Création d'un programme de gestion des vulnérabilités évolutif sur AWS

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Création d'un programme de gestion des vulnérabilités évolutif sur AWS

Table of Contents

Introduction 1
Public visé 2
Objectifs 2
Préparation 4
Définir un plan 4
Distribuer la propriété 5
Élaboration d'un programme de divulgation 7
Préparez votre environnement 8
Compte AWS structure 8
Balises 9
Bulletins de surveillance 10
Configuration des services de sécurité 10
Amazon Inspector 11
AWS Security Hub 12
Préparez-vous à attribuer les résultats 15
Utiliser les outils existants 15
Utilisation de Security Hub 17
Triage et correction 18
Attribuer les résultats 18
Évaluer et hiérarchiser les résultats 20
Corriger les résultats 21
Exemples 23
Exemple d'équipe de sécurité 23
Exemple d'équipe cloud 24
Exemple d'équipe de candidature 25
Signaler et améliorer 28
Réunions sur les opérations de sécurité 28
Informations sur le Security Hub 28
Conclusion et étapes suivantes 30
Ressources 32
AWS documentation de service 32
Autres AWS ressources 32
Historique du document 33
Glossaire 34

..... 34
A 35
B 38
C 40
D 43
E 48
F 50
G 51
H 52
I 54
L 56
M 57
O 62
P 64
Q 67
R 68
S 70
T 74
U 76
V 76
W 77
Z 78
..... lxxix

Création d'un programme de gestion des vulnérabilités évolutif sur AWS

Anna McAbee et Megan O'Neil, Amazon Web Services ()AWS

Octobre 2023 (historique du document)

Selon la technologie sous-jacente que vous utilisez, divers outils et analyses peuvent générer des résultats de sécurité dans un environnement cloud. Si aucun processus n'est en place pour traiter ces résultats, ils peuvent commencer à s'accumuler, aboutissant souvent à des milliers, voire à des dizaines de milliers de résultats en peu de temps. Toutefois, grâce à un programme structuré de gestion des vulnérabilités et à l'opérationnalisation appropriée de vos outils, votre entreprise peut gérer et trier un grand nombre de résultats provenant de sources diverses.

La gestion des vulnérabilités se concentre sur la découverte, la hiérarchisation, l'évaluation, la correction et le signalement des vulnérabilités. La gestion des correctifs, quant à elle, se concentre sur l'application de correctifs ou la mise à jour de logiciels afin de supprimer ou de corriger les failles de sécurité. La gestion des correctifs n'est qu'un aspect de la gestion des vulnérabilités. En général, nous recommandons d'établir à la fois un patch-in-place processus (également appelé mitigate-in-placeprocessus) pour traiter les scénarios critiques nécessitant la mise à jour immédiate, et un processus standard que vous exécuterez régulièrement afin de publier des Amazon Machine Images (AMI), des conteneurs ou des packages logiciels Amazon corrigés. Ces processus aident votre entreprise à réagir rapidement à une vulnérabilité de type « jour zéro ». Pour les systèmes critiques d'un environnement de production, l'utilisation d'un patch-in-place processus peut être plus rapide et plus fiable que le déploiement d'une nouvelle AMI au sein du parc. Pour les correctifs régulièrement programmés, tels que les correctifs de système d'exploitation (OS) et de logiciels, nous vous recommandons de créer et de tester à l'aide de processus de développement standard, comme vous le feriez pour toute modification logicielle. Cela permet une meilleure stabilité pour les modes de fonctionnement standard. Vous pouvez utiliser Patch Manager, une fonctionnalité de AWS Systems Manager ou d'autres produits tiers comme patch-in-place solutions. Pour plus d'informations sur l'utilisation de Patch Manager, voir Gestion des correctifs dans AWS Cloud Adoption Framework : Operations Perspective. Vous pouvez également utiliser EC2 Image Builder pour automatiser la création, la gestion et le déploiement d'images personnalisées up-to-date et d'images de serveur.

L'élaboration d'un programme de gestion des vulnérabilités évolutif AWS implique de gérer les vulnérabilités logicielles et réseau traditionnelles, en plus des risques liés à la configuration du

cloud. Un risque lié à la configuration du cloud, tel qu'un bucket Amazon Simple Storage Service (Amazon S3) non chiffré, doit suivre un processus de triage et de correction similaire à celui d'une vulnérabilité logicielle. Dans les deux cas, l'équipe d'application doit être propriétaire de la sécurité de son application, y compris de l'infrastructure sous-jacente, et en être responsable. Cette distribution de propriété est essentielle pour un programme de gestion des vulnérabilités efficace et évolutif.

Ce guide explique comment rationaliser l'identification et la correction des vulnérabilités afin de réduire le risque global. Utilisez les sections suivantes pour créer et itérer votre programme de gestion des vulnérabilités :

1. Préparation : préparez votre personnel, vos processus et votre technologie pour identifier, évaluer et corriger les vulnérabilités de votre environnement.
2. Triage et correction : transmettez les résultats de sécurité aux parties prenantes concernées, identifiez les mesures correctives appropriées, puis prenez les mesures correctives.
3. Créez des rapports et améliorez : utilisez des mécanismes de reporting pour identifier les opportunités d'amélioration, puis répétez votre programme de gestion des vulnérabilités.

L'élaboration d'un programme de gestion des vulnérabilités dans le cloud implique souvent des itérations. Classez les recommandations par ordre de priorité dans ce guide et revoyez régulièrement votre carnet de commandes pour rester au fait des évolutions technologiques et des exigences de votre entreprise.

Public visé

Ce guide est destiné aux grandes entreprises qui ont trois équipes principales responsables des découvertes liées à la sécurité : une équipe de sécurité, une équipe Cloud Center of Excellence (CCoE) ou une équipe cloud, et des équipes chargées des applications (ou des développeurs). Ce guide utilise les modèles d'exploitation d'entreprise les plus courants et s'appuie sur ces modèles d'exploitation pour permettre une réponse plus efficace aux constatations de sécurité et améliorer les résultats en matière de sécurité. Les organisations AWS qui l'utilisent peuvent avoir des structures et des modèles opérationnels différents ; toutefois, vous pouvez modifier de nombreux concepts de ce guide pour les adapter à différents modèles opérationnels et à de plus petites organisations.

Objectifs

Ce guide peut vous aider, vous et votre organisation, à :

- Élaborez des politiques pour rationaliser la gestion des vulnérabilités et garantir la responsabilisation
- Mettre en place des mécanismes pour répartir la responsabilité de la sécurité entre les équipes chargées des applications
- Configurez de manière appropriée AWS services conformément aux meilleures pratiques pour une gestion évolutive des vulnérabilités
- Répartissez la propriété des résultats de sécurité
- Établissez des mécanismes pour établir des rapports et itérer votre programme de gestion des vulnérabilités
- Améliorez la visibilité des résultats de sécurité et améliorez la posture de sécurité globale

Préparez votre programme évolutif de gestion des vulnérabilités

La préparation à l'élaboration d'un programme de gestion des vulnérabilités évolutif implique de former le personnel, de développer des processus et de mettre en œuvre la technologie appropriée conformément aux meilleures pratiques. Les personnes, les processus et les technologies sont tout aussi importants pour un programme de gestion des vulnérabilités efficace, et vous devez les intégrer étroitement pour gérer les vulnérabilités à grande échelle.

Cette section du guide passe en revue les mesures de base que vous pouvez prendre pour préparer votre programme évolutif de gestion des vulnérabilités. AWS

Rubriques

- Définir un plan de gestion des vulnérabilités
- Répartissez la propriété des titres
- Élaboration d'un programme de divulgation des vulnérabilités
- Préparez votre AWS environnement
- Surveillez les bulletins AWS de sécurité
- Configuration des services AWS de sécurité
- Préparez-vous à attribuer les résultats de sécurité

Définir un plan de gestion des vulnérabilités

La première étape de la préparation de votre programme de gestion des vulnérabilités dans le cloud consiste à définir votre plan de gestion des vulnérabilités. Ce plan inclut les politiques et les processus suivis par votre organisation. Ce plan doit être documenté et accessible à toutes les parties prenantes. Un plan de gestion des vulnérabilités est un document de haut niveau qui comprend généralement les sections suivantes :

- Objectifs et champ d'application — Décrivez les objectifs, les fonctions et le champ d'application de la gestion des vulnérabilités.
- Rôles et responsabilités — Répertoriez les parties prenantes de la gestion des vulnérabilités et détaillez leurs responsabilités.

- Définitions de la gravité et de la hiérarchisation des vulnérabilités : déterminez comment classer la gravité d'une vulnérabilité et comment la prioriser.
- Contrats de niveau de service (SLA) pour la correction : pour chaque niveau de gravité, définissez le délai maximal dont dispose le responsable de la correction pour résoudre un problème de sécurité. La conformité aux SLA faisant partie intégrante d'un programme de gestion des vulnérabilités efficace et évolutif, réfléchissez à la manière de vérifier si vous respectez ces SLA.
- Processus d'exception : détaillez le processus de soumission, d'approbation et de mise à jour des exceptions. Ce processus doit garantir que les exceptions sont légitimes, limitées dans le temps et suivies.
- Sources d'informations sur les vulnérabilités — Répertoriez les sources ou les outils qui génèrent des résultats de sécurité. Pour plus d'informations sur AWS services ce qui pourrait être une source de résultats de sécurité, consultez Configuration des services AWS de sécurité ce guide.

