Pôle STN

Sciences, Technologies et Numérique

Formation : Mathématiques Appliqués et Informatique
Spécialité : Informatique
Option : Systèmes, Réseaux et Infrastructures Virtuelles

MEMOIRE DE MASTER

Sujet : Utilisation de Services Natifs AWS pour la Sécurité en Cloud : Intégration de GuardDuty, Macie et Security Hub dans un SIEM

Soutenu par :
El Hadji Falilou Mbacké Mbaye

Le XX/XX/2024

Sous la direction de :
Pr Cherif Diallo

Foo nekk fooju la

Remerciements

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué à la réalisation de ce mémoire.

Je remercie tout particulièrement mon directeur de recherche, Pr Chérif Diallo, pour son encadrement, ses conseils avisés et son soutien constant tout au long de ce projet.

Je suis également reconnaissant envers les membres du corps professoral de l'université numérique Cheikh Hamidou KANE (UN-CHK) pour leur enseignement et leur encouragement. Merci à mes collègues et amis pour leurs encouragements et leur aide précieuse. Enfin, je remercie ma famille pour leur soutien indéfectible, leur patience et leur amour inconditionnel.

Dédicaces

Je dédie ce mémoire à tous ceux qui ont cru en moi et m'ont soutenu tout au long de ce parcours.

À ma famille, pour leur amour inconditionnel, leur soutien moral et leur patience.

À mes amis, pour leurs encouragements constants et leur compréhension durant les moments difficiles.

À mes professeurs et encadrants, pour leurs précieux conseils, leur expertise et leur disponibilité, sans lesquels ce travail n'aurait pas été possible.

Enfin, à tous ceux qui m'ont inspiré et motivé, je vous exprime ma profonde gratitude.

● Tables des matières

Table des matières

Remerciements i
Dédicaces ii
Sigles et Abréviations v
Avant propos vii
Liste des Figures viii
Introduction 1
CHAPITRE 1 : Introduction 3
1.1 Contexte et Problématique 4
1.2 Présentation des Systèmes SIEM et Leur Rôle 5
1.2.1 Définition du SIEM 5
1.2.2 Histoire du SIEM 6
1.2.3 Fonctionnement des SIEM 9
1.2.4 Avantages des SIEM dans les Environnements Cloud 10
1.2.5 Cas d'utilisation d'un SIEM moderne 12
1.2.6 Différence entre le SIEM et le SOAR 15
1.3 Spécificités et Défis de la Mise en Place d'un SIEM sur AWS 16
1.3.1 Spécificités de l'Environnement AWS 17
1.3.2 Défis de l'Intégration des SIEM sur AWS 17
1.3.3 Solutions pour Surmonter les Défis 19
1.4 Objectifs du Mémoire 19
CHAPITRE 2 : Connaissances Fondamentales 22
2.1 Concepts de base du Cloud Computing et de la sécurité du cloud. 23
2.1.1 Définition et Principes Fondamentaux 23
2.1.2 Les Principales Formes de Cloud Computing et Modèle de responsabilité partagée 24
2.1.3 Modèles de Déploiement Cloud 30
2.1.4 Avantages et Défis du Cloud Computing 31
2.2 Concepts de Cybersécurité 33
2.2.1 Aperçu des Principes et Techniques de Base 33

2.2.2 Techniques de Cybersécurité 34
2.2.3 Types de menaces de cybersécurité 35
2.2.4 Cas d'utilisation de la cybersécurité 36
2.3 Présentation de AWS GuardDuty, Macie, et Security Hub 37
2.3.1 Amazon GuardDuty 37
2.3.2 Amazon Macie 42
2.3.3 AWS Security Hub 46
2.4 Intégration des Services AWS avec SIEM 53
CHAPITRE 3 : Architecture et Étapes de Mise en Place 55
3.1 Architecture du SIEM sur AWS 56
3.1.1 Intégration des Services AWS 57
3.2 Étapes de Mise en Place 59
3.2.1 Configuration Initiale des Services AWS 59
3.2.2 Intégration et Automatisation des Workflows 64
3.2.3 Analyse et Visualisation des Logs 70
3.3 Automatisation du Déploiement de l'Architecture avec AWS CloudFormation 77
3.3.1 Fonctionnement 77
3.3.2 Cas d'Utilisation 78
3.3.3 Création de Templates CloudFormation 78
CHAPITRE 4 : Conclusion et Perspectives 85
4.1 Résumé des Résultats 86
4.2 Recommandations 86
4.3 Perspectives Futures 87
Glossaire 89
Bibliographie 91
Annexes 92

