer l'accès à AWS. Vous pouvez utiliser la fédération IAM pour gérer l'accès à la Console de gestion AWS et aux services et IAM Identity Center pour gérer l'accès aux applications professionnelles telles que Quick ou Amazon Q Business.

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

Étapes d'implémentation

Voici des recommandations générales pour la connexion. Les paramètres que vous configurez doivent être définis par la politique de votre entreprise ou suivre une norme telle que NIST 800-63.

- Require MFA (Demander l'authentification MFA). L'une des bonnes pratiques IAM consiste à exiger l'authentification multifactorielle pour les identités humaines et les charges de travail. L'activation de l'authentification multifactorielle (MFA) 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.
- Autorisez les utilisateurs à modifier 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 pour IAM Identity Center :

- IAM Identity Center fournit une politique de gestion de mots de passe prédéfinie lors de l'utilisation du répertoire par défaut qui définit la longueur, la complexité et les exigences de réutilisation de mots de passe.
- Activez l'authentification multifactorielle (MFA) et configurez le paramètre contextuel ou permanent pour la MFA lorsque la source d'identité est le répertoire par défaut, AWS Managed Microsoft AD, ou AD Connector.
- Permettez aux utilisateurs d'enregistrer leurs propres appareils MFA.

Recommandations pour le répertoire des groupes d'utilisateurs Amazon Cognito :

- Configurez les paramètres de sécurité du mot de passe.

- Exiger l'authentification multifactorielle (MFA) pour les utilisateurs.
- Utilisez les paramètres de sécurité avancés des groupes d'utilisateurs Amazon Cognito pour des fonctionnalités telles que l'authentification adaptative qui permet de bloquer les connexions suspectes.

Recommandations pour les utilisateurs IAM :

- Idéalement, vous utilisez IAM Identify Center ou la fédération directe. Cependant, vous aurez peut-être besoin des utilisateurs IAM. Dans ce cas, définissez une politique de gestion de mots de passe pour les utilisateurs IAM. Vous pouvez utiliser la politique de gestion de 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 l'authentification multifactorielle (MFA) afin que les utilisateurs soient autorisés à gérer leurs propres mots de passe et appareils MFA.

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 :

- Politique de mot de passe AWS IAM Identity Center
- Politique de mot de passe de l'utilisateur IAM
- Définition du mot de passe de l'utilisateur racine du Compte AWS
- Politique de mot de passe Amazon Cognito
- Informations d'identification AWS
- Bonnes pratiques de sécurité IAM

Vidéos connexes:

- Gestion des autorisations des utilisateurs à grande échelle avec IAM Identity Center AWS

- Maîtrise des identités dans chaque couche

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 escompté : pour réduire le risque d'informations d'identification à long terme, utilisez des informations d'identification temporaires dans la mesure du possible pour les identités humaines et les identités machine. Les informations d'identification à long terme créent de nombreux risques, tels que l'exposition par le biais de chargements dans des référentiels 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 utilisateur IAM 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 d'exposition au risque si cette bonne pratique n'est pas respectée : 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 de CLI adressées aux services AWS doivent, dans presque tous les cas, être signées à l'aide de clés d'accès AWS. Ces demandes peuvent être signées avec des informations d'identification temporaires ou à long terme. Vous ne devez utiliser des informations d'identification à long terme,

également appelées clés d'accès à long terme, que si vous utilisez un utilisateur IAM ou l'utilisateur racine du Compte AWS. Lorsque vous vous fédérez vers AWS ou que vous assumez un rôle IAM par le biais d'autres méthodes, des informations d'identification temporaires sont générées. Même lorsque vous accédez à la Console de gestion AWS 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

Identités humaines

Pour les identités du personnel comme les employés, les administrateurs, les développeurs et les opérateurs :

- Vous devez vous compter sur un fournisseur d'identité et exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS en utilisant des informations d'identification temporaires. La fédération de vos utilisateurs peut se faire soit par une fédération directe à chaque Compte AWS, soit en utilisant 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. Vos utilisateurs peuvent également demander des informations d'identification temporaires depuis 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.

Pour les identités tierces :

- Lorsque vous accordez à des tiers, tels que des fournisseurs de logiciel en tant que service (SaaS), l'accès aux ressources de votre Compte AWS, vous pouvez utiliser des rôles entre comptes et des politiques basées sur les ressources. En outre, vous pouvez utiliser le flux d'informations d'identification client d'octroi OAuth 2.0 Amazon Cognito pour les partenaires et clients SaaS B2B.

Pour les identités utilisateur qui accèdent à vos ressources AWS via des navigateurs Web, des applications client, des applications mobiles ou des outils de ligne de commande interactifs :

- Si vous devez autoriser des demandes permettant aux consommateurs ou aux clients d'accéder à vos ressources AWS, vous pouvez utiliser les groupes d'identités Amazon Cognito ou les groupes d'utilisateurs Amazon Cognito pour fournir des informations d'identification temporaires. Les autorisations pour ces 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.

Identités de machines

Pour les identités machine, vous devrez peut-être utiliser des informations d'identification à long terme. Dans ce cas, 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 pour accorder au service les autorisations nécessaires pour effectuer des actions AWS à l'aide d'informations d'identification temporaires. Il existe de nombreux modèles similaires pour AWS permettre aux services 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 pour demander des informations d'identification temporaires.
- Pour les systèmes sur site ou ceux qui s'exécutent en dehors d'AWS ces systèmes qui nécessitent un accès aux ressources AWS, vous pouvez utiliser Rôles Anywhere IAM.

Dans certains cas, les identifiants temporaires ne sont pas pris en charge et vous devez utiliser des informations d'identification à long terme. Dans ces cas, contrôlez et effectuez régulièrement une rotation de ces informations d'identification et effectuez régulièrement une rotation des clés d'accès. Pour les clés d'accès d'utilisateurs IAM à l'accès très restreint, envisagez d'utiliser les mesures de sécurité supplémentaires suivantes :

- Accordez des autorisations très restreintes :
  - Optez pour le principe du moindre privilège (soyez précis quant aux actions, aux ressources et aux conditions).

    - Envisagez d'accorder à l'utilisateur IAM uniquement l'opération AssumeRole pour un seul rôle spécifique. En fonction de l'architecture sur site, cette approche permet d'isoler et de sécuriser les informations d'identification IAM à long terme.
- Limitez les sources réseau et les adresses IP autorisées dans la politique d'approbation de rôle IAM.
- Surveillez l'utilisation et configurez des alertes pour des autorisations non utilisées ou abusives (à l'aide des filtres de métriques et des alarmes AWS CloudWatch Logs).
- Appliquez des limites d'autorisation (les politiques de contrôle des services (SCP) et les limites d'autorisation se complètent : les SCP sont grossières, tandis que les limites d'autorisation sont détaillées).
- Mettez en œuvre un processus pour provisionner et stocker en toute sécurité (dans un coffre-fort sur site) les informations d'identification.

Autres options pour les scénarios nécessitant des informations d'identification à long terme :

- Créez votre propre API de distribution de jetons (à l'aide d'Amazon API Gateway).
- Dans les scénarios où vous devez utiliser des informations d'identification à long terme ou des informations d'identification autres que des clés d'accès AWS (telles que les connexions à la base de données), vous pouvez utiliser un service conçu pour gérer la gestion des secrets, tel qu'AWS Secrets Manager. Secrets Manager simplifie la gestion, la rotation et le stockage sécurisé des secrets chiffrés. De nombreux services AWS prennent en charge une intégration directe avec Secrets Manager.
- Pour les intégrations multicloud, vous pouvez utiliser la fédération d'identité en fonction des informations d'identification de votre fournisseur de services d'informations d'identification (CSP) source (voir AWS STS AssumeRoleWithWebIdentity).

Pour plus d'informations sur la rotation des informations d'identification à long terme, veuillez consulter la rubrique 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 Informations d'identification
- Bonnes pratiques de sécurité IAM
- Rôles IAM
- IAM Identity Center
- Fournisseurs d'identité et fédération
- Rotation des clés d'accès
- Solutions partenaires de sécurité : accès et contrôle d'accès
- Utilisateur racine d'un compte AWS
- Accès à AWS via une identité de charge de travail native de Google Cloud Platform
- Comment accéder aux ressources AWS à partir de locataires Microsoft Entra ID à l'aide d'AWS Security Token Service

Vidéos connexes:

- Gestion des autorisations des utilisateurs à grande échelle avec IAM Identity Center AWS
- Maîtrise des identités dans chaque couche

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'informations d'identification 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 escompté : mise en œuvre d'un mécanisme de gestion sécurisée des informations d'identification des applications permettant d'atteindre 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 au respect de cette bonne pratique :

- Les secrets sont chiffrés au repos et en transit.
- L'accès aux informations d'identification est bloqué par le biais d'une API (considérez-la comme un distributeur automatique 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 d'exposition au risque si cette bonne pratique n'est pas respectée : 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 d'identification à long terme. Par exemple, au lieu du codage en dur une AWS clé d'accès secrète , 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 que AWS Secrets Manager, où ils peuvent être stockés, gérés et subir une rotation de manière centralisée et régulière.

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

Type d'informations d'identification	Description	Stratégie suggérée
Clés d'accès IAM	AWS Accès IAM et clés secrètes utilisés pour assumer des rôles IAM au sein d'une charge de travail	Remplacer : utilisez plutôt les rôles IAM attribués aux instances de calcul (telles que Amazon EC2 ou AWS Lambda). Pour l'interopérabilité avec des tiers qui ont besoin d'accéder aux ressources de votre compteCompte AWS, demandez-leur s'ils proposent AWS l'accès intercompte. Pour les applications mobiles,

Type d'informations d'identification	Description	Stratégie suggérée
		pensez à utiliser des informations d'identification temporaires via les groupes d'identités Amazon Cognito (identités fédérées). Pour les charges de travail exécutées en dehors de AWS, pensez à Rôles Anywhere IAM ou à AWS Systems Manager Hybrid Activations. Pour les conteneurs, consultez le rôle IAM de la tâche Amazon ECS ou le rôle IAM du nœud Amazon EKS.
Clés SSH	Clés privées Secure shell utilisées pour se connecter aux instances Linux EC2, manuellement ou dans le cadre d'un processus automatisé	Remplacer : utilisez AWS Systems Manager ou EC2 Instance Connect pour fournir un accès programmatique et humain aux instances EC2 à l'aide de rôles IAM.
Informations d'identification d'application et base de données	Mots de passe — chaîne de texte brut	Rotation : stockez les informations d'identification dans AWS Secrets Manager et établissez une rotation automatique si possible.

Type d'informations d'identification	Description	Stratégie suggérée
Informations d'identification d'administration Amazon RDS et Amazon Aurora	Mots de passe — chaîne de texte brut	Remplacer : utilisez l'intégration de Secrets Manager avec Amazon RDS ou Amazon Aurora. En outre, certains types de bases de données RDS peuvent utiliser des rôles IAM au lieu de mots de passe dans certains cas d'utilisation (pour plus de détails, voir Authentification de base de données IAM).
Jetons OAuth	Jetons secrets — chaîne de texte brut	Rotation : stockez les jetons dans AWS Secrets Manager et configurez la rotation automatique.
Jetons et clés API	Jetons secrets — chaîne de texte brut	Rotation : stockez dans AWS Secrets Manager et établissez une rotation automatique si 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 AWS service, 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, préférez la délégation de l'accès à un rôle IAM disposant de l'accès requis aux ressources de votre compte à la configuration d'un utilisateur IAM et à l'envoi au tiers de la clé d'accès secrète de cet utilisateur.

Dans de nombreux cas, la charge de travail nécessite le stockage des secrets nécessaires à l'interopérabilité avec d'autres services et ressources. AWS Secrets Manager est spécialement conçu

pour gérer en toute sécurité ces informations d'identification, ainsi que le stockage, l'utilisation et la rotation des jetons API, des mots de passe et d'autres informations d'identification.

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

Lorsque vous récupérez un secret, vous pouvez utiliser les composants de mise en cache côté client de Secrets Manager pour le mettre en cache en vue d'une utilisation future. Il est plus rapide de récupérer un secret mis en cache que de le récupérer à partir de Secrets Manager. De plus, étant donné que l'appel des API Secrets Manager implique des coûts, l'utilisation d'un cache peut réduire vos coûts. Pour connaître toutes les manières dont vous pouvez récupérer des secrets, consultez Obtenir des secrets.

> **Note**
>
> Certains langages peuvent vous obliger à implémenter votre propre chiffrement en mémoire pour la mise en cache côté client.

Étapes d'implémentation

1. Identifiez les chemins de code contenant des informations d'identification codées en dur à l'aide d'outils automatisés tels qu'Amazon CodeGuru.
   a. Utilisez Amazon CodeGuru pour analyser vos référentiels de code. Une fois l'examen terminé, filtrez sur Type=Secrets dans CodeGuru pour trouver les lignes de code problématiques.
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 est externe à AWS mais nécessite des informations d'identification IAM pour accéder aux ressources AWS, envisagez d'utiliser Rôles Anywhere IAM ou des activations hybrides AWS Systems Manager.

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 à partir de Secrets Manager dans votre code d'application.
        i. Les fonctions Lambda sans serveur peuvent utiliser une extension Lambda indépendante du langage.
        ii. Pour les instances ou les conteneurs EC2, AWS fournit un exemple de code côté client permettant de récupérer des secrets à partir de Secrets Manager dans plusieurs langages de programmation courants.
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.
    a. Envisagez l'utilisation d'un outil tel que git-secrets pour éviter l'ajout de nouveaux secrets à votre dépôt de code source.
5. Surveillez l'activité de Secrets Manager pour détecter tout signe d'utilisation inattendue, d'accès secret inapproprié ou de 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 :

- Mise en route avec AWS Secrets Manager
- Fournisseurs d'identité et fédération
- Amazon CodeGuru présente un détecteur de secrets

- Comment AWS Secrets Manager utilise-t-il AWS Key Management Service ?
- Chiffrement et déchiffrement de secret dans Secrets Manager
- Entrées du journal de Secrets Manager
- Amazon RDS annonce l'intégration avec AWS Secrets Manager

Vidéos connexes :

- Bonnes pratiques de gestion, d'extraction et de renouvellement des secrets à grande échelle
- Trouvez des secrets codés en dur à l'aide du détecteur de secrets Amazon CodeGuru
- Sécurisation des secrets des charges de travail hybrides à l'aide de AWS Secrets Manager

Ateliers connexes :

- Stockez, récupérez et gérez les informations d'identification sensibles dans AWS Secrets Manager
- Activations hybrides AWS Systems Manager

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 escompté : 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 Console de gestion AWS ou l'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 Gestion des identités et des accès AWS dans ce compte. La flexibilité d'IAM vous permet d'activer un fournisseur d'identité SAML 2.0 ou Open ID Connect (OIDC) distinct pour chaque Compte AWS et d'utiliser des attributs d'utilisateur fédéré pour le contrôle d'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 Console de gestion AWS pour permettre à l'utilisateur de s'authentifier de manière unique auprès de la Console de gestion AWS en assumant un rôle IAM. Vos utilisateurs peuvent également obtenir des informations d'identification d'API AWS temporaires à utiliser dans le AWS CLI ou AWS les SDK à partir de AWS STS en assumant le rôle IAM à l'aide d'une assertion SAML du fournisseur d'identité.

Pour fédérer vos utilisateurs en interne avec plusieurs comptes dans votre organisation AWS, vous pouvez utiliser AWS IAM Identity Center pour gérer de manière centralisée l'accès des utilisateurs en interne aux Comptes AWS et aux applications. Vous activez Identity Center pour votre organisation et configurez votre source d'identité. IAM Identity Center fournit un répertoire de sources d'identité 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 provisionnant automatiquement les utilisateurs et les groupes à l'aide de SCIM, ou en vous connectant à votre répertoire Microsoft AD à l'aide de 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'autorisation. Les utilisateurs de votre personnel peuvent s'authentifier par l'intermédiaire de votre fournisseur d'identité central pour se connecter au portail d'accès AWS et ouvrir une session unique dans le Comptes AWS et les applications cloud qui leur sont attribuées. Vos utilisateurs peuvent configurer la 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 aux applications AWS telles qu'Amazon SageMaker AI 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 utilisateur IAM 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 sont gérés en dehors de AWS et les utilisateurs peuvent accéder aux ressources AWS sous la forme d'une identité fédérée. Les identités fédérées utilisent les groupes définis par votre fournisseur d'identité centralisé. Vous devez identifier et supprimer les groupes IAM, les utilisateur IAM 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 à l'aide de rapports d'informations d'identification IAM, supprimer les utilisateurs IAM correspondants et supprimer les groupes IAM. Vous pouvez appliquer une Politique de contrôle des services (SCP) à votre organisation afin d'empêcher la création de nouveaux utilisateurs IAM et groupes, en renforçant cet accès à AWS via des identités fédérées.

> **Note**
>
> Vous êtes responsable de la gestion de la rotation des jetons d'accès SCIM, comme décrit dans la documentation relative au provisionnement automatique. En outre, vous êtes responsable de la rotation des certificats prenant en charge votre fédération d'identité.

Conseils pour les utilisateurs de vos applications Vous pouvez gérer les identités des utilisateurs de vos applications, telles qu'une application mobile, en utilisant Amazon Cognito comme fournisseur d'identité centralisé. Amazon Cognito assure 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 d'identité sociale de l'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 front-end et dorsal.

Étapes d'implémentation

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

- Fédérez les utilisateurs en interne à AWS à l'aide d'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 utilisateurs IAM et les groupes 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 Amazon Cognito pour l'authentification.

Ressources

Bonnes pratiques associées :

- SEC02-BP06 Utiliser 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 Gestion des identités et des accès AWS
- Mise en route avec l'administration déléguée d'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 - Gestion des identités et des accès AWS (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 : utilisation d'AWS IAM Identity Center pour assurer une gestion forte des identités

Outils associés :

- AWS Partenaires 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, et ces risques peuvent être réduits par une rotation régulière de ces informations.

Résultat souhaité : mettez en œuvre la rotation des informations d'identification afin de réduire les risques associés à l'utilisation à long terme des informations d'identification. 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 d'exposition au risque si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Lorsque vous ne pouvez pas compter sur des informations d'identification temporaires et que vous avez besoin d'informations d'identification à long terme, auditez les informations d'identification pour vous assurer que les contrôles définis tels que l'authentification multifactorielle (MFA) sont appliqués, qu'ils font l'objet d'une rotation régulière et qu'ils ont le 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 mettre hors service les clés d'accès au profit d'informations d'identification temporaires. Lorsque vous passez des utilisateurs Gestion des identités et des accès AWS (IAM) aux identités centralisées, vous pouvez générer un rapport d'informations d'identification pour 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 des normes de sécurité AWS Security Hub CSPM pour vérifier si les utilisateurs ont configuré l'authentification multifactorielle. Envisagez d'utiliser Rôles Anywhere IAM afin de fournir des

informations d'identification temporaires pour les identités des machines. 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

- Audit fréquent des informations d'identification : l'audit des identités configurées dans votre fournisseur d'identités et dans IAM aide à garantir 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 inter-comptes 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 pour configurer des alarmes pour des appels d'API spécifiques appelés dans votre environnement AWS. Amazon GuardDuty peut également vous avertir en cas d'activité inattendue, qui peut indiquer un accès trop permissif ou un accès involontaire aux informations d'identification IAM.
- Rotation régulière des informations d'identification : lorsque vous ne pouvez pas utiliser d'informations d'identification temporaires, alternez régulièrement les clés d'accès IAM à long terme (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 la rubrique Rotation des clés d'accès.
- Examiner les permissions IAM : pour améliorer la sécurité de votre Compte AWS, examinez et surveillez régulièrement chacune de vos politiques IAM. Vérifiez que les politiques respectent le principe du moindre privilège.
- Envisagez d'automatiser la création et la mise 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 Rôles Anywhere IAM pour remplacer les utilisateurs IAM par des identités de machines : Rôles Anywhere IAM vous permet d'utiliser des rôles dans des domaines que vous ne pouviez pas

utiliser auparavant, tels que les serveurs sur site. Rôles Anywhere IAM utilise un certificat X.509 approuvé afin de s'authentifier auprès d'AWS et de recevoir des informations d'identification temporaires. L'utilisation de Rôles Anywhere IAM 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 :

- Mise en route avec AWS Secrets Manager
- Bonnes pratiques IAM
- Fournisseurs d'identité et fédération
- Solutions partenaires de sécurité : accès et contrôle d'accès
- Informations d'identification de sécurité temporaires
- Obtention de rapports d'informations d'identification pour votre Compte AWS

Vidéos connexes :

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

SEC02-BP06 Utiliser des groupes d'utilisateurs et des attributs

La définition des autorisations en fonction des groupes d'utilisateurs et des attributs contribue à réduire le nombre et la complexité des politiques, ce qui simplifie la mise en œuvre du principe du moindre privilège. Vous pouvez utiliser des groupes d'utilisateurs pour gérer les autorisations

de nombreuses personnes en un seul endroit selon la fonction qu'elles occupent au sein de votre organisation. Les attributs, tels que le service, le projet ou l'emplacement, peuvent fournir une couche supplémentaire de portée des autorisations lorsque des personnes occupent une fonction similaire, mais pour des sous-ensembles de ressources différents.

Résultat escompté : vous pouvez appliquer des modifications aux autorisations selon la fonction de tous les utilisateurs qui exécutent cette fonction. L'appartenance aux groupes et les attributs régissent les autorisations des utilisateurs, ce qui réduit la nécessité de gérer les autorisations au niveau de chaque utilisateur. Les groupes et les attributs que vous définissez dans votre fournisseur d'identité (IdP) sont propagés automatiquement à vos environnements AWS.

Anti-modèles courants :

- Gestion des autorisations pour les utilisateurs individuels et duplication entre de nombreux utilisateurs.
- Définition de groupes à un niveau trop élevé, autorisations trop étendues accordées.
- Définition de groupes à un niveau trop détaillé, ce qui crée des duplications et de la confusion quant à l'appartenance.
- Utilisation de groupes avec des autorisations dupliquées sur des sous-ensembles de ressources lorsque des attributs peuvent être utilisés à la place.
- Aucune gestion de groupes, d'attributs et d'appartenances par le biais d'un fournisseur d'identité standardisé intégré à vos environnements AWS.
- Utilisation du chaînage des rôles lors de l'utilisation de sessions AWS IAM Identity Center

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

Directives d'implémentation

Les autorisations AWS sont définies dans des documents appelés politiques, qui sont associés à un principal, tel qu'un utilisateur, un groupe, un rôle ou une ressource. Vous pouvez mettre à l'échelle la gestion des autorisations en organisant les attributions d'autorisations (groupe, autorisations, compte) en fonction de la fonction, de la charge de travail et de l'environnement SDLC. En ce qui concerne le personnel, cela vous permet de définir des groupes selon la fonction occupée par les utilisateurs au sein de votre organisation, plutôt que selon les ressources auxquelles ils accèdent. Par exemple, un groupe WebAppDeveloper peut être associé à une politique pour configurer des services tels qu'Amazon CloudFront au sein d'un compte de développement. Un groupe `AutomationDeveloper` peut avoir des autorisations qui se chevauchent avec le groupe

`WebAppDeveloper`. Ces autorisations communes peuvent être saisies dans une politique distincte et associées aux deux groupes, au lieu de faire en sorte que les utilisateurs des deux fonctions appartiennent à un groupe `CloudFrontAccess`.

Outre les groupes, vous pouvez utiliser des attributs pour élargir l'accès. Par exemple, vous pouvez avoir un attribut de projet permettant aux utilisateurs de votre groupe `WebAppDeveloper` de définir l'accès aux ressources spécifiques à leur projet. L'utilisation de cette technique élimine la nécessité de créer différents groupes pour les développeurs d'applications qui travaillent sur différents projets si leurs autorisations sont par ailleurs les mêmes. La façon dont vous faites référence aux attributs dans les politiques d'autorisation dépend de leur source, qu'ils soient définis dans le cadre de votre protocole de fédération (tel que SAML, OIDC ou SCIM), en tant qu'assertions SAML personnalisées ou définis dans le cadre d'IAM Identity Center.

Étapes d'implémentation

1. Déterminez où vous allez définir les groupes et les attributs :
    a. En suivant les instructions fournies dans SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé, vous pouvez déterminer si vous devez définir des groupes et des attributs au sein de votre fournisseur d'identité, dans IAM Identity Center ou utiliser des groupes d'utilisateurs IAM dans un compte spécifique.
2. Définissez des groupes :
    a. Déterminez vos groupes selon la fonction et la portée de l'accès requis. Envisagez d'utiliser une structure hiérarchique ou des conventions de dénomination pour organiser efficacement les groupes.
    b. Si vous optez pour une définition au sein d'IAM Identity Center, créez des groupes et associez le niveau d'accès souhaité à l'aide d'ensembles d'autorisations.
    c. Si vous optez pour une définition au sein d'un fournisseur d'identité externe, déterminez si le fournisseur prend en charge le protocole SCIM et envisagez d'activer le provisionnement automatique au sein d'IAM Identity Center. Cette capacité synchronise la création, l'appartenance et la suppression de groupes entre votre fournisseur et IAM Identity Center.
3. Définissez des attributs :
    a. Si vous utilisez un fournisseur d'identité externe, les protocoles SCIM et SAML 2.0 fournissent certains attributs par défaut. Des attributs supplémentaires peuvent être définis et transmis à l'aide d'assertions SAML utilisant le nom de l'attribut `https://aws.amazon.com/SAML/Attributes/PrincipalTag`. Consultez la documentation de votre fournisseur d'identité pour obtenir des recommandations quant à la définition et la configuration d'attributs personnalisés.

b. Si vous définissez des rôles dans IAM Identity Center, activez la fonctionnalité de contrôle d'accès par attributs (ABAC) et définissez les attributs comme vous le souhaitez. Tenez compte des attributs qui correspondent à la stratégie de balisage des ressources ou à la structure de votre organisation.

Si vous avez besoin d'un chaînage des rôles IAM à partir des rôles IAM assumés via IAM Identity Center, les valeurs telles que `source-identity` et `principal-tags` ne se propagent pas. Pour plus de détails, consultez Activer et configurer les attributs pour le contrôle d'accès.

1. Déterminez la portée des autorisations en fonction des groupes et des attributs :
   a. Envisagez d'inclure dans vos politiques d'autorisation des conditions qui comparent les attributs de votre principal à ceux des ressources auxquelles vous accédez. Par exemple, vous pouvez définir une condition pour autoriser l'accès à une ressource uniquement si la valeur d'une clé de condition `PrincipalTag` correspond à la valeur d'une clé `ResourceTag` du même nom.
   b. Lorsque vous définissez des politiques ABAC, suivez les instructions figurant dans les bonnes pratiques et les exemples relatifs à l'autorisation ABAC.
   c. Passez régulièrement en revue et mettez à jour la structure de votre groupe et de vos attributs au fur et à mesure de l'évolution des besoins de votre organisation afin de garantir une gestion optimale des autorisations.

Ressources

Bonnes pratiques associées :

- SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège
- COST02-BP04 Mettre en œuvre des groupes et des rôles

Documents connexes :

- Bonnes pratiques IAM
- Gestion des identités dans IAM Identity Center
- Qu'est-ce que le contrôle d'accès par attributs (ABAC) pour AWS ?
- Contrôle d'accès par attributs (ABAC) dans IAM Identity Center
- Exemples de politique ABAC

Vidéos connexes :

- Gestion des autorisations des utilisateurs à grande échelle avec IAM Identity Center AWS
- Maîtrise des identités dans chaque couche

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 vous permettent de contrôler qui peut accéder à quoi et dans quelles conditions. En définissant des autorisations pour des identités humaines et des identités de machines spécifiques, vous leur donnez accès à des actions de service spécifiques sur des ressources spécifiques. En outre, vous pouvez spécifier les conditions qui doivent être remplies pour que l'accès soit accordé.

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

Politiques gérées : politiques autonomes basées sur une 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 en ligne maintiennent une relation un-à-un stricte entre une politique et 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 attachées à une ressource. Par exemple, une politique de compartiment S3 est une politique basée sur les ressources. Ces politiques accordent une autorisation à un principal 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 stratégies basées sur les ressources, consultez les services AWS qui fonctionnent avec IAM.

Les limites de permissions 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) dans AWS vous permet d'accorder des autorisations en fonction des attributs, qui sont appelés balises. Ces balises peuvent être attachées à des principaux IAM (utilisateurs ou rôles) et à des ressources AWS. Les administrateurs peuvent créer des politiques IAM réutilisables qui appliquent des autorisations en fonction des attributs du principal IAM. Par exemple, en tant qu'administrateur, vous pouvez utiliser une politique IAM unique pour accorder aux développeurs de votre organisation l'accès aux ressources AWS qui correspondent à leurs balises de projet. Lorsque l'équipe de développeurs ajoute des ressources aux projets, les autorisations sont automatiquement appliquées en fonction des attributs, ce qui élimine la nécessité de mettre à jour la politique pour chaque nouvelle ressource.

Les politiques de contrôle des services (SCP) des organisations définissent les autorisations maximales pour les comptes membres d'une organisation ou d'une unité d'organisation (OU). Les PCS 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 supposent 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 pour 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 barrières de protection des autorisations de votre organisation
- SEC03-BP06 Gérer l’accès en fonction du cycle de vie
- SEC03-BP07 Analyser l’accès public et intercompte
- 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

Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d’autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d’identité approprié et la méthode d’authentification et d’autorisation.

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

Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d’autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d’identité approprié et la méthode d’authentification et d’autorisation.

L’accès régulier à Comptes AWS au sein d’une organisation doit être assuré par un accès fédéré ou 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. AWS Les stratégies gérées établissent des politiques IAM prédéfinies qui couvrent les cas d'utilisation les plus courants.

Les services AWS, tels que AWS Secrets Manager et AWS Systems Manager Parameter Store, peuvent aider à dissocier les secrets de l'application ou de la charge de travail en toute sécurité. 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 Rôles Anywhere AWS IAM pour obtenir des informations d'identification de sécurité temporaires dans IAM pour les charges de travail qui s'exécutent en dehors d'AWS. Vos charges de travail peuvent utiliser les mêmes politiques IAM et rôles IAM que ceux que vous utilisez 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 lesquels vous avez besoin d'utilisateurs qui disposent d'un accès par programmation et d'informations d'identification à long terme, utilisez les informations les plus récentes de la clé d'accès pour faire pivoter et supprimer les clés d'accès.

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS en dehors de la Console de gestion AWS. La manière d'octroyer un accès par programmation dépend du type d'utilisateur qui accède à AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Recommandé) Utilisez des informations d'identification de la console temporaires pour signer des demandes par programmation destinées à la AWS CLI, aux kits AWS SDK ou aux API AWS.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour l'AWS CLI, consultez Connexion pour le développement local AWS dans le Guide de l'utilisateur

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
		de l'AWS Command Line Interface. • Pour les kits AWS SDK, consultez Connexion pour le développement local AWS dans le Guide de référence des outils et des kits AWS SDK.
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer des demandes par programmation destinées à la AWS CLI, aux AWS SDK ou aux API AWS.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour l'AWS CLI, consultez la rubrique Configuration de l'AWS CLI pour l'utilisation d'AWS IAM Identity Center dans le Guide de l'utilisateur AWS Command Line Interface. • Pour les kits SDK et les outils AWS ainsi que les API AWS, consultez la rubrique Authentification IAM Identity Center dans le Guide de référence des kits SDK et des outils AWS.
IAM	Utilisez des informations d'identification temporaires pour signer des demandes par programmation destinées à la AWS CLI, aux AWS SDK ou aux API AWS.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec des ressources AWS dans le Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes par programmation destinées à la AWS CLI, aux AWS SDK ou aux API AWS.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour l'AWS CLI, consultez la rubrique Authentification à l'aide des informations d'identification d'utilisateur IAM dans le Guide de l'utilisateur AWS Command Line Interface. • Pour les kits SDK et les outils AWS, consultez la rubrique Authentification à l'aide d'informations d'identification à long terme dans le Guide de référence des kits SDK et des outils AWS. • Pour les API AWS, consultez la rubrique Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Ressources

Documents connexes:

- Contrôle d'accès par attributs (ABAC)
- AWS IAM Identity Center
- Rôles Anywhere IAM
- AWS Politiques gérées par pour IAM Identity Center

- AWS Conditions des politiques IAM
- Cas d'utilisation de IAM
- Supprimer les informations d'identification inutiles
- Utilisation des stratégies
- Comment contrôler l'accès aux ressources AWS basées sur Compte AWS, OU, ou l'organisation
- Identifiez, organisez, et gérez les secrets de manière simple au travers de la recherche avancée dans AWS Secrets Manager

Vidéos connexes:

- Become an IAM Policy Master in 60 Minutes or Less
- 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

Accordez uniquement l'accès dont les utilisateurs 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 escompté : les utilisateurs ne disposent que des autorisations minimales requises pour leurs fonctions professionnelles spécifiques. Vous utilisez des Comptes AWS séparés pour isoler les développeurs des environnements de production. Lorsque les développeurs ont besoin d'accéder à des environnements de production pour des tâches spécifiques, un accès limité et contrôlé leur est accordé seulement pour la durée de ces tâches. Leur accès en production est immédiatement révoqué une fois qu'ils ont terminé les travaux nécessaires. Vous révisez régulièrement les autorisations et vous les révoquez rapidement lorsqu'elles ne sont plus nécessaires, par exemple lorsqu'un utilisateur change de rôle ou quitte l'organisation. Vous limitez les privilèges d'administrateur à un petit groupe de confiance afin de réduire l'exposition aux risques. Vous accordez aux comptes de machines ou de systèmes uniquement les autorisations minimales requises pour effectuer les tâches prévues.

Anti-modèles courants :

- Par défaut, vous accordez des autorisations d'administrateur aux utilisateurs.
- Vous utilisez le compte d'utilisateur racine pour les activités quotidiennes.
- Vous créez des politiques trop permissives sans les délimiter correctement.
- Vos révisions d'autorisations sont peu fréquentes, ce qui entraîne des dérives.
- Vous vous appuyez uniquement sur un contrôle d'accès basé sur les attributs pour l'isolation de l'environnement ou la gestion des autorisations.

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

Directives d'implémentation

Le principe du moindre privilège stipule que les identités ne devraient 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 ne disposent d'aucune autorisation. L'utilisateur racine dispose d'un accès complet par défaut et doit être étroitement contrôlé, surveillé et utilisé uniquement pour les tâches nécessitant un accès racine.

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 organisation AWS.

Vous pouvez également contrôler les demandes que les services AWS effectuent en votre nom, comme AWS CloudFormation qui crée une fonction AWS Lambda, à l'aide de la clé de condition CalledVia. Vous pouvez 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 vos équipes responsables de la charge de travail à créer leurs propres politiques IAM pour les systèmes qu'elles créent, mais seulement si elles appliquent une limite des autorisations afin de limiter le nombre maximal d'autorisations qu'elles peuvent accorder.