Bien que ces sections soient communes à toutes les entreprises de tailles et de secteurs d'activité différents, le plan de gestion des vulnérabilités de chaque organisation est unique. Vous devez élaborer un plan de gestion des vulnérabilités qui convient le mieux à votre organisation. Attendez-vous à réitérer votre plan au fil du temps pour intégrer les leçons apprises et l'évolution des technologies.

Répartissez la propriété des titres

Le modèle de responsabilitéAWS partagée définit comment AWS et ses clients partagent la responsabilité en matière de sécurité et de conformité dans le cloud. Dans ce modèle, AWS sécurise l'infrastructure qui exécute tous les services proposés dans le AWS Cloud, et les AWS clients sont responsables de la sécurisation de leurs données et de leurs applications.

Vous pouvez reproduire ce modèle au sein de votre organisation et répartir les responsabilités entre vos équipes chargées du cloud et des applications. Cela vous permet de faire évoluer vos programmes de sécurité dans le cloud de manière plus efficace, car les équipes chargées des applications prennent en charge certains aspects de sécurité de leurs applications. L'interprétation la plus simple du modèle de responsabilité partagée est que si vous avez accès à la configuration de la ressource, vous êtes responsable de la sécurité de cette ressource.

Pour répartir les responsabilités en matière de sécurité entre les équipes chargées des applications, il est essentiel de créer des outils de sécurité en libre-service qui aident les équipes chargées des applications à automatiser leurs tâches. Au départ, cela peut être un effort conjoint. L'équipe

de sécurité peut traduire les exigences de sécurité en outils d'analyse de code, puis les équipes d'application peuvent utiliser ces outils pour créer et partager des solutions avec leur communauté interne de développeurs. Cela contribue à améliorer l'efficacité des autres équipes qui doivent répondre à des exigences de sécurité similaires.

Le tableau suivant décrit les étapes à suivre pour attribuer la propriété aux équipes chargées des applications et fournit des exemples.

Étape	Action	Exemple
1	Définissez vos exigences en matière de sécurité — Quel est votre objectif ? Cela peut être dû à une norme de sécurité ou à une exigence de conformité.	Un exemple d'exigence de sécurité est l'accès au moindre privilège pour les identités d'applications.
2	Énumérer les contrôles pour une exigence de sécurité — Que signifie réellement cette exigence du point de vue du contrôle ? Que dois-je faire pour y parvenir ?	Pour obtenir le moindre privilège pour les identités d'applications, voici deux exemples de contrôles : • Utiliser des AWS Identity and Access Management rôles (IAM) • N'utilisez pas de caractères génériques dans les politiques IAM
3	Documenter les directives relatives aux contrôles — Avec ces contrôles, quels conseils pouvez-vous fournir à un développeur pour l'aider à se conformer au contrôle ?	Dans un premier temps, vous pouvez commencer par documenter des exemples de politiques simples, notamment des politiques IAM sécurisées et non sécurisées et des politiques de compartiment Amazon Simple Storage

Étape	Action	Exemple
		Service (Amazon S3). Vous pouvez ensuite intégrer des solutions d'analyse des politiques dans des pipelines d'intégration continue et de livraison continue (CI/CD), par exemple en utilisant des AWS Config règles pour une évaluation proactive.
4	Développez des artefacts réutilisables — Avec ces conseils, pouvez-vous rendre les choses encore plus faciles et développer des artefacts réutilisables pour les développeurs ?	Vous pouvez créer une infrastructure sous forme de code (IaC) pour déployer des politiques IAM conformes au principe du moindre privilège . Vous pouvez stocker ces artefacts réutilisables dans un référentiel de code.

Le libre-service peut ne pas répondre à toutes les exigences de sécurité, mais il peut fonctionner pour les scénarios standard. En suivant ces étapes, les entreprises peuvent donner à leurs équipes d'application les moyens de gérer une plus grande partie de leurs propres responsabilités en matière de sécurité de manière évolutive. Dans l'ensemble, le modèle de responsabilité distribuée conduit à des pratiques de sécurité plus collaboratives au sein de nombreuses organisations.

Élaboration d'un programme de divulgation des vulnérabilités

Pour une defense-in-depthapproche de gestion des vulnérabilités, créez un programme de divulgation des vulnérabilités afin que les personnes internes ou externes à votre organisation puissent signaler les vulnérabilités ou les risques de sécurité.

Pour les membres de votre organisation, établissez un processus pour signaler les risques ou les vulnérabilités. Cela peut se faire par le biais d'un système de billetterie ou par e-mail. Quel que soit le processus que vous choisissez, il est essentiel que vos employés soient au courant du processus et puissent facilement signaler les vulnérabilités ou les risques qu'ils rencontrent.

Pour les personnes extérieures à votre organisation, créez une page Web externe pour signaler les vulnérabilités de sécurité potentielles. À titre d'exemple, consultez la page Web sur les rapports de AWS vulnérabilité. Cette page Web doit également contenir des directives de divulgation visant à protéger les données et les actifs de votre organisation. Un programme de divulgation des vulnérabilités ne doit pas encourager les activités potentiellement dangereuses. Il est donc essentiel que vous disposiez d'une politique claire et de directives. La mise en place d'un programme de divulgation mature et responsable est un objectif à atteindre au fur et à mesure que vous développez votre programme. La plupart ne commencent pas par un programme de divulgation externe, et il faut du temps pour bien faire les choses.

Préparez votre AWS environnement

Avant de mettre en œuvre un outil de gestion des vulnérabilités, assurez-vous que votre AWS environnement est conçu pour prendre en charge un programme de gestion des vulnérabilités évolutif. La structure de vos politiques de balisage Comptes AWS et de celles de votre entreprise peut simplifier le processus de création d'un programme de gestion des vulnérabilités évolutif.

Développement d'une Compte AWS structure

AWS Organizationspermet de gérer et de gouverner de manière centralisée un AWS environnement au fur et à mesure que votre entreprise se développe et fait évoluer ses AWS ressources. Une organisation vous AWS Organizations consolide Comptes AWS en groupes logiques, ou unités organisationnelles, afin que vous puissiez les administrer en tant qu'unité unique. Vous gérez AWS Organizations à partir d'un compte dédié, appelé compte de gestion. Pour plus d'informations, veuillez consulter la rubrique Terminologie et concepts AWS Organizations.

Nous vous recommandons de gérer votre environnement AWS multi-comptes dans AWS Organizations. Cela permet de créer un inventaire complet des comptes et des ressources de votre entreprise. Cet inventaire complet des actifs est un aspect essentiel de la gestion des vulnérabilités. Les équipes de candidature ne doivent pas utiliser de comptes extérieurs à l'organisation.

AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives. Si vous n'avez pas encore créé d'environnement multi-comptes, AWS Control Tower c'est un bon point de départ.

Nous vous recommandons d'utiliser la structure de compte dédiée et les meilleures pratiques décrites dans l'architecture AWS de référence de sécurité (AWS SRA). Le compte Security Tooling doit servir

d'administrateur délégué pour vos services de sécurité. Plus d'informations sur la configuration de vos outils de gestion des vulnérabilités dans ce compte sont fournies plus loin dans ce guide. Hébergez les applications dans des comptes dédiés au sein de l'unité organisationnelle (UO) des charges de travail. Cela permet d'établir une forte isolation au niveau de la charge de travail et des limites de sécurité explicites pour chaque application. Pour plus d'informations sur les principes de conception et les avantages de l'utilisation d'une approche multi-comptes, voir Organiser votre AWS environnement à l'aide de plusieurs comptes (AWS livre blanc).

Disposer d'une structure de compte intentionnelle et gérer de manière centralisée les services de sécurité à partir d'un compte dédié sont des aspects essentiels d'un programme de gestion des vulnérabilités évolutif.

Définition, mise en œuvre et application des balises

Les balises sont des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources. Vous pouvez utiliser des balises pour fournir un contexte métier, tel que l'unité commerciale, le propriétaire de l'application, l'environnement et le centre de coûts. Le tableau suivant présente un ensemble d'exemples de balises.

Clé	Valeur
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
Environnement	Production

Les balises peuvent vous aider à hiérarchiser les résultats. Par exemple, cela peut vous aider à :

- Identifier le propriétaire d'une ressource chargé de corriger une vulnérabilité
- Suivez les applications ou les unités commerciales contenant un grand nombre de résultats
- Accroître la sévérité des résultats pour certaines classifications de données, telles que les informations personnelles identifiables (PII) ou les données du secteur des cartes de paiement (PCI)

- Identifiez le type de données dans l'environnement, telles que les données de test dans un environnement de développement de niveau inférieur ou les données de production

Pour vous aider à obtenir un balisage efficace à grande échelle, suivez les instructions de la section Élaborer votre stratégie de balisage dans Meilleures pratiques pour les AWS ressources de balisage (AWS livre blanc).

Surveillez les bulletins AWS de sécurité

Nous vous recommandons vivement AWS de consulter régulièrement et fréquemment les bulletins de sécurité. Les bulletins de sécurité peuvent vous informer de toute nouvelle vulnérabilité liée à la sécurité, des services concernés et des mises à jour applicables. Vous pouvez également vous abonner à un flux RSS pour les bulletins de sécurité et créer un processus pour intégrer et traiter ces bulletins dans le cadre de votre programme de gestion des vulnérabilités.