Sigles et Abréviations

AWS: Amazon Web Services

SIEM: Security Information and Event Management

IaaS: Infrastructure as a Service

PaaS: Platform as a Service

SaaS: Software as a Service

VPC: Virtual Private Cloud

DNS: Domain Name System

EC2: Elastic Compute Cloud

S3: Simple Storage Service

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

RBAC: Role-Based Access Control

ABAC: Attribute-Based Access Control

GDPR: General Data Protection Regulation

HIPAA: Health Insurance Portability and Accountability Act

MFA: Multi-Factor Authentication

ETL: Extract, Transform, Load

CLI: Command Line Interface

KMS: Key Management Service

SNS : Simple Notification Service

SLA : Service Level Agreement

Avant propos

Ce mémoire est le fruit de plusieurs mois de recherche et de travail acharné, visant à approfondir les connaissances sur la mise en place et la gestion d'un système de gestion des informations et des événements de sécurité (SIEM) dans un environnement cloud AWS. À travers ce document, nous explorerons les différentes composantes essentielles à la sécurité des infrastructures cloud, tout en proposant des méthodologies détaillées pour la configuration et l'optimisation d'un SIEM sur AWS.

Je tiens à exprimer ma gratitude envers tous ceux qui ont contribué à la réalisation de ce travail. Je remercie particulièrement mes encadrants pour leurs conseils avisés, ainsi que ma famille et mes amis pour leur soutien inébranlable.

L'objectif de ce mémoire est de fournir une compréhension claire et pratique des défis et des solutions liées à la sécurisation des environnements cloud à l'aide des technologies AWS. J'espère que ce travail servira de guide utile pour les professionnels de la cybersécurité et les étudiants intéressés par ce domaine en constante évolution.

Liste des Figures

Figure 1 Système de gestion des informations et des événements de sécurité 6
Figure 2: Fonctionnalité SIEM moderne 8
Figure 3: Architecture SIEM 9
Figure 4: Avantages du SIEM 11
Figure 5: Composants et capacités SIEM 13
Figure 6: Différence entre SIEM et SOAR 16
Figure 7: Architecture du cloud computing 23
Figure 8: services du cloud computing 25
Figure 9: Modèle de responsabilité partagée 27
Figure 10: Modèle de responsabilité partagée sur AWS 29
Figure 11: Types de cloud computing 30
Figure 12: Architecture Amazon GuardDuty 38
Figure 13: Architecture Am52azon Macie 43
Figure 14: Architecture AWS Security Hub 47
Figure 15: Architecture d'implémentation du SIEM 57
Figure 16: Diagramme illustrant l'implémentation 59
Figure 17: Code de la fonction Lambda 66
Figure 18: Fonctionnement de AWS CloudFormation 77
Figure 19: Code du modèle Cloudformation en YAML 81
Figure 20: Spécification des détails sur le déploiement avec Cloudformation 82
Figure 21: Evénement lors de la création du pile 83
Figure 22: Vérification des ressources 84

Introduction

. La cybersécurité est devenue un enjeu majeur avec l'augmentation de l'adoption des solutions cloud par les entreprises. Le cloud computing offre des avantages considérables tels que la flexibilité, l'évolutivité et la réduction des coûts, mais il introduit également de nouveaux défis en matière de sécurité. Les environnements cloud sont particulièrement vulnérables aux cyberattaques en raison de leur nature distribuée et de la diversité des services et des utilisateurs qu'ils supportent. Par conséquent, il est crucial d'établir des mesures de sécurité robustes pour protéger les données et les applications hébergées dans le cloud.