Étapes d'implémentation

- Implémentez des politiques de moindre privilège : attribuez des stratégies d'accès avec le moindre privilège aux groupes et rôles IAM pour rester cohérent avec le rôle ou la fonction de l'utilisateur que vous avez défini.
- Isolez les environnements de développement et de production via des Comptes AWS séparés : utilisez des Comptes AWS séparés pour les environnements de développement et de production, et contrôlez l'accès entre eux à l'aide de politiques de contrôle des services, de politiques de ressources et de politiques d'identité.
- Politiques de base relatives à l'utilisation de l'API : l'un des moyens de déterminer les autorisations nécessaires consiste à consulter les journaux AWS CloudTrail. Vous pouvez utiliser cette révision pour créer des autorisations adaptées aux actions effectivement réalisées par l'utilisateur dans AWS. IAM Access Analyzer peut générer automatiquement une politique IAM basée sur l'activité d'accès. Vous pouvez utiliser IAM Access Advisor au niveau de l'organisation ou du compte pour suivre les dernières informations consultées pour une stratégie donnée.
- 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 utile d'utiliser des politiques gérées par AWS pour les rôles professionnels courants, tels que la facturation, les administrateurs de base 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 de moindre privilège.
- Supprimez les autorisations inutiles : détectez et supprimez les entités, les informations d'identification et les autorisations IAM inutilisées afin d'appliquer le principe du moindre privilège. Vous pouvez utiliser l'Analyseur d'accès IAM pour identifier les accès externes et non utilisés, et la génération de politiques de l'Analyseur d'accès IAM peut aider à optimiser les politiques d'autorisation.
- Assurez-vous que les utilisateurs ont un accès limité aux environnements de production : les utilisateurs ne doivent avoir accès qu'aux environnements de production présentant 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 les limites des autorisations : une limite des autorisations est une fonctionnalité permettant d'utiliser une politique gérée qui définit les autorisations maximales qu'une politique basée sur l'identité peut accorder à une entité IAM. La limite d'autorisations d'une entité lui permet

d'effectuer uniquement les actions autorisées à la fois par ses politiques basées sur l'identité et ses limites d'autorisations.

- Affinez l'accès à l'aide du contrôle d'accès basé sur les attributs et des balises de ressources : un contrôle d'accès basé sur les attributs (ABAC) utilisant des balises de ressources peut être utilisé pour affiner les autorisations lorsqu'il est pris en charge. Vous pouvez utiliser un modèle ABAC qui compare les balises principales aux balises de ressources pour affiner l'accès en fonction des dimensions personnalisées que vous définissez. Cette approche permet de simplifier et de réduire le nombre de politiques d'autorisation au sein de votre organisation.
  - Il est recommandé d'utiliser uniquement ABAC pour le contrôle d'accès lorsque les principaux et les ressources appartiennent à votre organisation AWS. Les parties externes peuvent utiliser les mêmes noms de balises et les mêmes valeurs que votre organisation pour leurs propres principaux et ressources. Si vous vous appuyez uniquement sur ces paires nom-valeur pour accorder l'accès à des principaux ou à des ressources externes, vous pouvez fournir des autorisations involontaires.
- Utilisez des politiques de contrôle des services pour AWS Organizations : les politiques de contrôle des services contrôlent de façon centralisée les autorisations disponibles maximales pour les comptes membres de votre organisation. Il est important de noter que vous pouvez utiliser les politiques de contrôle des services pour limiter les autorisations des utilisateurs racine 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.
- Mettez en place une politique de cycle de vie des utilisateurs pour votre organisation : les politiques de cycle de vie des utilisateurs définissent les tâches à effectuer lorsque les utilisateurs sont intégrés dans AWS, changent de rôle ou de champ d'activité, ou n'ont plus besoin d'accéder à AWS. Examinez les autorisations à chaque étape du cycle de vie d'un utilisateur pour vous assurer qu'elles sont suffisamment restrictives et éviter les dérives.
- Établissez un calendrier régulier pour vérifier les autorisations et supprimer les autorisations inutiles : vous devez régulièrement vérifier l'accès des utilisateurs pour vérifier qu'il n'est pas trop permissif. AWS Config et l'Analyseur d'accès IAM peuvent aider lors des audits des autorisations des utilisateurs.
- Établissez une matrice des rôles professionnels : une matrice des rôles professionnels permet de visualiser les différents rôles et niveaux d'accès requis au sein de votre empreinte AWS. À l'aide d'une matrice des fonctions professionnelles, 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 à des utilisateurs ou à des rôles individuels.

Ressources

Documents connexes :

- Accorder le moindre privilège
- Limites des autorisations pour les entités IAM
- Techniques d'écriture de politiques IAM selon le principe de moindre privilège
- IAM Access Analyzer facilite la mise en œuvre d'autorisations de moindre privilège en générant des politiques IAM en fonction de l'activité d'accès
- Déléguez la gestion des autorisations aux développeurs en utilisant les limites des autorisations IAM
- Ajustement des autorisations à l'aide des dernières informations consultées
- Types de politiques IAM et leur utilisation
- Test des politiques IAM avec le simulateur de politiques IAM
- Barrières de protection dans AWS Control Tower
- Architectures Zero Trust : Une perspective AWS
- Comment implémenter le principe du moindre privilège avec CloudFormation StackSets
- Contrôle d'accès par attributs (ABAC)
- Réduction de la portée de la stratégie en affichant l'activité des utilisateurs
- Afficher l'accès au rôle
- Use Tagging to Organize Your Environment and Drive Accountability
- Stratégies de balisage AWS
- Balisage de ressources AWS

Vidéos connexes :

- Gestion des autorisations de prochaine génération
- Zero Trust : Une perspective AWS

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 leurs charges 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 escompté :

- 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 ainsi que les bonnes pratiques sont disponibles dans le pilier Fiabilité. Ils servent 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 utilisateurs et les rôles IAM, ainsi que les rôles IAM intercompte 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 pré-créant des ressources, vous n'êtes pas tributaire des API du plan de contrôle AWS (utilisées pour créer et modifier des ressources AWS) qui peuvent ne pas être disponibles en cas d'urgence. Par ailleurs, en créant au préalable les ressources IAM, vous n'avez pas besoin de prendre en compte les retards potentiels dus à une éventuelle cohérence.
- 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.
- Mettez en œuvre des mécanismes robustes de journalisation, de surveillance et d'alerte pour le processus et les mécanismes d'accès d'urgence. Générez des journaux d'audit détaillés pour toutes les tentatives réussies et échouées d'obtenir un accès d'urgence. Établissez une corrélation entre l'activité et les événements d'urgence en cours à partir de votre système de gestion des

incidents, et lancez des alertes lorsque des actions se produisent en dehors des périodes prévues ou lorsque le compte d'accès d'urgence est utilisé pendant les opérations normales. Le compte d'accès d'urgence ne doit être accessible qu'en cas d'urgence, car les procédures de bris de glace peuvent être considérées comme une porte dérobée. Intégrez-le à votre outil de gestion des informations et des événements de sécurité (SIEM) ou à AWS Security Hub CSPMpour signaler et auditer toutes les activités pendant la période d'accès d'urgence. À la reprise des activités normales, effectuez une rotation automatique des informations d'identification d'accès d'urgence et informez les équipes concernées.

- 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 en utilisant 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 utilisateurs IAM) 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 intercomptes 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 pré-créer un ensemble d'utilisateurs IAM pour vos administrateurs d'urgence dans le compte d'accès d'urgence avec des mots de passe robustes et des jetons MFA associés. Ces utilisateurs IAM 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 utilisateur IAM 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 utilisateurs IAM avec leurs mots de passe de longue durée de vie et leurs jetons MFA associés.
- Vous pouvez utiliser l'utilisateur racine 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 robuste et plusieurs jetons MFA pour l'utilisateur racine. 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 de 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 racine 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 racine. Vous devez auditer les événements du journal de votre coffre-fort d'entreprise pour identifier quel administrateur a extrait le mot de passe de l'utilisateur racine.

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 le IAM Identity Center auprès d'un fournisseur d'identité externe ou créer un fournisseur d'identité (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 IAM Identity Center ou Région AWS serait interrompue, nous vous recommandons de créer une configuration que vous pourrez utiliser pour assurer un accès temporaire à la Console de gestion AWS.

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 l'accès d'urgence à la Console de gestion AWS.

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 utilisateurs IAM et, éventuellement, les fournisseurs d'identité IAM. En outre, créez au préalable des rôles IAM intercomptes dans les Comptes AWS de la charge de travail et établir des relations d'approbation avec les rôles IAM correspondants dans le compte d'accès d'urgence. Vous pouvez utiliser CloudFormation StackSets avec AWS Organizations pour créer ces ressources dans les comptes membres de votre organisation.

- Créez les politiques de contrôle des services (SCP) AWS Organizations pour refuser la suppression et la modification des rôles IAM intercomptes 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 de votre 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 utilisateurs IAM : créez au préalable les utilisateurs IAM avec des mots de passe robustes et les dispositifs MFA associés.
  - Avec l'utilisateur racine du compte d'urgence : configurez l'utilisateur racine avec un mot de passe robuste 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 racine 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 la rubrique Configurez l'accès d'urgence à Console de gestion AWS, 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 (IdP) 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 Console de gestion AWS
- Activation de l'accès des utilisateurs fédérés SAML 2.0 à la Console de gestion AWS
- 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 - Gestion des identités et des accès AWS (IAM) deep dive

Exemples connexes:

- AWS Break Glass Role
- AWS Cadre de playbook client
- AWS Modèles de playbooks de réponse aux incidents

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 ainsi que les autorisations inutilisées pour les accès humains et machines.

Résultat escompté : les politiques d'autorisation doivent respecter le principe de 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 sans tous les privilèges d'administrateur.
- Maintien des politiques d'autorisation une fois qu'elles ne sont plus nécessaires.

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

Directives d'implémentation

Lorsque les équipes et les projets sont à leur début, 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 non utilisés. AWS peut également faciliter l'analyse de l'activité d'accès des utilisateurs et rôles IAM, notamment des clés d'accès, 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 par attributs (ABAC) peut contribuer à 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 : l'analyseur d'accès IAM vous aide à identifier les ressources de votre organisation et de vos comptes comme les compartiments Amazon Simple Storage Service (Amazon S3) ou les rôles IAM, qui sont partagées avec une entité externe.
- Utilisez la génération de politiques de l'Analyseur d'accès IAM : la génération de politiques de l'Analyseur d'accès IAM vous permet de créer des politiques d'autorisation précises reposant sur l'activité d'accès d'un utilisateur ou d'un rôle IAM.
- Testez les autorisations dans les environnements inférieurs avant la production : commencez par utiliser les environnements de développement et de test (sandbox) les moins critiques pour tester les autorisations requises pour les différentes fonctions professionnelles à l'aide de l'Analyseur d'accès IAM. Ensuite, renforcez progressivement et validez ces autorisations dans les environnements de test, d'assurance qualité et intermédiaires avant de les appliquer en production. Les environnements inférieurs peuvent avoir des autorisations plus souples au départ, car les politiques de contrôle des services (SCP) constituent un garde-fou en limitant le nombre maximal d'autorisations accordées.
- Déterminez un délai et une politique d'utilisation acceptables pour les utilisateurs et les rôles IAM : utilisez l'horodatage du dernier accès pour identifier les utilisateurs et les rôles non utilisés et les supprimer. Consultez les informations relatives aux services et actions consultées 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 spécifiques d'Amazon S3 dont votre rôle d'application a besoin et limiter l'accès du rôle à celles-ci uniquement. Les fonctionnalités relatives aux informations sur les derniers accès sont disponibles dans la Console de gestion AWS 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 n'enregistre pas les événements de données tels que l'activité au niveau des objets Amazon S3 (par exemple, `GetObject` et `DeleteObject`) ou les activités de tables 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:

- Accorder le moindre privilège
- Supprimer les informations d'identification inutiles
- Présentation de AWS CloudTrail?
- Utilisation des stratégies
- Journalisation et surveillance dans DynamoDB
- Utilisation de la journalisation des événements CloudTrail pour vos compartiments et objets Amazon S
- 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 - Gestion des identités et des accès AWS (IAM) deep dive

SEC03-BP05 Définir des barrières de protection des autorisations de votre organisation

Utilisez des barrières de protection pour réduire la portée des autorisations disponibles qui peuvent être accordées aux principaux. La chaîne d'évaluation des politiques d'autorisation inclut vos barrières de protection pour déterminer les autorisations effectives d'un principal lorsqu'il prend des décisions d'autorisation. Vous pouvez définir des barrières de protection à l'aide d'une approche par couches. Appliquez certaines barrières de protection de manière générale à l'ensemble de votre organisation et appliquez-en d'autres de manière granulaire aux sessions d'accès temporaires.

Résultat escompté : garantir une séparation claire des environnements en utilisant les Comptes AWS distincts. Les politiques de contrôle des services (SCP) sont utilisées pour définir des barrières de protection des autorisations à l'échelle de l'organisation. Des barrières de protection plus étendues sont définies aux niveaux hiérarchiques les plus proches de la racine de votre organisation, tandis que des barrières de protection plus strictes sont définies plus près du niveau des comptes individuels.

Lorsqu'elles sont prises en charge, les politiques de ressources définissent les conditions qu'un principal doit remplir pour accéder à une ressource. Les politiques relatives aux ressources définissent également l'ensemble des actions autorisées, le cas échéant. Les limites d'autorisation sont placées sur les principaux qui gèrent les autorisations de charge de travail, en déléguant la gestion des autorisations aux propriétaires individuels de la charge de travail.

Anti-modèles courants :

- Création d'un Comptes AWS membre au sein d'une organisation AWS, sans utiliser les SCP pour restreindre l'utilisation et les autorisations accordées à leurs informations d'identification racine.
- Attribution des autorisations en fonction du principe de moindre privilège, sans placer de barrières de protection sur l'ensemble maximum d'autorisations pouvant être accordées.
- S'appuyer sur le principe de refus implicite d'IAM AWS pour restreindre les autorisations, en étant sûr que les politiques n'accorderont pas d'autorisation explicite indésirable.
- Exécuter plusieurs environnements de charge de travail dans le même Compte AWS, puis s'appuyer sur des mécanismes tels que des VPC, des balises ou des politiques de ressources pour appliquer les limites d'autorisation.

Avantages de l'adoption de cette bonne pratique : les barrières de protection des autorisations contribuent à garantir le refus des autorisations indésirables, même lorsqu'une politique d'autorisation tente de le faire. Cette mesure peut simplifier la définition et la gestion des autorisations en réduisant la portée maximale des autorisations à prendre en compte.

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

Directives d'implémentation

Nous vous recommandons d'utiliser une approche par couches afin de définir les barrières de protection des autorisations de votre organisation. Cette approche réduit systématiquement l'ensemble maximum d'autorisations possibles à mesure que des couches supplémentaires sont

appliquées. Cela vous permet d'accorder l'accès sur la base du principe de moindre privilège, réduisant ainsi le risque d'accès involontaire dû à une mauvaise configuration des politiques.

La première étape pour établir des barrières de protection des autorisations consiste à isoler vos charges de travail et vos environnements dans des Comptes AWS distincts. Les principaux d'un compte ne peuvent pas accéder aux ressources d'un autre sans autorisation explicite, même lorsque les deux comptes appartiennent à la même organisation AWS ou à la même unité organisationnelle (OU). Vous pouvez utiliser les unités organisationnelles pour regrouper les comptes que vous souhaitez administrer en tant qu'unité unique.

L'étape suivante consiste à réduire le nombre maximum d'autorisations que vous pouvez accorder aux principaux au sein des comptes membres de votre organisation. Pour ce faire, vous pouvez utiliser des politiques de contrôle des services (SCP), que vous pouvez appliquer soit à une unité d'organisation, soit à un compte. Les SCP peuvent appliquer des contrôles d'accès courants, tels que la restriction de l'accès à des Régions AWS spécifiques, la protection contre la suppression des ressources ou la désactivation d'actions de service potentiellement risquées. Les SCP que vous appliquez à la racine de votre organisation n'affectent que ses comptes membres, et non le compte de gestion. Les SCP régissent uniquement les principaux au sein de votre organisation. Vos SCP ne régissent pas les principaux, extérieurs à votre organisation, qui accèdent à vos ressources.

Si vous utilisez AWS Control Tower, vous pouvez tirer parti de ses contrôles et de ses zones de destination comme base de vos garde-fous d'autorisations et de votre environnement multi-compte. Les zones de destination fournissent un environnement de base sécurisé préconfiguré avec des comptes distincts pour différentes charges de travail et applications. Les garde-fous appliquent des contrôles obligatoires en matière de sécurité, d'exploitation et de conformité par le biais d'une combinaison de politiques de contrôle des services (SCP), de règles AWS Config et d'autres configurations. Toutefois, lorsque vous utilisez les garde-fous et les zones de destination Control Tower en plus des politiques SCP personnalisées de l'organisation, il est essentiel de suivre les bonnes pratiques décrites dans la documentation AWS afin d'éviter les conflits et de garantir une bonne gouvernance. Reportez-vous aux recommandations AWS Control Tower pour AWS Organizations afin d'obtenir des recommandations détaillées sur la gestion des politiques SCP, des comptes et des unités organisationnelles (OU) dans un environnement Control Tower.

En respectant ces directives, vous pouvez tirer parti efficacement des garde-fous, des zones de destination et des politiques SCP personnalisées de Control Tower tout en atténuant les conflits potentiels et en garantissant une gouvernance et un contrôle appropriés de votre environnement AWS multi-compte.

Une autre étape consiste à utiliser les politiques de ressources IAM pour définir les actions disponibles que vous pouvez effectuées sur les ressources qu'elles régissent, ainsi que les conditions que le principal par intérim doit respecter. Vous pouvez donc autoriser toutes les actions pour le principal faisant partie de votre organisation (en utilisant la clé de condition PrincipalOrgId), ou restreindre les permissions à certaines actions spécifiques pour un rôle IAM particulier. Vous pouvez adopter une approche similaire avec des conditions dans les politiques d'approbation des rôles IAM. Si une politique d'approbation en matière de ressources ou de rôles désigne explicitement un principal dans le même compte que le rôle ou la ressource qu'elle gère, ce principal n'a pas besoin de politique IAM associée qui accorde les mêmes autorisations. Si le principal se trouve dans un compte différent de celui de la ressource, il a besoin d'une politique IAM associée qui accorde ces autorisations.

La plupart du temps, une équipe responsable d'une charge de travail souhaite gérer les autorisations requises pour sa charge de travail. Cette situation peut nécessiter la création de nouveaux rôles IAM et de nouvelles politiques d'autorisation. Vous pouvez saisir la portée maximale des autorisations que l'équipe peut accorder dans une limite d'autorisations IAM, puis associer ce document à un rôle IAM que l'équipe pourra utiliser pour gérer ses rôles et autorisations IAM. Cette approche peut lui donner la liberté de terminer son travail, tout en limitant les risques liés au fait de disposer d'un accès administratif IAM.

Une étape plus précise consiste à implémenter des techniques de gestion des accès privilégiés (PAM) et de gestion d'accès élevés temporaires (TEAM). Un exemple de PAM consiste à demander aux principaux de procéder à une authentification multifactorielle avant d'entreprendre des actions privilégiées. Pour plus d'informations, consultez la section Configuration de l'accès aux API protégé par MFA. TEAM a besoin d'une solution qui gère l'approbation et le délai pendant lequel un principal est autorisé à bénéficier d'un accès élevé. Une approche consiste à ajouter temporairement le principal à la politique d'approbation des rôles pour un rôle IAM dont l'accès est élevé. Une autre approche consiste, dans le cadre d'un fonctionnement normal, à réduire les autorisations accordées à un principal par un rôle IAM à l'aide d'une politique de session, puis à lever temporairement cette restriction pendant la période approuvée. Pour en savoir plus sur les solutions que AWS et validées par certains partenaires, consultez la section Accès élevé temporaire.

Étapes d'implémentation

1. Isolez vos charges de travail et vos environnements dans des Comptes AWS distincts.
2. Utilisez les SCP pour réduire le nombre maximum d'autorisations pouvant être accordées aux principaux sur les comptes membres de votre organisation.

   a. Lorsque vous définissez des politiques SCP pour réduire le nombre maximal d'autorisations pouvant être accordées aux principaux sur les comptes membres de votre organisation, vous pouvez choisir entre une approche avec liste d'autorisations ou liste de refus. La stratégie avec liste d'autorisations spécifie explicitement les accès autorisés et bloque implicitement tous les autres accès. La stratégie avec liste de refus spécifie explicitement les accès qui sont refusés et autorise par défaut tous les autres accès. Ces deux stratégies ont leurs avantages et leurs inconvénients, et le choix approprié dépend des exigences spécifiques et du modèle de risque de votre organisation. Pour plus de détails, consultez Stratégie d'utilisation des politiques SCP.
   b. En outre, passez en revue les exemples de politiques de contrôle des services pour comprendre comment élaborer efficacement des politiques SCP.
3. Utilisez les politiques relatives aux ressources IAM pour réduire la portée et spécifier les conditions des actions autorisées sur les ressources. Utilisez les conditions des politiques d'approbation relatives aux rôles IAM pour créer des restrictions quant à l'attribution des rôles.
4. Attribuez des limites d'autorisation IAM aux rôles IAM que les équipes de la charge de travail peuvent ensuite utiliser afin de gérer leurs propres rôles et autorisations IAM en matière de charge de travail.
5. Évaluez les solutions PAM et TEAM en fonction de vos besoins.

Ressources

Documents connexes:

- Périmètres de données sur AWS
- Mettez en place des barrières de protection des autorisations à l'aide de périmètres de données
- Logique d'évaluation de stratégies

Exemples associés:

- Exemples de politiques de contrôle des services

Outils associés:

- AWS Solution : gestion des accès élevés temporaires (TEAM
- Solutions validées de partenaires en matière de sécurité pour TEAM

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

Surveillez et ajustez les autorisations accordées à vos principaux (utilisateurs, rôles et groupes) tout au long de leur cycle de vie au sein de votre organisation. Ajustez les appartenances aux groupes lorsque les utilisateurs changent de rôle et supprimez l’accès lorsqu’un utilisateur quitte l’organisation.

Résultat escompté : vous surveillez et ajustez les autorisations tout au long du cycle de vie des principaux au sein de l’organisation, réduisant ainsi le risque de privilèges inutiles. Vous accordez l’accès approprié lorsque vous créez un utilisateur. Vous modifiez l’accès en fonction de l’évolution des responsabilités de l’utilisateur et vous supprimez l’accès lorsque l’utilisateur n’est plus actif ou s’il a quitté l’organisation. Vous gérez de manière centralisée les modifications apportées à vos utilisateurs, rôles et groupes. Vous utilisez l’automatisation pour propager les modifications à vos environnements AWS.

Anti-modèles courants :

- Accorder en amont des privilèges d’accès excessifs ou étendus aux identités, au-delà de ce qui est initialement requis.
- Ne pas examiner et ne pas ajuster les privilèges d’accès au fur et à mesure de l’évolution des rôles et des responsabilités des identités.
- Laisser des identités inactives ou résiliées avec des privilèges d’accès actifs. Cela augmente le risque d’accès non autorisé.
- Ne pas tirer parti de l’automatisation pour gérer le cycle de vie des identités.

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

Directives d’implémentation

Gérez et ajustez avec soin les privilèges d’accès que vous accordez aux identités (telles que les utilisateurs, les rôles, les groupes) tout au long de leur cycle de vie. Ce cycle de vie comprend la phase initiale d’intégration, les changements continus des rôles et des responsabilités, et le départ ou la résiliation éventuels. Gérez l’accès de manière proactive en fonction de l’étape du cycle de vie afin de maintenir un niveau d’accès approprié. Optez pour le principe du moindre privilège afin de réduire le risque de privilèges d’accès excessifs ou inutiles.

Vous pouvez gérer le cycle de vie des utilisateurs IAM directement dans le Compte AWS ou par le biais d’une fédération entre le fournisseur d’identité de votre personnel et AWS IAM Identity

Center. Pour les utilisateurs IAM, vous pouvez créer, modifier et supprimer des utilisateurs et leurs autorisations associées dans le Compte AWS. Pour les utilisateurs fédérés, vous pouvez utiliser IAM Identity Center afin de gérer leur cycle de vie en synchronisant les informations relatives aux utilisateurs et aux groupes provenant du fournisseur d'identité de votre organisation à l'aide du protocole System for Cross-domain Identity Management (SCIM).

SCIM est un protocole standard ouvert pour le provisionnement et le déprovisionnement automatisés des identités des utilisateurs sur différents systèmes. En intégrant votre fournisseur d'identité avec IAM Identity Center à l'aide de SCIM, vous pouvez synchroniser automatiquement les informations des utilisateurs et des groupes, ce qui aide à valider que les privilèges d'accès sont accordés, modifiés ou révoqués en fonction des modifications apportées à la source d'identité officielle de votre organisation.

Ajustez les privilèges en fonction de l'évolution des rôles et responsabilités des employés au sein de votre organisation. Vous pouvez utiliser les ensembles d'autorisations d'IAM Identity Center pour définir différents rôles ou responsabilités professionnels et les associer aux politiques et autorisations IAM Identity Center appropriées. Lorsque le rôle d'un employé change, vous pouvez mettre à jour l'ensemble d'autorisations qui lui a été attribué de façon à refléter ses nouvelles responsabilités. Vérifiez qu'il dispose de l'accès nécessaire tout en respectant le principe du moindre privilège.

Étapes d'implémentation

1. Définissez et documentez un processus de gestion des accès tout au long du cycle de vie, y compris les procédures relatives à l'octroi de l'accès initial, aux révisions périodiques et à la révocation de l'accès.
2. Mettez en œuvre les rôles, groupes et limites des autorisations IAM pour gérer l'accès collectivement et appliquer des niveaux d'accès maximaux autorisés.
3. Intégrez un fournisseur d'identité fédéré (tel que Microsoft Active Directory, Okta, Ping Identity) en tant que source officielle d'informations sur les utilisateurs et les groupes utilisant IAM Identity Center.
4. Utilisez le protocole SCIM pour synchroniser les informations sur les utilisateurs et les groupes provenant du fournisseur d'identité dans l'Identity Store d'IAM Identity Center.
5. Dans IAM Identity Center, créez des ensembles d'autorisations qui représentent les différents rôles ou responsabilités au sein de votre organisation. Définissez les politiques et les autorisations IAM appropriées pour chaque ensemble d'autorisations.
6. Mettez en œuvre des contrôles d'accès réguliers, une révocation rapide des accès et une amélioration continue du processus de gestion du cycle de vie des accès.

7. Formez et sensibilisez les employés aux bonnes pratiques de gestion des accès.

Ressources

Bonnes pratiques associées :

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

Documents connexes :

- Gérer votre source d'identité
- Gestion des identités dans IAM Identity Center
- Utilisation de AWS Identity and Access Management Access Analyzer
- Génération d'une politique de l'Analyseur d'accès IAM

Vidéos connexes :

- AWS re:Inforce 2023 - Manage temporary elevated access with AWS IAM Identity Center
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Invent 2022 - Harness power of IAM policies & rein in permissions w/Access Analyzer

SEC03-BP07 Analyser l'accès public et intercompte

Surveillez continuellement les résultats qui mettent en évidence l'accès public et intercompte. Limitez l'accès public et l'accès intercompte aux seules ressources spécifiques qui nécessitent cet accès.

Résultat escompté : connaitre quelles de vos 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 d'exposition au risque si cette bonne pratique n'est pas respectée : bas

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 basées sur les ressources, par exemple les politiques de compartiment Amazon Simple Storage Service (Amazon S3), ou en autorisant le principal d'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. Définir un processus d'approbation de toutes les ressources qui doivent être accessibles au public.

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

AWS Config peut signaler les ressources mal configurées et, par le biais de vérifications des politiques AWS Config, détecter les ressources dont l'accès public est configuré. Les services tels que AWS Control Tower et AWS Security Hub CSPM simplifient le déploiement des contrôles de détection et des barrières de protection sur AWS Organizations afin d'identifier et de corriger les ressources exposées au public. Par exemple, AWS Control Tower dispose d'une barrière de protection gérée qui peut détecter si des instantanés d'Amazon EBS sont restaurés par Comptes AWS.

Étapes d'implémentation

- Envisagez d'utiliser AWS Config for AWS Organizations : AWS Config vous permet d'agréger les résultats de plusieurs comptes d'un AWS Organizations vers un compte d'administrateur délégué. Cela fournit une vue complète et vous permet de déployer AWS Config Rules sur plusieurs comptes afin de détecter les ressources accessibles au public.

- Configurez AWS Identity and Access Management Access Analyzer : l'Analyseur d'accès IAM vous aide à identifier les ressources dans votre organisation et vos comptes, telles que les compartiments Amazon S3 ou les rôles IAM, qui sont partagés avec une entité externe.
- Utilisez la correction automatique AWS Config pour effectuer les modifications de la configuration de l'accès public des compartiments Amazon S3 : vous pouvez activer automatiquement les paramètres de blocage de l'accès public pour les compartiments Amazon S3.
- Implémentez la surveillance et les alertes pour déterminer si les compartiments Amazon S3 sont devenus publics : vous devez mettre en place un système de surveillance et d'alerte pour détecter si le blocage de l'accès public Amazon S3 est désactivé et si les compartiments Amazon S3 deviennent publics. En outre, si vous utilisez AWS Organizations, vous pouvez créer une politique de contrôle de services qui empêche toute modification des stratégies d'accès public d'Amazon S3. AWS Trusted Advisor vérifie les compartiments Amazon S3 dont les autorisations permettent un accès libre. 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 de compartiment. Vous pouvez également utiliser AWS Config pour surveiller l'accès public de vos compartiments Amazon S3. Pour plus d'informations, consultez la section Comment utiliser AWS Config pour surveiller et gérer les compartiments Amazon S3 autorisant l'accès public.

Lorsque vous examinez les contrôles d'accès pour les compartiments Amazon S3, il est important de prendre en compte la nature des données qui y sont stockées. Amazon Macie est un service conçu pour vous aider à découvrir et à protéger les données sensibles, telles que les données d'identification personnelle (PII), les informations protégées sur la santé (PHI) et les informations d'identification telles que les clés privées ou les clés d'accès AWS.

Ressources

Documents connexes :

- Utilisation de AWS Identity and Access Management Access Analyzer
- Bibliothèque de contrôles AWS Control Tower
- Norme concernant les bonnes pratiques de sécurité de base AWS
- AWS Config Règles gérées
- Référence de la vérification AWS Trusted Advisor

- Surveillance des résultats des vérifications AWS Trusted Advisor avec Amazon EventBridge
- Gestion des règles AWS Config pour tous les comptes de votre organisation
- AWS Config and AWS Organizations
- Mise à disposition de votre AMI au public pour son utilisation dans Amazon EC2

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 escompté : minimisez les accès involontaires en utilisant des méthodes sécurisées pour partager les ressources au sein de votre organisation et contribuer à votre initiative de prévention des pertes 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 obtenir des conseils prescriptifs sur l'analyse des ressources partagées en externe, voir SEC03-BP07 Analyser l'accès public et intercompte.

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 d'exposition au risque si cette bonne pratique n'est pas respectée : 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 visant à réduire l'accès externe aux seules ressources qui en ont besoin, et à établir un processus de surveillance continue et d'alerte automatique.

Le partage entre comptes au sein de AWS Organizations est pris en charge par un certain nombre de services AWS, tels que AWS Security Hub CSPM, 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 CSPM peut transférer les résultats des comptes individuels vers un compte central où vous pouvez voir tous ces résultats. AWS Backup peut prendre une sauvegarde pour une ressource et la partager entre les comptes. Vous pouvez utiliser AWS Resource Access Manager (AWS RAM) pour partager d'autres ressources communes, telles que des sous-réseaux VPC et des attachements de la passerelle de transit, AWS Network Firewall ou des pipelines d'IA Amazon SageMaker.

Pour empêcher votre compte de partager uniquement les ressources au sein de votre organisation, utilisez des politiques de contrôle des services (SCP) pour empêcher l'accès aux principaux externes. Lorsque vous partagez des ressources, combinez les contrôles basés sur l'identité et les contrôles réseau pour créer un périmètre de données pour votre organisation afin de la protéger contre tout accès non intentionnel. 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 d'un VPC et la condition

`AWS:PrincipalOrgId` pour garantir que les identités accédant à vos compartiments Amazon S3 appartiennent à votre organisation. Il est important de noter que les SCP ne s'appliquent pas aux rôles liés aux services ou aux principaux de service AWS.

Lorsque vous utilisez Amazon S3, désactivez les ACL pour votre compartiment Amazon S3 et utilisez les politiques IAM pour définir le contrôle d'accès. Pour restreindre l'accès à une origine Amazon S3 à partir d'Amazon CloudFront, migrez l'identité d'accès d'origine (OAI) vers le contrôle d'accès d'origine (OAC) qui prend en charge des fonctionnalités supplémentaires, dont 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 obtenir des conseils prescriptifs sur la gestion des autorisations de partage de ressources en externe, consultez la section Gestion des autorisations.

Étapes d'implémentation

1. Utilisez AWS Organizations : AWS Organizations est un service de gestion de comptes qui vous permet de consolider plusieurs Comptes AWS en une organisation que vous créez et gérez de façon centralisée. Vous pouvez regrouper vos comptes en unités d'organisation (OU) 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 utilisez un service AWS pour exécuter des tâches en votre nom dans les comptes membres de votre organisation, AWS Organizations crée un rôle lié à un service IAM (SLR) pour ce service dans chaque compte membre. Gérez l'accès approuvé à l'aide de la Console de gestion AWS, des API AWS ou de la AWS CLI. Pour obtenir des conseils prescriptifs sur l'activation de l'accès sécurisé, voir Utilisation d'AWS Organizations avec d'autres services AWS et services AWS que vous pouvez utiliser avec Organizations.
3. Établissez un périmètre de données : un périmètre de données fournit une délimitation claire de la confiance et de la propriété. Sur AWS, il est généralement représenté comme votre organisation AWS gérée par AWS Organizations, ainsi que par tous les réseaux ou systèmes sur site qui accèdent à vos ressources AWS. L'objectif du périmètre de données est de vérifier que l'accès est autorisé si l'identité est approuvée, si la ressource est approuvée et si le réseau est attendu. Toutefois, l'établissement d'un périmètre de données n'est pas une approche universelle. Évaluez et adoptez les objectifs de contrôle décrits dans le livre blanc Construire un périmètre sur AWS

sur la base de vos modèles de risques de sécurité et de vos exigences spécifiques. Vous devez examiner attentivement votre position unique en matière de risque et mettre en œuvre les contrôles périmétriques adaptés à vos besoins en matière de sécurité.

4. Utilisez le partage des ressources dans les services AWS et limitez en conséquence : de nombreux services AWS vous permettent de partager des ressources avec un autre compte ou de cibler une ressource d'un autre compte, comme Amazon Machine Images (AMI) et AWS Resource Access Manager (AWS RAM). Limitez l'API `ModifyImageAttribute` pour spécifier les comptes fiables avec lesquels partager l'AMI. Spécifiez la condition `ram:RequestedAllowsExternalPrincipals` lors de l'utilisation de AWS RAM pour limiter le partage à votre organisation uniquement, afin d'empêcher l'accès par des identités non fiables. Pour des conseils et des considérations prescriptifs, voir 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 transformer le partage de ressources en partage de ressources 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 intercompte
- 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
- Établissement d'un périmètre de données sur AWS : autoriser uniquement les identités fiables à accéder aux données de l'entreprise

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 stratégies relatives au périmètre des 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 du système administré par un tiers doit suivre la pratique de l'accès à la demande en appliquant le principe de moindre privilège avec des informations d'identification temporaires. En travaillant en étroite collaboration avec un tiers, vous pouvez réduire l'étendue de l'impact et du risque d'accès involontaire.