Configuration des services AWS de sécurité

AWS propose une variété de services de sécurité conçus pour protéger votre AWS environnement. Pour votre programme de gestion des vulnérabilités, nous vous recommandons d'activer les éléments suivants AWS services dans chaque compte :

- Amazon GuardDuty aide à détecter les menaces actives dans votre environnement. Une GuardDuty découverte pourrait vous aider à identifier une vulnérabilité inconnue qui a été exploitée dans votre environnement. Cela peut également vous aider à comprendre les effets d'une vulnérabilité non corrigée.
- AWS Healthfournit une visibilité continue sur les performances de vos ressources et sur la disponibilité de vos comptes AWS services et de vos comptes.
- AWS Identity and Access Management Access Analyzeranalyse les politiques basées sur les ressources de votre AWS environnement afin d'identifier les ressources partagées avec une entité externe. Cela peut vous aider à identifier les vulnérabilités associées à un accès involontaire à vos ressources et à vos données. Pour chaque instance d'une ressource qui est partagée en dehors de votre compte, l'IAM Access Analyzer génère un résultat.
- Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos AWS charges de travail pour détecter les vulnérabilités logicielles et les risques d'exposition involontaire au réseau.

- AWS Security Hubvous permet de vérifier que votre AWS environnement est conforme aux normes du secteur de la sécurité et d'identifier les risques liés à la configuration du cloud. Il fournit également une vue complète de votre état de AWS sécurité en agrégeant les résultats d'autres services de AWS sécurité et d'outils de sécurité tiers.

Cette section explique comment activer et configurer Amazon Inspector et Security Hub pour vous aider à établir un programme de gestion des vulnérabilités évolutif.

Utilisation d'Amazon Inspector dans votre programme de gestion des vulnérabilités

Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos instances Amazon Elastic Compute Cloud (Amazon EC2), les images de conteneur Amazon Elastic Container Registry (Amazon ECR) et les fonctions pour détecter les vulnérabilités logicielles et les expositions AWS Lambda involontaires au réseau. Vous pouvez utiliser Amazon Inspector pour gagner en visibilité et prioriser la résolution des vulnérabilités logicielles dans vos AWS environnements.

Amazon Inspector évalue en permanence votre environnement tout au long du cycle de vie de vos ressources. Il réanalyse automatiquement les ressources en réponse aux modifications susceptibles d'introduire une nouvelle vulnérabilité. Par exemple, il effectue une nouvelle analyse lorsque vous installez un nouveau package sur une instance EC2, lorsque vous installez un correctif ou lorsqu'un nouveau code CVE (Common Vulnerabilities and Exposures) affectant la ressource est publié. Lorsqu'Amazon Inspector identifie une vulnérabilité ou un chemin réseau ouvert, il produit un résultat que vous pouvez examiner. Le résultat fournit des informations complètes sur la vulnérabilité, notamment les suivantes :

- Score de risque d'Amazon Inspector
- Score du Common Vulnerability Scoring System (CVSS)
- Ressource affectée
- données de renseignement sur les vulnérabilités concernant le CVE fournies par Amazon Recorded Future, et Cybersecurity and Infrastructure Security Agency (CISA)
- Recommandations en matière de mesures correctives

Pour obtenir des instructions sur la configuration d'Amazon Inspector, consultez Getting started with Amazon Inspector. L'étape Activer Amazon Inspector de ce didacticiel propose deux options de

configuration : un environnement de compte autonome et un environnement multi-comptes. Nous vous recommandons d'utiliser l'option d'environnement multi-comptes si vous souhaitez surveiller plusieurs Comptes AWS membres d'une organisation dans AWS Organizations.

Lorsque vous configurez Amazon Inspector pour un environnement multi-comptes, vous désignez un compte de l'organisation comme administrateur délégué d'Amazon Inspector. L'administrateur délégué peut gérer les résultats et certains paramètres pour les membres de l'organisation. Par exemple, l'administrateur délégué peut consulter le détail des résultats agrégés pour tous les comptes des membres, activer ou désactiver les scans pour les comptes des membres et examiner les ressources numérisées. La AWS SRA vous recommande de créer un compte Security Tooling et de l'utiliser en tant qu'administrateur délégué d'Amazon Inspector.

Utilisation AWS Security Hub dans votre programme de gestion des vulnérabilités

L'élaboration d'un programme de gestion des vulnérabilités évolutif AWS implique de gérer les vulnérabilités logicielles et réseau traditionnelles, en plus des risques liés à la configuration du cloud. AWS Security Hubvous permet de vérifier que votre AWS environnement est conforme aux normes du secteur de la sécurité et d'identifier les risques liés à la configuration du cloud. Security Hub fournit également une vue complète de votre état de sécurité en AWS agrégeant les résultats de sécurité provenant d'autres services de AWS sécurité et d'outils de sécurité tiers.

Dans les sections suivantes, nous présentons les meilleures pratiques et les recommandations relatives à la configuration de Security Hub afin de soutenir votre programme de gestion des vulnérabilités :

- Configuration de Security Hub
- Mise en œuvre des normes du Security Hub
- Gérer les résultats du Security Hub
- Agrégation des résultats provenant d'autres services et outils de sécurité

Configuration de Security Hub

Pour les instructions de configuration, voir Configuration AWS Security Hub. Pour utiliser Security Hub, vous devez l'activer AWS Config. Pour plus d'informations, consultez la section Activation et configuration AWS Config dans la documentation du Security Hub.

Si vous êtes intégré à AWS Organizations, depuis le compte de gestion de l'organisation, vous désignez un compte comme administrateur délégué du Security Hub. Pour obtenir des instructions, consultez la section Désignation de l'administrateur délégué du Security Hub. La AWS SRA vous recommande de créer un compte Security Tooling et de l'utiliser en tant qu'administrateur délégué du Security Hub.

L'administrateur délégué a automatiquement accès à la configuration de Security Hub pour tous les comptes membres de l'organisation et à la consultation des résultats associés à ces comptes. Nous vous recommandons d'activer AWS Config Security Hub dans tous Régions AWS vos Comptes AWS. Vous pouvez configurer Security Hub pour traiter automatiquement les nouveaux comptes d'organisation comme des comptes membres du Security Hub. Pour obtenir des instructions, consultez la section Gestion des comptes des membres appartenant à une organisation.

Mise en œuvre des normes du Security Hub

Security Hub génère des résultats en effectuant des contrôles de sécurité automatisés et continus par rapport aux contrôles de sécurité. Les commandes sont associées à une ou plusieurs normes de sécurité. Les contrôles vous aident à déterminer si les exigences d'une norme sont respectées.

Lorsque vous activez une norme dans Security Hub, Security Hub active automatiquement les contrôles qui s'appliquent à la norme. Security Hub utilise des AWS Config règles pour effectuer la plupart de ses contrôles de sécurité. Vous pouvez activer ou désactiver les normes Security Hub à tout moment. Pour plus d'informations, consultez la section Contrôles et normes de sécurité dans AWS Security Hub. Pour une liste complète des normes, consultez la référence des normes Security Hub.

Si votre organisation n'a pas encore de norme de sécurité préférée, nous vous recommandons d'utiliser la norme AWS Foundational Security Best Practices (FSBP). Cette norme est conçue pour détecter quand Comptes AWS et quand les ressources s'écartent des meilleures pratiques en matière de sécurité. AWS organise cette norme et la met régulièrement à jour pour couvrir les nouvelles fonctionnalités et les nouveaux services. Après avoir trié les résultats du FSBP, envisagez d'activer d'autres normes.

Gérer les résultats du Security Hub

Security Hub propose plusieurs fonctionnalités qui vous aident à traiter un grand nombre de résultats provenant de l'ensemble de votre organisation et à comprendre l'état de sécurité de votre AWS environnement. Pour vous aider à gérer les résultats, nous vous recommandons d'activer les deux fonctionnalités de Security Hub suivantes :

- Utilisez l'agrégation entre régions pour agréger les résultats, trouver des mises à jour, des informations, contrôler les statuts de conformité et les scores de sécurité de plusieurs régions d'agrégation Régions AWS à une seule.
- Utilisez les résultats de contrôle consolidés pour réduire le bruit de recherche en supprimant les résultats dupliqués. Lorsque les résultats de contrôle consolidés sont activés dans votre compte, Security Hub génère une seule nouvelle découverte ou mise à jour pour chaque contrôle de sécurité d'un contrôle, même si un contrôle s'applique à plusieurs normes activées.

Agrégation des résultats provenant d'autres services et outils de sécurité

Outre la génération de résultats de sécurité, vous pouvez utiliser Security Hub pour agréger les données de recherche provenant de plusieurs solutions AWS services de sécurité tierces prises en charge. Cette section se concentre sur l'envoi de résultats de sécurité à Security Hub. La section suivante explique comment intégrer Security Hub à des produits qui peuvent recevoir les résultats de Security Hub. Préparez-vous à attribuer les résultats de sécurité

Il existe de nombreux AWS services produits tiers et solutions open source que vous pouvez intégrer à Security Hub. Si vous ne faites que commencer, nous vous recommandons de procéder comme suit :

1. Activer l'intégration AWS services : la plupart AWS service des intégrations qui envoient des résultats à Security Hub sont automatiquement activées une fois que vous avez activé Security Hub et le service intégré. Pour votre programme de gestion des vulnérabilités, nous vous recommandons d'activer Amazon Inspector GuardDuty AWS Health, Amazon et IAM Access Analyzer dans chaque compte. Ces services envoient automatiquement leurs résultats à Security Hub. Pour obtenir la liste complète des AWS service intégrations prises en charge, consultez la section AWS services qui envoie les résultats à Security Hub.