Les systèmes de gestion des informations et des événements de sécurité (SIEM) sont des outils essentiels pour la cybersécurité moderne. Ils permettent de centraliser, analyser et corréler les logs et les événements de sécurité provenant de diverses sources pour détecter les comportements anormaux et réagir rapidement aux incidents de sécurité. Un SIEM efficace peut fournir une visibilité complète sur l'ensemble de l'infrastructure IT, aider à la détection des menaces en temps réel, et faciliter la conformité avec les réglementations en matière de sécurité.

Amazon Web Services (AWS) est l'une des plateformes cloud les plus populaires, offrant une large gamme de services pour héberger et gérer les applications et les données. Toutefois, la sécurisation de ces environnements cloud nécessite une approche spécifique. AWS propose plusieurs services natifs de sécurité, tels que GuardDuty, Macie et Security Hub, qui peuvent être intégrés avec un SIEM pour fournir une solution de sécurité complète. L'intégration de ces services natifs présente des défis uniques, notamment la gestion de la volumétrie des données, l'optimisation des performances et la maîtrise des coûts.

Amazon Web Services (AWS) est l'une des plateformes cloud les plus populaires, offrant une large gamme de services pour héberger et gérer des applications et des données. Cependant, la sécurisation de ces environnements cloud nécessite une approche spécifique en raison de leur complexité et de la diversité des services et des utilisateurs. Les défis incluent la gestion de la volumétrie des données, l'optimisation des performances et la maîtrise des coûts. L'intégration de services natifs AWS tels que GuardDuty, Macie et Security Hub avec un SIEM peut répondre à ces défis en fournissant des capacités de détection avancées et une gestion centralisée des alertes.

Au Sénégal, la recherche sur la cybersécurité et les systèmes SIEM dans les environnements cloud est menée par des institutions académiques. Ces institutions collaborent souvent avec des partenaires internationaux et des organisations locales pour promouvoir la cybersécurité et développer des solutions adaptées aux besoins locaux. Le gouvernement sénégalais, par le biais de Sénégal Numérique S.A (SENUM SA.) (Ex ADIE), joue un rôle crucial dans la mise en œuvre des politiques de cybersécurité et dans la promotion des meilleures pratiques.

À l'échelle internationale, des recherches significatives sont menées sur l'intégration des services de sécurité natifs AWS avec les systèmes SIEM. Les publications académiques et les rapports industriels mettent en évidence les avantages et les défis de cette intégration, notamment en termes de performance, d'évolutivité et de rentabilité des solutions de sécurité. Des conférences et des journaux spécialisés en cybersécurité, tels que le IEEE Symposium on Security and Privacy, fournissent une plateforme pour la diffusion des dernières découvertes et innovations dans ce domaine.

Ce mémoire se concentrera sur l'utilisation des services natifs AWS (GuardDuty, Macie, et Security Hub) pour renforcer la sécurité des environnements cloud à travers leur intégration avec un système SIEM. Les principaux objectifs de cette recherche sont :

- **Analyser les avantages et les inconvénients d'un SIEM sur AWS :** Évaluer les bénéfices et les limitations de l'utilisation des services natifs AWS pour la détection et la réponse aux incidents de sécurité.
- **Décrire les étapes de mise en place :** Fournir une méthodologie détaillée pour l'intégration des services AWS avec un SIEM, en mettant en lumière les meilleures pratiques et les solutions aux défis courants.
- **Évaluer la performance et l'efficacité du système :** Mesurer l'efficacité du système SIEM intégré dans la détection et la gestion des incidents de sécurité, ainsi que son impact sur la performance globale de l'infrastructure cloud.