Résultat escompté : vous évitez d'utiliser des informations d'identification à long terme Gestion des identités et des accès AWS (IAM) telles que des clés d'accès et des clés secrètes, car elles présentent un risque de sécurité en cas d'utilisation abusive. Vous utilisez plutôt des rôles IAM et des informations d'identification temporaires pour améliorer votre niveau de sécurité et minimiser les frais opérationnels liés à la gestion des informations d'identification à long terme. Lorsque vous accordez

l'accès à un tiers, vous utilisez un identifiant unique universel (UUID) comme ID externe dans la politique d'approbation IAM et vous maintenez sous votre contrôle les politiques IAM attachées au rôle afin de garantir un accès sur la base du moindre privilège. Pour obtenir des conseils prescriptifs sur l'analyse des ressources partagées en externe, consultez SEC03-BP07 Analyser l'accès public et intercompte.

Anti-modèles courants :

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

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : 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. Définissez également 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 les Rôles Anywhere IAM afin de gérer les rôles IAM pour des applications autres que AWS qui utilisent des 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, comme l'AWS Well-Architected Tool qui permet le partage d'une charge de travail avec d'autres Comptes AWS et AWS Resource Access Manager qui 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 accéder aux comptes externes. Les rôles intercomptes réduisent la quantité d'informations sensibles stockées par les comptes externes et les tiers pour servir leurs clients. Les rôles intercomptes vous permettent d'accorder l'accès aux ressources

AWS de votre compte en toute sécurité à un tiers, par exemple aux partenaires AWS ou à d'autres comptes de votre organisation, tout en préservant la capacité de gérer et d'auditer cet accès. Il se peut que le tiers vous fournisse des services à partir d'une infrastructure hybride ou qu'il extraie des données vers un emplacement externe. Rôles Anywhere IAM vous permet d'autoriser des charges de travail tierces à interagir en toute sécurité avec vos charges de travail AWS et de réduire encore le besoin d'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. Faites preuve d'une diligence raisonnable et garantissez un accès sécurisé aux fournisseurs SaaS tiers. Lorsque vous partagez des ressources avec des fournisseurs SaaS tiers, faites preuve de toute la diligence appropriée pour vous assurer qu'ils adoptent une approche sûre et responsable de l'accès à vos ressources AWS. Évaluez leur modèle de responsabilité partagée pour comprendre les mesures de sécurité qu'ils fournissent et celles qui relèvent de votre responsabilité. Assurez-vous que le fournisseur SaaS dispose d'un processus sécurisé et auditable pour accéder à vos ressources, y compris l'utilisation d'identifiants externes et les principes d'accès sur la base du moindre privilège. L'utilisation d'identifiants externes permet de résoudre le problème de l'adjoint confus.

   Mettez en œuvre des contrôles de sécurité pour garantir un accès sécurisé et le respect du principe du moindre privilège lorsque vous accordez l'accès à des fournisseurs SaaS tiers. Cela peut inclure l'utilisation d'identifiants externes, d'identifiants uniques universels (UUID) et de politiques d'approbation IAM qui limitent l'accès au strict nécessaire. Travaillez en étroite collaboration avec le fournisseur SaaS pour établir des mécanismes d'accès sécurisés, passez régulièrement en revue son accès à vos ressources AWS et effectuez des audits pour garantir le respect de vos exigences de sécurité.
3. Rendez obsolètes les informations d'identification à long terme fournies par le client. Rendez obsolète l'utilisation d'informations d'identification à long terme et utilisez des rôles intercomptes ou Rôles Anywhere IAM. Si vous devez utiliser des informations d'identification à long terme, élaborez un plan pour migrer vers un accès basé sur les rôles. Pour plus de détails sur la gestion des clés, consultez Gestion des identités. Collaborez également avec votre équipe Compte AWS et le tiers pour établir un dossier d¦exploitation d'atténuation des risques. Pour obtenir des conseils prescriptifs sur la réponse à un incident de sécurité et l'atténuation de son impact potentiel, consultez Réponse aux incidents.
4. Vérifiez que la configuration est guidée par des instructions prescriptives ou qu'elle est automatisée. L'ID externe n'est pas considéré 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 d'usurper la configuration.

Vous ou le tiers 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.

La politique créée pour l'accès intercompte à vos comptes doit respecter le principe de 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 pour 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 devez surveiller les changements via une détection des dérives dans le cadre de la pratique d'audit.

5. Tenez compte des 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 de 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 obtenir des conseils prescriptifs sur les méthodes de détection, consultez la section Bonnes pratiques en matière de détection.

Ressources

Bonnes pratiques associées :

- SEC02-BP02 Utiliser des informations d'identification temporaires

- SEC03-BP05 Définir des garde-fous des autorisations pour votre organisation
- SEC03-BP06 Gérer l’accès en fonction du cycle de vie
- SEC03-BP07 Analyser l’accès public et intercompte
- SEC04 Détection

Documents connexes :

- Le propriétaire du compartiment accorde une autorisation multicompte à des objets qu’il ne possède pas
- Comment utiliser des politiques d’approbation avec les rôles IAM
- Déléguer l’accès entre des Comptes AWS à l’aide des rôles IAM
- Comment accéder aux ressources d’un autre Compte AWS à l’aide d’IAM ?
- Bonnes pratiques de sécurité dans IAM
- Logique d’évaluation des politiques intercomptes
- Procédure d’utilisation d’un ID externe lorsque vous accordez l’accès à vos ressources AWS à un tiers
- Collecte d’informations à partir de ressources AWS CloudFormation créées dans des comptes externes avec des ressources personnalisées
- Utilisation sécurisée d’identifiants externes pour accéder à des comptes AWS détenus par d’autres
- Extension des rôles IAM à des charges de travail situées en dehors d’IAM avec Rôles Anywhere IAM

Vidéos connexes :

- Comment accorder à des utilisateurs ou des rôles situés dans un Compte AWS distinct l’accès à mon Compte AWS ?
- AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less
- AWS Knowledge Center Live : Bonnes pratiques IAM et décisions de conception

Exemples connexes :

- Configuration de l'accès intercompte à Amazon DynamoDB
- Outil de requête réseau AWS STS

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
- SEC04-BP02 Capturer les journaux, les résultats et les métriques dans des emplacements standardisés
- SEC04-BP03 Corréler et enrichir les alertes de sécurité
- SEC04-BP04 Lancer la correction pour les ressources non conformes

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 escompté : une organisation doit être en mesure de récupérer de manière fiable et cohérente les journaux des événements de sécurité des services et des applications AWS en temps opportun lorsque cela est nécessaire pour remplir un processus ou une obligation interne, comme une réponse à un 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 du respect de cette bonne pratique : mettez en œuvre un mécanisme d'analyse des causes profondes (RCA) pour les incidents de sécurité et une source de preuves pour vos obligations en matière de gouvernance, de risque et de conformité.

Niveau d'exposition au risque si cette bonne pratique n'est pas respectée : 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 utilisez les sources de journaux. Avant une enquête de sécurité, vous devez saisir les journaux pertinents pour reconstruire rétroactivement l’activité dans un Compte AWS. Sélectionnez les sources de journaux pertinentes pour vos charges de travail.

  Les critères de sélection des sources de journaux 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 rétention de 90 jours des événements de gestion qui peuvent être récupérés via l’historique des événements CloudTrail à l’aide de la Console de gestion AWS, de la AWS CLI ou d’un AWS SDK. Pour une conservation et une visibilité prolongées des événements liés aux données, créez un journal CloudTrail et associez-le à un compartiment Amazon S3, et éventuellement à un groupe de journaux Amazon CloudWatch. Vous pouvez également créer un CloudTrail Lake, qui conserve les journaux CloudTrail pendant une période maximale de sept ans et fournit une fonction de requête basée sur SQL

  AWS recommande aux clients utilisant un VPC d’activer le trafic réseau et les journaux DNS à l’aide des journaux de flux VPC et des journaux de requêtes d’Amazon Route 53 Resolver, respectivement, et de les diffuser vers 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 comment et 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 journal au format Apache Parquet et au format Open Cybersecurity Schema Framework (OCSF), qui est prêt à être interrogé. 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 résultats 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 des fonctionnalités cloud — Journalisation et événements du Guide de réponse aux incidents de sécurité AWS.

- Recherchez des capacités de journalisation pour chaque service et application AWS : chaque service et application AWS vous propose des options de stockage des journaux, chacune ayant ses propres capacités de conservation et de cycle de vie. Amazon Simple Storage Service (Amazon S3) et Amazon CloudWatch sont les deux services de stockage de journaux les plus courants. 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 Amazon CloudWatch Logs, 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 dépend généralement de l'outil de requête que vous utilisez, des capacités de conservation, de la familiarité et du 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 qu'Amazon Athena.

  Un groupe de journaux CloudWatch offre un stockage durable et une installation de requête intégrée via CloudWatch Logs Insights.
- Identifiez la rétention 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.

- Utilisez 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 de votre organisation, consultez les instructions de configuration de journalisation spécifiques :
  - Configurer AWS CloudTrail Trail
  - Configurer des journaux de flux VPC
  - Configurer Amazon GuardDuty Finding Export
  - Configurer l'enregistrement AWS Config
  - Configurer le trafic ACL AWS WAF Web
  - Configurer les journaux de trafic réseau AWS Network Firewall
  - Configurer les journaux d'accès Elastic Load Balancing
  - Configurer les journaux de requête Amazon Route 53 Resolver
  - Configurer les journaux Amazon RDS
  - Configurer les journaux du 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 journal, 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 (SIEM) 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.

- Utiliser les journaux pour les alertes : AWS fournit des alertes par le biais de plusieurs services de sécurité :
  - AWS Config surveille et enregistre les configurations de vos ressources AWS et permet d'automatiser l'évaluation et la remédiation par rapport aux configurations souhaitées.
  - Amazon 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. GuardDuty ingère, agrège et analyse les informations provenant de sources telles que les événements de gestion et de données AWS CloudTrail, les journaux DNS, les journaux de flux 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 CSPM 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 et détections, consultez la section Détection dans le Guide de réponse aux incidents de sécurité AWS.

Ressources

Bonnes pratiques associées:

- SEC04-BP02 Capturer les journaux, les résultats et les métriques dans des emplacements standardisés
- SEC07-BP04 Définir la gestion évolutive du cycle de vie des données
- SEC10-BP06 Prédéployer les outils

Documents connexes :

- Guide d'intervention en cas d'incident de sécurité AWS
- Premiers pas avec Amazon Security Lake
- Démarrer : Amazon CloudWatch Logs

Vidéos connexes:

- AWS re:Invent 2022 - Introducing Amazon Security Lake

Exemples connexes:

- Assistant Log Enabler pour AWS
- AWS Security Hub CSPM Exportation historique des résultats

SEC04-BP02 Capturer les journaux, les résultats et les métriques dans des emplacements standardisés

Les équipes de sécurité s'appuient sur les journaux et les résultats pour analyser les événements susceptibles d'indiquer une activité non autorisée ou des modifications involontaires. Afin de simplifier cette analyse, capturez les journaux de sécurité et les résultats dans des emplacements standardisés. Vous pourrez ainsi rendre disponibles les points de données intéressants pour la corrélation et simplifier les intégrations d'outils.

Résultat escompté : vous disposez d'une approche standardisée pour collecter, analyser et visualiser les données de journal, les résultats et les métriques. Les équipes de sécurité peuvent corréler, analyser et visualiser efficacement les données de sécurité provenant de systèmes disparates afin de découvrir les événements de sécurité potentiels et d'identifier les anomalies. Des systèmes de gestion des informations et des événements de sécurité (SIEM) ou d'autres mécanismes sont intégrés pour interroger et analyser les données des journaux afin de répondre rapidement, de suivre et de faire remonter les événements de sécurité.

Anti-modèles courants :

- Les équipes possèdent et gèrent indépendamment la journalisation et la collecte de métriques qui ne sont pas conformes à la stratégie de journalisation de l'organisation.
- Les équipes ne disposent pas de contrôles d'accès adéquats pour restreindre la visibilité et la modification des données collectées.
- Les équipes ne gèrent pas leurs journaux de sécurité, leurs résultats et leurs métriques dans le cadre de leur politique de classification des données.
- Les équipes négligent les exigences de souveraineté et de localisation des données lors de la configuration des collections de données.

Avantages du respect de cette bonne pratique : une solution de journalisation standardisée pour collecter et interroger les données et les événements des journaux améliore les informations dérivées des informations qu'ils contiennent. La configuration d'un cycle de vie automatisé pour les données de journal collectées peut permettre de réduire les coûts liés au stockage des journaux. Vous pouvez créer un contrôle d'accès précis pour les informations de journal collectées en fonction de la sensibilité des données et des modèles d'accès nécessaires à vos équipes. Vous pouvez intégrer des outils pour corréler, visualiser et déduire des informations à partir des données.

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

Directives d'implémentation

La croissance de l'utilisation d'AWS au sein d'une organisation entraîne une augmentation du nombre de charges de travail et d'environnements distribués. Dans la mesure où chaque charge de travail et environnement génère des données sur l'activité qui s'y déroule, la capture et le stockage de ces données localement constituent un défi pour les opérations de sécurité. Les équipes de sécurité utilisent des outils tels que les systèmes de gestion des informations et des événements de sécurité (SIEM) pour collecter des données à partir de sources distribuées et effectuer des flux de travail de corrélation, d'analyse et de réponse. Ces opérations requièrent la gestion d'un ensemble complexe d'autorisations pour accéder aux différentes sources de données et impliquent des frais supplémentaires liés à l'exploitation des processus d'extraction, transformation et chargement (ETL).

Pour surmonter ces difficultés, pensez à agréger toutes les sources pertinentes de données des journaux de sécurité dans un compte Log Archive, comme décrit dans la section Organisation de votre environnement AWS à l'aide de plusieurs comptes. Cela inclut toutes les données liées à la sécurité provenant de votre charge de travail et les journaux générés par les services AWS, tels que AWS CloudTrail, AWS WAF, Elastic Load Balancing et Amazon Route 53. La saisie de ces données dans des emplacements standardisés dans un Compte AWS avec des autorisations intercomptes appropriées présente plusieurs avantages. Cette pratique permet d'empêcher l'altération des journaux dans les charges de travail et les environnements compromis, fournit un point d'intégration unique pour des outils supplémentaires et propose un modèle plus simplifié pour configurer la conservation et le cycle de vie des données. Évaluez les impacts de la souveraineté des données, des périmètres de conformité et d'autres réglementations afin de déterminer si plusieurs emplacements de stockage de données de sécurité et périodes de conservation sont nécessaires.

Pour faciliter la capture et la standardisation des journaux et des résultats, évaluez Amazon Security Lake dans votre compte d'archivage des journaux. Vous pouvez configurer Security Lake pour

ingérer automatiquement les données provenant de sources courantes telles que CloudTrail, Route 53, Amazon EKS et les journaux de flux VPC. Vous pouvez également configurer AWS Security Hub CSPM en tant que source de données dans Security Lake, ce qui vous permet de corréler les résultats d'autres services AWS, tels qu'Amazon GuardDuty et Amazon Inspector, avec les données de vos journaux. Vous pouvez également utiliser des intégrations de sources de données tierces ou configurer des sources de données personnalisées. Toutes les intégrations normalisent vos données au format OCSF (Open Cybersecurity Schema Framework) et sont stockées dans des compartiments Amazon S3 sous forme de fichiers Parquet, éliminant ainsi le besoin de traitement ETL.

Le stockage des données de sécurité dans des emplacements standardisés fournit des fonctionnalités analytiques avancées. AWS vous recommande de déployer des outils d'analyse de sécurité qui fonctionnent dans un environnement AWS dans un compte Security Tooling distinct de votre compte d'archivage des journaux. Cette approche vous permet de mettre en œuvre des contrôles approfondis afin de protéger l'intégrité et la disponibilité des journaux et du processus de gestion des journaux, indépendamment des outils qui y accèdent. Envisagez d'utiliser des services tels qu'Amazon Athena pour exécuter des requêtes à la demande qui mettent en corrélation plusieurs sources de données. Vous pouvez également intégrer des outils de visualisation, tels que Quick. Les solutions optimisées par l'IA sont de plus en plus disponibles et peuvent exécuter des fonctions telles que la conversion des résultats en résumés lisibles par l'homme et l'interaction en langage naturel. L'intégration de ces solutions est généralement plus simple si vous disposez d'un emplacement de stockage de données standardisé pour les requêtes.

Étapes d'implémentation

1. Création des comptes d'archivage des journaux et d'outils de sécurité
   a. À l'aide d'AWS Organizations, créez les comptes d'archivage des journaux et d'outils de sécurité dans une unité organisationnelle de sécurité. Si vous utilisez AWS Control Tower pour gérer votre organisation, les comptes d'archivage des journaux et d'outils de sécurité sont créés automatiquement pour vous. Configurez les rôles et les autorisations pour accéder à ces comptes et les administrer selon les besoins.
2. Configurer vos emplacements de données de sécurité standardisés
   a. Déterminez votre stratégie pour créer des emplacements de données de sécurité standardisés. Vous pouvez y parvenir grâce à des options telles que des approches d'architecture de lac de données courantes, des produits de données tiers ou Amazon Security Lake. AWS vous recommande de capturer les données de sécurité à partir des Régions AWS qui sont activées pour vos comptes, même lorsque vous ne les utilisez pas activement.
3. Configurer la publication des sources de données dans vos emplacements standardisés

   a. Identifiez les sources de vos données de sécurité et configurez-les pour les publier dans vos emplacements standardisés. Évaluez les options permettant d'exporter automatiquement les données dans le format souhaité, par opposition à celles nécessitant le développement de processus ETL. Avec Amazon Security Lake, vous pouvez collecter des données à partir de sources AWS prises en charge et de systèmes tiers intégrés.

4. Configurer des outils pour accéder à vos emplacements standardisés
   a. Configurez des outils tels qu'Amazon Athena, Quick ou des solutions tierces pour disposer de l'accès requis à vos emplacements standardisés. Configurez ces outils de façon à ce qu'ils fonctionnent à partir du compte d'outils de sécurité avec un accès en lecture intercompte au compte d'archivage des journaux, le cas échéant. Créez des abonnés dans Amazon Security Lake pour permettre à ces outils d'accéder à vos données.

Ressources

Bonnes pratiques associées:

- SEC01-BP01 Séparer les charges de travail à l'aide de comptes
- SEC07-BP04 Définir la gestion du cycle de vie des données
- SEC08-BP04 Appliquer le contrôle d'accès
- OPS08-BP02 Analyse des journaux de charge de travail

Documents connexes:

- Livres blancs AWS : organisation de votre environnement AWS à l'aide de comptes multiple
- Conseils prescriptifs AWS : architecture de référence de sécurité AWS (SRA AWS)
- AWS Conseils prescriptifs : guide journalisation et surveillance pour les propriétaires d'applications

Exemples connexes:

- Agrégation, recherche et visualisation des données de journal provenant de sources distribuées avec Amazon Athena et Quick
- Comment visualiser les résultats d'Amazon Security Lake avec Quick
- Génération d'informations optimisées par l'IA pour Amazon Security Lake à l'aide d'Amazon SageMaker AI Studio et d'Amazon Bedrock

- Identification des anomalies de cybersécurité dans vos données Amazon Security Lake à l'aide de l'IA Amazon SageMaker
- Ingestion, transformation et diffusion des événements publiés par Amazon Security Lake sur Amazon OpenSearch Service
- Simplification de l'analyse des journaux AWS CloudTrail via la génération de requêtes en langage naturel dans CloudTrail Lake

Outils associés:

- Amazon Security Lake
- Intégrations des partenaires Amazon Security Lake
- Cadre de schéma de cybersécurité ouvert (OCSF)
- Amazon Athena
- Quick
- Amazon Bedrock

SEC04-BP03 Corréler et enrichir les alertes de sécurité

Les activités inattendues peuvent générer plusieurs alertes de sécurité provenant de différentes sources, ce qui nécessite une corrélation et un enrichissement supplémentaires pour comprendre le contexte complet. Mettez en œuvre une corrélation et un enrichissement automatisés des alertes de sécurité afin de permettre une identification et une réponse plus précises aux incidents.

Résultat escompté : au fur et à mesure que l'activité génère différentes alertes au sein de vos charges de travail et de vos environnements, des mécanismes automatisés mettent en corrélation les données et les enrichissent avec des informations supplémentaires. Ce prétraitement permet de mieux comprendre l'événement, ce qui aide vos enquêteurs à déterminer sa criticité et s'il s'agit d'un incident qui requiert une réponse officielle. Ce processus réduit la charge de travail de vos équipes de surveillance et d'enquête.

Anti-modèles courants :

- Différents groupes de personnes étudient les résultats et les alertes générés par différents systèmes, sauf si les exigences relatives à la séparation des tâches en disposent autrement.

- Votre organisation achemine tous les résultats de sécurité et toutes les données d'alerte vers des emplacements standard, mais demande aux enquêteurs d'effectuer une corrélation et un enrichissement manuels.
- Vous vous fiez uniquement à l'intelligence des systèmes de détection des menaces pour rendre compte des résultats et établir la criticité.

Avantages du respect de cette bonne pratique : la corrélation et l'enrichissement automatisés des alertes contribuent à réduire la charge cognitive globale et la préparation manuelle des données requises par vos enquêteurs. Cette pratique permet de réduire le temps nécessaire pour déterminer si l'événement représente un incident et lancer une réponse officielle. Un contexte supplémentaire vous permet également d'évaluer avec précision la gravité réelle d'un événement, car celle-ci peut être supérieure ou inférieure à ce que suggère une alerte.

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

Directives d'implémentation

Les alertes de sécurité peuvent provenir de nombreuses sources différentes dans AWS, y compris :

- Des services tels qu'Amazon GuardDuty, AWS Security Hub CSPM, Amazon Macie, Amazon Inspector, AWS Config, AWS Identity and Access Management Access Analyzer et Analyseur d'accès réseau
- Alertes issues de l'analyse automatique des journaux de service AWS, d'infrastructure et d'application, telles que celles issues de Security Analytics pour Amazon OpenSearch Service.
- Alarmes en réponse à des modifications de votre activité de facturation provenant de sources telles qu'Amazon CloudWatch, Amazon EventBridge ou AWS Budgets.
- Des sources tierces, telles que les flux de renseignements sur les menaces et les solutions des partenaires de sécurité d'AWS Partner Network.
- Contact par AWS Trust & Safety ou par d'autres sources, telles que des clients ou des employés internes.
- Utilisez Threat Technique Catalog by AWS (TTC) pour aider à identifier et à corréler le comportement des acteurs menaçants grâce à l'identification des indicateurs de compromission (IoC). TTC est une extension du framework MITRE ATT&CK, qui catégorise tous les comportements et techniques connus et observés des acteurs menaçants dirigés contre les ressources AWS.

Dans leur forme la plus fondamentale, les alertes contiennent des informations sur qui (le principal ou l'identité) fait quoi (les mesures prises) à quoi (les ressources affectées). Pour chacune de ces sources, déterminez s'il existe des moyens de créer des mappages entre les identifiants de ces identités, actions et ressources afin d'effectuer une corrélation. À cet effet, vous pouvez notamment intégrer des sources d'alerte à un outil de gestion des informations et des événements de sécurité (SIEM) afin d'effectuer une corrélation automatique, créer vos propres pipelines et traitements de données, ou mettre en place une combinaison de ces deux solutions.

Amazon Detective est un exemple de service capable d'effectuer une corrélation pour vous. Detective ingère en permanence les alertes provenant de différentes sources AWS et tierces. Il utilise différentes formes d'informations pour créer un graphique visuel de leurs relations afin de faciliter les enquêtes.

Alors que la criticité initiale d'une alerte facilite l'établissement des priorités, le contexte dans lequel l'alerte s'est produite détermine sa véritable criticité. Par exemple, Amazon GuardDuty peut vous avertir qu'une instance Amazon EC2 de votre charge de travail demande un nom de domaine inattendu. GuardDuty peut attribuer à elle seule une faible criticité à cette alerte. Cependant, une corrélation automatique avec d'autres activités au moment de l'alerte peut révéler que plusieurs centaines d'instances EC2 ont été déployées sous la même identité, ce qui augmente les coûts d'exploitation globaux. Dans ce cas, le contexte de l'événement corrélé justifierait une nouvelle alerte de sécurité et la criticité pourrait être portée à un niveau élevé, ce qui accélérerait la mise en place d'une réponse.

Étapes d'implémentation

1. Identifiez les sources d'informations relatives aux alertes de sécurité. Comprenez comment les alertes de ces systèmes représentent l'identité, l'action et les ressources afin de déterminer où une corrélation est possible.
2. Mettez en place un mécanisme permettant de capturer les alertes provenant de différentes sources. À cette fin, pensez à des services tels que Security Hub CSPM, EventBridge et CloudWatch.
3. Identifiez les sources pour la corrélation et l'enrichissement des données. Les exemples de sources incluent AWS CloudTrail, les journaux de flux VPC, les journaux de Route 53 Resolver et les journaux d'infrastructure et d'application. Tout ou partie de ces journaux peuvent être consommés par le biais d'une seule intégration avec Amazon Security Lake.
4. Intégrez les alertes à vos sources de corrélation et d'enrichissement des données pour créer des contextes d'événements de sécurité plus détaillés et établir leur criticité.

a. Amazon Detective, les outils SIEM ou d'autres solutions tierces peuvent effectuer automatiquement un certain niveau d'ingestion, de corrélation et d'enrichissement.

b. Vous pouvez également utiliser des services AWS pour créer le vôtre. Par exemple, vous pouvez invoquer une fonction AWS Lambda pour exécuter une requête Amazon Athena par rapport à AWS CloudTrail ou Amazon Security Lake, et publier les résultats dans EventBridge.

Ressources

Bonnes pratiques associées:

- SEC10-BP03 Préparer les fonctionnalités d'analyse poussée
- OPS08-BP04 Création d'alertes exploitables
- REL06-BP03 Envoyer des notifications (traitement et alarmes en temps réel)

Documents connexes:

- AWS Guide d'intervention en cas d'incident de sécurité

Exemples connexes:

- Comment enrichir les résultats AWS Security Hub CSPM grâce aux métadonnées des comptes

Outils associés :

- Amazon Detective
- Amazon EventBridge
- AWS Lambda
- Amazon Athena

SEC04-BP04 Lancer la correction pour les ressources non conformes

Vos contrôles de détection peuvent signaler la présence de ressources non conformes à vos exigences de configuration. Vous pouvez lancer des mesures correctives définies par programme,

manuellement ou automatiquement, afin de corriger ces ressources et de minimiser les impacts potentiels. Lorsque vous définissez des mesures correctives par programmation, vous pouvez agir rapidement et avec cohérence.

Bien que l'automatisation puisse améliorer les opérations de sécurité, vous devez la mettre en œuvre et la gérer avec soin. Mettez en place des mécanismes de supervision et de contrôle appropriés pour vérifier que les réponses automatisées sont efficaces, précises et conformes aux politiques organisationnelles et à la propension au risque.

Résultat escompté : vous définissez les normes de configuration des ressources ainsi que les étapes à suivre pour corriger les ressources détectées comme étant non conformes. Dans la mesure du possible, vous avez défini les mesures correctives par programmation afin qu'elles puissent être lancées manuellement ou automatiquement. Des systèmes de détection sont en place pour identifier les ressources non conformes et publier des alertes dans des outils centralisés surveillés par votre personnel de sécurité. Ces outils vous permettent d'exécuter vos corrections programmatiques, manuellement ou automatiquement. Les mesures correctives automatiques sont dotées de mécanismes de supervision et de contrôle appropriés pour régir leur utilisation.

Anti-modèles courants :

- Vous mettez en œuvre l'automatisation, mais vous ne parvenez pas à tester ni à valider de manière approfondie les mesures correctives. Cela peut avoir des conséquences imprévues, telles que la perturbation des opérations commerciales légitimes ou l'instabilité du système.
- Vous améliorez les temps de réponse et les procédures grâce à l'automatisation, mais sans surveillance appropriée et sans mécanismes permettant une intervention et un discernement humains en cas de besoin.
- Vous vous fiez uniquement aux mesures correctives, au lieu de les intégrer dans le cadre d'un programme plus large de réponse aux incidents et de reprise.

Avantages du respect de cette bonne pratique : les corrections automatiques peuvent répondre aux erreurs de configuration plus rapidement que les processus manuels, ce qui vous permet de minimiser les impacts commerciaux potentiels et de réduire les opportunités d'utilisation involontaire. Lorsque vous définissez des mesures correctives de manière programmatique, elles sont appliquées de manière cohérente, ce qui réduit le risque d'erreur humaine. L'automatisation peut également gérer simultanément un plus grand volume d'alertes, ce qui est particulièrement important dans les environnements fonctionnant à grande échelle.

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

Directives d’implémentation

Comme décrit dans SEC01-BP03 Identifier et valider les objectifs de contrôle, des services tels que AWS Config et AWS Security Hub CSPM peuvent vous aider à surveiller la configuration des ressources de vos comptes afin de garantir leur conformité à vos exigences. Lorsque des ressources non conformes sont détectées, des services tels que AWS Security Hub CSPM peuvent aider à acheminer les alertes de manière appropriée et à prendre des mesures correctives. Ces solutions fournissent à vos enquêteurs de sécurité un emplacement central qui leur permet de surveiller les problèmes et de prendre des mesures correctives.

Outre AWS Security Hub CSPM, AWS a introduit Security Hub Advanced. Ce service, annoncé lors de re:Invent 2025, transforme la façon dont les entreprises hiérarchisent leurs problèmes de sécurité les plus critiques et répondent à grande échelle pour protéger leurs environnements cloud. La solution améliorée de Security Hub utilise désormais des données analytiques avancées pour corréler, enrichir et hiérarchiser automatiquement les signaux de sécurité dans votre environnement cloud. Security Hub s’intègre parfaitement avec Amazon GuardDuty, Amazon Inspector, Amazon Macie et AWS Security Hub CSPM. Les résultats corrélés dans Security Hub peuvent aboutir à une nouvelle découverte, appelée découverte d’exposition, qui inclut une trajectoire d’attaque supposée basée sur les vulnérabilités détectées dans chaque ressource.

Alors que certaines situations de ressources non conformes sont uniques et requièrent un discernement humain pour être résolues, d’autres situations ont besoin d’une réponse standard que vous pouvez définir par programmation. Par exemple, une solution standard à un problème de configuration du groupe de sécurité VPC peut consister à supprimer les règles d’interdiction et à en informer le propriétaire. Les réponses peuvent être définies dans les fonctions AWS Lambda, les documents AWS Systems Manager Automation ou via d’autres environnements de code que vous préférez. Assurez-vous que l’environnement est capable de s’authentifier auprès d’AWS à l’aide d’un rôle IAM avec le moins d’autorisations nécessaires pour prendre des mesures correctives.

Une fois que vous avez défini la correction souhaitée, vous pouvez ensuite déterminer le moyen par lequel vous préférez la lancer. AWS Config peut initier des mesures correctives pour vous. Si vous utilisez Security Hub CSPM, vous pouvez le faire par le biais d’actions personnalisées, ce qui entraîne la publication des informations de résultat sur Amazon EventBridge. Une règle EventBridge peut ensuite lancer votre correction. Vous pouvez configurer les corrections via Security Hub CSPM pour qu’elles s’exécutent automatiquement ou manuellement.

Pour la correction programmatique, nous vous recommandons de disposer de journaux et d’audits complets des actions entreprises, ainsi que de leurs résultats. Passez en revue et analysez ces

journaux pour évaluer l'efficacité des processus automatisés et identifier les domaines à améliorer. Capturez les journaux dans Amazon CloudWatch Logs et les résultats des mesures correctives sous forme de notes de résultat dans Security Hub CSPM.

Comme point de départ, pensez à Automated Security Response on AWS, qui propose des correctifs prédéfinis pour résoudre les erreurs de configuration de sécurité courantes.

Étapes d'implémentation

1. Analysez et hiérarchisez les alertes.
    a. Regroupez les alertes de sécurité provenant de différents services AWS dans Security Hub CSPM pour centraliser la visibilité, la hiérarchisation et les mesures correctives.
2. Élaborez des mesures correctives.
    a. Utilisez des services tels que Systems Manager et AWS Lambda pour exécuter des corrections programmatiques.
3. Configurez la façon dont les mesures correctives sont lancées.
    a. À l'aide de Systems Manager, définissez des actions personnalisées qui publient les résultats dans EventBridge. Configurez ces actions de façon à ce qu'elles soient lancées manuellement ou automatiquement.
    b. Vous pouvez également utiliser Amazon Simple Notification Service (SNS) pour envoyer des notifications et des alertes aux parties prenantes concernées (comme l'équipe de sécurité ou les équipes de réponse aux incidents) pour une intervention manuelle ou une escalade, si nécessaire.
4. Passez en revue et analysez les journaux de correction afin d'en vérifier l'efficacité et de les améliorer.
    a. Envoyez une sortie de journal à CloudWatch Logs. Enregistrez les résultats sous forme de notes de résultat dans Security Hub CSPM.

Ressources

Bonnes pratiques associées:

- SEC06-BP03 Réduire la gestion manuelle et l'accès interactif

Documents connexes:

- AWS Guide d’intervention en cas d’incident de sécurité - Détection

Exemples connexes:

- Automated Security Response on AWS
- Surveiller les paires de clés d’instance EC2 à l’aide de AWS Config
- Créer des règles AWS Config personnalisées à l’aide de stratégies AWS CloudFormation Guard
- Corriger automatiquement les instances et clusters de base de données Amazon RDS non chiffrés

Outils associés:

- AWS Systems Manager Automation
- Automated Security Response on AWS

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 connaître les régions, les zones de disponibilité, les AWS Local Zones et les AWS Outposts, qui sont des composants de l’infrastructure globale sécurisée AWS.

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 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.

AWS Les régions 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 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 offre les services, l'infrastructure et les modèles d'exploitation AWS natifs à la quasi-totalité de centres de données, d'espaces de colocalisation d'infrastructures ou d'installations 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
- Protection du calcul

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 confiance zéro. 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 : Présentation à la loupe des applications sans serveur pour obtenir des conseils sur la sécurité sans serveur.

Bonnes pratiques

- SEC05-BP01 Créer des couches réseau
- SEC05-BP02 Contrôler le flux de trafic au sein de vos couches réseau
- SEC05-BP03 Mettre en œuvre une protection basée sur l'inspection
- SEC05-BP04 Automatiser la protection du réseau

SEC05-BP01 Créer des couches réseau

Segmentez la topologie de votre réseau en différentes couches en procédant à des regroupements logiques des composants de votre charge de travail en fonction de la sensibilité des données et de leurs exigences en matière d'accès. Faites la distinction entre les composants qui requièrent un accès entrant depuis Internet, comme les points de terminaison Web publics, et ceux qui requièrent uniquement un accès interne, comme les bases de données.