   > **Note**
   >
   > AWS Health envoie les résultats à Security Hub si l'une des conditions suivantes est remplie :
   >
   > - La découverte est associée à un service AWS de sécurité
   > - Le code de type de recherche contient les mots`security`, ou `abuse` `certificate`
   > - Le AWS Health service de recherche est `risk` ou `abuse`

2. Configurer des intégrations tierces : pour obtenir la liste des intégrations actuellement prises en charge, voir Intégrations de produits partenaires tiers disponibles. Sélectionnez tous les outils supplémentaires qui peuvent envoyer des résultats à Security Hub ou en recevoir. Vous possédez peut-être déjà certains de ces outils tiers. Suivez les instructions du produit pour configurer l'intégration avec Security Hub.

Préparez-vous à attribuer les résultats de sécurité

Dans cette section, vous configurez les outils que vos équipes utilisent pour gérer et attribuer les résultats de sécurité. Cette section inclut les options suivantes :

- Gérez les résultats dans les outils et les flux de travail existants— Cette option s'intègre AWS Security Hub aux systèmes existants que vos équipes utilisent pour gérer leurs tâches quotidiennes, tels que le carnet de produits. Cette option est recommandée pour les équipes qui ont mis en place des outils pour gérer leurs flux de travail.
- Gérez les résultats dans Security Hub— Cette option configure les notifications relatives aux événements du Security Hub afin que l'équipe appropriée reçoive une alerte et puisse traiter la découverte dans Security Hub.

Décidez quel flux de travail convient le mieux à vos équipes et assurez-vous que les résultats de sécurité peuvent être transmis rapidement à leurs propriétaires respectifs.

Gérez les résultats dans les outils et les flux de travail existants

Nous recommandons des intégrations supplémentaires à Security Hub pour les entreprises qui ont mis en place des outils que les équipes utilisent pour gérer ou effectuer leurs tâches quotidiennes. Vous pouvez importer les données de recherche de Security Hub sur plusieurs plateformes technologiques. En voici quelques exemples :

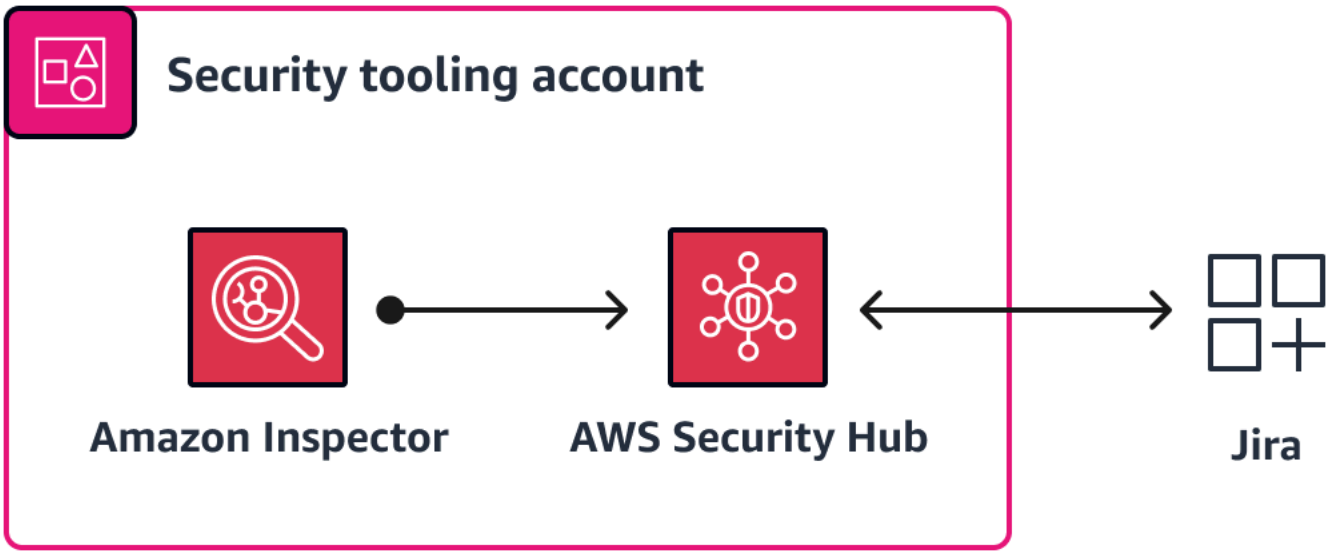
- Les systèmes de gestion des informations et des événements de sécurité (SIEM) aident les équipes de sécurité à trier les événements de sécurité opérationnels. Les systèmes SIEM fournissent une analyse en temps réel des alertes de sécurité générées par les applications et le matériel réseau.
- Les systèmes de gouvernance, de gestion des risques et de conformité (GRC) aident les équipes chargées de la conformité et de la gouvernance à surveiller les données de gestion des risques et à établir des rapports à ce sujet. Les outils GRC sont des applications logicielles que les

entreprises peuvent utiliser pour gérer les politiques, évaluer les risques, contrôler l'accès des utilisateurs et rationaliser la conformité. Vous pouvez utiliser les outils GRC pour intégrer les processus métier, réduire les coûts et améliorer l'efficacité.

- Les systèmes de gestion des carnets de produits et de billetterie aident les équipes chargées des applications et du cloud à gérer les fonctionnalités et à hiérarchiser les tâches de développement. Atlassian Jiraet Microsoft Azure DevOpssont des exemples de ces systèmes.

L'intégration directe des résultats du Security Hub à ces systèmes d'entreprise existants peut améliorer le temps moyen de restauration (MTTR) et les résultats en matière de sécurité, car le flux de travail opérationnel quotidien n'a pas à changer. Les équipes peuvent réagir et tirer des enseignements des résultats de sécurité beaucoup plus rapidement, car elles n'ont pas à utiliser des flux de travail et des outils distincts. Grâce à l'intégration, le traitement des problèmes de sécurité fait partie du flux de travail standard normal.

Security Hub s'intègre à plusieurs produits partenaires tiers. Pour obtenir une liste complète et des instructions, consultez la section Intégrations de produits partenaires tiers disponibles dans la documentation de Security Hub. Les intégrations courantes incluent Atlassian - Jira Service Management, l'intégration bidirectionnelle AWS Security Hub avec le Jira logiciel, et. ServiceNow – ITSM Le schéma suivant montre comment configurer Amazon Inspector pour envoyer les résultats à Security Hub, puis configurer Security Hub pour envoyer tous les résultats àJira.



Gérez les résultats dans Security Hub

Vous pouvez créer un système de notification basé sur le cloud pour les résultats du Security Hub en utilisant EventBridge les règles Amazon et les rubriques Amazon Simple Notification Service (Amazon SNS). Ce système informe l'équipe appropriée d'une découverte lors de sa création. Pour cette approche, la stratégie multi-comptes décrite dans le présent document Développement d'une Compte AWS structure est essentielle, car les applications sont séparées en comptes dédiés. Cela vous permet d'informer les bonnes équipes pour chaque résultat.

Les équipes chargées de la sécurité ou du cloud peuvent choisir de recevoir des événements de la part de tous Comptes AWS. Dans ce cas, créez une EventBridge règle dans le compte d'administrateur délégué de Security Hub et abonnez-vous à une rubrique Amazon SNS qui informe ces équipes. Pour les équipes chargées des applications, configurez une EventBridge règle et une rubrique SNS dans leurs comptes d'application respectifs. Lorsqu'une découverte du Security Hub est détectée dans un compte d'application, l'équipe responsable en est informée.

Security Hub envoie déjà automatiquement tous les nouveaux résultats et toutes les mises à jour des résultats existants EventBridge sous la forme d'événements Security Hub Findings - Imported. Chaque événement Security Hub Findings - Imported contient une seule constatation. Vous pouvez appliquer des filtres aux EventBridge règles afin qu'une recherche ne déclenche la règle que si la recherche correspond aux filtres. Pour obtenir des instructions, voir Configuration d'une EventBridge règle pour l'envoi automatique des résultats. Pour plus d'informations sur la création et l'abonnement à des rubriques Amazon SNS, consultez Configuration d'Amazon SNS.

Lorsque vous utilisez cette approche, tenez compte des points suivants :

- Pour les équipes chargées des applications, créez des EventBridge règles au sein de chacune d'elles Compte AWS et à l' Région AWS endroit où l'application est hébergée.
- Pour les équipes chargées de la sécurité et du cloud, créez des EventBridge règles dans le compte d'administrateur délégué du Security Hub. Cela informe les équipes de toutes les découvertes dans les comptes des membres.
- Amazon SNS envoie une notification chaque jour si le statut de la constatation de sécurité est. `NEW` Si vous souhaitez désactiver les notifications quotidiennes, vous pouvez créer une AWS Lambda fonction personnalisée qui change le statut de la recherche de `NEW` à une `NOTIFIED` fois que l'abonné Amazon SNS a reçu la notification.

Triez et corrigez les résultats de sécurité dans votre environnement AWS

Le tri d'un constat de sécurité implique de le transmettre aux parties prenantes appropriées, d'évaluer et de prioriser le résultat, puis d'y remédier. Cette section passe en revue chacune de ces étapes en détail et fournit des recommandations en matière d'évolutivité et d'efficacité. Il comprend également des exemples pour illustrer le processus de triage et de remédiation.