Résultat souhaité : les couches de votre réseau font partie d'une approche intégrée de défense en profondeur de la sécurité qui complète la stratégie d'authentification et d'autorisation des identités de vos charges de travail. Les couches sont positionnées en fonction de la sensibilité des données et des exigences d'accès, avec des mécanismes de flux de trafic et de contrôle appropriés.

Anti-modèles courants :

- Vous créez toutes les ressources dans un seul VPC ou sous-réseau.
- Vous construisez vos couches réseau sans tenir compte des exigences de sensibilité des données, du comportement des composants ou des fonctionnalités.

- Vous utilisez les VPC et les sous-réseaux par défaut pour toutes les considérations relatives à la couche réseau et vous ne tenez pas compte de l'influence des services gérés par AWS sur votre topologie.

Avantages du respect de cette bonne pratique : la mise en place de couches réseau est la première étape pour limiter les chemins inutiles à travers le réseau, en particulier ceux qui mènent à des systèmes et à des données critiques. Il est donc plus difficile pour les acteurs non autorisés d'accéder à votre réseau et aux ressources supplémentaires qu'il contient. Les couches réseau individuelles présentent l'avantage de réduire la portée de l'analyse des systèmes d'inspection, par exemple pour la détection des intrusions ou la prévention des programmes malveillants. Cela réduit le risque de faux positifs et les frais de traitement inutiles.

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

Directives d'implémentation

Lors de la conception d'une architecture de charge de travail, il est courant de séparer les composants en différentes couches en fonction de leur responsabilité. Par exemple, une application Web peut comporter une couche de présentation, une couche d'application et une couche de données. Vous pouvez adopter une approche similaire lors de la conception de la topologie de votre réseau. Les contrôles réseau sous-jacents peuvent vous aider à faire respecter les exigences d'accès aux données de votre charge de travail. Par exemple, dans une architecture d'application Web à trois niveaux, vous pouvez stocker vos fichiers de couche de présentation statique sur Amazon S3 et les diffuser à partir d'un réseau de diffusion de contenu (CDN), tel qu'Amazon CloudFront. La couche application peut comporter des points de terminaison publics qu'un Application Load Balancer (ALB) sert dans un sous-réseau public Amazon VPC (similaire à une zone démilitarisée, ou DMZ), les services principaux étant déployés dans des sous-réseaux privés. La couche de données, qui héberge des ressources telles que des bases de données et des systèmes de fichiers partagés, peut résider dans des sous-réseaux privés différents des ressources de votre couche d'application. À chacune de ces limites de couche (CDN, sous-réseau public, sous-réseau privé), vous pouvez déployer des contrôles qui permettent uniquement au trafic autorisé de franchir ces limites.

Comme pour la modélisation des couches réseau en fonction de l'objectif fonctionnel des composants de votre charge de travail, tenez également compte de la sensibilité des données traitées. Dans l'exemple de l'application Web, bien que tous vos services de charge de travail puissent résider dans la couche d'application, différents services peuvent traiter des données avec des niveaux de sensibilité différents. Le cas échéant, il peut être approprié de diviser la couche

d'application en utilisant plusieurs sous-réseaux privés, différents VPC dans le même Compte AWS, voire différents VPC dans différents Comptes AWS pour chaque niveau de sensibilité des données, en fonction de vos exigences de contrôle.

La cohérence du comportement des composants de votre charge de travail est un autre facteur à prendre en compte pour les couches réseau. Si nous poursuivons avec le même exemple, dans la couche d'application, vous pouvez avoir des services qui acceptent des entrées provenant d'utilisateurs finaux ou d'intégrations de systèmes externes qui sont intrinsèquement plus risquées que les entrées d'autres services. Il peut notamment s'agir du téléchargement de fichiers, de scripts de code à exécuter, de l'analyse d'e-mails, etc. Le fait de placer ces services dans leur propre couche réseau contribue à créer une limite d'isolation plus forte autour d'eux et peut empêcher leur comportement unique de créer des alertes faussement positives dans les systèmes d'inspection.

Dans le cadre de votre conception, réfléchissez à l'influence de l'utilisation des services gérés par AWS sur la topologie de votre réseau. Découvrez comment des services tels qu'Amazon VPC Lattice peuvent faciliter l'interopérabilité des composants de votre charge de travail entre les couches réseau. Lors de l'utilisation de AWS Lambda, effectuez le déploiement dans vos sous-réseaux VPC, sauf s'il y a raisons spécifiques de ne pas le faire. Déterminez où les points de terminaison d'un VPC et AWS PrivateLink peuvent simplifier le respect des politiques de sécurité qui limitent l'accès aux passerelles Internet.

Étapes d'implémentation

1. Passez en revue l'architecture de votre charge de travail. Regroupez logiquement les composants et les services selon les fonctions qu'ils remplissent, la sensibilité des données traitées et leur comportement.
2. En ce qui concerne les composants qui répondent à des demandes provenant d'Internet, pensez à utiliser des équilibreurs de charge ou d'autres proxys pour fournir des points de terminaison publics. Explorez l'évolution des contrôles de sécurité en utilisant des services gérés, tels que CloudFront, Amazon API Gateway, Elastic Load Balancing, et AWS Amplify pour héberger des points de terminaison publics.
3. Pour les composants exécutés dans des environnements informatiques, tels que les instances Amazon EC2, les conteneurs AWS Fargate ou les fonctions Lambda, déployez-les dans des sous-réseaux privés en fonction de vos groupes dès la première étape.
4. Pour les services AWS entièrement gérés, tels qu'Amazon DynamoDB, Amazon Kinesis ou Amazon SQS, envisagez d'utiliser des points de terminaison d'un VPC par défaut pour l'accès via des adresses IP privées.

Ressources

Bonnes pratiques associées :

- REL02 Planification de votre topologie réseau
- PERF04-BP01 Compréhension de l'impact de la mise en réseau sur les performances

Vidéos connexes :

- AWS re:Invent 2023 - AWS networking foundations

Exemples connexes :

- Exemples de VPC
- Access container applications privately on Amazon ECS by using AWS Fargate, AWS PrivateLink, and a Network Load Balancer
- Serve static content in an Amazon S3 bucket through a VPC by using Amazon CloudFront

SEC05-BP02 Contrôler le flux de trafic au sein de vos couches réseau

Au sein des couches de votre réseau, segmentez davantage pour limiter le trafic uniquement aux flux nécessaires à chaque charge de travail. Tout d'abord, concentrez-vous sur le contrôle du trafic entre Internet ou d'autres systèmes externes vers une charge de travail et votre environnement (trafic nord-sud). Ensuite, examinez les flux entre les différents composants et systèmes (trafic est-ouest).

Résultat souhaité : vous autorisez uniquement les flux réseau nécessaires aux composants de vos charges de travail pour communiquer entre eux, avec leurs clients et avec tout autre service dont ils dépendent. Votre conception prend en compte des facteurs tels que les entrées et sorties publiques par rapport aux entrées et sorties privées, la classification des données, les réglementations régionales et les exigences en matière de protocole. Dans la mesure du possible, vous privilégiez les flux point à point par rapport à l'appairage réseau dans le cadre du principe du moindre privilège.

Anti-modèles courants :

- Vous adoptez une approche de la sécurité du réseau basée sur le périmètre et vous ne contrôlez le flux de trafic qu'à la limite des couches de votre réseau.
- Vous supposez que tout le trafic au sein d'une couche réseau est authentifié et autorisé.

- Vous appliquez des contrôles à votre trafic d'entrée ou de sortie, mais pas aux deux.
- Vous vous fiez uniquement aux composants de votre charge de travail et aux contrôles réseau pour authentifier et autoriser le trafic.

Avantages du respect de cette bonne pratique : cette pratique permet de réduire le risque de mouvements non autorisés au sein de votre réseau et ajoute une couche d'autorisation supplémentaire à vos charges de travail. En contrôlant le flux de trafic, vous pouvez limiter l'ampleur de l'impact d'un incident de sécurité et accélérer la détection et la réponse.

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

Directives d'implémentation

Alors que les couches réseau aident à définir les limites entre les composants de votre charge de travail qui remplissent une fonction, un niveau de sensibilité des données et un comportement similaires, vous pouvez créer un niveau de contrôle du trafic nettement plus précis en utilisant des techniques permettant de segmenter davantage les composants au sein de ces couches, conformément au principe du moindre privilège. Au sein de AWS, les couches de réseau se caractérisent avant tout selon des plages d'adresse IP au sein d'un VPC Amazon. Les couches peuvent également être définies à l'aide de différents VPC, par exemple pour regrouper les environnements de microservices par domaine d'activité. Lorsque vous utilisez plusieurs VPC, négociez le routage à l'aide d'un AWS Transit Gateway. Bien que cela permette de contrôler le trafic au niveau de la couche 4 (adresses IP et plages de ports) à l'aide de groupes de sécurité et de tables de routage, vous pouvez renforcer le contrôle grâce à des services supplémentaires, tels que AWS PrivateLink, le pare-feu DNS Amazon Route 53 Resolver, AWS Network Firewall et AWS WAF.

Comprenez et inventoriez le flux de données et les exigences de communication de vos charges de travail en termes de parties initiatrices de connexion, de ports, de protocoles et de couches réseau. Évaluez les protocoles disponibles pour établir des connexions et transmettre des données afin de sélectionner ceux qui répondent à vos exigences de protection (par exemple, HTTPS plutôt que HTTP). Capturez ces exigences à la fois aux limites de vos réseaux et au sein de chaque couche. Une fois ces exigences identifiées, explorez les options permettant d'autoriser uniquement le trafic requis à circuler à chaque point de connexion. Un bon point de départ consiste à utiliser des groupes de sécurité au sein de votre VPC, car ils peuvent être associés à des ressources utilisant une interface réseau Elastic (ENI), telles que des instances Amazon EC2, des tâches Amazon ECS, des pods Amazon EKS ou des bases de données Amazon RDS. Contrairement à un pare-feu de couche 4, un groupe de sécurité peut avoir une règle qui autorise le trafic provenant d'un autre

groupe de sécurité en fonction de son identifiant, minimisant ainsi les mises à jour à mesure que les ressources du groupe changent au fil du temps. Vous pouvez également filtrer le trafic à l'aide de règles entrantes et sortantes à l'aide de groupes de sécurité.

Lorsque le trafic se déplace entre des VPC, il est courant d'utiliser l'appairage de VPC pour un routage simple ou AWS Transit Gateway pour un routage complexe. Grâce à ces approches, vous facilitez les flux de trafic entre la plage d'adresses IP des réseaux source et de destination. Toutefois, si votre charge de travail ne nécessite que des flux de trafic entre des composants spécifiques de différents VPC, envisagez d'utiliser une connexion point à point à l'aide de AWS PrivateLink. Pour ce faire, identifiez quel service doit agir en tant que producteur et lequel doit agir en tant que consommateur. Déployez un équilibreur de charge compatible pour le producteur, activez PrivateLink en conséquence, puis acceptez une demande de connexion du consommateur. Le service producteur se voit ensuite attribuer une adresse IP privée provenant du VPC du consommateur, que celui-ci peut utiliser pour effectuer des demandes ultérieures. Cette approche réduit le besoin d'appairage entre les réseaux. Incluez les coûts du traitement des données et de l'équilibrage de charge dans le cadre de l'évaluation de PrivateLink.

Bien que les groupes de sécurité et PrivateLink aident à contrôler le flux entre les composants de vos charges de travail, il est également important de savoir comment contrôler les domaines DNS auxquels vos ressources sont autorisées à accéder (le cas échéant). En fonction de la configuration DHCP de vos VPC, vous pouvez envisager deux services AWS différents à cette fin. La plupart des clients utilisent le service DNS Route 53 Resolver par défaut (également appelé serveur Amazon DNS ou AmazonProvideDDNS) disponible pour les VPC à l'adresse +2 de leur plage d'adresses CIDR. Avec cette approche, vous pouvez créer des règles de pare-feu DNS et les associer à votre VPC afin de déterminer les actions à entreprendre pour les listes de domaines que vous fournissez.

Si vous n'utilisez pas le Route 53 Resolver, ou si vous souhaitez le compléter par des fonctionnalités d'inspection et de contrôle de flux plus approfondies allant au-delà du filtrage de domaine, envisagez de déployer un AWS Network Firewall. Ce service inspecte les paquets individuels en utilisant des règles sans ou avec état afin de déterminer s'il est nécessaire de refuser ou d'autoriser le trafic. Vous pouvez adopter une approche similaire pour filtrer le trafic Web entrant vers vos points de terminaison publics à l'aide de AWS WAF. Pour plus d'informations sur ces services, voir SEC05-BP03 Mettre en œuvre une protection basée sur l'inspection.

Étapes d'implémentation

1. Identifiez les flux de données requis entre les composants de vos charges de travail.

2. Appliquez plusieurs contrôles avec une approche de défense en profondeur pour le trafic entrant et sortant, notamment en utilisant des groupes de sécurité et des tables de routage.
3. Utilisez des pare-feux pour définir un contrôle précis du trafic réseau entrant, sortant et transitant par vos VPC, comme Route 53 Resolver DNS Firewall, AWS Network Firewall et AWS WAF. Envisagez d'utiliser le AWS Firewall Manager pour configurer et gérer de manière centralisée les règles de pare-feu au sein de votre organisation.

Ressources

Bonnes pratiques associées :

- REL03-BP01 Choisir comment segmenter votre charge de travail
- SEC09-BP02 Application du chiffrement en transit

Documents connexes :

- Bonnes pratiques de sécurité pour votre VPC
- Conseils d'optimisation du réseau AWS
- Conseils pour la sécurité du réseau sur AWS
- Sécuriser le trafic réseau sortant de votre VPC dans le AWS Cloud

Outils associés :

- AWS Firewall Manager

Vidéos connexes :

- AWS Transit Gateway reference architectures for many VPCs
- Accélération et protection des applications avec Amazon CloudFront, AWS WAF, et AWS Shield
- AWS re:Inforce 2023: Firewalls and where to put them

SEC05-BP03 Mettre en œuvre une protection basée sur l'inspection

Configurez des points d'inspection du trafic entre les couches de votre réseau afin de vous assurer que les données en transit correspondent aux catégories et aux modèles attendus. Analysez les flux

de trafic, les métadonnées et les modèles pour identifier et détecter les événements, et y répondre plus efficacement.

Résultat souhaité : le trafic qui passe d'une couche à l'autre de votre réseau est inspecté et autorisé. Les décisions d'autorisation et de refus sont basées sur des règles explicites, des informations sur les menaces et des écarts par rapport aux comportements de base. Les protections deviennent plus strictes à mesure que le trafic se rapproche des données sensibles.

Anti-modèles courants :

- S'appuyer uniquement sur les règles de pare-feu basées sur les ports et les protocoles. Ne pas tirer parti des systèmes intelligents.
- Créer des règles de pare-feu basées sur des modèles de menaces actuels spécifiques susceptibles de changer.
- Inspecter uniquement le trafic transitant des sous-réseaux privés vers des sous-réseaux publics, ou des sous-réseaux publics vers Internet.
- Ne pas disposer d'une vue de base de votre trafic réseau à utiliser à titre de comparaison afin de détecter les anomalies de comportement.

Avantages du respect de cette bonne pratique : les systèmes d'inspection vous permettent de créer des règles intelligentes, telles que l'autorisation ou le refus du trafic uniquement lorsque certaines conditions relatives aux données de trafic existent. Bénéficiez d'ensembles de règles gérés par les partenaires AWS et basés sur les informations les plus récentes sur les menaces, à mesure que le paysage des menaces évolue au fil du temps. Cela réduit les frais liés à la mise à jour des règles et à la recherche d'indicateurs de compromis, réduisant ainsi le risque de faux positifs.

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

Directives d'implémentation

Contrôlez avec précision votre trafic réseau dynamique et apatride à l'aide AWS Network Firewall d'autres pare-feux et systèmes de prévention des intrusions (IPS) AWS Marketplace que vous pouvez déployer derrière un Gateway Load Balancer (). GWLB AWS Network Firewall prend en charge les IPS spécifications open source compatibles avec Suricata pour protéger votre charge de travail.

Les solutions AWS Network Firewall des fournisseurs qui utilisent un GWLB prennent en charge différents modèles de déploiement de l'inspection en ligne. Par exemple, vous pouvez effectuer une

inspection sur une VPC base individuelle, la centraliser dans le cadre d'une inspection VPC ou la déployer dans un modèle hybride dans lequel le trafic est-ouest passe par une inspection VPC et où les entrées Internet sont inspectées par inspection. VPC Une autre considération est de savoir si la solution prend en charge le déballage de Transport Layer Security (TLS), permettant une inspection approfondie des paquets pour les flux de trafic initiés dans les deux sens. Pour plus d'informations et des détails détaillés sur ces configurations, consultez le guide des bonnes pratiques AWS Network Firewall.

Si vous utilisez des solutions qui effectuent des out-of-band inspections, telles que l'analyse pcap des données par paquets provenant d'interfaces réseau fonctionnant en mode promiscuité, vous pouvez configurer VPC la mise en miroir du trafic. Le trafic en miroir est pris en compte dans la bande passante disponible de vos interfaces et il est soumis aux mêmes frais de transfert de données que le trafic non mis en miroir. Vous pouvez voir si des versions virtuelles de ces appliances sont disponibles sur le AWS Marketplace, qui peut prendre en charge le déploiement en ligne derrière unGWLB.

Pour les composants qui effectuent des transactions via des protocoles HTTP basés, protégez votre application contre les menaces courantes à l'aide d'un pare-feu pour applications Web (WAF). AWS WAFest un pare-feu d'applications Web qui vous permet de surveiller et de bloquer les demandes HTTP (S) conformes à vos règles configurables avant de les envoyer à Amazon API Gateway CloudFront, Amazon AWS AppSync ou à un Application Load Balancer. Envisagez une inspection approfondie des paquets lorsque vous évaluez le déploiement de votre pare-feu d'applications Web, car certains nécessitent que vous vous arrêtiez TLS avant d'inspecter le trafic. Pour commencer AWS WAF, vous pouvez l'utiliser AWS Managed Rulesen combinaison avec les vôtres ou utiliser les intégrations de partenaires existantes.

Vous pouvez gérer de manière centralisée AWS WAF, AWS Shield Advanced AWS Network Firewall, et les groupes VPC de sécurité Amazon au sein de votre AWS organisation avec AWS Firewall Manager.

Étapes d'implémentation

1. Déterminez si vous pouvez élargir la portée des règles d'inspection, par exemple par le biais d'une inspectionVPC, ou si vous avez besoin d'une approche plus précise par VPC approche.
2. Pour les solutions d'inspection en ligne :
   a. Si vous l'utilisez AWS Network Firewall, créez des règles, des politiques de pare-feu et le pare-feu lui-même. Une fois ceux-ci configurés, vous pouvez acheminer le trafic vers le point de terminaison du pare-feu pour permettre l'inspection.

   b. Si vous utilisez une appliance tierce avec un Gateway Load Balancer (GWLB), déployez et configurez votre appliance dans une ou plusieurs zones de disponibilité. Créez ensuite votreGWLB, le service de point de terminaison, le point de terminaison et configurez le routage de votre trafic.

3. Pour les solutions out-of-band d'inspection :

   1. Activez la mise en miroir VPC du trafic sur les interfaces où le trafic entrant et sortant doit être reflété. Vous pouvez utiliser EventBridge les règles Amazon pour appeler une AWS Lambda fonction afin d'activer la mise en miroir du trafic sur les interfaces lorsque de nouvelles ressources sont créées. Dirigez les sessions de mise en miroir du trafic vers le Network Load Balancer situé devant votre appareil qui traite le trafic.

4. Pour les solutions de trafic Web entrant :

   a. Pour configurer AWS WAF, commencez par configurer une liste de contrôle d'accès Web (WebACL). Le Web ACL est un ensemble de règles comportant une action par défaut (ALLOWouDENY) traitée en série qui définit la manière dont vous gérez le WAF trafic. Vous pouvez créer vos propres règles et groupes ou utiliser des groupes de règles AWS gérés sur votre site WebACL.

   b. Une fois votre site Web ACL configuré, associez-le à une AWS ressource (Application Load Balancer, API Gateway REST API ou CloudFront distribution, par exemple) pour commencer à protéger le trafic Web. ACL

Ressources

Documents connexes :

- Qu’est-ce que le Traffic Mirroring ?
- Mise en œuvre de l’inspection du trafic en ligne à l’aide d’appareils de sécurité tiers
- AWS Network Firewall exemples d'architectures avec routage
- Architecture d'inspection centralisée avec AWS Gateway Load Balancer et AWS Transit Gateway

Exemples connexes :

- Bonnes pratiques pour le déploiement de Gateway Load Balancer
- TLSconfiguration d'inspection pour le trafic de sortie crypté et AWS Network Firewall

Outils associés :

- AWS Marketplace IDS/IPS

SEC05-BP04 Automatiser la protection du réseau

Automatisez le déploiement des protections de votre réseau à l'aide de DevOps pratiques telles que l'infrastructure sous forme de code (IaC) et les pipelines CI/CD. Ces pratiques peuvent vous aider à suivre les modifications apportées aux protections de votre réseau via un système de contrôle de version, à réduire le temps nécessaire au déploiement des modifications et à détecter si les protections de votre réseau s'écartent de la configuration souhaitée.

Résultat souhaité : vous définissez les protections du réseau à l'aide de modèles et vous les validez dans un système de contrôle de version. Les pipelines automatisés sont lancés lorsque de nouvelles modifications sont apportées pour orchestrer les tests et le déploiement. Des vérifications des politiques et d'autres tests statiques sont en place pour valider les modifications avant le déploiement. Vous déployez les modifications dans un environnement intermédiaire afin de vérifier que les contrôles fonctionnent comme prévu. Le déploiement dans vos environnements de production est également effectué automatiquement une fois les contrôles approuvés.

Anti-modèles courants :

- Attendre de chaque équipe responsable de la charge de travail qu'elle définisse individuellement sa pile réseau complète, ses protections et ses automatisations. Ne pas publier les aspects standard de la pile réseau et des protections de manière centralisée pour que les équipes chargées de la charge de travail puissent les utiliser.
- S'appuyer sur une équipe réseau centrale pour définir tous les aspects du réseau, les protections et les automatisations. Ne pas déléguer les aspects spécifiques à la charge de travail de la pile réseau et des protections à l'équipe responsable de cette charge de travail.
- Trouver le juste équilibre entre la centralisation et la délégation entre une équipe réseau et les équipes responsables des charges de travail, sans appliquer des normes de test et de déploiement cohérentes à vos modèles IaC et à vos pipelines CI/CD. Ne pas capturer les configurations requises dans les outils qui vérifient la conformité de vos modèles.

Avantages du respect de cette bonne pratique : l'utilisation de modèles pour définir les protections de votre réseau vous permet de suivre et de comparer les modifications au fil du temps avec un système de contrôle de version. L'utilisation de l'automatisation pour tester et déployer les modifications crée

de la standardisation et de la prévisibilité, ce qui augmente les chances de réussite du déploiement et réduit les configurations manuelles répétitives.

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

Directives d’implémentation

Un certain nombre de contrôles de protection réseau décrits dans SEC05-BP02 Contrôlez les flux de trafic au sein de vos couches réseau et SEC05-BP03 Mettre en œuvre une protection basée sur l'inspection s'accompagnent de systèmes de règles gérés qui peuvent être mis à jour automatiquement en fonction des dernières informations sur les menaces. Les exemples de protection de vos points de terminaison Web incluent les règles AWS WAF gérées et l'DDoSatténuation AWS Shield Advanced automatique de la couche d'application. Utilisez des groupes de règles gérées AWS Network Firewall pour vous tenir au courant des listes de domaines de mauvaise réputation et des signatures de menaces.

Au-delà des règles gérées, nous vous recommandons d'utiliser DevOps des pratiques pour automatiser le déploiement des ressources de votre réseau, des protections et des règles que vous spécifiez. Vous pouvez capturer ces définitions dans AWS CloudFormation ou dans un autre outil d’infrastructure en tant que code (IaC) de votre choix, les valider dans un système de contrôle de version et les déployer à l’aide de pipelines CI/CD. Utilisez cette approche DevOps pour bénéficier des avantages traditionnels de la gestion des contrôles de votre réseau, tels que des versions plus prévisibles, des tests automatisés à l'aide d'outils tels que AWS CloudFormation Guard, et la détection des écarts entre votre environnement déployé et la configuration souhaitée.

Sur la base des décisions que vous avez prises dans le cadre de SEC05-BP01 Create network layers, vous pouvez avoir adopté une approche de gestion centralisée pour créer VPCs des couches dédiées aux flux d'entrée, de sortie et d'inspection. Comme décrit dans l'architecture AWS de référence de sécurité (AWS SRA), vous pouvez les définir VPCs dans un compte d'infrastructure réseau dédié. Vous pouvez utiliser des techniques similaires pour définir de manière centralisée les charges de travail VPCs utilisées dans d'autres comptes, leurs groupes de sécurité, leurs AWS Network Firewall déploiements, les règles du résolveur Route 53 et les configurations de DNS pare-feu, ainsi que d'autres ressources réseau. Vous pouvez partager ces ressources avec vos autres comptes grâce à AWS Resource Access Manager. Cette approche vous permet de simplifier les tests automatisés et le déploiement de vos contrôles réseau sur le compte Réseau, en ne gérant qu’une seule destination. Vous pouvez le faire dans un modèle hybride, dans lequel vous déployez et partagez certains contrôles de manière centralisée et déléguez d’autres contrôles aux différentes équipes responsables des charges de travail et à leurs comptes respectifs.

Étapes d’implémentation

1. Déterminez quels aspects du réseau et des protections sont définis de manière centralisée et quels aspects peuvent être gérés par vos équipes qui s’occupent des charges de travail.
2. Créez des environnements pour tester et déployer les modifications apportées à votre réseau et à ses protections. Par exemple, utilisez un compte de test réseau et un compte de production réseau.
3. Déterminez comment vous allez stocker et gérer vos modèles dans un système de contrôle de version. Stockez les modèles centraux dans un référentiel distinct des référentiels de charge de travail, tandis que les modèles de charge de travail peuvent être stockés dans des référentiels spécifiques à cette charge de travail.
4. Créez des pipelines CI/CD pour tester et déployer des modèles. Définissez des tests pour vérifier les erreurs de configuration et vérifier que les modèles sont conformes aux normes de votre entreprise.

Ressources

Bonnes pratiques associées :

- SEC01-BP06 Automatiser le déploiement des contrôles de sécurité standard

Documents connexes :

- AWS Security Reference Architecture - Network account

Exemples connexes :

- Architecture de référence des pipelines de déploiement d’AWS
- NetDevSecOpspour moderniser les déploiements AWS réseau
- Intégration des tests AWS CloudFormation de sécurité AWS Security Hub CSPM et AWS CodeBuild des rapports

Outils associés :

- AWS CloudFormation
- AWS CloudFormation Guard

- cfn_nag

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, etc. 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 vulnérabilités
- SEC06-BP02 Provisionner des calculs à partir d'images renforcées
- SEC06-BP03 Réduire la gestion manuelle et l'accès interactif
- SEC06-BP04 Valider l'intégrité du logiciel
- SEC06-BP05 Automatiser la protection du calcul

SEC06-BP01 Gérer les vulnérabilités

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

Résultat escompté : vous disposez d'une solution qui analyse en permanence votre charge de travail pour détecter les vulnérabilités logicielles, les défauts potentiels et l'exposition involontaire au réseau. Vous avez établi des processus et des procédures pour identifier, hiérarchiser et corriger ces vulnérabilités en fonction de critères d'évaluation des risques. En outre, vous avez mis en place une gestion automatisée des correctifs pour vos instances de calcul. Votre programme de gestion des vulnérabilités est intégré au cycle de vie de votre développement logiciel, avec des solutions pour analyser votre code source dans le cadre du pipeline CI/CD.

Anti-modèles courants :

- Absence de programme de gestion des vulnérabilités.
- 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.

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

Directives d'implémentation

La gestion des vulnérabilités est essentielle au maintien d'un environnement cloud sécurisé et robuste. Elle implique un processus complet qui inclut des analyses de sécurité, l'identification et la hiérarchisation des problèmes, ainsi que des opérations d'application de correctifs pour résoudre les vulnérabilités identifiées. L'automatisation joue un rôle essentiel dans ce processus car elle facilite l'analyse continue des charges de travail pour détecter d'éventuels problèmes et une exposition involontaire du réseau, ainsi que les efforts de correction.

Le modèle de responsabilité partagée AWS est un concept fondamental qui sous-tend la gestion des vulnérabilités. Selon ce modèle, AWS est responsable de la sécurisation de l'infrastructure sous-jacente, y compris du matériel, des logiciels, de la mise en réseau et des installations exécutant les services AWS. À l'inverse, vous êtes responsable de la sécurisation de vos données, des configurations de sécurité et des tâches de gestion associées aux services tels que les instances Amazon EC2 et les objets Amazon S3.

AWS propose une gamme de services pour soutenir les programmes de gestion des vulnérabilités. Amazon Inspector analyse en permanence les charges de travail AWS pour détecter les vulnérabilités logicielles et les accès réseau involontaires, tandis que le Gestionnaire de correctifs d'AWS Systems Manager permet de gérer les correctifs sur l'ensemble des instances Amazon EC2. Ces services peuvent être intégrés à AWS Security Hub CSPM, un service de gestion de la posture de sécurité dans le cloud qui automatise les contrôles de sécurité AWS, centralise les alertes de sécurité et fournit une vue complète de la posture de sécurité d'une organisation. De plus, la sécurité Amazon CodeGuru utilise l'analyse du code statique pour identifier les problèmes potentiels dans les applications Java et Python pendant la phase de développement.

En incorporant les pratiques de gestion des vulnérabilités au cycle de vie du développement logiciel, vous pouvez traiter les vulnérabilités de manière proactive avant qu'elles soient introduites dans les environnements de production, ce qui réduit le risque d'événements de sécurité et minimise l'impact potentiel des vulnérabilités.

Étapes d'implémentation

1. Comprendre le modèle de responsabilité partagée : passez en revue le modèle de responsabilité partagée AWS pour comprendre vos responsabilités en matière de sécurisation de vos charges de travail et de vos données dans le cloud. AWS est responsable de la sécurisation de l'infrastructure cloud sous-jacente, tandis que vous êtes responsable de la sécurisation de vos applications, de vos données et des services que vous utilisez.
2. Mettre en œuvre une analyse des vulnérabilités : configurez un service d'analyse des vulnérabilités, tel qu'Amazon Inspector, pour analyser automatiquement vos instances de calcul (par exemple, les machines virtuelles, les conteneurs ou les fonctions sans serveur) afin de détecter les vulnérabilités logicielles, les défauts potentiels et l'exposition involontaire du réseau.
3. Établir des processus de gestion des vulnérabilités : définissez des processus et des procédures pour identifier, hiérarchiser et corriger les vulnérabilités. Cela peut inclure la mise en place de programmes réguliers d'analyse des vulnérabilités, l'établissement de critères d'évaluation des risques et la définition de délais de correction en fonction de la gravité de la vulnérabilité.
4. Configurer la gestion des correctifs : utilisez un service de gestion des correctifs pour automatiser le processus d'application des correctifs à vos instances de calcul, tant pour les systèmes d'exploitation que pour les applications. Vous pouvez configurer le service pour rechercher les correctifs manquants dans les instances et les installer automatiquement selon un calendrier. Envisagez d'utiliser le Gestionnaire de correctifs d'AWS Systems Manager pour fournir cette fonctionnalité.
5. Configurer une protection contre les programmes malveillants : implémentez des mécanismes pour détecter les logiciels malveillants dans votre environnement. Par exemple, vous pouvez utiliser des outils tels qu'Amazon GuardDuty pour analyser, détecter et signaler les logiciels malveillants dans les volumes EC2 et EBS. GuardDuty peut également analyser les objets récemment chargés sur Amazon S3 pour détecter d'éventuels logiciels malveillants ou virus et prendre des mesures pour les isoler avant qu'ils ne soient ingérés dans les processus en aval.
6. Intégrer l'analyse des vulnérabilités dans les pipelines CI/CD : si vous utilisez un pipeline CI/CD pour le déploiement de votre application, intégrez des outils d'analyse des vulnérabilités dans votre pipeline. Des outils tels que la sécurité Amazon CodeGuru et des options open source peuvent analyser votre code source, vos dépendances et vos artefacts pour détecter d'éventuels problèmes de sécurité.
7. Configurer un service de surveillance de la sécurité : configurez un service de surveillance de la sécurité, tel qu'AWS Security Hub CSPM, pour obtenir une vue complète de votre posture de sécurité sur plusieurs services cloud. Le service doit collecter les résultats de sécurité provenant

de diverses sources et les présenter dans un format normalisé pour faciliter leur hiérarchisation et leur correction.

8. Mettre en œuvre un test de pénétration des applications Web : si votre application est une application Web et que votre organisation possède les compétences nécessaires ou peut engager une assistance extérieure, envisagez de mettre en œuvre un test de pénétration des applications Web afin d'identifier les vulnérabilités potentielles de votre application.
9. Automatiser avec une infrastructure en tant que code : utilisez des outils d'infrastructure en tant que code (IaC), tels qu'AWS CloudFormation, pour automatiser le déploiement et la configuration de vos ressources, y compris les services de sécurité mentionnés précédemment. Cette pratique vous aide à créer une architecture de ressources plus cohérente et standardisée sur plusieurs comptes et environnements.
10. Surveiller et améliorer continuellement : surveillez en permanence l'efficacité de votre programme de gestion des vulnérabilités et apportez les améliorations nécessaires. Passez en revue les résultats de sécurité, évaluez l'efficacité de vos efforts de correction et ajustez vos processus et outils en conséquence.

Ressources

Documents connexes :

- AWS Systems Manager
- Présentation de la sécurité de AWS Lambda
- Amazon CodeGuru
- Gestion automatisée et améliorée des vulnérabilités pour les charges de travail dans le cloud grâce au nouvel Amazon Inspector
- Automatiser la gestion et la correction des vulnérabilités dans AWS à l'aide d'Amazon Inspector et AWS Systems Manager — Partie 1

Vidéos connexes :

- Sécurisation des services sans serveur et de conteneur
- Security best practices for the Amazon EC2 instance metadata service

SEC06-BP02 Provisionner des calculs à partir d'images renforcées

Réduisez les possibilités d’accès involontaire à vos environnements d’exécution en les déployant à partir d’images renforcées. Acquérez uniquement les dépendances d’exécution, telles que les images de conteneurs et les bibliothèques d’applications, à partir de registres fiables et vérifiez leurs signatures. Créez vos propres registres privés pour stocker des images et des bibliothèques fiables à utiliser dans vos processus de création et de déploiement.

Résultat souhaité : vos ressources de calcul sont provisionnées à partir d’images de référence renforcées. Vous récupérez les dépendances externes, telles que les images de conteneurs et les bibliothèques d’applications, uniquement à partir de registres fiables et vous vérifiez leurs signatures. Celles-ci sont stockées dans des registres privés à des fins de référence pour vos processus de création et de déploiement. Vous analysez et mettez à jour régulièrement les images et les dépendances pour vous protéger contre les vulnérabilités récemment découvertes.

Anti-modèles courants :

- Acquérir des images et des bibliothèques à partir de registres fiables, mais sans vérifier leur signature ni effectuer d’analyses de vulnérabilité avant de les utiliser.
- Renforcer les images, mais ne pas les tester régulièrement pour détecter de nouvelles vulnérabilités ou ne pas les mettre à jour vers la dernière version.
- Installer ou ne pas supprimer les packages logiciels qui ne sont pas nécessaires pendant le cycle de vie prévu de l’image.
- S’appuyer uniquement sur l’application de correctifs pour maintenir à jour les ressources de calcul de production. L’application de correctifs à elle seule peut encore entraîner une dérive des ressources de calcul par rapport à la norme renforcée au fil du temps. Il est également possible que l’application de correctifs ne parvienne pas à supprimer les programmes malveillants qui ont pu être installés par un acteur malveillant lors d’un événement de sécurité.

Avantages du respect de cette bonne pratique : le renforcement des images permet de réduire le nombre de chemins disponibles dans votre environnement d’exécution susceptibles de permettre un accès involontaire à des utilisateurs ou à des services non autorisés. Cela peut également réduire l’ampleur de l’impact en cas d’accès involontaire.

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

Directives d’implémentation

Pour renforcer vos systèmes, utilisez les dernières versions des systèmes d’exploitation, des images de conteneurs et des bibliothèques d’applications. Appliquez des correctifs aux problèmes connus. Minimisez le système en supprimant la totalité des applications, services, pilotes d’appareils, utilisateurs par défaut et autres informations d’identification inutiles. Prenez toutes les autres mesures nécessaires, telles que la désactivation des ports pour créer un environnement disposant uniquement des ressources et des fonctionnalités requises pour vos charges de travail. À partir de cette situation de référence, vous pouvez ensuite installer les logiciels, les agents ou les autres processus dont vous avez besoin à des fins telles que la surveillance de la charge de travail ou la gestion des vulnérabilités.

Vous pouvez réduire le fardeau que représente le renforcement des systèmes en utilisant les conseils fournis par des sources fiables, tels que les guides de mise en œuvre technique de sécurité du Center for Internet Security (CISDISA) et de la Defense Information Systems Agency (STIGs) (). Nous vous recommandons de commencer par une Amazon Machine Image (AMI) publiée par un partenaire AWS ou par un APN partenaire, et d'utiliser AWS EC2Image Builder pour automatiser la configuration en fonction d'une combinaison appropriée de STIG contrôles CIS et de commandes.

Bien qu'il existe des images renforcées et des recettes EC2 Image Builder qui appliquent les CIS DISA STIG recommandations du mode opératoire, il se peut que leur configuration empêche le bon fonctionnement de votre logiciel. Dans ce cas, vous pouvez partir d'une image de base non renforcée, installer votre logiciel, puis appliquer progressivement CIS des contrôles pour tester leur impact. Pour tout CIS contrôle qui empêche l'exécution de votre logiciel, testez si vous pouvez plutôt mettre en œuvre les recommandations de renforcement plus précises. DISA Gardez une trace des différents CIS contrôles et DISA STIG configurations que vous êtes en mesure d'appliquer avec succès. Utilisez-les pour définir vos recettes de durcissement d'image dans EC2 Image Builder en conséquence.

Pour les charges de travail conteneurisées, les images renforcées de Docker sont disponibles dans le référentiel public Amazon Elastic Container Registry () ECR. Vous pouvez utiliser EC2 Image Builder pour renforcer les images des conteneurs en parallèleAMIs.

Comme pour les systèmes d'exploitation et les images de conteneurs, vous pouvez obtenir des packages de code (ou des bibliothèques) à partir de référentiels publics, via des outils tels que pip, npm, Maven et. NuGet Nous vous recommandons de gérer les packages de code en intégrant des référentiels privés, comme dans AWS CodeArtifact, à des référentiels publics fiables. Cette intégration peut gérer la récupération, le stockage et la conservation des packages up-to-date pour vous. Les processus de création de votre application peuvent ensuite obtenir et tester la dernière

version de ces packages en même temps que votre application, à l'aide de techniques telles que l'analyse de la composition logicielle (SCA), les tests statiques de sécurité des applications (SAST) et les tests dynamiques de sécurité des applications (DAST).

Pour les charges de travail sans serveur qui l'utilisent AWS Lambda, simplifiez la gestion des dépendances des packages à l'aide des couches Lambda. Utilisez des couches Lambda afin de configurer un ensemble de dépendances standard qui sont partagées entre différentes fonctions dans une archive autonome. Vous pouvez créer et gérer des couches par le biais de leur propre processus de création, ce qui permet à vos fonctions de rester centralisées up-to-date.

Étapes d’implémentation

- Renforcez les systèmes d’exploitation. Utilisez des images de base provenant de sources fiables comme base pour développer votre système renforcéAMIs. Utilisez EC2Image Builder pour personnaliser le logiciel installé sur vos images.
- Renforcez les ressources conteneurisées. Configurez les ressources conteneurisées de manière à respecter les bonnes pratiques en matière de sécurité. Lorsque vous utilisez des conteneurs, implémentez la numérisation d'ECRimages dans votre pipeline de génération et régulièrement par rapport à votre référentiel d'images pour rechercher CVEs dans vos conteneurs.
- Lorsque vous utilisez une implémentation sans serveur avec AWS Lambda, utilisez des couches Lambda pour séparer le code des fonctions de l'application et les bibliothèques dépendantes partagées. La signature de code pour Lambda permet de s’assurer que seul du code approuvé s’exécute dans vos fonctions Lambda.

Ressources

Bonnes pratiques associées :

- OPS05-BP05 Effectuer la gestion des correctifs

Vidéos connexes :

- Une plongée approfondie dans le domaine de AWS Lambda la sécurité

Exemples connexes :

- Créez rapidement une version STIG conforme à AMI l'aide d'EC2Image Builder

- Création de meilleures images de conteneurs
- Utilisation de couches Lambda pour simplifier votre processus de développement
- Développez et déployez des AWS Lambda couches à l'aide d'un framework sans serveur
- Création d'un pipeline end-to-end AWS DevSecOps CI/CD avec des outils et des logiciels open source SCA SAST DAST

SEC06-BP03 Réduire la gestion manuelle et l’accès interactif

Utilisez l’automatisation pour effectuer des tâches de déploiement, de configuration, de maintenance et d’investigation dans la mesure du possible. Envisagez l’accès manuel aux ressources de calcul en cas de procédures d’urgence ou dans des environnements sécurisés (environnement de test [sandbox]), lorsque l’automatisation n’est pas disponible.

Résultat escompté : les scripts programmatiques et les documents d’automatisation (runbooks) capturent les actions autorisées sur vos ressources informatiques. Ces runbooks sont lancés soit automatiquement, par le biais de systèmes de détection des changements, soit manuellement, lorsque le jugement humain est requis. L’accès direct aux ressources de calcul n’est disponible qu’en cas d’urgence, lorsque l’automatisation n’est pas disponible. Toutes les activités manuelles sont enregistrées et intégrées à un processus de révision afin d’améliorer continuellement vos capacités d’automatisation.

Anti-modèles courants :

- Accès interactif aux instances Amazon EC2 avec des protocoles tels que SSH ou RDP.
- Gestion des connexions utilisateur individuelles, telles que celles des utilisateurs locaux `/etc/passwd` ou Windows.
- Partage d’un mot de passe ou d’une clé privée pour accéder à une instance entre plusieurs utilisateurs.
- Installation manuelle des logiciels et création ou mise à jour des fichiers de configuration.
- Mise à jour ou correction manuelle des logiciels.
- Connexion à une instance pour résoudre les problèmes.

Avantages du respect de cette bonne pratique : la réalisation d’actions automatisées vous aide à réduire le risque opérationnel lié à des modifications involontaires et à des erreurs de configuration. La suppression de l’utilisation de Secure Shell (SSH) et du protocole RDP (Remote Desktop

Protocol) pour l'accès interactif réduit l'étendue de l'accès à vos ressources de calcul. Cette opération supprime un chemin commun pour les actions non autorisées. La saisie de vos tâches de gestion des ressources de calcul dans des documents d'automatisation et des scripts programmatiques fournit un mécanisme permettant de définir et d'auditer l'ensemble des activités autorisées à un niveau de détail précis.

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

Directives d'implémentation

La connexion à une instance est une approche classique de l'administration du système. Après avoir installé le système d'exploitation du serveur, les utilisateurs se connectent généralement manuellement pour configurer le système et installer les logiciels souhaités. Pendant la durée de vie du serveur, les utilisateurs peuvent se connecter pour effectuer des mises à jour logicielles, appliquer des correctifs, modifier des configurations et résoudre des problèmes.

L'accès manuel présente toutefois un certain nombre de risques. Il requiert la présence d'un serveur qui écoute les requêtes, par exemple un service SSH ou RDP, capable de fournir un chemin potentiel vers un accès non autorisé. Cela augmente également le risque d'erreur humaine associée à l'exécution d'étapes manuelles. Ces étapes peuvent entraîner des incidents liés à la charge de travail, une corruption ou une destruction de données, ou d'autres problèmes de sécurité. L'accès humain requiert également des protections contre le partage d'informations d'identification, ce qui entraîne des frais de gestion supplémentaires.

Pour atténuer ces risques, vous pouvez implémenter une solution d'accès à distance basée sur des agents, comme AWS Systems Manager. AWS Systems Manager Agent (SSM Agent) lance un canal chiffré et ne dépend donc pas de l'écoute des demandes émanant de l'extérieur. Envisagez de configurer l'agent SSM pour établir ce canal sur un point de terminaison d'un VPC.

Systems Manager vous permet de contrôler avec précision la manière dont vous pouvez interagir avec vos instances gérées. Vous définissez les automatisations à exécuter, qui peut les exécuter et quand elles peuvent être exécutées. Systems Manager peut appliquer des correctifs, installer des logiciels et apporter des modifications de configuration sans accès interactif à l'instance. Systems Manager peut également fournir un accès à un shell distant et enregistrer chaque commande invoquée, ainsi que sa sortie, pendant la session dans les journaux et Amazon S3. AWS CloudTrail enregistre les invocations d'API Systems Manager à des fins d'inspection.

Étapes d'implémentation

1. Installez AWS Systems Manager Agent (SSM Agent) sur vos instances Amazon EC2. Vérifiez si SSM Agent est inclus et démarré automatiquement dans le cadre de votre configuration d'AMI de base.
2. Vérifiez que les rôles IAM associés à vos profils d'instance EC2 incluent la politique IAM gérée `AmazonSSMManagedInstanceCore`.
3. Désactivez SSH, RDP et les autres services d'accès à distance exécutés sur vos instances. Pour cela, exécutez des scripts configurés dans la section des données utilisateur de vos modèles de lancement ou créez des AMI personnalisées à l'aide d'outils tels qu'EC2 Image Builder.
4. Vérifiez que les règles d'entrée des groupes de sécurité applicables à vos instances EC2 n'autorisent pas l'accès sur le port 22/tcp (SSH) ni le port 3389/tcp (RDP). Mettez en œuvre la détection et l'alerte en cas de groupes de sécurité mal configurés à l'aide de services tels que AWS Config.
5. Définissez les automatisations, les runbooks et les commandes d'exécution appropriés dans Systems Manager. Utilisez les politiques IAM pour définir qui peut effectuer ces actions et les conditions dans lesquelles elles sont autorisées. Testez minutieusement ces automatisations dans un environnement hors production. Invoquez ces automatisations si nécessaire, au lieu d'accéder à l'instance de manière interactive.
6. Utilisez AWS Systems Manager Session Manager pour fournir un accès interactif aux instances lorsque cela est nécessaire. Activez la journalisation des activités de session pour conserver une piste d'audit dans Amazon CloudWatch Logs ou Amazon S3.

Ressources

Bonnes pratiques associées :

- REL08-BP04 Effectuer le déploiement à l'aide d'une infrastructure immuable

Exemples connexes :

- Remplacement de l'accès SSH pour réduire les frais de gestion et de sécurité avec AWS Systems Manager

Outils associés :

- AWS Systems Manager

Vidéos connexes :

- Controlling User Session Access to Instances in AWS Systems Manager Session Manager

SEC06-BP04 Valider l'intégrité du logiciel

Utilisez la vérification cryptographique pour valider l’intégrité des artefacts logiciels (y compris les images) utilisés par votre charge de travail. Signez vos logiciels de manière cryptographique afin de vous protéger contre les modifications non autorisées exécutées dans vos environnements de calcul.

Résultat souhaité : tous les artefacts proviennent de sources fiables. Les certificats des sites Web des fournisseurs sont validés. Les artefacts téléchargés sont vérifiés cryptographiquement par leur signature. Vos propres logiciels sont signés cryptographiquement et vérifiés par vos environnements informatiques.

Anti-modèles courants :

- Faire confiance aux sites Web de fournisseurs réputés pour obtenir des artefacts logiciels, mais ignorer les avis d’expiration des certificats. Procéder aux téléchargements sans confirmer la validité des certificats.
- Valider les certificats des sites Web des fournisseurs, mais sans vérifier cryptographiquement les artefacts téléchargés depuis ces sites Web.
- S’appuyer uniquement sur des condensés ou des hachages pour valider l’intégrité des logiciels. Les hachages établissent que les artefacts n’ont pas été modifiés par rapport à leur version d’origine, mais ils ne valident pas leur source.
- Ne pas signer vos propres logiciels, codes ou bibliothèques, même s’ils ne sont utilisés que dans le cadre de vos propres déploiements.

Avantages du respect de cette bonne pratique : la validation de l’intégrité des artefacts dont dépend votre charge de travail permet d’empêcher les logiciels malveillants de pénétrer dans vos environnements informatiques. La signature de vos logiciels contribue à vous protéger contre toute exécution non autorisée dans vos environnements de calcul. Sécurisez votre chaîne d’approvisionnement logicielle en signant et en vérifiant le code.

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

Directives d’implémentation

Les images du système d’exploitation, les images de conteneurs et les artefacts de code sont souvent distribués avec des contrôles d’intégrité disponibles, par exemple via un condensé ou un hachage. Cela permet aux clients de vérifier l’intégrité en calculant leur propre hachage de la charge utile et en s’assurant qu’il est identique à celui publié. Bien que ces vérifications permettent de vérifier que la charge utile n’a pas été falsifiée, elles ne permettent pas de valider que la charge utile provient de la source d’origine (sa provenance). La vérification de la provenance nécessite un certificat délivré par une autorité de confiance pour signer numériquement l’artefact.

Si vous utilisez un logiciel téléchargé ou des artefacts dans votre charge de travail, vérifiez si le fournisseur fournit une clé publique pour la vérification des signatures numériques. Voici quelques exemples de la façon dont AWS fournit une clé publique et des instructions de vérification pour les logiciels que nous publions :

- EC2Image Builder : vérifier la signature du téléchargement de l' AWS TOEinstallation
- AWS Systems Manager: Vérification de la signature de l'SSMagent
- Amazon CloudWatch : vérification de la signature du package d' CloudWatch agent

Intégrez la vérification des signatures numériques dans les processus que vous utilisez pour obtenir et renforcer les images, comme indiqué dans SEC06-BP02 Provisionner le calcul à partir d'images renforcées.

Vous pouvez utiliser AWS Signer pour gérer la vérification des signatures, ainsi que votre propre cycle de vie de signature de code pour vos propres logiciels et artefacts. AWS Lambda et Amazon Elastic Container Registry proposent des intégrations avec Signer pour vérifier les signatures de votre code et de vos images. À l’aide des exemples de la section Ressources, vous pouvez intégrer Signer à vos pipelines d’intégration et de diffusion continues (CI/CD) afin d’automatiser la vérification des signatures et la signature de vos propres codes et images.

Ressources

Documents connexes :

- Signature cryptographique pour les conteneurs
- Meilleures pratiques pour sécuriser votre pipeline de création d'images de conteneur en utilisant AWS Signer

- Annonce de la signature d'images de conteneurs avec AWS Signer et Amazon EKS
- Configuration de la signature de code pour AWS Lambda
- Bonnes pratiques et modèles avancés pour la signature de code Lambda
- Signature de code à l'aide d' AWS Certificate Manager une autorité de certification privée et de AWS Key Management Service clés asymétriques

Exemples connexes :

- Automatisez la signature du code Lambda avec Amazon et CodeCatalyst AWS Signer
- Signature et validation des OCI artefacts avec AWS Signer

Outils associés :

- AWS Lambda
- AWS Signer
- AWS Certificate Manager
- AWS Key Management Service
- AWS CodeArtifact

SEC06-BP05 Automatiser la protection du calcul

Automatisez les opérations de protection informatique afin de réduire le besoin d’intervention humaine. Utilisez l’analyse automatique pour détecter les problèmes potentiels au sein de vos ressources informatiques et y remédier grâce à des réponses programmatiques automatisées ou à des opérations de gestion de flotte. Intégrez l’automatisation à vos processus CI/CD pour déployer des charges de travail fiables avec des dépendances à jour.

Résultat escompté : les systèmes automatisés effectuent toutes les analyses et tous les correctifs des ressources informatiques. Vous utilisez la vérification automatique pour vérifier que les images logicielles et les dépendances proviennent de sources fiables et qu’elles n’ont pas été falsifiées. Les charges de travail sont automatiquement vérifiées pour détecter les dépendances à jour et sont signées pour garantir la fiabilité des environnements informatiques AWS. Des mesures correctives automatisées sont lancées lorsque des ressources non conformes sont détectées.

Anti-modèles courants :

- Suivre la pratique d'une infrastructure immuable, mais ne pas avoir de solution en place pour l'application de correctifs d'urgence ou le remplacement des systèmes de production.
- Utiliser l'automatisation pour corriger les ressources mal configurées, mais ne pas mettre en place de mécanisme de remplacement manuel. Dans certains cas, vous devrez ajuster les exigences et suspendre les automatisations jusqu'à ce que vous apportiez ces modifications.

Avantages du respect de cette bonne pratique : l'automatisation peut réduire le risque d'accès et d'utilisation non autorisés de vos ressources informatiques. Elle contribue à éviter que les erreurs de configuration soient transférées dans les environnements de production, et à détecter et corriger ces erreurs le cas échéant. L'automatisation facilite également la détection des accès et utilisations non autorisés des ressources de calcul afin de réduire le temps de réponse. Vous pouvez ainsi réduire la portée globale de l'impact du problème.

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

Directives d'implémentation

Vous pouvez appliquer les automatisations décrites dans les pratiques du pilier de sécurité pour protéger vos ressources de calcul. SEC06-BP01 Gérer les failles décrit comment vous pouvez utiliser Amazon Inspector dans vos pipelines CI/CD et pour analyser en permanence vos environnements d'exécution à la recherche de vulnérabilités et d'expositions courantes (CVE) connues. Vous pouvez utiliser AWS Systems Manager pour appliquer des correctifs ou effectuer des redéploiements à partir d'images récentes via des runbooks automatisés afin de maintenir votre flotte informatique à jour avec les derniers logiciels et bibliothèques. Utilisez ces techniques pour limiter la nécessité de mettre en place des processus manuels et des accès interactifs à vos ressources de calcul. Pour en savoir plus, consultez SEC06-BP03 Réduire la gestion manuelle et l'accès interactif.

L'automatisation joue également un rôle dans le déploiement de charges de travail fiables, comme décrit dans SEC06-BP02 Provisionner le calcul à partir d'images renforcées et SEC06-BP04 Valider l'intégrité du logiciel. Vous pouvez utiliser des services tels qu'EC2 Image Builder, AWS Signer, AWS CodeArtifact et Amazon Elastic Container Registry (ECR) pour télécharger, vérifier, construire et stocker des images et des dépendances de code renforcées et approuvées. Outre Inspector, chacun d'entre eux peut jouer un rôle dans votre processus CI/CD, de sorte que votre charge de travail n'est mise en production qu'après confirmation que ses dépendances sont à jour et proviennent de sources fiables. Votre charge de travail est également signée afin que les environnements informatiques AWS tels que AWS Lambda et Amazon Elastic Kubernetes Service (EKS) puissent vérifier qu'elle n'a pas été falsifiée avant de l'autoriser à s'exécuter.

Au-delà de ces contrôles préventifs, vous pouvez également utiliser l'automatisation dans vos contrôles de détection pour vos ressources de calcul. À titre d'exemple, AWS Security Hub CSPM offre la norme NIST 800-53 Rev. 5 qui inclut des contrôles tels que [EC2.8] Les instances EC2 doivent utiliser Instance Metadata Service Version 2 (IMDSv2). IMDSv2 utilise les techniques d'authentification de session, de blocage des requêtes contenant un en-tête HTTP X-Forwarded-For et un TTL réseau 1 pour arrêter le trafic provenant de sources externes afin de récupérer des informations sur l'instance EC2. Cette vérification dans Security Hub CSPM permet de détecter quand les instances EC2 utilisent IMDSv1 et de lancer une correction automatique. Apprenez-en plus sur la détection et les corrections automatisées dans SEC04-BP04 Initier la correction des ressources non conformes.

Étapes d'implémentation

1. Automatisez la création d'AMI sécurisées, conformes et renforcées avec EC2 Image Builder. Vous pouvez produire des images qui intègrent des contrôles issus des références du Center for Internet Security (CIS) ou des normes du Security Technical Implementation Guide (STIG) à partir des images de base d'AWS et des partenaires APN.
2. Automatisez la gestion de la configuration. Appliquez et validez des configurations sécurisées dans vos ressources de calcul automatiquement à l'aide d'un service ou d'un outil de gestion de la configuration.
    a. Gestion de configuration automatisée à l'aide de AWS Config
    b. Gestion automatisée de la posture de sécurité et de conformité à l'aide de AWS Security Hub CSPM
3. Automatisez l'application des correctifs ou le remplacement des instances Amazon Elastic Compute Cloud (Amazon EC2). AWS Le gestionnaire de correctifs Systems Manager automatise le processus d'application des correctifs aux instances gérées avec des types de mises à jour liés à la sécurité et d'autres types. Vous pouvez utiliser le Gestionnaire de correctifs pour appliquer des correctifs pour les systèmes d'exploitation et les applications.
    a. Gestionnaire de correctifs d'AWS Systems Manager
4. Automatisez l'analyse des ressources de calcul pour détecter les vulnérabilités et risques communs (CVE), et intégrez des solutions d'analyse de sécurité à votre pipeline de création.
    a. Amazon Inspector
    b. Analyse d'image ECR

5. Pensez à Amazon GuardDuty pour la détection automatique des malwares et des menaces afin de protéger les ressources informatiques. GuardDuty peut également identifier les problèmes potentiels lorsqu'une fonction AWS Lambda est invoquée dans votre environnement AWS.
   a. Amazon GuardDuty
6. Envisagez les solutions des Partenaires AWS. AWS Les Partenaires proposent des 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.
   a. Sécurité de l'infrastructure

Ressources

Bonnes pratiques associées :

- SEC01-BP06 Automatiser le déploiement des contrôles de sécurité standard

Documents connexes :

- Profiter de tous les avantages d'IMDSv2 et désactiver IMDSv1 sur l'ensemble de votre infrastructure AWS

Vidéos connexes :

- Security best practices for the Amazon EC2 instance metadata service

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
- Protection des données au repos
- Protection des données en transit

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 Comprendre votre schéma de classification des données
- SEC07-BP02 Appliquer des contrôles de protection des données en fonction de la sensibilité des données
- SEC07-BP03 Automatiser l'identification et la classification
- SEC07-BP04 Définir la gestion évolutive du cycle de vie des données

SEC07-BP01 Comprendre votre schéma de classification des données

Comprenez la classification des données traitées par votre charge de travail, ses exigences en matière de traitement, les processus métier associés, l'endroit où les données sont stockées et qui

en est le propriétaire. Votre système de classification et de traitement des données doit tenir compte des exigences légales et de conformité applicables à votre charge de travail, ainsi que des contrôles de données nécessaires. La compréhension des données est la première étape du processus de classification des données.

Résultat escompté : les types de données présents dans votre charge de travail sont bien compris et documentés. Des contrôles appropriés sont en place pour protéger les données sensibles en fonction de leur classification. Ces contrôles régissent les considérations suivantes : qui est autorisé à accéder aux données et dans quel but, où les données sont stockées, la politique de chiffrement de ces données et la manière dont les clés de chiffrement sont gérées, le cycle de vie des données et leurs exigences de conservation, les processus de destruction appropriés, les processus de sauvegarde et de restauration mis en place et l'audit de l'accès.

Anti-modèles courants :

- Ne pas établir de politique officielle de classification des données pour définir les niveaux de sensibilité des données et leurs exigences de traitement.
- Ne pas bien comprendre les niveaux de sensibilité des données de votre charge de travail et ne pas saisir ces informations dans la documentation relative à l'architecture et aux opérations.
- Ne pas appliquer les contrôles appropriés à vos données en fonction de leur sensibilité et de leurs exigences, comme indiqué dans votre politique de classification et de traitement des données.
- Ne pas fournir de rétroaction sur les exigences de classification et de traitement des données aux propriétaires des politiques.

Avantages liés au respect de cette bonne pratique : cette pratique élimine toute ambiguïté quant au traitement approprié des données dans le cadre de votre charge de travail. L'application d'une politique officielle qui définit les niveaux de sensibilité des données de votre organisation et les protections requises peut vous aider à vous conformer aux réglementations légales et aux autres attestations et certifications de cybersécurité. Les propriétaires de la charge de travail peuvent savoir en toute confiance où sont stockées les données sensibles et quels contrôles de protection sont en place. La consignation de ces informations dans la documentation aide les nouveaux membres de l'équipe à mieux les comprendre et à gérer les contrôles dès qu'ils commencent à occuper leur fonction. Ces pratiques peuvent également contribuer à réduire les coûts en dimensionnant correctement les contrôles pour chaque type de données.

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

Directives d'implémentation

Lors de la conception d'une charge de travail, vous pouvez réfléchir aux moyens de protéger les données sensibles de manière intuitive. Par exemple, dans une application multilocataire, il est intuitif de considérer les données de chaque locataire comme sensibles et de mettre en place des protections afin qu'un locataire ne puisse pas accéder aux données d'un autre. De même, vous pouvez concevoir des contrôles d'accès intuitifs de telle sorte que seuls les administrateurs puissent modifier les données, tandis que les autres utilisateurs ne bénéficient que d'un accès en lecture, voire d'aucun accès.

En définissant et en saisissant ces niveaux de sensibilité des données dans les politiques, ainsi que leurs exigences en matière de protection des données, vous pouvez identifier formellement quelles données se trouvent dans votre charge de travail. Vous pouvez ensuite déterminer si les contrôles appropriés sont en place, s'ils peuvent être audités et quelles réponses sont pertinentes en cas de mauvaise gestion des données.

Pour mieux identifier l'emplacement de données sensibles dans votre charge de travail, envisagez d'utiliser un catalogue de données. Un catalogue de données est une base de données qui cartographie les données de votre organisation, leur emplacement, leur niveau de sensibilité et les contrôles mis en place pour protéger ces données. En outre, envisagez d'utiliser des balises de ressources le cas échéant. Par exemple, vous pouvez appliquer une balise possédant une clé de balise de `Classification` et une valeur de balise de `PHI` pour les informations de santé protégées (PHI), et une autre balise possédant une clé de balise de `Sensitivity` et une valeur de balise de `High`. Les services tels que AWS Config peuvent ensuite être utilisés pour surveiller les modifications apportées à ces ressources et vous avertir si elles font l'objet d'une modification les rendant non conformes à vos exigences de protection (telles que la modification des paramètres de chiffrement). Vous pouvez capturer la définition standard de vos clés de balise et les valeurs acceptables à l'aide des politiques de balises, une fonctionnalité d'AWS Organizations. Il est déconseillé d'avoir une clé ou une valeur de balise qui contient des données privées ou sensibles.

Étapes d'implémentation

1. Comprenez le schéma de classification des données et les exigences de protection de votre organisation.
2. Identifiez les types de données sensibles traitées par vos charges de travail.
3. Capturez les données dans un catalogue de données qui fournit une vue unique de l'emplacement des données dans l'organisation et du niveau de sensibilité de ces données.

4. Envisagez d'utiliser le balisage au niveau des ressources et des données, le cas échéant, pour baliser les données en fonction de leur niveau de sensibilité et d'autres métadonnées opérationnelles susceptibles de faciliter la surveillance et la réponse aux incidents.
   a. Les politiques de balisage d'AWS Organizations peuvent être utilisées pour appliquer les normes de balisage.

Ressources

Bonnes pratiques associées :

- SUS04-BP01 Mettre en œuvre une politique de classification des données

Documents connexes :

- Livre blanc sur la classification des données
- Bonnes pratiques en matière de balisage des ressources AWS

Exemples connexes :

- Syntaxe d'une stratégie de balise AWS Organizations et exemples

Outils associés

- AWS Tag Editor

SEC07-BP02 Appliquer des contrôles de protection des données en fonction de la sensibilité des données

Appliquez des contrôles de protection des données qui fournissent un niveau de contrôle approprié pour chaque classe de données définie dans votre politique de classification. Cette pratique peut vous permettre de protéger les données sensibles contre tout accès et toute utilisation non autorisés, tout en préservant la disponibilité et l'utilisation des données.

Résultat escompté : vous disposez d'une politique de classification qui définit les différents niveaux de sensibilité des données au sein de votre organisation. Pour chacun de ces niveaux de sensibilité, vous avez publié des directives claires concernant les services et sites de stockage et de traitement

approuvés, ainsi que leur configuration requise. Vous mettez en œuvre les contrôles pour chaque niveau en fonction du niveau de protection requis et des coûts associés. Vous avez mis en place une surveillance et des alertes afin de détecter si des données sont présentes dans des emplacements non autorisés, traitées dans des environnements non autorisés, consultées par des acteurs non autorisés ou si la configuration des services associés devient non conforme.

Anti-modèles courants :

- Appliquer le même niveau de contrôles de protection à toutes les données. Cela peut entraîner un surprovisionnement des contrôles de sécurité pour les données peu sensibles ou une protection insuffisante des données hautement sensibles.
- Ne pas impliquer les parties prenantes concernées des équipes chargées de la sécurité, de la conformité et des opérations lors de la définition des contrôles de protection des données.
- Surveiller les frais opérationnels et les coûts associés à la mise en œuvre et à la maintenance des contrôles de protection des données.
- Ne pas procéder à des examens périodiques des contrôles de protection des données pour préserver l'alignement avec les politiques de classification.
- Ne pas disposer d'un inventaire complet des emplacements des données au repos et en transit.

Avantages liés au respect de cette bonne pratique : en alignant vos contrôles sur le niveau de classification de vos données, votre organisation peut investir dans des niveaux de contrôle plus élevés si nécessaire. Cela peut inclure l'augmentation des ressources consacrées à la sécurisation, à la surveillance, à la mesure, à la correction et à la production de rapports. Lorsque moins de contrôles sont nécessaires, vous pouvez améliorer l'accessibilité et l'exhaustivité des données pour votre personnel, vos clients ou vos administrés. Cette approche offre à votre organisation une grande flexibilité en matière d'utilisation des données, tout en respectant les exigences de protection des données.

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

Directives d'implémentation

La mise en œuvre de contrôles de protection des données basés sur les niveaux de sensibilité des données implique plusieurs étapes clés. Tout d'abord, identifiez les différents niveaux de sensibilité des données au sein de votre architecture de charge de travail (public, interne, confidentiel et restreint) et évaluez où vous stockez et traitez ces données. Définissez ensuite les limites d'isolement autour des données en fonction de leur niveau de sensibilité. Nous vous recommandons de séparer

les données en différents Comptes AWS, en utilisant des politiques de contrôle des services (SCP) pour restreindre les services et les actions autorisés pour chaque niveau de sensibilité des données. Vous pouvez ainsi créer des limites d'isolement solides et appliquer le principe du moindre privilège.

Après avoir défini les limites d'isolement, implémentez les contrôles de protection appropriés en fonction des niveaux de sensibilité des données. Consultez les bonnes pratiques en matière de protection des données au repos et de protection des données en transit pour mettre en œuvre des contrôles pertinents tels que le chiffrement, les contrôles d'accès et l'audit. Envisagez des techniques telles que la création de jeton ou l'anonymisation pour réduire le niveau de sensibilité de vos données. Simplifiez l'application de politiques de données cohérentes dans l'ensemble de votre entreprise grâce à un système centralisé de création/décréation de jeton.

Surveillez et testez en permanence l'efficacité des contrôles mis en œuvre. Régulièrement, passez en revue et mettez à jour le schéma de classification des données, les évaluations des risques et les contrôles de protection à mesure que le paysage des données et les menaces de votre organisation évoluent. Alignez les contrôles de protection des données mis en œuvre avec les réglementations, normes et exigences légales pertinentes du secteur. En outre, sensibilisez et formez les employés à la sécurité pour les aider à comprendre le système de classification des données et leurs responsabilités en matière de traitement et de protection des données sensibles.

Étapes d'implémentation

1. Identifiez la classification et les niveaux de sensibilité des données au sein de votre charge de travail.
2. Définissez des limites d'isolement pour chaque niveau et déterminez une stratégie d'application.
3. Évaluez les contrôles que vous définissez pour régir l'accès, le chiffrement, l'audit, la conservation et les autres éléments requis par votre politique de classification des données.
4. Évaluez les options permettant de réduire le niveau de sensibilité des données le cas échéant, par exemple en utilisant la création de jeton ou l'anonymisation.
5. Vérifiez vos contrôles à l'aide de tests et de contrôles automatisés de vos ressources configurées.

Ressources

Bonnes pratiques associées :

- PERF03-BP01 Utiliser un magasin de données dédié le mieux adapté à vos besoins en matière de stockage des données et d'accès aux données
- COST04-BP05 Appliquer les politiques de conservation des données

Documents connexes :

- Livre blanc sur la classification des données
- Bonnes pratiques en matière de sécurité, d'identité et de conformité
- Meilleures pratiques pour AWS KMS.
- Bonnes pratiques et fonctionnalités de chiffrement pour les services AWS

Exemples connexes :

- Création d'une solution de création de jeton sans serveur pour masquer les données sensibles
- Comment utiliser la création de jeton pour améliorer la sécurité des données et réduire la portée de l'audit

Outils associés :

- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- AWS Organizations

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. L'utilisation de l'automatisation pour améliorer la détermination manuelle réduit le risque d'erreur humaine et d'exposition.

Résultat escompté : vous êtes en mesure de vérifier si les contrôles appropriés sont en place en fonction de votre politique de classification et de manutention. Les outils et services automatisés vous aident à identifier et à classer le niveau de sensibilité de vos données. L'automatisation vous aide également à surveiller en permanence vos environnements afin de détecter et d'alerter si des données sont stockées ou traitées de manière non autorisée, pour que des mesures correctives puissent être prises rapidement.

Anti-modèles courants :

- S'appuyer uniquement sur des processus manuels pour l'identification et la classification des données, ce qui peut être source d'erreur et prendre beaucoup de temps. Cela peut entraîner une

classification des données inefficace et incohérente, en particulier lorsque les volumes de données augmentent.

- Ne pas disposer de mécanismes pour suivre et gérer les ressources de données dans l'ensemble de l'organisation.
- Perdre de vue la nécessité d'une surveillance et d'une classification continues des données au fur et à mesure de leur évolution au sein de l'organisation.