Rubriques

- Définir la propriété des résultats de sécurité
- Évaluez et hiérarchisez les résultats de sécurité
- Corriger les résultats de sécurité
- Exemples de triage et de correction des résultats de sécurité

Définir la propriété des résultats de sécurité

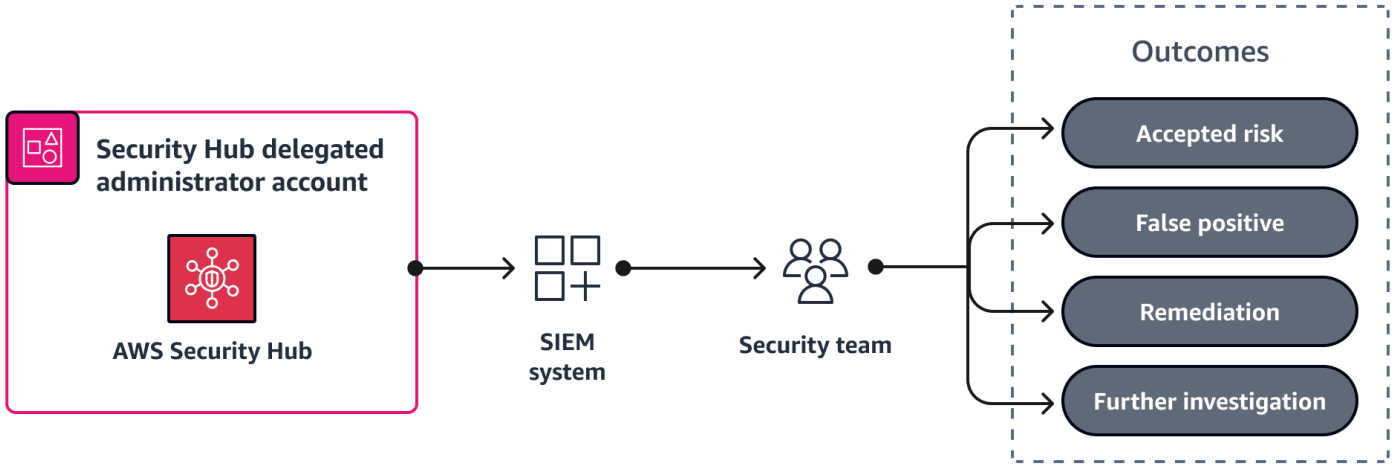
Définir un modèle de propriété pour trier les résultats de sécurité peut s'avérer difficile, mais ce n'est pas nécessairement le cas. Le paysage de la sécurité évolue constamment, et les professionnels doivent faire preuve de flexibilité pour s'adapter à ces changements. Adoptez une approche flexible pour développer votre modèle de propriété en fonction des résultats de sécurité. Votre modèle initial doit permettre à vos équipes d'agir immédiatement. Nous recommandons de commencer par une logique de propriété de base et de l'affiner au fil du temps. Si vous tardez à définir les critères de propriété parfaits, le nombre de résultats de sécurité continuera d'augmenter.

Pour faciliter l'attribution des résultats aux équipes et aux ressources appropriées, nous vous recommandons de les intégrer AWS Security Hub à tous les systèmes existants que vos équipes utilisent pour gérer leurs tâches quotidiennes. Par exemple, vous pouvez intégrer Security Hub à des systèmes de gestion des informations et des événements de sécurité (SIEM) ou à des systèmes de gestion des dossiers de produits et de billetterie. Pour plus d’informations, consultez Préparez-vous à attribuer les résultats de sécurité dans ce guide.

Voici un exemple de modèle de propriété que vous pouvez utiliser comme point de départ :

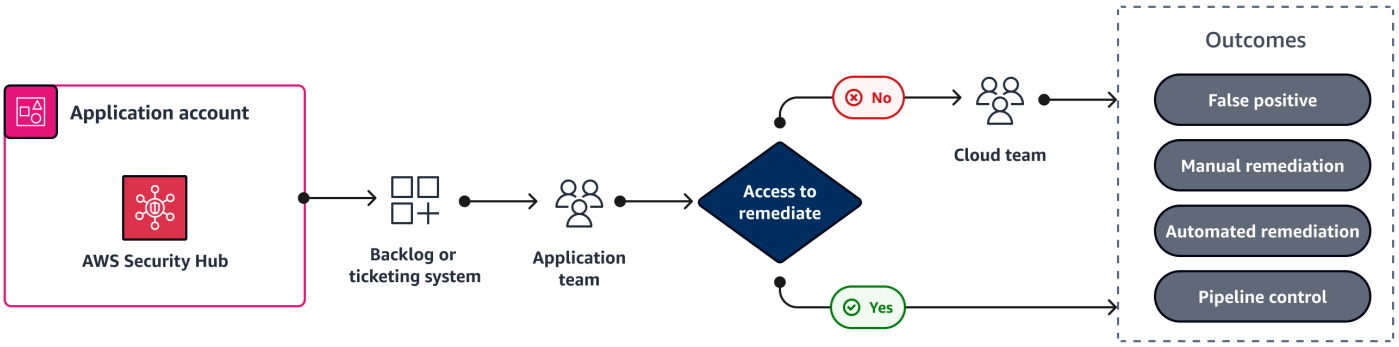
- L'équipe de sécurité examine les menaces potentiellement actives et aide à évaluer et à hiérarchiser les résultats de sécurité. L'équipe de sécurité possède l'expertise et les outils

nécessaires pour évaluer correctement le contexte. Ils comprennent les données supplémentaires liées à la sécurité qui les aident à évaluer et à hiérarchiser les vulnérabilités et à enquêter sur les événements de détection des menaces. Si une évaluation de la gravité ou des ajustements supplémentaires sont nécessaires, consultez la Évaluez et hiérarchisez les résultats de sécurité section de ce guide. Pour un exemple, consultez Exemple d'équipe de sécurité ce guide.



- Diffusez les résultats de sécurité entre les équipes du cloud et des applications : comme indiqué dans la Répartissez la propriété des titres section, l'équipe qui a accès à la configuration de la ressource est responsable de sa configuration sécurisée. Les équipes chargées des applications sont responsables des résultats de sécurité liés aux ressources qu'elles créent et configurent, et l'équipe du cloud est responsable des résultats de sécurité liés aux configurations étendues. Dans la plupart des cas, les équipes chargées des applications n'ont pas accès à la modification de configurations étendues AWS servicesAWS Control Tower, telles que les politiques de contrôle des services (SCP) AWS Organizations, les configurations VPC liées au réseau et l'IAM Identity Center.AWS

  Dans les environnements multicomptes qui séparent les applications en comptes dédiés, vous pouvez généralement intégrer les résultats liés à la sécurité du compte dans le backlog ou le système de billetterie de l'application. À partir de ce système, l'équipe cloud ou l'équipe chargée de l'application peut traiter le résultat. Pour des exemples, consultez Exemple d'équipe cloud ou Exemple d'équipe de candidature dans ce guide.



- Attribuez les résultats non résolus restants à l'équipe cloud : les résultats résiduels peuvent être liés à des paramètres par défaut ou à des configurations étendues que l'équipe cloud peut traiter. C'est probablement cette équipe qui possède le plus de connaissances historiques et d'accès pour résoudre le problème. Dans l'ensemble, il s'agit généralement d'un sous-ensemble nettement inférieur du total des résultats.

Évaluez et hiérarchisez les résultats de sécurité

Un élément essentiel d'un programme de gestion des vulnérabilités efficace est la capacité d'évaluer et de hiérarchiser les résultats de sécurité. C'est là qu'entrent en jeu le contexte, l'historique de l'organisation et le réglage des systèmes de détection. La hiérarchisation des résultats de sécurité permet d'établir la vitesse appropriée pour le niveau de réponse.

Pour Amazon Inspector et Amazon AWS Security Hub GuardDuty, les résultats contiennent une étiquette ou un score de gravité. Nous vous recommandons de donner la priorité à l'investigation de tous les résultats critiques et très graves dans Security Hub, y compris les résultats liés à la norme Foundational Security Best Practices (FSBP), Amazon Inspector et. GuardDuty Pour trouver des étiquettes de gravité, les scores sont déterminés comme suit :

- Le score Amazon Inspector est un score hautement contextualisé pour chaque résultat. Il est calculé en corrélant les informations du score de base du système CVSS (Common Vulnerability Scoring System) avec les résultats d'accessibilité du réseau et les données d'exploitabilité. À l'aide de ce score, vous pouvez hiérarchiser les résultats afin de vous concentrer sur les résultats les plus critiques et les ressources vulnérables. Outre le score, Amazon Inspector fournit également des informations améliorées sur les vulnérabilités relatives aux vulnérabilités et expositions courantes (CVE). Il s'agit d'un résumé des informations disponibles sur le CVE auprès d'Amazon ainsi que de sources de renseignement de sécurité standard, telles que Recorded Future et la Cybersecurity and Infrastructure Security Agency (CISA). Par exemple, Amazon Inspector peut

fournir les noms des kits de malwares connus utilisés pour exploiter une vulnérabilité. Pour plus d'informations, consultez Vulnerability Intelligence.