Avantages liés au respect de cette bonne pratique : l'automatisation de l'identification et de la classification des données peut permettre une application plus cohérente et plus précise des contrôles de protection des données, réduisant ainsi le risque d'erreur humaine. L'automatisation peut également fournir une visibilité sur l'accès et le mouvement des données sensibles, ce qui vous permet de détecter les manipulations non autorisées et de prendre des mesures correctives.

Niveau de risque encouru si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Bien que le discernement humain soit souvent utilisé pour classer les données pendant les phases initiales de conception d'une charge de travail, envisagez de mettre en place des systèmes qui automatisent l'identification et la classification des données de test à titre de contrôle préventif. Par exemple, les développeurs peuvent disposer d'un outil ou d'un service leur permettant d'analyser des données représentatives afin de déterminer leur sensibilité. Au sein d'AWS, vous pouvez télécharger des ensembles de données dans Amazon S3 et les analyser à l'aide d'Amazon Macie, Amazon Comprehend ou Amazon Comprehend Medical. De même, envisagez d'analyser les données dans le cadre de tests unitaires et d'intégration afin de détecter les endroits où des données sensibles ne sont pas attendues. Les alertes sur les données sensibles à ce stade peuvent mettre en évidence les lacunes en matière de protection avant le déploiement en production. D'autres fonctionnalités, telles que la détection des données sensibles dans AWS Glue, Amazon SNS et Amazon CloudWatch, peuvent également être utilisées pour détecter les informations personnelles et prendre des mesures d'atténuation. Pour tout outil ou service automatisé, comprenez comment il définit les données sensibles et enrichissez-le avec d'autres solutions humaines ou automatisées pour combler les lacunes si nécessaire.

À des fins de détection, utilisez une surveillance continue de vos environnements pour identifier si des données sensibles sont stockées de manière non conforme. Cela peut permettre de détecter des situations telles que l'émission de données sensibles dans des fichiers journaux ou leur copie dans un environnement d'analytique des données sans anonymisation ou suppression appropriée.

Les données stockées dans Amazon S3 peuvent être surveillées en permanence afin de détecter les données sensibles à l'aide d'Amazon Macie.

Étapes d'implémentation

1. Passez en revue le schéma de classification des données au sein de votre organisation, décrit dans le document SEC07-BP01.
   a. En comprenant le schéma de classification des données de votre organisation, vous pouvez établir des processus précis d'identification et de classification automatisées conformes aux politiques de votre entreprise.
2. Effectuez une analyse initiale de vos environnements pour une identification et une classification automatisées.
   a. Une analyse initiale complète de vos données peut vous aider à comprendre de manière exhaustive où se trouvent les données sensibles dans vos environnements. Lorsqu'une analyse complète n'est pas requise au départ ou ne peut pas être réalisée en amont pour des raisons de coût, évaluez si les techniques d'échantillonnage des données sont appropriées pour obtenir vos résultats. Par exemple, Amazon Macie peut être configuré de façon à effectuer une vaste opération automatisée de découverte des données sensibles dans vos compartiments S3. Cette capacité utilise des techniques d'échantillonnage pour effectuer de manière rentable une analyse préliminaire de l'emplacement des données sensibles. Une analyse plus approfondie des compartiments S3 peut ensuite être réalisée à l'aide d'une tâche de découverte des données sensibles. D'autres magasins de données peuvent également être exportés vers S3 en vue de leur analyse par Macie.
   b. Établissez le contrôle d'accès défini dans le document SEC07-BP02 pour vos ressources de stockage de données identifiées lors de votre analyse.
3. Configurez des analyses continues de vos environnements.
   a. La capacité de découverte automatique des données sensibles de Macie peut être utilisée afin d'effectuer des analyses continues de vos environnements. Les compartiments S3 connus qui sont autorisés à stocker des données sensibles peuvent être exclus à l'aide d'une liste d'autorisation dans Macie.
4. Intégrez l'identification et la classification à vos processus de construction et de test.
   a. Identifiez les outils que les développeurs peuvent utiliser pour analyser la sensibilité des données pendant le développement des charges de travail. Utilisez ces outils dans le cadre des tests d'intégration pour vous avertir lorsque des données sensibles sont inattendues et empêcher tout déploiement ultérieur.

5. Mettez en œuvre un système ou un runbook pour agir lorsque des données sensibles sont détectées dans des emplacements non autorisés.
   a. Limitez l'accès aux données utilisant la correction automatique. Par exemple, vous pouvez déplacer ces données vers un compartiment S3 à accès restreint ou baliser l'objet si vous utilisez le contrôle d'accès par attributs (ABAC). Envisagez également de masquer les données lorsqu'elles sont détectées.
   b. Alertez vos équipes de protection des données et de réponse aux incidents pour qu'elles étudient la cause racine de l'incident. Tous les enseignements qu'elles identifient peuvent aider à prévenir de futurs incidents.

Ressources

Documents connexes :

- AWS Glue : Détecter et traiter les données sensibles
- Utilisation des identifiants de données gérés dans Amazon SNS
- Amazon CloudWatch Logs : Aider à protéger les données sensibles des journaux grâce au masquage

Exemples connexes :

- Activation de la classification des données pour la base de données Amazon RDS avec Macie
- Détection de données sensibles dans DynamoDB avec Macie

Outils associés :

- Amazon Macie
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Glue

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

Comprenez vos exigences relatives au cycle de vie des données en fonction de vos différents niveaux de classification et de traitement des données. Cela peut inclure la manière dont les

données sont traitées lorsqu'elles entrent pour la première fois dans votre environnement, la manière dont les données sont transformées, ainsi que les règles relatives à leur destruction. Tenez compte de facteurs tels que les périodes de conservation, l'accès, l'audit et le suivi de la provenance.

Résultat escompté : vous classez les données le plus près possible du point et de l'heure d'ingestion. Lorsque la classification des données requiert un masquage, une création de jeton ou d'autres processus réduisant le niveau de sensibilité, vous effectuez ces actions le plus près possible du point et de l'heure de l'ingestion.

Vous supprimez les données conformément à votre politique lorsqu'il n'est plus approprié de les conserver, en fonction de leur classification.

Anti-modèles courants :

- Mettre en œuvre une approche universelle de la gestion du cycle de vie des données, sans tenir compte des différents niveaux de sensibilité et des exigences d'accès.
- Envisager la gestion du cycle de vie uniquement du point de vue des données utilisables ou des données sauvegardées, mais pas des deux.
- Supposer que les données entrées dans votre charge de travail sont valides, sans établir leur valeur ni leur provenance.
- S'appuyer sur la durabilité des données pour remplacer la sauvegarde et la protection des données.
- Conserver les données au-delà de leur utilité et de la période de conservation requise.

Avantages du respect de cette bonne pratique : une stratégie de gestion du cycle de vie des données bien définie et évolutive permet de maintenir la conformité réglementaire, d'améliorer la sécurité des données, d'optimiser les coûts de stockage et de permettre un accès et un partage efficaces des données tout en maintenant les contrôles appropriés.

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

Directives d'implémentation

Les données d'une charge de travail sont souvent dynamiques. La forme qu'elles prennent lors de leur entrée dans votre environnement de charge de travail peut être différente de celle prise pour le stockage ou l'utilisation dans la logique métier, les rapports, l'analytique ou le machine learning. De plus, la valeur des données peut évoluer au fil du temps. Certaines données sont de nature

temporelle et perdent de la valeur à mesure qu'elles vieillissent. Réfléchissez à l'impact de ces modifications sur l'évaluation de vos données dans le cadre de votre système de classification des données et des contrôles associés. Dans la mesure du possible, utilisez un mécanisme de cycle de vie automatisé, tel que les stratégies de cycle de vie d'Amazon S3 et le gestionnaire de cycle de vie Amazon Data, pour configurer vos processus de conservation, d'archivage et d'expiration des données. Pour les données stockées dans DynamoDB, vous pouvez utiliser la fonctionnalité Time To Live (TTL) pour définir un horodatage d'expiration par élément.

Faites la distinction entre les données qui peuvent être utilisées et celles qui sont stockées en tant que sauvegarde. Envisagez d'utiliser AWS Backup pour automatiser la sauvegarde des données entre les services AWS. Les instantanés Amazon EBS permettent de copier un volume EBS et de le stocker à l'aide des fonctionnalités S3, notamment le cycle de vie, la protection des données et l'accès aux mécanismes de protection. Deux de ces mécanismes sont le verrouillage d'objet S3 et AWS Backup Vault Lock, qui peuvent vous apporter une sécurité et un contrôle supplémentaires sur vos sauvegardes. Gérez une séparation claire des tâches et des accès pour les sauvegardes. Isolez les sauvegardes au niveau du compte afin de préserver la séparation avec l'environnement affecté lors d'un événement.

Un autre aspect de la gestion du cycle de vie consiste à enregistrer l'historique des données au fur et à mesure de leur progression dans votre charge de travail, ce que l'on appelle le suivi de la provenance des données. Vous avez ainsi l'assurance de savoir d'où viennent les données, si des transformations ont été effectuées, quel propriétaire ou processus a appliqué ces modifications et quand. Le fait de disposer de cet historique contribue à résoudre les problèmes et à réaliser des enquêtes lors d'événements de sécurité potentiels. Par exemple, vous pouvez journaliser les métadonnées relatives aux transformations dans une table Amazon DynamoDB. Au sein d'un lac de données, vous pouvez conserver des copies des données transformées dans différents compartiments S3 pour chaque étape du pipeline de données. Stockez les informations relatives au schéma et à l'horodatage dans un AWS Glue Data Catalog. Quelle que soit la solution adoptée, tenez compte des exigences de vos utilisateurs finaux afin de déterminer l'outillage approprié dont vous avez besoin pour établir des rapports sur la provenance de vos données. Cela vous aidera à déterminer la meilleure façon de suivre la provenance des données.

Étapes d'implémentation

1. Analysez les types de données, les niveaux de sensibilité et les exigences d'accès de la charge de travail pour classer les données et définir des stratégies de gestion du cycle de vie appropriées.
2. Concevez et mettez en œuvre des politiques de conservation des données et des processus de destruction automatisés conformes aux exigences légales, réglementaires et organisationnelles.

3. Établissez des processus et une automatisation pour une surveillance, un audit et un ajustement continus des stratégies, contrôles et politiques de gestion du cycle de vie des données en fonction de l'évolution des exigences et des réglementations en matière de charge de travail.
   a. Détectez les ressources pour lesquelles la gestion automatique du cycle de vie n'est pas activée avec AWS Config.

Ressources

Bonnes pratiques associées :

- COST04-BP05 Appliquer les politiques de conservation des données
- SUS04-BP03 Utiliser des politiques pour gérer le cycle de vie de vos jeux de données

Documents connexes :

- Livre blanc sur la classification des données
- AWS Blueprint for Ransomware Defense
- Guide DevOps : Améliorer la traçabilité grâce au suivi de la provenance des données

Exemples connexes :

- Comment protéger les données sensibles pendant tout leur cycle de vie dans AWS
- Créer un lignage de données pour les lacs de données à l'aide de AWS Glue, d'Amazon Neptune et de Spline

Outils associés :

- AWS Backup
- Amazon Data Lifecycle Manager
- AWS Identity and Access Management Access Analyzer

Protection des données au repos

Les 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.

Le 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, en utilisant un outil tel qu'Amazon CloudWatch Logs 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-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 au repos adaptées à votre charge de travail.

Résultat escompté : vous disposez d'un mécanisme de gestion de clés évolutif, reproductible et automatisé. Ce mécanisme applique un accès sur la base du moindre privilège aux éléments de clé et fournit le juste équilibre entre la disponibilité, la confidentialité et l'intégrité des clés. Vous surveillez l'accès aux clés et, si une rotation des éléments de clé est requise, vous effectuez leur rotation à l'aide d'un processus automatisé. Vous ne permettez pas à des opérateurs humains d'accéder aux éléments de clé.

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 du 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

Le chiffrement des données au repos est un contrôle de sécurité fondamental. Pour mettre en œuvre ce contrôle, votre charge de travail a besoin d'un mécanisme permettant de stocker et de gérer en toute sécurité les éléments de clé utilisés 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 140-3 niveau 3 pour protéger vos clés. Il n'existe aucun mécanisme permettant d'exporter les clés AWS KMS en texte brut.

Lorsque vous déployez des charges de travail à l'aide d'une stratégie multi-compte, vous devez conserver les clés AWS KMS dans le même compte que la charge de travail qui les utilise. Ce modèle distribué délègue la responsabilité de la gestion des clés AWS KMS à votre équipe. Dans d'autres cas d'utilisation, votre organisation peut 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 éléments de clé sont stockés, vous devez contrôler étroitement l'accès aux clés en utilisant des stratégies de clé et des politiques IAM. Les stratégies de clé constituent le principal moyen de contrôler l'accès à une clé AWS KMS. En outre, les octrois de clés AWS KMS peuvent fournir un accès aux services AWS pour chiffrer et déchiffrer les données en votre nom. Passez en revue les recommandations en matière de contrôle d'accès à vos clés AWS KMS.

Vous devez 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. Portez une attention particulière 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 dans AWS KMS sont soumises à un délai d'attente, qui est de 30 jours par défaut et de 7 jours au minimum, ce qui donne aux administrateurs le temps d'examiner ces actions et d'annuler la demande 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, vous devez utiliser le chiffrement d'enveloppe pour protéger vos données. AWS Encryption SDK 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 de gestion des clés appropriées (gérées par AWS ou gérées par le client) pour la clé.
   a. 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 stratégies les concernant.

   b. Lorsque vous utilisez des clés gérées par le client, pensez au magasin de clé 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 magasins de clés personnalisés avec AWS CloudHSM ou le magasin de clés 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.
   a. Comment les services AWS utilisent AWS KMS
   b. Pour plus d'informations sur les options de chiffrement proposées par un service AWS, consultez la rubrique Chiffrement au repos dans le guide de l'utilisateur ou le 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.
   a. Premiers pas : AWS Key Management Service (AWS KMS)
   b. Passez en revue les bonnes pratiques en matière de contrôle d'accès à vos clés AWS KMS.
4. Envisagez d'utiliser AWS Encryption SDK : utilisez AWS Encryption SDK avec l'intégration de AWS KMS lorsque votre application doit chiffrer des données côté client.
   a. AWS Encryption SDK
5. Activez l'Analyseur d'accès IAM pour examiner et envoyer automatiquement des notifications si les stratégies de clés AWS KMS sont trop génériques.
   a. Envisagez d'utiliser des contrôles de politique personnalisés pour vérifier qu'une mise à jour de la politique de ressources n'accorde pas un accès public aux clés KMS.
6. Activez Security Hub CSPM pour recevoir des notifications en cas de mauvaise configuration de stratégies de 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.

a. Certaines organisations préfèrent séparer les activités de journalisation AWS KMS à un emplacement distinct. Pour plus de détails, consultez la section Journalisation des appels d'API AWS KMS avec CloudTrail du guide du développeur AWS KMS.

Ressources

Documents connexes:

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

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

Chiffrez les données privées au repos pour préserver leur confidentialité et offrir une couche de protection supplémentaire contre la divulgation ou l'exfiltration involontaire des données. Le chiffrement protège les données de manière à ce qu'elles ne puissent pas être lues ou consultées sans être préalablement déchiffrées. Inventoriez et contrôlez les données non chiffrées afin d'atténuer les risques associés à l'exposition des données.

Résultat escompté : vous disposez de mécanismes qui chiffrent les données privées par défaut lorsqu'elles sont au repos. Ces mécanismes contribuent à préserver la confidentialité des données et offre une couche de protection supplémentaire contre la divulgation ou l'exfiltration involontaires des données. Vous maintenez un inventaire des données non chiffrées et vous comprenez les contrôles mis en place pour les protéger.

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

Directives d'implémentation

Mappez les clés de chiffrement aux classifications de données dans vos charges de travail. Cette approche permet de se protéger contre un accès trop permissif lorsque vous utilisez une seule clé de chiffrement ou un très petit nombre de clés de chiffrement pour vos données (voir SEC07-BP01 Comprendre votre schéma de classification des données).

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 Elastic Compute Cloud (Amazon EC2), vous pouvez définir un chiffrement par défaut sur les comptes pour que les nouveaux volumes EBS 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 stratégies de clés.

En outre, des services tels qu'Amazon Simple Storage Service (Amazon S3) chiffrent désormais tous les nouveaux objets par défaut. Cette implémentation offre une sécurité renforcée sans aucun impact sur les performances.

D'autres services, comme Amazon Elastic Compute Cloud (Amazon EC2) ou Amazon Elastic File System (Amazon EFS), prennent en charge les paramètres de chiffrement par défaut. Vous pouvez également utiliser AWS Config Rules pour vérifier automatiquement que vous utilisez le chiffrement pour les volumes Amazon Elastic Block Store (Amazon EBS), les instances Amazon Relational Database Service (Amazon RDS), les compartiments Amazon S3 et d'autres services au sein de votre organisation.

AWS fournit également des options de chiffrement côté client, ce qui vous permet de chiffrer les données avant de les télécharger dans le cloud. AWS Encryption SDK fournit un moyen de chiffrer vos données à l'aide du chiffrement d'enveloppe. Vous fournissez la clé de wrapping et 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. Le client de chiffrement Amazon DynamoDB vous permet également de chiffrer et de signer les éléments avant de les télécharger dans une table DynamoDB.

Étapes d'implémentation

- Configurer le chiffrement par défaut pour les nouveaux volumes Amazon EBS : indiquez que vous souhaitez que tous les nouveaux volumes Amazon EBS soient créés sous forme chiffrée, avec la possibilité d'utiliser la clé par défaut fournie par AWS ou une clé que vous créez.
- Configurer des Amazon Machine Images (AMI) chiffrées : la copie d'une AMI existante avec le chiffrement configuré chiffrera automatiquement les volumes racine et les instantanés.
- Configurer le chiffrement Amazon RDS : configurez le chiffrement pour vos clusters de base de données Amazon RDS et vos instantanés au repos en activant l'option de chiffrement.
- Créer et configurer des clés AWS KMS avec des stratégies qui limitent l'accès aux principaux appropriés pour chaque classification de 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.

- Configurer le chiffrement dans des services AWS supplémentaires : pour les autres services AWS que vous utilisez, passez en revue la documentation de sécurité de ce service afin d'en déterminer les options de chiffrement.

Ressources

Documents connexes :

- Outils de chiffrement AWS
- AWS Encryption SDK
- Livre blanc sur les informations cryptographiques AWS KMS
- AWS Key Management Service
- Services et outils cryptographiques AWS
- Chiffrement Amazon EBS
- Chiffrement par défaut pour les volumes Amazon EBS
- Chiffrement des ressources Amazon RDS
- Comment activer le chiffrement par défaut pour un compartiment Amazon S3 ?
- 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 l'automatisation pour valider et appliquer les contrôles des données au repos. Utilisez l'analyse automatique pour détecter les erreurs de configuration de vos solutions de stockage de données et effectuez des corrections par le biais d'une réponse programmatique automatisée dans la mesure du possible. Intégrez l'automatisation à vos processus de CI/CD afin de détecter les erreurs de configuration du stockage de données avant leur déploiement en production.

Résultat escompté : les systèmes automatisés analysent et surveillent les emplacements de stockage de données pour détecter les erreurs de configuration des commandes, les accès non autorisés et les utilisations inattendues. La détection d'emplacements de stockage mal configurés déclenche des mesures correctives automatisées. Les processus automatisés créent des sauvegardes de données et stockent des copies immuables en dehors de l'environnement d'origine.

Anti-modèles courants :

- Ne pas prendre en compte les options permettant d'activer des paramètres de chiffrement par défaut, lorsque le chiffrement est pris en charge.
- Ne pas prendre en compte les événements de sécurité, en plus des événements opérationnels, lors de la formulation d'une stratégie de sauvegarde et de restauration automatisée.
- Ne pas appliquer les paramètres d'accès public pour les services de stockage.
- Ne pas surveiller ni auditer vos contrôles pour protéger les données au repos.

Avantages du respect de cette bonne pratique : l'automatisation permet de prévenir le risque de mauvaise configuration de vos emplacements de stockage de données. Cela permet d'éviter que des erreurs de configuration ne pénètrent dans vos environnements de production. Grâce à cette bonne pratique, vous pouvez également détecter et corriger les erreurs de configuration, le cas échéant.

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

Directives d'implémentation

L'automatisation est un thème récurrent dans les pratiques de protection de vos données au repos. SEC01-BP06 Automatiser le déploiement de contrôles de sécurité standard décrit comment vous pouvez capturer la configuration de vos ressources à l'aide de modèles d'infrastructure en tant que code (IaC), tels que AWS CloudFormation. Ces modèles sont validés dans un système de contrôle de version et sont utilisés pour déployer des ressources sur AWS via un pipeline CI/CD. Ces techniques s'appliquent également à l'automatisation de la configuration de vos solutions de stockage de données, telles que les paramètres de chiffrement des compartiments Amazon S3.

Vous pouvez vérifier si les paramètres que vous définissez dans les modèles IaC ont été configurés correctement dans vos pipelines CI/CD à l'aide de règles dans AWS CloudFormation Guard. Vous pouvez surveiller les paramètres qui ne sont pas encore disponibles dans CloudFormation ou dans d'autres outils IaC pour détecter toute mauvaise configuration avec AWS Config. Les alertes générées par Config en cas d'erreur de configuration peuvent être corrigées automatiquement,

comme décrit dans SEC04-BP04 Initier les mesures de correction pour les ressources non conformes.

L'utilisation de l'automatisation dans le cadre de votre stratégie de gestion des autorisations fait également partie intégrante des protections automatisées des données. SEC03-BP02 Accorder l'accès au moindre privilège et SEC03-BP04 Réduire les autorisations en continu décrivent la configuration de stratégies d'accès au moindre privilège qui sont surveillées en permanence par AWS Identity and Access Management Access Analyzer pour générer des résultats lorsque les autorisations peuvent être réduites. Au-delà de l'automatisation des autorisations de surveillance, vous pouvez configurer Amazon GuardDuty pour détecter tout comportement anormal d'accès aux données pour vos volumes EBS (via une instance EC2), vos compartiments S3 et les bases de données Amazon Relational Database Service prises en charge.

L'automatisation joue également un rôle dans la détection des données sensibles stockées dans des emplacements non autorisés. SEC07-BP03 Automatiser l'identification et la classification décrit comment Amazon Macie peut surveiller vos compartiments S3 pour détecter les données sensibles inattendues et générer des alertes susceptibles de déclencher une réponse automatique.

Suivez les pratiques décrites dans REL09 Données de sauvegarde pour développer une stratégie automatisée de sauvegarde et de restauration des données. La sauvegarde et la restauration des données sont aussi importantes pour la restauration après des événements de sécurité que pour des événements opérationnels.

Étapes d'implémentation

1. Capturez la configuration du stockage de données dans des modèles IaC. Utilisez des contrôles automatisés dans vos pipelines CI/CD pour détecter les erreurs de configuration.
   a. Vous pouvez utiliser vos modèles d'infrastructure en tant que code pour CloudFormation et utiliser CloudFormation Guard pour vérifier que les modèles sont bien configurés.
   b. Utilisez AWS Config pour exécuter des règles dans un mode d'évaluation proactif. Utilisez ce paramètre pour vérifier la conformité d'une ressource en tant qu'étape de votre pipeline CI/CD avant de la créer.
2. Surveillez les ressources pour détecter les erreurs de configuration du stockage de données.
   a. Paramétrez AWS Config pour qu'il surveille les ressources de stockage de données afin de détecter les modifications apportées aux configurations de contrôle et pour générer des alertes afin d'invoquer des mesures correctives lorsqu'il détecte une mauvaise configuration.
   b. Consultez SEC04-BP04 Lancer la correction des ressources non conformes pour plus de conseils sur les corrections automatisées.

3. Surveillez et réduisez continuellement les autorisations d'accès aux données grâce à l'automatisation.
    a. IAM Access Analyzer peut fonctionner en continu pour générer des alertes lorsque les autorisations sont susceptibles d'être réduites.
4. Surveillez et signalez les comportements anormaux en matière d'accès aux données.
    a. GuardDuty surveille à la fois les signatures de menaces connues et les écarts par rapport aux comportements d'accès de base pour les ressources de stockage de données telles que les volumes EBS, les compartiments S3 et les bases de données RDS.
5. Surveillez les données sensibles et donnez l'alerte si certaines d'entre elles sont stockées dans des endroits inattendus.
    a. Utilisez Amazon Macie pour analyser en permanence vos compartiments S3 à la recherche de données sensibles.
6. Automatisez les sauvegardes sécurisées et chiffrées de vos données.
    a. AWS Backup est un service géré qui crée des sauvegardes chiffrées et sécurisées de diverses sources de données sur AWS. Elastic Disaster Recovery vous permet de copier les charges de travail complètes du serveur et de maintenir une protection continue des données avec un objectif de point de reprise (RPO) mesuré en secondes. Vous pouvez configurer les deux services de façon à ce qu'ils fonctionnent ensemble pour automatiser la création de sauvegardes de données et leur copie vers des emplacements de basculement. Vous pouvez ainsi garantir la disponibilité de vos données lorsqu'elles sont touchées par des événements opérationnels ou de sécurité.

Ressources

Bonnes pratiques associées :

- SEC01-BP06 Automatiser le déploiement des contrôles de sécurité standard
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège
- SEC03-BP04 Limiter les autorisations au minimum requis en permanence
- SEC04-BP04 Lancer la correction pour les ressources non conformes
- SEC07-BP03 Automatiser l'identification et la classification
- REL09-BP02 Sécuriser et chiffrer les sauvegardes
- REL09-BP03 Effectuer automatiquement la sauvegarde des données

Documents connexes :

- Conseils prescriptifs AWS : chiffrer automatiquement les volumes Amazon EBS existants et nouveaux
- Gestion des risques liés aux rançongiciels sur AWS à l'aide du NIST Cybersecurity Framework (CSF)

Exemples connexes :

- Comment utiliser des règles proactives AWS Config et des hooks AWS CloudFormation pour empêcher la création de ressources cloud non conformes
- Automatiser et gérer de manière centralisée la protection des données pour Amazon S3 avec AWS Backup
- AWS re:Invent 2023 - Implement proactive data protection using Amazon EBS snapshots
- AWS re:Invent 2022 - Build and automate for resilience with modern data protection

Outils associés :

- AWS CloudFormation Guard
- Registre des règles AWS CloudFormation Guard
- IAM Access Analyzer
- Amazon Macie
- AWS Backup
- Reprise après sinistre Elastic

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. Appliquez les contrôles d'accès conditionnel et de moindre privilège. Empêchez l'octroi d'un accès public à vos données.

Résultat escompté : vous vérifiez que seuls les utilisateurs autorisés peuvent accéder aux données lorsqu'ils en ont besoin. Vous protégez vos données avec des sauvegardes régulières et la gestion des versions pour éviter toute modification ou suppression intentionnelle ou involontaire des

données. Vous 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 d'exposition au risque si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Il est important de protéger les données au repos pour préserver leur intégrité, leur confidentialité et leur conformité aux exigences réglementaires. Vous pouvez mettre en œuvre plusieurs contrôles pour y parvenir, notamment le contrôle d'accès, l'isolation, l'accès conditionnel et la gestion des versions.

Vous pouvez appliquer le contrôle d'accès selon le principe du moindre privilège, qui fournit uniquement les autorisations nécessaires aux utilisateurs et aux services pour qu'ils effectuent leurs tâches. Cela inclut l'accès aux clés de chiffrement. Passez en revue vos politiques AWS Key Management Service (AWS KMS) pour vous assurer que le niveau d'accès que vous accordez est approprié et que les conditions appropriées s'appliquent.

Vous pouvez séparer les données en fonction de différents niveaux de classification en utilisant des Comptes AWS distincts pour chaque niveau, et gérer ces comptes à l'aide d'AWS Organizations. Cette isolation contribue à empêcher tout accès non autorisé et minimise le risque d'exposition des données.

Examinez régulièrement le niveau d'accès accordé dans les politiques de compartiment Amazon S3. Évitez d'utiliser des compartiments publiquement accessibles en lecture ou en écriture à moins que cela ne soit absolument nécessaire. Envisagez d'utiliser AWS Config pour détecter les compartiments publiquement disponibles et Amazon CloudFront pour diffuser du contenu à partir

d'Amazon S3. Vérifiez que les compartiments qui ne doivent pas autoriser l'accès public sont configurés correctement pour l'empêcher.

Mettez en œuvre des mécanismes de gestion des versions et de verrouillage d'objets pour les données critiques stockées dans Amazon S3. La gestion des versions d'Amazon S3 préserve les versions précédentes des objets pour permettre de récupérer les données en cas de suppression ou de remplacement accidentels. Le verrouillage d'objet Amazon S3 fournit un contrôle d'accès obligatoire pour les objets, ce qui empêche leur suppression ou leur remplacement, même par l'utilisateur racine, jusqu'à l'expiration du verrou. En outre, le verrouillage du coffre-fort Amazon Glacier propose une fonctionnalité similaire pour les archives stockées dans Amazon Glacier.

Étapes d'implémentation

1. Appliquez un contrôle d'accès selon le principe du moindre privilège :
    - Passez en revue les autorisations d'accès accordées aux utilisateurs et aux services, et vérifiez que ces derniers ne disposent que des autorisations nécessaires à l'exécution de leurs tâches.
    - Passez en revue l'accès aux clés de chiffrement en vérifiant les politiques AWS Key Management Service (AWS KMS).
2. Séparez les données en fonction des différents niveaux de classification :
    - Utilisez des Comptes AWS distincts pour chaque niveau de classification des données.
    - Gérez ces comptes avec AWS Organizations.
3. Passez en revue les autorisations relatives aux objets et aux compartiments Amazon S3 :
    - Examinez régulièrement le niveau d'accès accordé dans les politiques de compartiment Amazon S3.
    - Évitez d'utiliser des compartiments publiquement accessibles en lecture ou en écriture à moins que cela ne soit absolument nécessaire.
    - Envisagez d'utiliser AWS Config pour détecter les compartiments disponibles publiquement.
    - Utilisez Amazon CloudFront pour diffuser du contenu à partir d'Amazon S3.
    - Vérifiez que les compartiments qui ne doivent pas autoriser l'accès public sont configurés correctement pour l'empêcher.
    - Vous pouvez appliquer le même processus de révision aux bases de données et à toutes les autres sources de données qui utilisent l'authentification IAM, telles que SQS ou les entrepôts de données tiers.
4. Utilisez l'Analyseur d'accès AWS IAM :

- Vous pouvez configurer l'Analyseur d'accès AWS IAM pour analyser des compartiments Amazon S3 et générer des résultats lorsqu'une politique S3 accorde l'accès à une entité externe.

5. Implémentez des mécanismes de gestion des versions et de verrouillage d'objet:
   - Utilisez la gestion des versions d'Amazon S3 pour préserver les versions précédentes des objets et permettre de récupérer les données en cas de suppression ou de remplacement accidentels.
   - Utilisez le verrouillage d'objet Amazon S3 pour fournir un contrôle d'accès obligatoire pour les objets, ce qui empêche leur suppression ou leur remplacement, même par l'utilisateur racine, jusqu'à l'expiration du verrou.
   - Utilisez le verrouillage du coffre-fort Amazon Glacier pour les archives stockées dans Amazon Glacier.
6. Utilisez l'inventaire Amazon S:
   - Vous pouvez utiliser l'inventaire Amazon S3 pour auditer et signaler le statut de réplication et de chiffrement de vos objets S3.
7. Vérifiez les autorisations de partage Amazon EBS et d'AMI:
   - Passez en revue vos autorisations de partage pour Amazon EBS et le partage d'AMI afin de vous assurer que vos images et volumes ne sont pas partagés avec des Comptes AWS en dehors de votre charge de travail.
8. Passez régulièrement en revue les partages d'AWS Resource Access Manager :
   - Vous pouvez utiliser AWS Resource Access Manager pour partager des ressources, telles que des politiques AWS Network Firewall, des règles d'Amazon Route 53 Resolver et des sous-réseaux, au sein de vos VPC Amazon.
   - 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:

- AWS KMS Livre blanc sur les informations cryptographiques
- Introduction à la gestion des autorisations d'accès à vos ressources Amazon S
- Présentation de la gestion de l'accès à vos ressources AWS KMS
- AWS Config Rules
- Amazon S3 + Amazon CloudFront : une combinaison parfaite dans le cloud
- Utilisation de la gestion des versions
- Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet Amazon S
- Partager un instantané Amazon EBS
- AMI partagées
- Hébergement d'une application d'une seule page sur Amazon S3
- AWS Clés de condition globale
- Crééation d'un périmètre des données sur AWS

Vidéos connexes :

- Securing Your Block Storage on AWS

Protection des données en transit

Les 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.

Données sécurisées entre des sites VPC ou sur site : vous pouvez les utiliser AWS PrivateLink pour créer une connexion réseau sécurisée et privée entre Amazon Virtual Private Cloud (Amazon VPC) ou une connectivité sur site avec des 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 Application du chiffrement en transit
- SEC09-BP03 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 escompté : 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 d'exposition au risque 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 Autorité de certification privée AWS (CA privée AWS). 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 privés en utilisant CA privée AWS et s'intègre à de nombreux autres services gérés par AWS pour fournir des certificats TLS sécurisés pour les charges de travail. ACM peut également délivrer des certificats reconnus publiquement à partir d'Amazon Trust Services. Les certificats publics d'ACM peuvent être utilisés sur des charges de travail destinées au public, car les navigateurs et les systèmes d'exploitation modernes approuvent par défaut ces certificats.

CA privée AWS 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, CA privée AWS 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 Rôles Anywhere IAM 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.

Outre ACM et CA privée AWS, AWS IoT Core fournit un support spécialisé pour le provisionnement, la gestion et le déploiement de certificats PKI sur les appareils IoT. AWS IoT Core fournit des mécanismes spécialisés pour intégrer des appareils IoT dans votre infrastructure à clé publique à grande échelle.

Certains services AWS, tels qu'Amazon API Gateway et Elastic Load Balancing, proposent leurs propres fonctionnalités d'utilisation de certificats pour sécuriser les connexions des applications.

Par exemple, API Gateway et Application Load Balancer (ALB) prennent en charge le protocole TLS mutuel (mTLS) à l'aide de certificats client que vous créez et exportez à l'aide de la Console de gestion AWS, de CLI ou des API.

Considérations relatives à l'établissement d'une hiérarchie d'autorité de certification privée

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 Planifier votre déploiement CA privée AWS.

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 d'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 CA privée AWS 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 être utilisé pour émettre de nombreux types de certificats d'entité finale à l'aide du CA privée AWS.
    - 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.

- Envisagez d'utiliser les fonctionnalités mTLS natives dans des services tels qu'Amazon API Gateway ou Application Load Balancer.

2. Mettez en œuvre le renouvellement automatisé des certificats dans la mesure du possible :
   - Utilisez le renouvellement géré par 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.
   - Vous pouvez générer des rapports d'audit qui répertorient les certificats émis et 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 certificats (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-BP03 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
- Bonnes pratiques en matière d'AC privée
- Comment utiliser AWS RAM pour partager votre compte croisé Private CA

Vidéos connexes:

- Activer Private CA AWS Certificate Manager (atelier)

Exemples connexes:

- Atelier sur les autorités de certification privées
- Atelier sur la gestion des appareils IoT (y compris le provisionnement des appareils)

Outils associés:

- Plugin pour Kubernetes cert-manager pour utiliser CA privée AWS

SEC09-BP02 Application du 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 escompté : vous chiffrez le trafic réseau entre vos ressources et Internet afin de limiter l'accès non autorisé aux données. Vous chiffrez le trafic réseau au sein de votre environnement AWS interne en fonction de vos exigences de sécurité. Vous chiffrez les données en transit à l'aide des protocoles TLS sécurisés et de suites de chiffrement.

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 d'exposition au risque si cette bonne pratique n'est pas respectée : 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 HTTP non sécurisés peuvent être audités et bloqués dans un cloud privé virtuel (VPC) dans le cadre de l'utilisation de groupes de sécurité. Les requêtes HTTP peuvent être également redirigées automatiquement vers HTTPS dans Amazon CloudFront ou sur un Application Load Balancer. Vous pouvez utiliser une politique de compartiment Amazon Simple Storage Service (Amazon S3) pour restreindre la possibilité de charger des objets via HTTP, en imposant l'utilisation du protocole HTTPS pour les chargements d'objets vers votre ou vos compartiments. 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 appellent les API AWS en utilisant au moins le protocole TLS 1.2, car AWS a rendu en février 2024 obsolète l'utilisation des versions de TLS antérieures. Nous vous recommandons d'utiliser TLS 1.3. Si vous avez des exigences particulières en matière de chiffrement en transit, vous pouvez trouver des solutions tierces dans AWS Marketplace.

Étapes d'implémentation

- Appliquer 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 de périphérie : configurez le protocole HTTPS avec Amazon CloudFront et utilisez un profil de sécurité adapté à votre posture de sécurité et à votre cas d'utilisation.
- Utiliser 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.
- Configurer des protocoles sécurisés dans les équilibreurs de charge : sélectionnez une politique de sécurité fournissant les suites de chiffrement les plus puissantes prises en charge par les clients qui se connecteront à l'écouteur. Créez un écouteur HTTPS pour votre Application Load Balancer.
- Configurer des protocoles sécurisés dans Amazon Redshift : configurez votre cluster pour exiger une connexion SSL (Secure Socket Layer) ou TLS (Transport Layer Security).

- Configurer des protocoles sécurisés : consultez la documentation de service AWS pour déterminer les capacités de chiffrement en transit.
- Configurez un accès sécurisé lors du téléchargement vers des compartiments Amazon S3 : utilisez les contrôles de stratégie de compartiment Amazon S3 pour garantir un accès sécurisé aux données.
- Envisagez d'utiliser AWS Certificate Manager : ACM vous permet de provisionner, de gérer et de déployer des certificats TLS publics à utiliser avec des services AWS.
- Envisagez d'utiliser Autorité de certification privée AWS pour les besoins du PKI privé : CA privée AWS vous permet de créer des hiérarchies d'autorités de certification (AC) privées pour délivrer des certificats X.509 d'entité finale qui peuvent être utilisés pour créer des canaux TLS cryptés.

Ressources

Documents connexes :

- Utilisation du protocole HTTPS avec CloudFront
- Connexion de votre VPC à des réseaux distants utilisant AWS Virtual Private Network
- Création d'un écouteur HTTPS pour votre Application Load Balancer
- Didacticiel : Configurer SSL/TLS sur Amazon Linux 2
- Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données
- Configuration des options de sécurité des connexions

SEC09-BP03 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 escompté : une charge de travail avec un plan de données et un plan de contrôle bien définis circulent entre les services. 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 au respect 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 d'exposition au risque 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 les flux de trafic entre les services qui constituent une charge de travail.
- Le trafic nord-sud représente les flux de 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 de service AWS utilisent le protocole de signature AWS Signature Version 4 (SigV4) pour authentifier l'appelant, quel que soit le réseau d'où provient 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 tels qu'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 le protocole SIGv4, vous pouvez utiliser Gestion des identités et des accès AWS Rôles Anywhere (IAM) sur la ressource hors 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 Autorité de certification privée AWS (CA privée AWS). Vous pouvez utiliser des services tels qu'Amazon API Gateway pour fournir une authentification mTLS pour les communications inter-charges de travail ou intra-charge de travail. Application Load Balancer prend également en charge mTLS pour les charges de travail orientées côté interne ou externe. 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 autorisateur JSON Web Token (JWT) permettant aux charges de travail de restreindre l'accès aux routes d'API à l'aide des JWT émis par des fournisseurs d'identité OIDC ou 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

- Définissez et documentez les flux de votre réseau de 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 de l'exécution d'un exercice de modélisation des menaces, comme décrit dans SEC01-BP07 Identifier les menaces et hiérarchiser les mesures d'atténuation à l'aide d'un modèle de menace.
- Établissez des contrôles réseau : tenez compte des capacités AWS permettant d'établir 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 limiter les flux de données entre les ressources.
  - Envisagez d'utiliser AWS PrivateLink pour communiquer à la fois avec AWS et les services 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.
- Mettez en œuvre l'authentification et l'autorisation pour tous les services de votre charge de travail : choisissez l'ensemble de services AWS le plus approprié pour fournir des flux de trafic authentifiés et cryptés dans votre charge de travail.
  - Pensez à Amazon VPC Lattice pour sécuriser les communications entre services. VPC Lattice peut utiliser l'authentification SigV4 combinée à des politiques d'authentification pour contrôler l'accès de service à service.
  - Pour la communication de service à service à l'aide de mTLS, envisagez d'utiliser API Gateway ou Application Load Balancer. CA privée AWS peut être utilisé pour établir une hiérarchie d'autorité de certification privée capable d'émettre des certificats à utiliser avec mTLS.
  - Lors de l'intégration à des services utilisant OAuth 2.0 ou OIDC, envisagez d'utiliser API Gateway avec l'autorisateur JWT.

    - Pour la communication entre votre charge de travail et les appareils IoT, envisagez AWS IoT Core, qui propose plusieurs options pour le chiffrement et l'authentification du trafic réseau.
- Surveillez les accès non autorisés : surveillez en permanence les canaux de communication imprévus, les principaux non autorisés qui tentent d'accéder à des ressources protégées et les autres modèles d'accès inappropriés.
    - Si vous utilisez VPC Lattice pour gérer l'accès à vos services, pensez à activer et à 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 réseau et vérifier régulièrement la présence d'anomalies.
    - Reportez-vous au Guide de réponse aux incidents de sécurité AWS et à la section Réponse aux incidents du pilier Sécurité AWS Well-Architected Framework pour plus de conseils sur la planification, la simulation et la réponse aux incidents de sécurité.

Ressources

Bonnes pratiques associées :

- SEC03-BP07 Analyser l'accès public et intercompte
- 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 :

- Évaluation des méthodes de contrôle d'accès pour sécuriser les API Amazon API Gateway
- Configuration de l'authentification TLS mutuelle pour une API REST
- Comment sécuriser les points de terminaison HTTP API Gateway avec l'autorisateur JWT
- Autoriser les appels directs vers les services AWS à l'aide du fournisseur d'informations d'identification AWS IoT Core
- Guide d'intervention en cas d'incident de sécurité AWS

Vidéos connexes :

- AWS re:invent 2022: Introducing VPC Lattice

- AWS re:invent 2020: Serverless API authentication for HTTP APIs on AWS

Exemples connexes :

- Atelier Amazon VPC Lattice
- Épisode 1 de Zero-Trust — L'atelier Phantom Service Perimeter

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
- Objectifs de conception de la réponse cloud
- Préparation
- Opérations
- Activité postérieure à l'incident

Aspects de la réponse aux incidents AWS

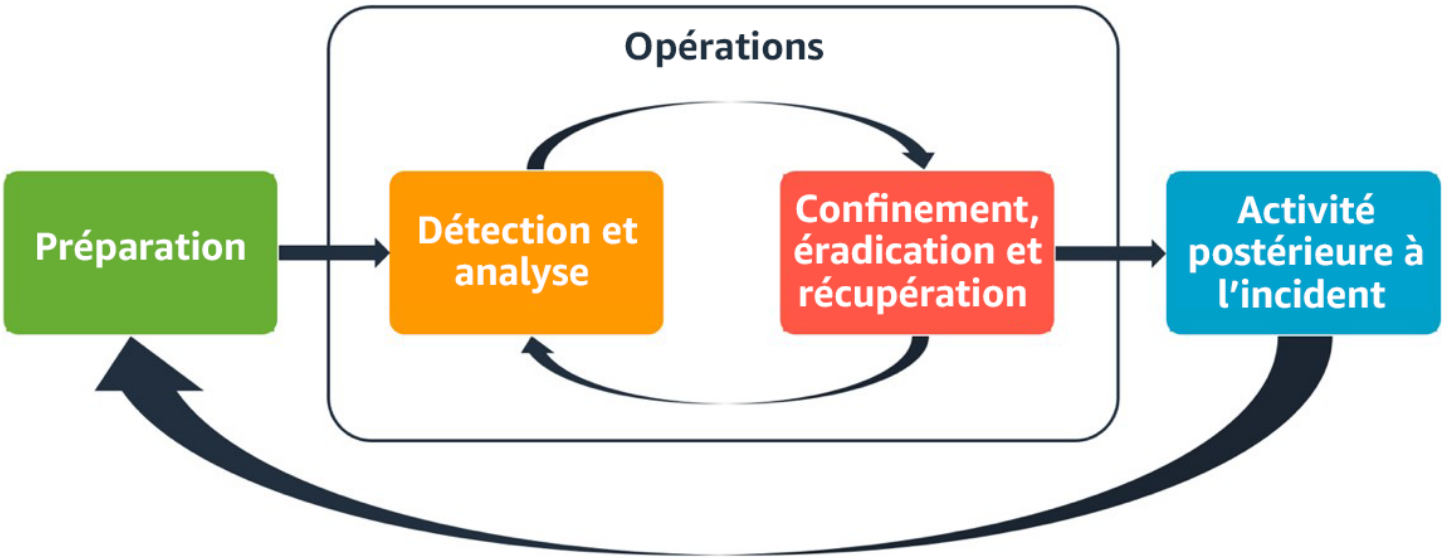
Tous les utilisateurs AWS d'une organisation doivent avoir une connaissance de base des processus de réponse aux incidents de sécurité. Le personnel de sécurité doit, quant à lui, savoir comment répondre aux problèmes de sécurité. L'éducation, la formation et l'expérience sont essentielles à la réussite 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 base d'un programme de réponse aux incidents réussi dans le cloud repose sur la préparation, les opérations et l'activité post-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.
- Opération : 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 post-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 Guide, restent 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, vos 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 vos modèles de réponse dans le cloud où se trouvent l'événement et les données.

- Connaître ses ressources et ses besoins : 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 des mécanismes de redéploiement : si une anomalie de sécurité peut être attribuée à une mauvaise configuration, la remédiation peut être aussi simple que de supprimer l'écart 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 dans la mesure du 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.
- Choisissez 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.
- Apprenez et améliorez 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 :

- Personnel : 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.
- 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.
- 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.

Résultat escompté : vous disposez d'une liste des principaux membres du personnel, de leurs coordonnées et des rôles qu'ils jouent lorsqu'ils répondent à un événement de sécurité. Vous consultez régulièrement ces informations et vous les mettez à jour de façon à refléter les changements de personnel du point de vue des outils internes et externes. Lorsque vous documentez ces informations, vous tenez compte de tous les fournisseurs de services et fournisseurs tiers, y compris les partenaires de sécurité, les fournisseurs de cloud et les applications de logiciel en tant que service (SaaS). Lors d'un événement de sécurité, le personnel est disponible avec le niveau de responsabilité, de contexte et d'accès approprié pour être en mesure de réagir et de récupérer.

Anti-modèles courants :

- Ne pas gérer une liste actualisée des principaux membres du personnel avec leurs coordonnées, leurs rôles et leurs responsabilités lorsqu'ils répondent à des événements de sécurité.
- Supposer que tout le monde comprend les personnes, les dépendances, l'infrastructure et les solutions lors de la réponse et de la reprise après un événement.
- Ne pas disposer d'un document ou d'un référentiel de connaissances représentant la conception d'une infrastructure ou d'une application clé.
- Ne pas disposer de processus d'intégration appropriés permettant aux nouveaux employés de contribuer efficacement à la réponse à un événement de sécurité, par exemple en effectuant des simulations d'événements.
- Aucune procédure de remontée n'est en place lorsque le personnel clé est temporairement indisponible ou s'il ne répond pas lors d'événements de sécurité.

Avantages liés au respect de cette bonne pratique : cette pratique réduit le temps de triage et de réponse consacré à l'identification du personnel approprié et de ses rôles lors d'un événement. Minimisez le temps perdu lors d'un événement en tenant à jour une liste des principaux membres du personnel et de leurs rôles afin de pouvoir faire le tri des personnes appropriées et de les aider à récupérer après un événement.

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

Directives d'implémentation

Identifier les postes clés au sein de votre organisation : tenez à jour une liste des employés au sein de votre organisation que vous devez impliquer. Passez régulièrement en revue et mettez à jour ces informations en cas de changements au sein du personnel, par exemple des changements organisationnels, des promotions et des changements d'équipe. Cette étape est particulièrement

importante pour les rôles clés tels que les gestionnaires d'incidents, les intervenants en cas d'incident et le responsable des communications.

- Gestionnaire d'incidents : les gestionnaires d'incidents ont une autorité globale lors de la réponse à l'événement.
- Intervenants en cas d'incidents : les intervenants en cas d'incidents sont responsables des activités d'enquête et de correction. Ces personnes peuvent varier en fonction du type d'événement, mais il s'agit généralement de développeurs et d'équipes opérationnelles responsables de l'application concernée.
- Responsable des communications : le responsable des communications est responsable des communications internes et externes, en particulier avec les agences publiques, les régulateurs et les clients.
- Processus d'intégration : formez et intégrez régulièrement les nouveaux employés afin de les doter des compétences et des connaissances nécessaires pour contribuer efficacement aux efforts de réponse aux incidents. Incorporez des simulations et des exercices pratiques dans le cadre du processus d'intégration afin de faciliter leur préparation.
- Experts en la matière (PME) : dans le cas d'équipes distribuées et autonomes, nous vous recommandons d'identifier une PME pour les charges de travail critiques. Ils fournissent des informations sur le fonctionnement et la classification des données des charges de travail critiques impliquées dans l'événement.

Exemple de format de table :

```
  | Role | Name | Contact Information | Responsibilities |
1 | ——- | ——- | ——- | ——- |
2 | Incident Manager | Jane Doe| jane.doe@example.com | Overall authority during
 response |
3 | Incident Responder | John Smith | john.smith@example.com | Investigation and
 remediation |
4 | Communications Lead | Emily Johnson | emily.johnson@example.com | Internal and
 external communications |
5 | Communications Lead | Michael Brown | michael.brown@example.com | Insights on
 critical workloads |
```

Envisagez d'utiliser la fonctionnalité AWSSystems Manager Incident Manager pour capturer les contacts clés, définir un plan d'intervention, automatiser les plannings d'astreinte et définir des plans d'escalade. Automatisez et alternez tout le personnel grâce à un calendrier d'astreinte, de sorte

que la responsabilité de la charge de travail soit partagée entre ses propriétaires. Cela favorise les bonnes pratiques, telles que l'émission de métriques et de journaux pertinents, ainsi que la définition de seuils d'alarme importants pour la charge de travail.

Identifier les partenaires externes : les entreprises utilisent des outils conçus par des fournisseurs indépendants de logiciels (ISV), des partenaires et des sous-traitants pour créer des solutions différenciantes pour leurs clients. Impliquez le personnel clé de ces parties qui peut vous aider à répondre à un incident et à récupérer après un incident. Nous vous recommandons de vous inscrire au niveau approprié d'Support afin d'accéder rapidement à des experts AWS en la matière par le biais d'une demande d'assistance. Envisagez des agencements similaires avec tous les fournisseurs de solutions critiques pour les charges de travail. Certains événements de sécurité obligent les entreprises cotées en bourse à informer les agences publiques et les régulateurs concernés de l'événement et de ses impacts. Dressez une liste avec les coordonnées des départements concernés et des personnes responsables, et veillez à ce qu'elle reste à jour.

Étapes d'implémentation

1. Mettez en place une solution de gestion des incidents.
   a. Envisagez de déployer Incident Manager dans votre compte d'outils de sécurité.
2. Définissez les contacts dans votre solution de gestion des incidents.
   a. Définissez au moins deux types de canaux de communication pour chaque contact (SMS, téléphone ou e-mail, par exemple), afin de pouvoir avec certitude joindre les personnes concernées lors d'un incident.
3. Définissez un plan d'intervention.
   a. Identifiez les contacts les plus appropriés à impliquer lors d'un incident. Définissez des plans de remontée en fonction des rôles du personnel à impliquer, plutôt que des contacts individuels. Envisagez d'inclure des contacts susceptibles d'être chargés d'informer les entités externes, même s'ils ne sont pas directement impliqués dans la résolution de l'incident.

Ressources

Bonnes pratiques associées:

- OPS02-BP03 Les activités opérationnelles ont des propriétaires identifiés responsables de leurs performances

Documents connexes:

- AWS Guide d’intervention en cas d’incident de sécurité

Exemples connexes:

- AWS Cadre du playbook du client
- Prepare for and respond to security incidents in your environment AWS

Outils associés:

- AWS Systems Manager Incident Manager

Vidéos connexes:

- L’approche d’Amazon en matière de sécurité pendant le développement

SEC10-BP02 Développer des plans de gestion des incidents

Le premier document à élaborer pour la réponse aux incidents est le plan d’intervention en cas d’incident. Le plan d’intervention en cas d’incident 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 d’exposition au risque 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 métier et aux exigences de conformité. Par exemple, si vous exécutez des charges de travail dans AWS qui sont conformes à FedRAMP aux États-Unis, suivez les recommandations fournies dans le document NIST SP 800-61 Guide relatif à la gestion de la sécurité informatique. De la même manière, lorsque vous exécutez des charges de travail qui stockent des données d'identification personnelle (PII), réfléchissez à la façon de protéger ces données et de résoudre les problèmes liés à la résidence et à l'utilisation des données.

Lorsque vous élaborez un plan de gestion des incidents pour vos charges de travail dans AWS, commencez par le modèle de responsabilité partagée AWS pour élaborer une approche de défense approfondie en matière d'intervention en cas d'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. Le Guide sur les interventions en cas d'incident de sécurité AWS 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

1. Définissez les rôles et les responsabilités au sein de votre organisation pour gérer les événements de sécurité. Cela devrait impliquer des représentants de différents départements, notamment :
   - Ressources humaines (RH)
   - Équipe de direction
   - Département juridique
   - Propriétaires et développeurs d'applications (experts spécifiques ou SME)
2. Désignez clairement les intervenants responsables, redevables, consultés et informés (RACI, Responsible, Accountable, Consulted, Informed) lors d'un incident. Créez une matrice RACI pour faciliter une communication rapide et directe, et désignez clairement le leadership aux différentes étapes d'un événement.
3. Impliquez les propriétaires et les développeurs d'applications (SME) lors d'un incident, car ils peuvent fournir des informations et un contexte précieux pour la mesure de l'impact. Établissez des relations avec ces SME et mettez en pratique des scénarios de réponse aux incidents avec elles avant qu'un véritable incident se produise.

4. Impliquez des partenaires de confiance ou des experts externes dans le processus d'enquête ou de réponse, car ils peuvent apporter une expertise et un point de vue supplémentaires.
5. Alignez vos rôles et plans de gestion des incidents sur les réglementations locales ou les exigences de conformité qui régissent votre organisation.
6. Mettez en pratique et testez régulièrement vos plans de réponse aux incidents, et impliquez tous les rôles et responsabilités définis. Cela contribue à rationaliser le processus et à vérifier que vous disposez d'une réponse coordonnée et efficace aux incidents de sécurité.
7. Passez en revue et mettez à jour les rôles, les responsabilités et la matrice RACI régulièrement ou à mesure que votre structure organisationnelle ou vos exigences changent.

Comprenez les équipes d'intervention et le support AWS

- AWS Support
  - Support propose un large choix de formules qui vous permettent d'accéder aux outils et aux compétences nécessaires pour garantir la réussite et la santé 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.
  - Considérez le Centre d'assistance dans Console de gestion AWS (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 Support est contrôlé par Gestion des identités et des accès AWS. Pour plus d'informations sur l'accès aux fonctionnalités Support, consultez Démarrer avec Support.
- AWS Équipe de réponse aux incidents clients (CIRT)
  - 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 Support.
- Réponse aux incidents de sécurité AWS

    - Annoncé à l'occasion de re:Invent 2024, Réponse aux incidents de sécurité AWS est un service géré de réponse aux incidents de sécurité qui associe la technologie de triage moderne et une intervention humaine. Le service ingère tous les résultats de GuardDuty et les résultats tiers envoyés à AWS Security Hub CSPM pour triage afin d'avertir le client uniquement des résultats nécessitant une enquête. Le service fournit également un portail permettant de soumettre des cas réactifs en cas d'événement de sécurité remarqué par le client et de bénéficier de l'assistance d'une équipe AWS avancée de réponse aux incidents.
- Support de réponse aux attaques DDoS
    - AWS propose AWS Shield, qui est un service de protection DDoS (Distributed Denial of Service) géré qui protège les applications Web s'exécutant sous AWS. Shield assure une détection continue et une atténuation automatique des risques pour minimiser les temps d'arrêt et la latence des applications, afin qu'il ne soit pas nécessaire d'avoir recours à 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 relative aux 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 appliquant les bonnes pratiques pour gérer votre infrastructure, AMS permet de réduire les coûts et risques de fonctionnement. AMS automatise les activités courantes telles que les demandes de modification, la surveillance, la gestion des correctifs, la sécurité et les services de sauvegarde, et fournit des services pour l'intégralité du cycle de vie pour mettre en service, exécuter et soutenir votre infrastructure.
    - 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 d'intervention en cas d'incident

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

- Présentation de l'équipe d'intervention en cas d'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.
- Plan de communication : détaille les coordonnées et la manière dont vous communiquez lors d'un incident.
- Méthodes de communication relative à la sauvegarde : 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 l'intervention en cas d'incident 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 priorité 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 d'intervention en cas d'incident de chaque organisation est unique. Vous devez élaborer un plan d'intervention en cas d'incident qui convient le mieux à votre organisation.

Ressources

Bonnes pratiques associées :

- SEC04 Détection

Documents connexes :

- Guide d'intervention en cas d'incident de sécurité AWS
- 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 d'exposition au risque 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 permettant de commencer à renforcer les capacités de criminalistique dans le AWS Cloud, consultez Stratégies relatives à l'environnement d'investigation judiciaire dans le AWS Cloud.

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.
- Production de rapports : présentez les informations issues de la phase d'analyse.

Étapes d'implémentation

Préparer 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 intervenir en cas d'incident, 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 :

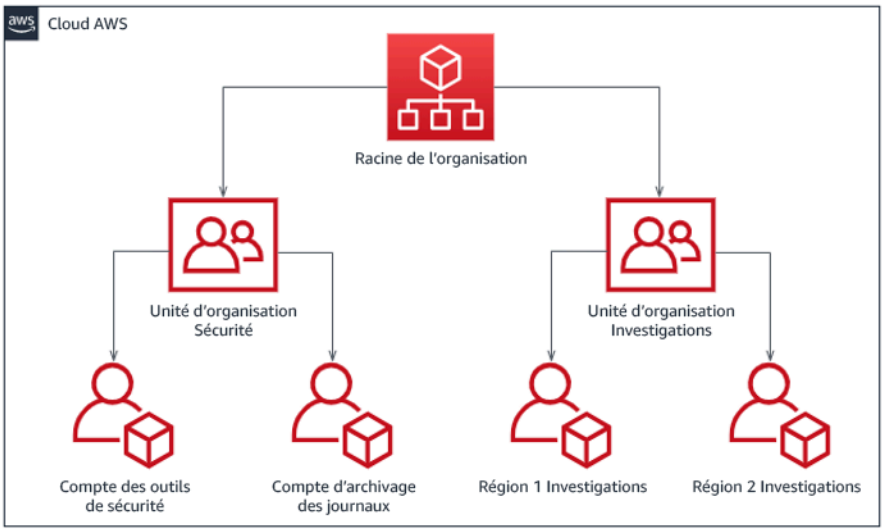
- Archivage des journaux : regroupez les journaux dans un d'archivage de journaux Compte AWS avec des autorisations limitées.

- 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 les régions USA Est (Virginie du Nord) (`us-east-1`) et USA Ouest (Oregon) (`us-west-2`), vous aurez deux comptes dans l'unité d'organisation médico-légale : un pour `us-east-1` et un 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

Conservez les sauvegardes et les 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 en savoir plus sur ces services et approches de la sauvegarde et de la récupération, reportez-vous au Recommandation en matière de sauvegarde et de récupération et à Utiliser les sauvegardes pour récupérer après un incident 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, reportez-vous aux 10 meilleures pratiques de sécurité en matière de sauvegarde 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.

Automatisez la criminalistique

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 de réponse automatique aux incidents et de criminalistique
- Orchestrateur d'analyse poussée automatisée pour for 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 des recommandations et les 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 d'exposition au risque 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 prévus : créez des playbooks pour les incidents que vous anticipez. Cela inclut des menaces telles que le déni de service (DoS), les rançongiciels et la compromission des informations d'identification.

- Constatations ou alertes de sécurité connues : créez des playbooks pour vos résultats et alertes de sécurité connus, tels que les résultats d'Amazon GuardDuty. Lorsque vous recevez un résultat de GuardDuty, le playbook doit indiquer des étapes claires pour éviter de mal gérer ou d'ignorer l'alerte. Pour plus de détails et de conseils de correction, consultez Correction des problèmes de sécurité découverts par GuardDuty.

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.

L'équipe AWS de réponse aux incidents client (CIRT) a publié un référentiel GitHub contenant des guides opérationnels de réponse aux incidents, organisés par scénario de menace, type et ressource. Ces guides opérationnels peuvent être adaptés pour s'aligner sur vos procédures de réponse aux incidents existantes ou servir de base à l'élaboration de nouvelles procédures.

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 ?
- Prérequis : quels journaux, mécanismes de détection et outils automatisés sont requis pour ce scénario d'incident ? Quelle est la notification attendue ?
- Informations de communication et d'escalade : qui est impliqué et quelles sont ses coordonnées ? Quelles sont les responsabilités de chacune des parties prenantes ?
- Étapes d'intervention : 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 ?
  - Détection : comment l'incident sera-t-il détecté ?
  - Analyse : comment l'étendue de l'impact sera-t-elle déterminée ?
  - Contenu : comment l'incident sera-t-il isolé pour en limiter la portée ?
  - Éradication : comment éliminer la menace de l'environnement ?
  - Remise : comment le système ou la ressource concernés seront-ils remis en production ?
- Résultats escomptés : 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 pour les playbooks d'intervention en cas d'incident
- Élaborer vos propres playbooks d'intervention en cas d'incident
- Modèles de guides d'intervention en cas d'incident
- Création d'un runbook de réponse aux incidents AWS à l'aide de playbooks Jupyter et 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 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 des mécanismes d'escalade 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, ainsi que pour les tâches de réponse aux incidents, nous vous recommandons de mettre en œuvre la fédération d'identités et l'escalade 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 pour effectuer ses 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. La bonne façon de procéder consiste à utiliser AWS Security Token Service et les politiques de session pour 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, un accès d'urgence aux bris de verre doit être configuré pour permettre une enquête et une résolution rapide des incidents. Nous vous recommandons d'utiliser un utilisateur, un groupe ou un rôle doté des autorisations appropriées pour effectuer des tâches et accéder aux ressources AWS. Utiliser l'utilisateur racine uniquement pour les tâches qui nécessitent des informations d'identification. 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 dédiés. Les comptes 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 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 des stratégies de mot de passe d'un niveau de sécurité élevé à l'authentification multifactorielle (MFA). Si les playbooks de réponse aux incidents ne nécessitent qu'un accès à la Console de gestion AWS, 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 politiques IAM ou des politiques de contrôle des services (SCP), comme mentionné dans les bonnes pratiques de sécurité AWS pour les AWS Organizations SCP. 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 racine d'un compte AWS ne soit pas utilisé, à moins qu'ils ne soient nécessaires 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 des informations d'identification de l'utilisateur racine et du jeton d'authentification multifactorielle.

Pour configurer les politiques IAM pour les 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 de réponse aux incidents pour assumer des rôles IAM d'intervention en cas d'incident 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. Veillez à ce que toutes

les demandes de `AssumeRole` pour ces rôles soient enregistrées dans CloudTrail et fassent l'objet d'une alerte, et à ce que toutes les actions effectuées à l'aide de ces rôles soient enregistrées.

Il est vivement recommandé de nommer les comptes utilisateur et rôles IAM afin d'en faciliter la recherche dans les journaux CloudTrail. Un exemple serait de nommer les comptes IAM *<USER_ID>*`-BREAK-GLASS` et les rôles IAM `BREAK-GLASS-ROLE`.

CloudTrail est utilisé pour enregistrer l'activité des API dans vos comptes AWS et doit être utilisé pour configurer les alertes relatives à l'utilisation des rôles d'ntervention en cas d'incidents. Consultez la publication de blog sur la configuration des alertes lorsque les clés racine sont utilisées. Les instructions peuvent être modifiées pour configurer le filtre métrique Amazon CloudWatch afin de filtrer 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. Celle-ci peut inclure des instances Amazon Elastic Compute Cloud, des bases de données Amazon Relational Database Service ou des plateformes de logiciel en tant que service (SaaS). Il est fortement recommandé d'utiliser AWS Systems Manager Session Manager pour tous les accès administratifs aux instances Amazon EC2 plutôt que d'utiliser les protocoles natifs tels que SSH ou RDP. 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 à l'aide des documents AWS Systems Manager Run Command, qui peuvent réduire les erreurs des utilisateurs et accélérer le temps de restauration. 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.

Enfin, la gestion des comptes IAM de réponse aux incidents doit être ajoutée à vos processus Joiners, Movers et Leavers et revue et testée périodiquement pour vérifier que seul l'accès prévu est autorisé.

Ressources

Documents connexes :

- Gérer les accès temporaires à votre environnement AWS
- Guide d'intervention en cas d'incident de sécurité AWS
- Reprise après sinistre AWS Elastic
- 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
- Configuration d'accès inter-compte pour MFA
- Utilisation de l'analyseur d'accès IAM pour générer des politiques IAM
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment
- Comment recevoir des notifications lorsque les clés d'accès racine de votre AWS sont utilisées
- Create fine-grained session permissions using IAM managed policies
- Accès en mode « bris de glace »

Vidéos connexes :

- Automatisation de la réponse aux incidents et de l'analyse poussée dans AWS
- DIY guide to runbooks, incident reports, and incident response
- Prepare for and respond to security incidents in your AWS environment

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 d'exposition au risque 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, 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 stratégie de balisage. 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 l'intervention en cas d'incidents de sécurité
- SEC04-BP01 Configurer une journalisation de service et d'application

Permettre aux services de sécurité de prendre en charge la détection et l'intervention

AWS fournit des fonctionnalités 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 Définitions des fonctionnalités du cloud et la page d'accueil de réponse aux incidents de sécurité.

Élaboration et mise en œuvre d'une stratégie de marquage

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 la section Marquage de vos ressourcesAWS. 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 en savoir plus sur la mise en œuvre et l'application, reportez-vous à Mettre en œuvre une stratégie de balisage AWS des ressources à l'aide de politiques de balises AWS et de politiques de contrôle des services (SCP).

Ressources

Bonnes pratiques Well-Architected connexes:

- SEC04-BP01 Configurer une journalisation de service et d'application
- SEC04-BP02 Capturer les journaux, les résultats et les métriques dans des emplacements standardisés

Documents connexes:

- Stratégies de journalisation pour l'intervention en cas d'incidents de sécurité
- Définitions des fonctionnalités cloud de réponse aux incidents

Exemples connexes:

- Détection des menaces et réponse avec Amazon GuardDuty et Amazon Detective
- Atelier Security Hub
- Gestion des vulnérabilités avec Amazon Inspector

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 « tests de simulation de panne ») 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 d'intervention en cas d'incident.
- Possibilité de répondre à des vecteurs moins courants.

Niveau de risque encouru si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Il existe trois principaux types de simulations :

- Exercices sur table : 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.
- Exercces 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. Définir les éléments essentiels de l'exercice : définissez le scénario de simulation et les objectifs de la simulation. Les deux doivent être acceptés par les dirigeants.

2. Identifier 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. Concevoir et tester 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. Faciliter 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. Élaborer le rapport après action (AAR) : identifier 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 :

- Réponse aux incidents dans AWS

Vidéos connexes :

- AWS GameDay - Security Edition
- Exécution de simulations de réponses efficaces aux incidents de sécurité

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, confinement, éradication et rétablissement. 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 être en mesure de répondre efficacement à un événement de sécurité actif.

Pour en savoir plus, consultez la section Opérations du Guide de réponse 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 de leçons apprises et d'une capacité d'analyse des causes profondes permettra non seulement d'améliorer les capacités de réponse aux incidents, mais aussi d'éviter 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 d'exposition au risque si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Il est important de mettre en œuvre un cadre des leçons apprises 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 :
  - Personnes
    - 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 ?
  - 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 ?
  - 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 – Établir un cadre pour tirer des enseignements des incidents (langue française non garantie)AWS
- Guide du NCSC CAF – Leçons apprises

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 directives de mise en œuvre se concentrent sur quatre domaines : organisation et culture, sécurité du pipeline, sécurité dans le pipeline et 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 Mener des examens de code
- 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

Offrez à votre équipe une formation sur les pratiques de développement et d'exploitation sécurisées, afin de l'aider à créer des logiciels sécurisés et de haute qualité. Cette pratique aide votre équipe à prévenir, détecter et corriger les problèmes de sécurité à un stade précoce du cycle de développement. Envisagez une formation qui couvre la modélisation des menaces, les pratiques de codage sécurisé et l'utilisation des services pour des configurations et des opérations sécurisées. Donnez à votre équipe un accès à la formation par le biais de ressources en libre-service et recueillez régulièrement leurs commentaires en vue de son amélioration continue.

Résultat escompté : vous dotez votre équipe des connaissances et des compétences nécessaires pour concevoir et créer des logiciels en tenant compte de la sécurité dès le départ. Grâce à une formation sur la modélisation des menaces et les pratiques de développement sécurisé, votre équipe possède une connaissance approfondie des risques de sécurité potentiels et comprend mieux comment les atténuer au cours du cycle de développement logiciel (SDLC). Cette approche proactive de la sécurité fait partie de la culture de votre équipe et vous permet d'identifier et de résoudre rapidement les problèmes de sécurité potentiels. Par conséquent, votre équipe fournit des logiciels et des fonctionnalités sécurisés et de haute qualité de manière plus efficace, ce qui accélère le délai de livraison global. Vous avez une culture collaborative et inclusive de la sécurité au sein de votre organisation, et la responsabilité de la sécurité est partagée entre tous ses acteurs.

Anti-modèles courants:

- Vous attendez un examen de la sécurité pour tenir compte des propriétés de sécurité d'un système.