- Chaque GuardDuty constatation est associée à un niveau de gravité et à une valeur qui reflètent le risque potentiel qu'elle présente pour votre environnement. Ce niveau et cette valeur sont déterminés par les ingénieurs AWS de sécurité. Par exemple, un niveau de `High` gravité indique qu'une ressource est compromise et qu'elle est activement utilisée à des fins non autorisées. Nous vous recommandons de traiter une GuardDuty constatation de `High` gravité comme une priorité et d'y remédier immédiatement pour empêcher toute nouvelle utilisation non autorisée.
- La gravité d'une constatation de contrôle du Security Hub dépend de la difficulté à exploiter et de la probabilité de compromission. La difficulté est déterminée par le degré de sophistication ou de complexité requis pour utiliser la faiblesse afin de réaliser un scénario de menace. La probabilité d'une compromission indique la probabilité que le scénario de menace entraîne une interruption ou une violation de vos ressources AWS services ou de vos ressources.

Pour ajuster les résultats, vous pouvez supprimer ou archiver des résultats spécifiques directement dans la console de service correspondante ou en utilisant l'API du service. En outre, vous pouvez modifier les résultats dans Security Hub à l'aide de règles d'automatisation. GuardDuty et les résultats d'Amazon Inspector sont automatiquement envoyés à Security Hub. Vous pouvez utiliser les règles d'automatisation pour mettre à jour automatiquement (par exemple en modifiant la gravité) ou supprimer les résultats en temps quasi réel, en fonction de critères que vous définissez. Lorsque vous créez des règles d'automatisation, nous vous recommandons d'ajouter du contexte à la description de la règle, par exemple la date de création ou de modification, son créateur et les raisons pour lesquelles la règle est nécessaire. Ces informations sont souvent utiles pour référence future.

Corriger les résultats de sécurité

Après avoir évalué et hiérarchisé une constatation, l'action suivante consiste à la corriger. Il existe de nombreuses mesures différentes que vous pouvez prendre pour remédier à une constatation. Pour les vulnérabilités logicielles, vous pouvez mettre à jour le système d'exploitation ou appliquer un correctif. Pour obtenir des informations sur la configuration du cloud, vous pouvez mettre à jour la configuration des ressources. En général, les mesures que vous prenez pour remédier à la situation peuvent être regroupées selon l'un des résultats suivants :

- Correction manuelle : vous apportez manuellement un correctif à la vulnérabilité, par exemple en modifiant les propriétés d'une AWS ressource pour activer le chiffrement. Si le résultat provient

d'un check géré dans Security Hub, il inclut un lien vers des instructions permettant de corriger manuellement le résultat.

- Artefact réutilisable : vous mettez à jour l'infrastructure sous forme de code (IaC) pour corriger la vulnérabilité et vous savez que d'autres pourraient bénéficier d'une solution similaire. Envisagez de télécharger l'iAc mis à jour et un bref résumé de la résolution dans un référentiel de code partagé interne.
- Correction automatique — La vulnérabilité est automatiquement corrigée par le biais de mécanismes que vous avez créés.
- Contrôle du pipeline : vous appliquez un contrôle au sein de votre pipeline d'intégration continue et de livraison continue (CI/CD) qui empêche le déploiement en cas de vulnérabilité.
- Risque accepté — Vous ne prenez aucune mesure ni ne mettez en œuvre de contrôle compensatoire, et vous acceptez le risque que présente la vulnérabilité. Suivez le risque accepté dans un emplacement dédié, tel qu'un registre des risques.
- Faux positif : vous ne prenez aucune mesure car vous avez déterminé que le résultat n'identifiait pas correctement une vulnérabilité.

La liste complète des différentes actions que vous pouvez entreprendre et des outils que vous pouvez utiliser pour remédier à une vulnérabilité n'est pas abordée dans ce guide. Cependant, certains services et outils pouvant vous aider à corriger les vulnérabilités à grande échelle méritent d'être soulignés, notamment :

- Le gestionnaire de correctifs, une fonctionnalité de AWS Systems Manager, automatise le processus d'application des correctifs aux nœuds gérés à la fois avec des mises à jour liées à la sécurité et d'autres types de mises à jour. Vous pouvez utiliser le Gestionnaire de correctifs pour appliquer des correctifs pour les systèmes d'exploitation et les applications.
- AWS Firewall Managervous permet de configurer et de gérer de manière centralisée les règles de pare-feu pour l'ensemble de vos comptes et applications dans AWS Organizations. À mesure que de nouvelles applications sont créées, Firewall Manager facilite la mise en conformité des nouvelles applications et ressources en appliquant un ensemble commun de règles de sécurité.
- Automated Security AWS Response on est une AWS solution qui fonctionne avec Security Hub et fournit des actions de réponse et de correction prédéfinies basées sur les normes de conformité du secteur et les meilleures pratiques en matière de menaces de sécurité.

Exemples de triage et de correction des résultats de sécurité

Cette section fournit des exemples de processus de triage pour les équipes chargées de la sécurité, du cloud et des applications. Il décrit les types de constatations que chaque équipe aborde couramment et fournit un exemple de la manière d'y répondre. Des conseils de remédiation de haut niveau sont également inclus.

Les exemples suivants sont inclus dans cette section :

- Exemple d'équipe de sécurité : création d'une règle d'automatisation du Security Hub
- Exemple d'équipe cloud : modification des configurations VPC
- Exemple d'équipe chargée de l'application : création d'une AWS Config règle

Exemple d'équipe de sécurité : création d'une règle d'automatisation du Security Hub

L'équipe de sécurité reçoit les résultats relatifs à la détection des menaces, y compris les GuardDuty résultats d'Amazon. Pour obtenir la liste complète des types de GuardDuty recherche classés par type de AWS ressource, consultez la section Types de recherche dans la GuardDuty documentation. Les équipes de sécurité doivent être familiarisées avec tous ces types de constatations.

Dans cet exemple, l'équipe de sécurité accepte le niveau de risque associé aux résultats de sécurité dans un fichier Compte AWS utilisé uniquement à des fins d'apprentissage et ne contenant pas de données importantes ou sensibles. Le nom de ce compte est`sandbox`, et l'identifiant du compte est`123456789012`. L'équipe de sécurité peut créer une règle AWS Security Hub d'automatisation qui supprime tous les GuardDuty résultats de ce compte. Ils peuvent soit créer une règle à partir d'un modèle, qui couvre de nombreux cas d'utilisation courants, soit créer une règle personnalisée. Dans Security Hub, nous vous recommandons de prévisualiser les résultats des critères pour vérifier que la règle renvoie les résultats escomptés.

> **Note**
>
> Cet exemple met en évidence les fonctionnalités des règles d'automatisation. Nous ne recommandons pas de supprimer tous les GuardDuty résultats d'un compte. Le contexte est important, et chaque organisation doit choisir les résultats à supprimer en fonction du type de données, de la classification et des contrôles d'atténuation.

Les paramètres utilisés pour créer cette règle d'automatisation sont les suivants :

- Règle :
  - Le nom de la règle est `Suppress findings from Sandbox account`
  - La description de la règle est `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`
- Critères :
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- Action automatisée :
  - `Workflow.status` est `SUPPRESSED`

Pour plus d'informations, consultez la section Règles d'automatisation dans la documentation du Security Hub. Les équipes de sécurité disposent de nombreuses options pour étudier les menaces détectées et y remédier. Pour obtenir des conseils détaillés, consultez le Guide de réponse aux incidents de AWS sécurité. Nous vous recommandons de consulter ce guide pour confirmer que vous avez mis en place des processus de réponse aux incidents solides.

Exemple d'équipe cloud : modification des configurations VPC

L'équipe cloud est chargée de trier et de corriger les résultats de sécurité présentant des tendances communes, tels que les modifications des paramètres AWS par défaut susceptibles de ne pas convenir à votre cas d'utilisation. Ces résultats ont tendance à affecter de nombreuses Comptes AWS ressources, telles que les configurations VPC, ou à inclure une restriction qui doit être appliquée à l'ensemble de l'environnement. Dans la plupart des cas, l'équipe cloud apporte des modifications manuelles ponctuelles, telles que l'ajout ou la mise à jour d'une politique.

Une fois que votre organisation a utilisé un AWS environnement pendant un certain temps, vous constaterez peut-être l'apparition d'un ensemble d'anti-modèles. Un anti-modèle est une solution fréquemment utilisée pour un problème récurrent où la solution est contre-productive, inefficace ou moins efficace qu'une alternative. Comme alternative à ces anti-modèles, votre organisation peut utiliser des restrictions plus efficaces à l'échelle de l'environnement, telles que les politiques de contrôle des AWS Organizations services (SCP) ou les ensembles d'autorisations IAM Identity

Center. Les SCP et les ensembles d'autorisations peuvent imposer des restrictions supplémentaires pour les types de ressources, par exemple en empêchant les utilisateurs de configurer un bucket Amazon Simple Storage Service (Amazon S3) public. Bien qu'il puisse être tentant de restreindre toutes les configurations de sécurité possibles, il existe des limites de taille pour les SCP et les ensembles d'autorisations. Nous recommandons une approche équilibrée en matière de contrôles préventifs et de détection.