- Vous laissez toutes les décisions en matière de sécurité à une équipe de sécurité centrale.
- Vous ne communiquez pas sur la manière dont les décisions prises au cours du cycle de développement logiciel sont liées aux attentes ou aux politiques générales de l'organisation en matière de sécurité.
- Vous effectuez trop tard 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 d'exposition au risque si cette bonne pratique n'est pas respectée : moyen

Directives d'implémentation

Pour créer des logiciels sécurisés et de haute qualité, formez votre équipe aux pratiques courantes de développement et d'exploitation sécurisés des applications. Cette pratique peut aider votre équipe à prévenir, détecter et corriger les problèmes de sécurité plus tôt dans le cycle de développement, ce qui peut raccourcir le délai de livraison.

Pour mettre en œuvre cette pratique, envisagez de former votre équipe à la modélisation des menaces à l'aide de ressources AWS, telles que l'atelier sur la modélisation des menaces. La modélisation des menaces peut aider votre équipe à comprendre les risques de sécurité potentiels et à concevoir des systèmes en tenant compte de la sécurité dès le départ. En outre, vous pouvez fournir un accès à une formation AWS Training and Certification, du secteur ou destinée aux partenaires AWS sur les pratiques de développement sécurisées. Pour plus de détails sur une approche globale de la conception, du développement, de la sécurisation et de l'exploitation efficace à grande échelle, consultez le Guide AWS DevOps.

Définissez et communiquez clairement le processus d'examen de la sécurité de votre organisation et définissez les responsabilités de votre équipe, de l'équipe chargée de la sécurité et des autres parties prenantes. Publiez des conseils en libre-service, des exemples de code et des modèles illustrant comment répondre à vos exigences en matière de sécurité. Vous pouvez fournir des configurations préapprouvées et sécurisées et réduire les besoins en configurations personnalisées à l'aide de

services AWS tels qu'AWS CloudFormation, Cloud Development Kit AWS (AWS CDK) (AWS CDK) Constructs et Service Catalog.

Recueillez régulièrement les commentaires de votre équipe sur son expérience du processus d'examen de la sécurité et de la formation, et mettez à profit ces commentaires pour vous améliorer en permanence. Organisez des tests de simulation de panne ou des campagnes de lutte contre les bogues pour identifier et résoudre les problèmes de sécurité tout en améliorant les compétences de votre équipe.

Étapes d'implémentation

1. Identifier les besoins de formation : évaluez le niveau de compétence actuel et les lacunes en matière de connaissances au sein de votre équipe en ce qui concerne les pratiques de développement sécurisées par le biais d'enquêtes, d'examens de code ou de discussions avec les membres de l'équipe.
2. Planifier la formation : sur la base des besoins identifiés, créez un plan de formation qui couvre des sujets pertinents tels que la modélisation des menaces, les pratiques de codage sécurisé, les tests de sécurité et les pratiques de déploiement sécurisé. Utilisez des ressources telles que l'atelier sur la modélisation des menaces, AWS Training and Certification et les programmes de formation destinés au secteur ou aux partenaires AWS.
3. Planifier et offrir des formations : planifiez des ateliers ou des sessions de formation réguliers pour votre équipe. Ils peuvent être dispensés par un instructeur ou à un rythme personnalisé, selon les préférences et la disponibilité de votre équipe. Encouragez les exercices pratiques et les exemples pratiques pour renforcer l'apprentissage.
4. Définir un processus d'examen de la sécurité : collaborez avec votre équipe de sécurité et les autres parties prenantes pour définir clairement le processus d'examen de la sécurité pour vos applications. Documentez les responsabilités de chaque équipe ou personne impliquée dans ce processus, y compris votre équipe de développement, votre équipe de sécurité et les autres parties prenantes concernées.
5. Créer des ressources en libre-service : développez des recommandations, des exemples de code et des modèles en libre-service pour illustrer comment répondre aux exigences de votre entreprise en matière de sécurité. Envisagez de fournir des configurations préapprouvées et sécurisées et de réduire les besoins en configurations personnalisées à l'aide de services AWS tels que CloudFormation, AWS CDK Constructs et Service Catalog.
6. Communiquer et partager : communiquez efficacement à votre équipe le processus d'examen de la sécurité et les ressources en libre-service disponibles. Organisez des ateliers ou des sessions

de formation pour familiariser votre équipe à ces ressources et vérifiez qu'elle comprend comment les utiliser.

7. Recueillir des commentaires et s'améliore : collectez régulièrement les commentaires de votre équipe sur son expérience du processus d'examen de la sécurité et de la formation. Utilisez ces commentaires pour identifier les domaines à améliorer et affiner en permanence les supports de formation, les ressources en libre-service et le processus d'examen de la sécurité.
8. Réaliser des exercices de sécurité : organisez des tests de simulation de panne ou des campagnes de lutte contre les bogues pour identifier et résoudre les problèmes de sécurité au sein de vos applications. Ces exercices permettent non seulement de découvrir des vulnérabilités potentielles, mais constituent également des opportunités d'apprentissage pratique pour votre équipe, visant à améliorer ses compétences en matière de développement et d'exploitation sécurisés.
9. Continuer à apprendre et à s'améliorer : encouragez votre équipe à rester au fait des derniers outils, techniques et pratiques de développement sécurisé. Passez en revue et mettez à jour régulièrement vos supports et ressources de formation afin de refléter l'évolution du contexte et des bonnes pratiques de sécurité.

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 et la certification
- Comment envisager la gouvernance de la sécurité dans le cloud
- Comment aborder la modélisation des menaces
- Accélérer l'entraînement – The AWS Skills Guild
- AWS Sagas DevOps

Vidéos connexes:

- Proactive security: Considerations and approaches

Exemples connexes:

- Atelier sur la modélisation des menaces
- Sensibilisation des développeurs à l'industrie

Services connexes:

- AWS CloudFormation
- Cloud Development Kit AWS (AWS CDK) (AWS CDK) Constructions
- Service Catalog

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 escompté : l'objectif des tests automatisés est de fournir un moyen programmatique de détecter les problèmes potentiels à un stade précoce et fréquent 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 d'exposition au risque 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. NIST Quality Group propose une comparaison des analyseurs de sécurité du code source, qui inclut des outils open source pour les scanners de code d'octets et les scanners 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 Q Developer fournit des recommandations de code, y compris des analyses de sécurité, dans l'IDE du générateur. La sécurité Amazon CodeGuru peut identifier les problèmes critiques, les problèmes de sécurité et les bogues difficiles à détecter lors du développement d'applications, et fournit des recommandations pour améliorer la qualité du code. L'extraction de la nomenclature logicielle (SBOM) vous permet également d'extraire un enregistrement formel contenant les détails et les relations des différents composants utilisés dans la création de votre logiciel. Cela vous permet d'informer la gestion des vulnérabilités et d'identifier rapidement les dépendances des logiciels ou des composants, et les risques liés à la chaîne d'approvisionnement.

L'Atelier sur la sécurité pour les développeurs utilise des outils pour développeurs AWS tels qu'AWS CodeBuild, AWS CodeCommit et AWS CodePipeline pour l'automatisation du pipeline de versions comprenant 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.
- Automated Security Helper (ASH) est un exemple d'outil d'analyse de sécurité de code open source.

- La réalisation de tests ou d'analyses de code à l'aide d'outils automatisés, tels qu'Amazon Q Developer intégré aux IDE pour développeurs et la sécurité Amazon CodeGuru pour l'analyse du code lors de la validation, permet aux créateurs d'obtenir des commentaires au bon moment.
- Lorsque vous créez avec AWS Lambda, Amazon Inspector peut vous permettre de scanner le code de l'application dans vos fonctions.
- 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.
- Pour extraire la nomenclature logicielle dans le cadre de vos pipelines CI/CD, utilisez Amazon Inspector SBOM Generator pour produire des nomenclatures logicielles pour les archives, les images de conteneur, les répertoires, les systèmes locaux et les fichiers binaires Go et Rust compilés au format SBOM CycloneDX.

Ressources

Bonnes pratiques associées:

- Guide DevOps : DL.CR.3 Établissement de critères d'achèvement clairs pour les tâches liées au code

Documents connexes:

- Livraison et déploiement continus

- AWS Partenaires disposant de la compétence DevOps
- AWS Partenaires disposant de compétences en sécurité pour la sécurité des applications
- Choisir une approche CI/CD Well-Architected
- Détection de secrets dans la sécurité Amazon CodeGuru
- Bibliothèque de détection de la sécurité Amazon CodeGuru
- Accelerate deployments on AWS with effective governance
- Comment AWS automatise les déploiements en toute sécurité et sans intervention

- Comment la sécurité Amazon CodeGuru vous aide à équilibrer efficacement la sécurité et la rapidité

Vidéos connexes:

- Hands-off: Automating continuous delivery pipelines at Amazon
- Automating cross-account CI/CD pipelines
- Processus de développement logiciel chez Amazon
- Tests des logiciels et des systèmes chez Amazon

Exemples connexes:

- Sensibilisation des développeurs à l'industrie
- Automated Security Helper (ASH)
- AWS CodePipeline Gouvernance – GitHub

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 escompté : les tests de pénétration sont utilisés pour détecter, corriger et 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 d'exposition au risque 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

- Disposez d'un processus structuré pour définir le périmètre des tests de pénétration. 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:

- AWS Penetration Testing fournit des conseils détaillés pour les tests de pénétration sur AWS
- Accelerate deployments on AWS with effective governance
- AWS Security Competency Partners
- Modernize your penetration testing architecture on AWS Fargate
- AWS Fault Injection Simulator

Exemples connexes:

- Automatisez les tests d'API avec AWS CodePipeline (GitHub)
- Assistant de sécurité automatisé (GitHub)

SEC11-BP04 Mener des examens de code

Mettez en œuvre des examens de code pour vérifier la qualité et la sécurité d'un logiciel en cours de développement. Les examens de code impliquent que des membres de l'équipe autres que l'auteur du code d'origine examinent le code pour détecter les problèmes et les vulnérabilités potentiels et vérifier le respect des normes et des bonnes pratiques de codage. Ce processus permet de détecter les erreurs, les incohérences et les failles de sécurité qui auraient pu être omises par le développeur d'origine. Utilisez des outils automatisés pour faciliter les examens de code.

Résultat escompté : vous incluez des examens de code pendant le développement afin d'améliorer la qualité du logiciel en cours d'écriture. Vous perfectionnez les membres moins expérimentés de l'équipe grâce aux enseignements identifiés lors de l'examen de code. Vous identifiez les opportunités d'automatisation et soutenez le processus d'examen de code à l'aide d'outils et de tests automatisés.

Anti-modèles courants:

- Vous n'effectuez pas d'examen de code avant le déploiement.
- La même personne écrit et examine le code.
- Vous n'utilisez pas d'automatisation ni d'outils pour assister ou orchestrer les examens de code.
- Vous ne formez pas les concepteurs à la sécurité des applications avant qu'ils procèdent à l'examen 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 d'exposition au risque si cette bonne pratique n'est pas respectée : moyen

Directives d’implémentation

Les examens de code permettent de vérifier la qualité et la sécurité du logiciel au cours de son développement. Les examens manuels impliquent qu’un membres de l’équipe autre que l’auteur du code d’origine examine le code pour détecter les problèmes et les vulnérabilités potentiels et vérifie le respect des normes et des bonnes pratiques de codage. Ce processus permet de détecter les erreurs, les incohérences et les failles de sécurité qui auraient pu être omises par le développeur d’origine.

Envisagez d’utiliser la sécurité Amazon CodeGuru pour vous aider à effectuer des examens de code automatisés. La sécurité CodeGuru utilise le machine learning et un raisonnement automatisé pour analyser votre code et identifier les vulnérabilités de sécurité et les problèmes de codage potentiels. Intégrez des examens de code automatisés à vos référentiels de code existants et à vos pipelines d’intégration continue/de déploiement continu (CI/CD).

Étapes d’implémentation

1. Établissez un processus d’examen de code:
   - Définissez à quel moment les examens de code doivent avoir lieu, par exemple avant de fusionner le code dans la branche principale ou avant de le déployer en production.
   - Déterminez qui doit participer au processus d’examen de code, par exemple les membres de l’équipe, les développeurs senior et les experts en sécurité.
   - Décidez de la méthodologie d’examen de code, y compris du processus et des outils à utiliser.
2. Configurez les outils d’examen de code:
   - Évaluez et sélectionnez les outils d’examen de code qui répondent aux besoins de votre équipe, tels que les demandes d’extraction GitHub ou la sécurité CodeGuru.
   - Intégrez les outils choisis à vos référentiels de code et à vos pipelines CI/CD existants.
   - Configurez ces outils pour appliquer les exigences d’examen de code, telles que le nombre minimal de réviseurs et les règles d’approbation.
3. Définissez une liste de contrôle et des directives d’examen de code:
   - Créez une liste de contrôle ou des directives d’examen de code explicitant ce qui doit être examiné. Tenez compte de facteurs tels que la qualité du code, les vulnérabilités de sécurité, le respect des normes de codage et les performances.
   - Partagez la liste de contrôle ou les directives avec l’équipe de développement et vérifiez que tout le monde comprend les attentes.
4. Formez les développeurs aux bonnes pratiques d’examen de code:

- Offrez à votre équipe une formation sur la manière de mener des examens de code efficaces.
- Sensibilisez votre équipe aux principes de sécurité des applications et aux vulnérabilités courantes à rechercher lors des examens.
- Encouragez le partage des connaissances et les sessions de programmation en binômes pour perfectionner les membres moins expérimentés de l'équipe.

5. Mettez en œuvre le processus d'examen de code:
   - Intégrez l'étape d'examen de code dans votre flux de travail de développement, par exemple en créant une demande d'extraction et en affectant des réviseurs.
   - Exigez que les modifications de code fassent l'objet d'un examen de code avant la fusion ou le déploiement.
   - Encouragez une communication ouverte et des commentaires constructifs pendant le processus d'examen.
6. Surveillez et améliorez:
   - Vérifiez régulièrement l'efficacité de votre processus d'examen de code et recueillez les commentaires de l'équipe.
   - Identifiez les opportunités d'automatisation ou d'amélioration des outils afin de rationaliser le processus d'examen de code.
   - Mettez à jour et affinez en permanence la liste de contrôle ou les directives d'examen de code en fonction des enseignements tirés et des bonnes pratiques du secteur.
7. Favorisez une culture d'examen de code:
   - Soulignez l'importance des examens de code pour maintenir la qualité et la sécurité du code.
   - Célébrez les réussites et les enseignements tirés du processus d'examen de code.
   - Favorisez un environnement de collaboration et de soutien dans lequel les développeurs se sentent à l'aise pour effectuer et recevoir des commentaires.

Ressources

Bonnes pratiques associées:

- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication

Documents connexes:

- Guide DevOps : DL.CR.2 Réalisation d'un examen par les pairs des modifications de code

- À propos des pull requests dans GitHub

Exemples connexes:

- Automatisation des examens de code avec la sécurité Amazon CodeGuru
- Automatisation de la détection des vulnérabilités de sécurité et des bogues dans les pipelines CI/CD à l'aide de la CLI de sécurité Amazon CodeGuru

Vidéos connexes:

- Amélioration continue de la qualité du code avec la sécurité Amazon CodeGuru

SEC11-BP05 Centralisation des services pour les packages et les dépendances

Fournissez des services centralisés pour permettre à vos équipes d'obtenir des packages logiciels et d'autres dépendances. Les packages peuvent ainsi être validés avant d'être inclus dans le logiciel que vous écrivez. De plus, une source de données est disponible pour l'analyse des logiciels utilisés dans votre organisation.

Résultat escompté : vous créez votre charge de travail à partir de packages logiciels externes en plus du code que vous écrivez. Cela simplifie la mise en œuvre de fonctionnalités utilisées de manière répétée, telles qu'un analyseur JSON ou une bibliothèque de chiffrement. Vous centralisez les sources de ces packages et dépendances afin que votre équipe de sécurité puisse les valider avant leur utilisation. Vous utilisez cette approche en conjonction avec les flux de tests manuels et automatisés pour accroître la confiance dans la qualité du logiciel que vous développez.

Anti-modèles courants:

- Vous extrayez des packages de référentiels arbitraires sur Internet.
- Vous ne testez pas 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 d'exposition au risque 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 mettre en œuvre un moyen efficace d'ajouter des packages au référentiel lorsque des mises à jour sont effectuées ou que de nouvelles exigences apparaissent. Les services AWS tels que AWS CodeArtifact ou des solutions partenaires AWS similaires offrent cette fonctionnalité.

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:

- Guide DevOps : DL.CS.2 Signature des artefacts de code après chaque build
- Niveaux de la chaîne d'approvisionnement pour les artefacts logiciels (SLSA)

Exemples connexes:

- Accelerate deployments on AWS with effective governance
- Renforcez la sécurité de vos packages avec le kit d'outils CodeArtifact Package Origin Control
- Pipeline de publication de packages multi-régions (GitHub)
- Publication de modules Node.js sur AWS CodeArtifact à l'aide de AWS CodePipeline (GitHub)
- Exemple de pipeline Java CodeArtifact AWS CDK (GitHub)
- Distribuer des packages .NET NuGet privés avec CodeArtifact AWS (GitHub)

Vidéos connexes:

- Proactive security: Considerations and approaches
- The AWS Philosophy of Security (re:Invent 2017)
- When security, safety, and urgency all matter: Handling Log4Shell

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 escompté : la version de votre charge de travail que vous testez est la version que vous déployez, et le déploiement est effectué de manière cohérente à chaque fois. Vous externalisez la configuration de votre charge de travail, ce qui vous permet de déployer dans différents environnements sans modification. Vous utilisez la signature cryptographique de vos packages logiciels pour vérifier que rien ne change d'un environnement à l'autre.

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

Directives d'implémentation

Pour maintenir une infrastructure d'applications robuste et fiable, mettez en œuvre des pratiques de déploiement sécurisées et automatisées. Cette pratique implique de supprimer l'accès humain persistant aux environnements de production, d'utiliser des outils CI/CD pour les déploiements et d'externaliser les données de configuration spécifiques à l'environnement. En suivant cette approche, vous pouvez améliorer la sécurité, réduire le risque d'erreurs humaines et rationaliser le processus de déploiement.

Vous pouvez créer votre structure de Compte AWS pour supprimer l'accès humain persistant aux environnements de production. Cette pratique minimise le risque de modifications non autorisées ou accidentelles, ce qui améliore l'intégrité de vos systèmes de production. Au lieu d'un accès humain direct, vous pouvez utiliser des outils CI/CD tels que AWS CodeBuild et AWS CodePipeline pour effectuer des déploiements. Vous pouvez utiliser ces services pour automatiser les processus de création, de test et de déploiement, ce qui réduit les interventions manuelles et améliore la cohérence.

Pour renforcer encore la sécurité et la traçabilité, vous pouvez signer vos packages d'applications après les avoir testés et valider ces signatures lors du déploiement. Pour ce faire, utilisez des outils cryptographiques tels que AWS Signer ou AWS Key Management Service (AWS KMS). En signant et en vérifiant les packages, vous pouvez vous assurer que vous ne déployez que du code autorisé et validé dans vos environnements.

En outre, votre équipe peut concevoir votre charge de travail pour obtenir des données de configuration spécifiques à l'environnement à partir d'une source externe, telle que AWS Systems Manager Parameter Store. Cette pratique sépare le code d'application des données de configuration, ce qui vous permet de gérer et de mettre à jour les configurations indépendamment sans modifier le code d'application lui-même.

Pour rationaliser le provisionnement et la gestion de l'infrastructure, envisagez d'utiliser des outils d'infrastructure en tant que code (IaC) tels qu'AWS CloudFormation ou AWS CDK. Vous pouvez utiliser ces outils pour définir votre infrastructure en tant que code, ce qui améliore la cohérence et la répétabilité des déploiements dans différents environnements.

Envisagez d'utiliser des déploiements canary pour valider la réussite du déploiement de votre logiciel. Les déploiements canary impliquent le déploiement de modifications sur un sous-ensemble d'instances ou d'utilisateurs avant leur déploiement dans l'environnement de production tout entier. Vous pouvez ainsi surveiller l'impact des modifications et revenir en arrière si nécessaire, ce qui minimise le risque de problèmes généralisés.

Suivez les recommandations décrites dans le livre blanc Organisation de votre environnement AWS à l'aide de comptes multiples. Ce livre blanc fournit des conseils sur la manière de séparer les environnements (par exemple de développement, intermédiaire et de production) dans des Comptes AWS distincts, ce qui améliore encore la sécurité et l'isolation.

Étapes d'implémentation

1. Configurez la structure de Compte AWS :
   - Suivez les instructions du livre blanc Organisation de votre environnement AWS à l'aide de comptes multiples pour créer des Comptes AWS distincts pour les différents environnements (par exemple, de développement, intermédiaire et de production).
   - Configurez les contrôles d'accès et les autorisations appropriés pour chaque compte afin de limiter l'accès humain direct aux environnements de production.
2. Implémentez un pipeline CI/CD:
   - Configurez un pipeline CI/CD à l'aide de services tels qu'AWS CodeBuild et AWS CodePipeline.
   - Configurez le pipeline pour créer, tester et déployer automatiquement votre code d'application dans les environnements respectifs.
   - Intégrez des référentiels de code au pipeline CI/CD pour le contrôle des versions et la gestion du code.
3. Signez et vérifiez les packages d'applications:
   - Signez vos packages d'application une fois qu'ils ont été testés et validés à l'aide de AWS Signer ou AWS Key Management Service (AWS KMS).
   - Configurez le processus de déploiement pour vérifier les signatures des packages d'applications avant de les déployer dans les environnements cibles.
4. Externalisez les données de configuration:

- Stockez les données de configuration spécifiques à l'environnement dans AWS Systems Manager Parameter Store.
- Modifiez votre code d'application pour récupérer les données de configuration depuis Parameter Store pendant le déploiement ou l'exécution.

5. Mettez en œuvre une infrastructure en tant que code (IaC):
   - Utilisez des outils d'infrastructure en tant que code tels qu'AWS CloudFormation ou AWS CDK pour définir et gérer votre infrastructure en tant que code.
   - Créez des modèles CloudFormation ou des scripts CDK pour provisionner et configurer les ressources AWS nécessaires pour votre application.
   - Intégrez l'infrastructure en tant que code à votre pipeline CI/CD pour déployer automatiquement les modifications d'infrastructure en même temps que les modifications du code d'application.
6. Mettez en œuvre des déploiements canary:
   - Configurez votre processus de déploiement pour prendre en charge les déploiements canary, dans lesquels les modifications sont appliquées à un sous-ensemble d'instances ou d'utilisateurs avant d'être déployées dans l'environnement de production tout entier.
   - Utilisez des services tels qu'AWS CodeDeploy ou AWS ECS pour gérer les déploiements canary et surveiller l'impact des modifications.
   - Mettez en œuvre des mécanismes de restauration pour pouvoir rétablir la version stable précédente si des problèmes sont détectés au cours du déploiement canary.
7. Surveillez et auditez:
   - Configurez des mécanismes de surveillance et de journalisation pour suivre les déploiements, les performances des applications et les modifications de l'infrastructure.
   - Utilisez des services tels qu'Amazon CloudWatch et AWS CloudTrail pour collecter et analyser des journaux et des métriques.
   - Mettez en œuvre des audits et des contrôles de conformité pour vérifier le respect des bonnes pratiques de sécurité et des exigences réglementaires.
8. Améliorez continuellement:
   - Passez en revue et mettez à jour régulièrement vos pratiques de déploiement et incorporez les commentaires et les enseignements tirés des déploiements précédents.
   - Automatisez autant que possible le processus de déploiement afin de réduire les interventions manuelles et les erreurs humaines potentielles.
   - Collaborez avec des équipes interfonctionnelles (par exemple, des opérations ou de la sécurité) pour aligner et améliorer continuellement les pratiques de déploiement.

En suivant ces étapes, vous pouvez mettre en œuvre des pratiques de déploiement sécurisées et automatisées dans votre environnement AWS, ce qui améliore la sécurité, réduit le risque d'erreurs humaines et rationalise le processus de déploiement.

Ressources

Bonnes pratiques associées:

- SEC11-BP02 Automatisation des tests tout au long du cycle de développement et de publication
- DL.CI.2 Déclenchement automatique de la génération lors de modifications du code source

Documents connexes:

- Accelerate deployments on AWS with effective governance
- Automating safe, hands-off deployments
- 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 bleus/verts 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 escompté : les pipelines que vous utilisez pour créer et déployer votre logiciel suivent les mêmes pratiques recommandées que toute autre charge de travail de votre environnement. Les tests que vous implémentez dans vos pipelines ne sont pas modifiables par les équipes qui les utilisent. Vous ne donnez aux pipelines que les autorisations nécessaires aux déploiements qu'ils effectuent à l'aide d'informations d'identification temporaires. Vous mettez en œuvre des protections pour empêcher les pipelines de se déployer dans les mauvais environnements. Vous configurez vos pipelines pour qu'ils émettent un état afin que l'intégrité de vos environnements de génération 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 d'exposition au risque si cette bonne pratique n'est pas respectée : élevé

Directives d'implémentation

Vos pipelines de déploiement constituent un élément essentiel du cycle de développement de votre logiciel et devraient suivre les mêmes principes et pratiques de sécurité que toute autre charge de travail dans votre environnement. Cela inclut la mise en œuvre de contrôles d'accès appropriés, la validation des entrées et l'examen et l'audit réguliers des autorisations associées à votre infrastructure CI/CD.

Vérifiez que les équipes responsables de la création et du déploiement des applications ne sont pas en mesure de modifier ou de contourner les tests et les contrôles de sécurité mis en œuvre dans vos pipelines. Cette séparation des préoccupations permet de préserver l'intégrité de vos processus de création et de déploiement.

Comme point de départ, envisagez d'utiliser l'architecture de référence des pipelines de déploiement AWS. Cette architecture de référence fournit une base sécurisée et évolutive pour la construction de vos pipelines CI/CD sur AWS.

En outre, vous pouvez utiliser des services tels qu'AWS Identity and Access Management Access Analyzer pour générer des politiques IAM de moindre privilège à la fois pour les autorisations de votre pipeline et comme étape de votre pipeline pour vérifier les autorisations de charge de travail. Cela permet de vérifier que vos pipelines et vos charges de travail disposent uniquement des autorisations nécessaires pour leurs fonctions spécifiques, ce qui réduit le risque d'accès ou d'actions non autorisés.

Étapes d'implémentation

- Commencez par l'architecture de référence des pipelines de déploiement AWS.
- Envisagez d'utiliser AWSIAM Access Analyzer pour générer par programmation des politiques IAM de moindre privilège pour les pipelines.
- Intégrez vos pipelines à la surveillance et aux alertes afin d'être averti en cas d'activité inattendue ou anormale. Pour les services gérés par AWS, Amazon EventBridge vous permet de router les données vers des cibles comme AWS Lambda ou Amazon Simple Notification Service (Amazon SNS).

Ressources

Documents connexes:

- AWS Architecture de référence des pipelines de déploiement d
- Surveillance de AWS CodePipeline
- Bonnes pratiques de sécurité pour AWS CodePipeline

Exemples connexes:

- Tableau de bord de surveillance DevOps (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 toujours valider ces décisions au cours d’un examen, mais le fait de donner la responsabilité de la sécurité aux équipes de concepteurs 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 escompté : vous avez intégré la prise en charge de la sécurité et la prise de décision dans vos équipes. Vous avez formé vos équipes à la façon de réfléchir à la sécurité ou vous avez renforcé les équipes en y intégrant ou associant des personnes chargées de la sécurité. Vos équipes prennent ainsi des décisions de meilleure qualité en matière de sécurité plus tôt dans le cycle de développement.

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

Directives d'implémentation

Commencez par suivre les instructionsSEC11-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:

- Comment aborder la modélisation des menaces
- Comment envisager la gouvernance de la sécurité dans le cloud
- Création par AWS du programme Security Guardians, un mécanisme de répartition de la prise en charge de la sécurité
- Comment créer un programme Security Guardians pour répartir la prise en charge de la sécurité

Vidéos connexes:

- Proactive security: Considerations and approaches
- Conseils relatifs à l'outillage et à la culture AppSec fournis par AWS et Toyota Motor North America

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 grâce aux fonctions programmatiques, aux AWS fonctionnalités et aux services décrits dans ce paper.

AWS s'efforce de vous aider à créer et à exploiter des architectures qui protègent les informations, les systèmes et les actifs tout en apportant une valeur commerciale.

Collaborateurs

Les personnes et organisations suivantes ont contribué à l'élaboration du présent document :

- Jay Michael, architecte principal de solutions de sécurité, Amazon Web Services
- Kiaan Sumeet, consultant principal en sécurité, Amazon Web Services
- Michael Fischer, architecte principal de solutions, Amazon Web Services
- Conor Colgan, architecte principal de solutions, Amazon Web Services
- Dave Walker, architecte de solutions principal, sécurité et conformité, Amazon Web Services
- Patrick Palmer, architecte de solutions principal, sécurité et conformité, Amazon Web Services
- Monka Vu Minh, consultante en sécurité, Amazon Web Services
- Kurt Kumar, Senior Security Consultant, Amazon Web Services
- Fahima Khan, architecte des solutions de sécurité, Amazon Web Services
- Mutaz Hajeer, architecte des solutions de sécurité, Amazon Web Services
- Luis Pastor, architecte des solutions de sécurité, Amazon Web Services
- Colin Igbokwe, architecte des solutions de sécurité, Amazon Web Services
- Geoff Sweet, architecte des solutions de sécurité, Amazon Web Services
- Anthony Harvey, architecte des solutions de sécurité, Amazon Web Services
- Sowjanya Rajavaram, architecte des solutions de sécurité, Amazon Web Services
- Krishna Prasad, architecte principal de solutions, Amazon Web Services
- Faisal Farooq, architecte principal de solutions, Amazon Web Services
- Arun Krishnaswamy, architecte principal de solutions, Amazon Web Services
- Dan Girard, architecte principal de solutions, Amazon Web Services
- Marc Luescher, architect principal de solutions, Amazon Web Services
- Kyle Nicodemus, responsable technique de compte principal, Amazon Web Services
- Irina Szabo, responsable technique de compte principal, Amazon Web Services
- Arun Sivaraman, architecte de solutions principal, Amazon Web Services
- Stephen Novak, gestionnaire des comptes techniques, Amazon Web Services
- Jonathan Risbrook, gestionnaire des comptes techniques, Amazon Web Services
- Freddy Kasprzykowski, responsable des services financiers mondiaux, Amazon Web Services
- Pat Gaw, consultant principal en sécurité, Amazon Web Services

- Jason Garman, architecte principal de solutions de sécurité, Amazon Web Services
- Mark Keating, architecte principal de solutions de sécurité, Amazon Web Services
- Zach Miller, architecte principal de solutions de sécurité, Amazon Web Services
- Maitreya Ranganath, architecte principal de solutions de sécurité, Amazon Web Services
- Reef Dsouza, architecte principal de solutions, Amazon Web Services
- Brad Burnett, architecte des solutions de sécurité, Amazon Web Services
- Matt Saner, directeur principal de l'architecture des solutions de sécurité, Amazon Web Services
- Priyank Ghedia, architecte des solutions de sécurité, Amazon Web Services
- Arthur Mnev, architecte des solutions de sécurité, Amazon Web Services
- Kyle Dickinson, architecte des solutions de sécurité, Amazon Web Services
- Kevin Boland, architecte des solutions de sécurité, Amazon Web Services
- Anna McAbee, architecte des solutions de sécurité, Amazon Web Services
- Recep Meric Degirmenci, architecte senior des solutions de sécurité, Amazon Web Services
- Daniel Salzedo, responsable principal des produits techniques de sécurité, Amazon Web Services
- Jake Izumi, architecte principal de solutions, Amazon Web Services
- Bert Bullough, architecte principal de solutions, Amazon Web Services
- Robert McCall, architecte de solutions, Amazon Web Services
- Angela Chao, ESL TAM, AWS Support aux entreprises, Amazon Web Services
- Pratima Singh, spécialiste senior de la sécurité ANZ architecte de solutions principal, Amazon Web Services
- Darran Boyd, principal, bureau du RSSI, sécurité AWS, Amazon Web Services
- Byron Pogson, architecte des solutions de sécurité, Amazon Web Services

Suggestions de lecture

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 avec de nouvelles directives dans les domaines suivants : SEC 2, SEC 3, SEC 4, SEC 6, SEC 7, SEC 8, SEC 9, SEC 10 et SEC 11. Les directives ont été mises à jour et affinées dans l'ensemble du pilier.	6 novembre 2024
Mises à jour des conseils sur les bonnes pratiques	Des mises à jour à grande échelle des bonnes pratiques ont été effectuées dans l'ensemble du pilier. Plusieurs bonnes pratiques réorganisées et consolidées. Changements significatifs dans les SEC 1, 4, 5, 6, 7, 8 et 9.	27 juin 2024
Mises à jour des conseils sur les bonnes pratiques	Les bonnes pratiques ont été mises à jour avec de nouvelles directives dans les domaines suivants : gestion sécurisée de vos charges de travail et protection des données en transit.	6 décembre 2023
Mises à jour des conseils sur les bonnes pratiques	Mises à jour majeures des conseils et des bonnes pratiques dans Intervention en cas d'incident.	3 octobre 2023

	Mises à jour de plusieurs bonnes pratiques dans Préparation. Deux nouveaux domaines ont été ajoutés à la réponse aux incidents : les opérations et les activités après l'incident. Nouvelle bonne pratique : SEC10-BP08 Établir un cadre pour tirer des enseignements des incidents.	
Mises à jour des conseils sur les bonnes pratiques	Les bonnes pratiques ont été mises à jour avec de nouveaux conseils dans les domaines suivants : préparation et simulation.	13 juillet 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).	10 avril 2023
Livre blanc mis à jour	Les bonnes pratiques ont été mises à jour avec de nouvelles recommandations en matière d'implémentation.	15 décembre 2022
Livre blanc mis à jour	Développement des bonnes pratiques et ajout de plans d'amélioration.	20 octobre 2022
Mise à jour mineure	Mise à jour des informations IAM pour refléter les bonnes pratiques actuelles.	28 juin 2022

Mise à jour mineure	Ajout d'informations AWS PrivateLink supplémentaires et correction des liens corrompus .	19 mai 2022
Mise à jour mineure	Ajouté AWS PrivateLink.	6 mai 2022
Mise à jour mineure	Suppression du langage non inclusif.	22 avril 2022
Mise à jour mineure	Ajout d'informations sur l'nalyseur d'accès réseau du VPC.	2 février 2022
Mise à jour mineure	Correction d'un lien rompu.	27 mai 2021
Mise à jour mineure	Modifications rédactionnelles dans tout le document.	17 mai 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.	7 mai 2021
Mise à jour mineure	Mise à jour des liens.	10 mars 2021
Mise à jour mineure	Correction d'un lien rompu.	15 juillet 2020
Mises à jour du nouveau cadre	Mise à jour des conseils sur la gestion des comptes, des identités et des autorisations.	8 juillet 2020

Mises à jour du 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.	30 avril 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.	1er juillet 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.	1er mai 2017
Publication initiale	Pilier Sécurité - AWS Well-Architected Framework publié.	1er novembre 2016

Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de AWS produits et les pratiques actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations AWS de ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne les modifie pas.

© 2023, Amazon Web Services, Inc. ou ses sociétés apparentées. Tous droits réservés.

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.