Voici quelques contrôles issus de la norme AWS Security Hub Foundational Security Best Practices (FSBP) dont l'équipe cloud pourrait être responsable :

- [EC2.2] Le groupe de sécurité VPC par défaut ne doit pas autoriser le trafic entrant et sortant
- [EC2.6] La journalisation des flux VPC doit être activée dans tous les VPC
- [EC2.23] Les passerelles de transit Amazon EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- [CloudTrail.1] CloudTrail doit être activé et configuré avec au moins un journal multirégional incluant des événements de gestion de lecture et d'écriture
- [Config.1] AWS Config doit être activé

Dans cet exemple, l'équipe du cloud étudie une découverte concernant le contrôle FSBP EC2.2. La documentation de ce contrôle recommande de ne pas utiliser le groupe de sécurité par défaut car il permet un accès étendu via les règles entrantes et sortantes par défaut. Comme le groupe de sécurité par défaut ne peut pas être supprimé, il est recommandé de modifier les paramètres des règles afin de limiter le trafic entrant et sortant. Pour résoudre efficacement ce problème, l'équipe du cloud doit utiliser les mécanismes établis pour modifier les règles des groupes de sécurité pour tous les VPC, car chaque VPC possède ce groupe de sécurité par défaut. Dans la plupart des cas, les équipes cloud gèrent les configurations VPC à l'aide de AWS Control Towerpersonnalisations ou d'un outil d'infrastructure en tant que code (IaC), tel que ou. HashiCorp TerraformAWS CloudFormation

Exemple d'équipe chargée de l'application : création d'une AWS Config règle

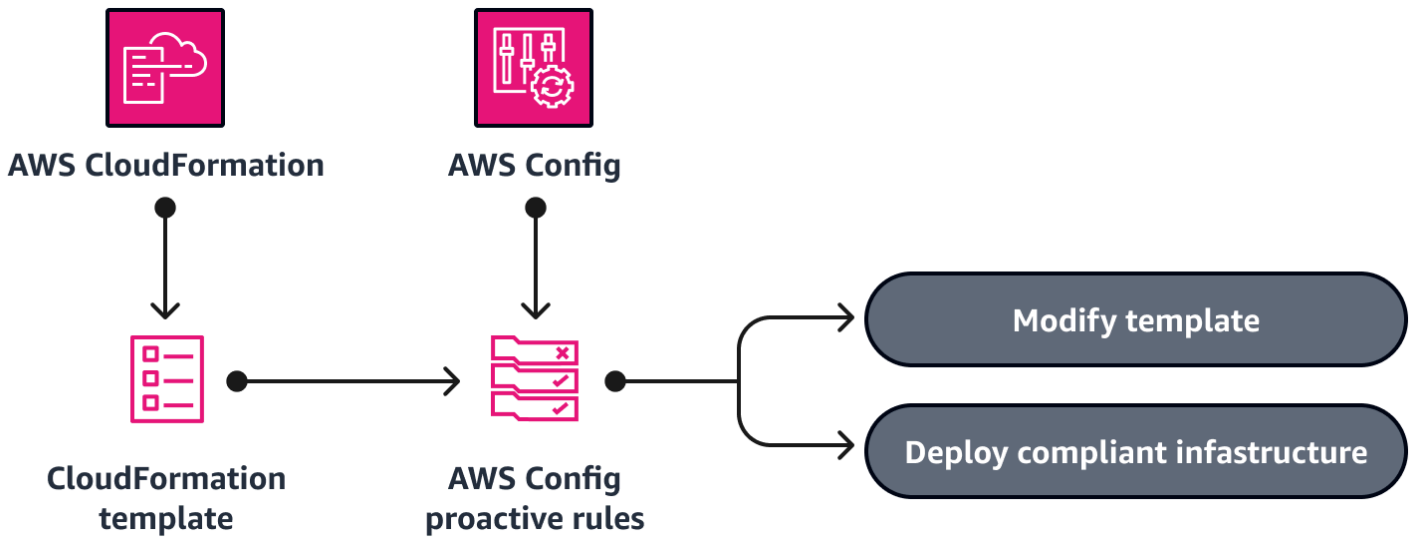
Voici quelques contrôles issus de la norme de sécurité Security Hub Foundational Security Best Practices (FSBP) dont l'application ou l'équipe de développement peut être responsable :

- [CloudFront.1] CloudFront les distributions doivent avoir un objet racine par défaut configuré

- [EC2.19] Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé
- [CodeBuild.1] CodeBuild GitHub ou les URL du dépôt source de Bitbucket doivent utiliser OAuth
- [ECS.4] Les conteneurs ECS doivent fonctionner comme des conteneurs non privilégiés
- [ELB.1] Application Load Balancer doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS

Dans cet exemple, l'équipe chargée de l'application traite d'une constatation concernant le contrôle FSBP EC2.19. Ce contrôle vérifie si le trafic entrant non restreint pour les groupes de sécurité est accessible aux ports spécifiés présentant le risque le plus élevé. Ce contrôle échoue si l'une des règles d'un groupe de sécurité autorise le trafic entrant `::/0` depuis `0.0.0.0/0` ou vers ces ports. La documentation de ce contrôle recommande de supprimer les règles qui autorisent ce trafic.

Outre la prise en compte de la règle du groupe de sécurité individuel, il s'agit d'un excellent exemple de découverte qui devrait aboutir à une nouvelle AWS Config règle. En utilisant le mode d'évaluation proactive, vous pouvez contribuer à empêcher le déploiement de règles de groupe de sécurité risquées à l'avenir. Le mode proactif évalue les ressources avant leur déploiement afin d'éviter les erreurs de configuration des ressources et les problèmes de sécurité associés. Lors de la mise en œuvre d'un nouveau service ou d'une nouvelle fonctionnalité, les équipes chargées des applications peuvent appliquer des règles en mode proactif dans le cadre de leur pipeline d'intégration et de livraison continues (CI/CD) afin d'identifier les ressources non conformes. L'image suivante montre comment utiliser une AWS Config règle proactive pour confirmer que l'infrastructure définie dans un AWS CloudFormation modèle est conforme.



Cet exemple permet d'obtenir une autre efficacité importante. Lorsqu'une équipe d'application crée une AWS Config règle proactive, elle peut la partager dans un référentiel de code commun afin que d'autres équipes d'application puissent l'utiliser.

Chaque résultat associé à un contrôle Security Hub contient des informations détaillées sur le résultat et un lien vers les instructions pour résoudre le problème. Bien que les équipes cloud puissent être confrontées à des problèmes nécessitant une correction manuelle ponctuelle, nous recommandons, le cas échéant, de mettre en place des contrôles proactifs permettant d'identifier les problèmes le plus tôt possible dans le processus de développement.

Signalez et améliorez votre programme de gestion des vulnérabilités

Un reporting efficace pour la gestion des vulnérabilités implique l'examen des données, le suivi des tendances et le partage des connaissances. Cela donne de la visibilité et aide les équipes à améliorer le niveau de sécurité de leur organisation dans le AWS Cloud.

Organiser des réunions mensuelles sur les opérations de sécurité

Les réunions mensuelles sur les opérations de sécurité constituent un mécanisme efficace pour promouvoir le maintien de l'appropriation, de la responsabilisation et de l'alignement au sein des équipes. Au cours de la réunion, les parties prenantes des équipes chargées de la sécurité, du cloud et des applications examinent les données pour identifier les résultats de sécurité exceptionnels, les résultats non conformes aux accords de niveau de service (SLA) et les équipes qui ont le plus de résultats.

Ces réunions aident vos équipes à identifier les défauts, tels que les opportunités d'ajouter des restrictions supplémentaires. Les contrôles préventifs et les opportunités d'automatisation peuvent également être découverts et partagés. Les réunions permettent également d'identifier ce qui fonctionne et ce qui ne fonctionne pas bien dans le programme de gestion des vulnérabilités afin que vous puissiez apporter des améliorations.

En examinant les données, en identifiant les anti-modèles et les problèmes, et en partageant des informations sur les contrôles et les automatisations, les équipes peuvent obtenir des informations précieuses et apporter des améliorations continues susceptibles de renforcer leur posture de sécurité et de réduire leurs SLA liés à la sécurité.

Utilisez les informations du Security Hub pour identifier les anti-modèles

AWS Security Hub les informations peuvent également vous aider à identifier les anti-modèles et à suivre vos progrès en matière de correction des résultats. Un aperçu du Security Hub est un ensemble de résultats connexes. Il identifie un domaine de sécurité qui nécessite une attention et une intervention particulières. Les informations du Security Hub peuvent vous aider à identifier des exigences spécifiques et à élaborer des rapports. Security Hub propose plusieurs informations

intégrées et gérées. Pour suivre les problèmes de sécurité propres à votre AWS environnement et à votre utilisation, vous pouvez créer des informations personnalisées.

Conclusion et étapes suivantes

En résumé, un programme de gestion des vulnérabilités efficace nécessite une préparation minutieuse et nécessite que vous activiez les bons outils et intégrations, que vous affiniez ces outils, que vous triiez efficacement les problèmes et que vous établissiez des rapports et des améliorations en permanence. En suivant les meilleures pratiques décrites dans ce guide, les entreprises peuvent créer un programme de gestion des vulnérabilités évolutif AWS afin de sécuriser leurs environnements cloud.

Vous pouvez étendre ce programme pour inclure d'autres vulnérabilités et découvertes liées à la sécurité, telles que les vulnérabilités de sécurité des applications. AWS Security Hub prend en charge les intégrations de produits personnalisés. Envisagez d'utiliser Security Hub comme point d'intégration pour des outils et produits de sécurité supplémentaires. Cette intégration vous permet de tirer parti des processus et des flux de travail que vous avez déjà établis dans votre programme de gestion des vulnérabilités, tels que l'intégration directe avec les arriérés de produits et les réunions mensuelles de révision de la sécurité.

Le tableau suivant résume les phases et les actions décrites dans ce guide.

Phase	Éléments d’action
Préparation	• Définissez un plan de gestion des vulnérabilités. • Répartissez la propriété des résultats. • Élaborer un programme de divulgation des vulnérabilités. • Développez une Compte AWS structure. • Définissez, implémentez et appliquez les balises. • Surveillez les bulletins AWS de sécurité. • Activez Amazon Inspector avec un administrateur délégué. • Activez Security Hub avec un administrateur délégué. • Activez les normes du Security Hub.

Phase	Éléments d’action
	• Configurez l'agrégation interrégionale de Security Hub. • Activez les résultats de contrôle consolidés dans Security Hub. • Configurez et gérez les intégrations de Security Hub, y compris les intégrations en aval applicables avec les systèmes SIEM, GRC, de backlog de produits ou de billetterie
Triage et correction	• Suivez les résultats sur la base d'une stratégie multi-comptes. • Transmettez les résultats aux équipes chargées de la sécurité, du cloud, des applications ou des développeurs. • Ajustez les résultats de sécurité pour vous assurer qu'ils sont exploitables pour votre environnement spécifique. • Développez des mécanismes de correction automatisés, dans la mesure du possible. • Mettez en œuvre des contrôles du pipeline CI/CD ou d'autres garde-fous qui aident à prévenir les découvertes de sécurité, dans la mesure du possible. • Utilisez les règles d'automatisation du Security Hub pour augmenter ou supprimer les résultats.
Signaler et améliorer	• Organisez des réunions mensuelles sur les opérations de sécurité. • Utilisez les informations du Security Hub pour identifier les anti-modèles.

Ressources

AWS documentation de service

- Intégrations de produits ()AWS Security Hub
- Intégration AWS Security Hub dans Jira Service Management Cloud (AWS Security Hub)
- Règles d'automatisation (AWS Security Hub)
- Règles d'évaluation proactives (AWS Config)
- Gestionnaire de correctifs (AWS Systems Manager)

Autres AWS ressources

- Bonnes pratiques en matière de balisage AWS des ressources (AWS livre blanc)
- Réponse de sécurité automatisée activée AWS (bibliothèque de AWS solutions)
- AWS Guide de réponse aux incidents de sécurité (guideAWS technique)
- AWS bulletins de sécurité

Historique du document

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

Modification	Description	Date
Publication initiale	—	12 octobre 2023

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. Pour suggérer des entrées, veuillez utiliser le lien Faire un commentaire à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Oracle sur une instance EC2 dans le. AWS Cloud
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration active-passive.

migration active-passive

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

Fonction SQL qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent `SUM` et`MAX`.

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une solution alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour le processus de découverte et d'analyse du portefeuille et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter Qu'est-ce que l'intelligence artificielle ?

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur la façon dont les AIOps sont utilisées dans la stratégie de migration AWS , veuillez consulter le guide d'intégration des opérations.

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, cohérence, isolement, durabilité (ACID)

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez ABAC pour AWS dans la documentation AWS Identity and Access Management (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Un emplacement distinct au sein d'un Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, la AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer

l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

AWS Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

Un bot destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les appels d'API suspects et les actions similaires. Pour plus d'informations, veuillez consulter Data in a behavior graph dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi endianité.

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, connus sous le nom de mauvais robots, sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de robots infectés par des logiciels malveillants et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, c'est un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur Implementation break-glass procedures dans le guide Well-Architected AWS .

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCoE

Voir le Centre d'excellence du cloud.

CDC

Consultez la section Capture des données de modification.

capture des données de modification (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez utiliser la CDC à diverses fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser AWS Fault Injection Service (AWS FIS) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données localement, avant que la cible ne les AWS service reçoive.

Centre d'excellence cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, consultez les articles du CCoE sur le blog de stratégie AWS Cloud d'entreprise.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie informatique de pointe.

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section Création de votre modèle d'exploitation cloud.

étapes d'adoption du cloud

Les quatre phases que les entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Voir base de données de gestion de configuration.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub ou AWS CodeCommit. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, AWS

Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, consultez la section Packs de conformité dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes source, de génération, de test, intermédiaire et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du AWS Well-Architected Framework. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir Création d'un périmètre de données sur AWS.

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir langage de définition de base de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de

la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte AWS membre pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations .

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir environnement.

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique Contrôles de détection dans Implementing security controls on AWS.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSM étend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un schéma en étoile, table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un sinistre. Pour plus d'informations, consultez Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur l'utilisation du design piloté par domaine avec le modèle de figuier étrangleur, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

DR

Consultez la section Reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower

pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au cloud computing, l'informatique de pointe peut réduire la latence des communications et améliorer le temps de réponse.

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres principaux Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre

service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité, le MES et la gestion de projet) pour une entreprise.

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes dans la documentation AWS Key Management Service (AWS KMS).

environment

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un pipeline CI/CD, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures,

la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le guide d'implémentation du programme.

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. L'EDA est réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un schéma en étoile. Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir la succursale.

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec :AWS.

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en « 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données via la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

G

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le flux de travail basé sur les troncs est l'approche moderne préférée.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée brownfield. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités d'organisation (UO). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. AWS propose AWS SCT qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir

constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation de l'historien

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l'identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l'AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIoT

Voir Internet industriel des objets.

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures mutables. Pour plus d'informations, consultez les meilleures pratiques de déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un

premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Terme introduit par Klaus Schwab en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau entre les VPC (identiques ou Régions AWS différents), Internet et les réseaux sur site. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section Qu'est-ce que l'IoT ?.

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, veuillez consulter Machine learning model interpretability with AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Consultez la section Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement

de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

lift and shift

Voir 7 Rs.

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi endianité.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter Machine Learning.

branche principale

Voir la succursale.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles

ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

AWS services qui AWS gère la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

MAP

Voir Migration Acceleration Program.

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore lorsqu'il fonctionne. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

Tous, à l' Comptes AWS exception du compte de gestion, qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

MAILLES

Voir le système d'exécution de la fabrication.

Transport télémétrique en file d'attente de messages (MQTT)

Protocole de communication léger machine-to-machine (M2M), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.

microservice

Petit service indépendant qui communique via des API bien définies et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou

à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie à l'aide d'API légères. Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir une base opérationnelle solide pour passer au cloud, et pour aider à compenser le coût initial des migrations. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la stratégie de migration AWS.

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 AWS avec le service de migration d'applications.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le. AWS Cloud La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'outil MPA (connexion requise) est disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du AWS CAF. Pour plus d'informations, veuillez consulter le guide de préparation à la migration. La MRA est la première phase de la stratégie de migration AWS.

stratégie de migration

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. Pour plus d'informations, reportez-vous aux 7 R de ce glossaire et à Mobiliser votre organisation pour accélérer les migrations à grande échelle.

ML

Voir apprentissage automatique.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de

gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez la section Stratégie de modernisation des applications dans le AWS Cloud.

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le AWS Cloud.

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter Decomposing monoliths into microservices.

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation d'une infrastructure immuable comme meilleure pratique.

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

OPC-UA

Voir Open Process Communications - Architecture unifiée.

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. L'OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat de niveau de service (SLA).

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, évaluer, prévenir ou réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de l'industrie 4.0.

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le guide d'intégration des opérations.

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). L'OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les requêtes dynamiques PUT adressées au compartiment S3. DELETE

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés ne peuvent accéder au contenu d'un compartiment S3 que par le biais d'une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

OU

Voir l'examen de l'état de préparation opérationnelle.

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique Limites des autorisations dans la documentation IAM.

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les

exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les informations personnelles identifiables.

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter Evaluating migration readiness.

predicate

Une condition de requête qui renvoie `true` ou`false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

Entité AWS capable d'effectuer des actions et d'accéder aux ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

Confidentialité dès la conception

Une approche de l'ingénierie des systèmes qui prend en compte la confidentialité tout au long du processus d'ingénierie.

zones hébergées privées

Conteneur qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

publier/souscrire (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données relationnelle SQL.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

Voir responsable, responsable, consulté, informé (RACI).

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

Matrice RASCI

Voir responsable, responsable, consulté, informé (RACI).

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir 7 Rs.

Région

Un ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir 7 Rs.

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. La haute disponibilité et la reprise après sinistre sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez AWS Cloud Résilience.

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, redevable, consulté et informé (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique Responsive controls dans Implementing security controls on AWS.

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

rotation

Processus de mise à jour périodique d'un secret pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations d' AWS API sans que vous ayez à créer

un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, voir Que contient le secret d'un Secrets Manager ? dans la documentation de Secrets Manager.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : préventifs, détectifs, réactifs et proactifs.

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs

qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par celui AWS service qui les reçoit.

Politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

point de terminaison du service

URL du point d'entrée pour un AWS service. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique AWS service endpoints dans Références générales AWS.

contrat de niveau de service (SLA)

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service (SLI)

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de niveau de service.

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Consultez les informations de sécurité et le système de gestion des événements.

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, consultez la section Approche progressive de la modernisation des applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme

un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

Plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer ces tests.

T

balises

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources.

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir environnement.

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux sur site. Pour plus d'informations, voir Qu'est-ce qu'une passerelle de transit dans la AWS Transit Gateway documentation.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données. Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir environnement.

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

Appairage de VPC

Connexion entre deux VPC qui vous permet d'acheminer le trafic à l'aide d'adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

Fonction SQL qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

Consultez le cadre de qualification des charges de travail AWS.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une vulnérabilité de type « jour zéro ».

vulnérabilité de type « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

application zombie

Application dont l'utilisation moyenne du processeur et de la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

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