CHAPITRE 1 : *Introduction*

1.1 Contexte et Problématique

Importance de la Cybersécurité dans les Environnements Cloud

Avec l'essor du cloud computing, la cybersécurité est devenue un enjeu primordial pour les entreprises modernes. Les infrastructures cloud, bien qu'offrant des avantages considérables en termes de flexibilité, d'évolutivité et de réduction des coûts, posent également des défis spécifiques en matière de sécurité. Ces environnements distribués et multi-utilisateurs sont particulièrement vulnérables aux cyberattaques. Protéger les données et les applications hébergées dans le cloud nécessite des mesures de sécurité robustes et adaptées aux caractéristiques uniques de cette infrastructure.

Les menaces cybernétiques évoluent constamment, obligeant les entreprises à rester vigilantes pour protéger leurs actifs numériques. Les attaques par ransomware, les violations de données et les menaces internes sont des exemples de risques auxquels les environnements cloud peuvent être exposés. Assurer la sécurité dans le cloud ne se limite pas aux protections techniques mais inclut également la conformité aux réglementations et une gestion rigoureuse des risques.

Rôle des SIEM dans la Cybersécurité

Les systèmes de gestion des informations et des événements de sécurité (SIEM) sont essentiels pour la cybersécurité des environnements cloud. Les SIEM collectent, agrègent et analysent les logs et les événements de sécurité provenant de diverses sources au sein de l'infrastructure cloud. Leur objectif principal est de détecter les comportements anormaux et de permettre une réponse rapide aux incidents de sécurité.

Les fonctionnalités clés des SIEM incluent :

- **Collecte de Logs** : Centralisation des données de sécurité provenant de différents systèmes, applications et réseaux.
- **Analyse en Temps Réel** : Surveillance continue des événements pour détecter les anomalies et les menaces potentielles.
- **Corrélation des Événements** : Identification des schémas de comportement malveillant en corrélant les événements de sécurité.
- **Gestion des Incidents** : Automatisation des réponses aux incidents et fourniture d'outils pour la gestion des alertes.
- **Rapports de Conformité** : Génération de rapports pour démontrer la conformité aux réglementations de sécurité .

En utilisant des solutions SIEM, les entreprises peuvent améliorer leur capacité à détecter et à répondre aux menaces en temps réel, ce qui est crucial pour protéger les environnements cloud contre les cyberattaques. Les SIEM fournissent également des informations précieuses pour l'analyse post-incident et la prise de décision stratégique en matière de sécurité.

La cybersécurité dans les environnements cloud est d'une importance capitale pour les entreprises modernes. Les SIEM jouent un rôle crucial en offrant une visibilité complète sur les activités de sécurité, en détectant rapidement les menaces et en facilitant une réponse efficace aux incidents. En combinant les avantages des SIEM avec des stratégies de sécurité cloud robustes, les entreprises peuvent renforcer leur posture de sécurité et protéger leurs actifs numériques contre les cybermenaces.

1.2 Présentation des Systèmes SIEM et Leur Rôle

1.2.1 Définition du SIEM

Un SIEM, ou Security Information and Event Management (Système de gestion des informations et des événements de sécurité), est un système essentiel en cybersécurité. Il collecte des logs et des événements de divers systèmes et dispositifs de sécurité, puis normalise ces données pour les analyser efficacement. Cela permet de créer des visualisations, des alertes, des recherches et des rapports.

Les équipes de sécurité utilisent souvent le SIEM comme tableau de bord principal pour leurs opérations quotidiennes. Les analystes se servent de cet outil pour surveiller continuellement les systèmes, rechercher des menaces, examiner et résoudre les incidents. Le SIEM aide à identifier rapidement les anomalies et à réagir en temps réel, renforçant ainsi la sécurité globale de l'organisation.

Le SIEM offre aussi des fonctionnalités de recherche avancée et de reporting, fournissant des informations précieuses pour la prise de décision et la conformité réglementaire. En centralisant les données de sécurité, il permet une gestion plus efficace et une réponse rapide aux incidents, protégeant ainsi les infrastructures informatiques contre les cybermenaces.

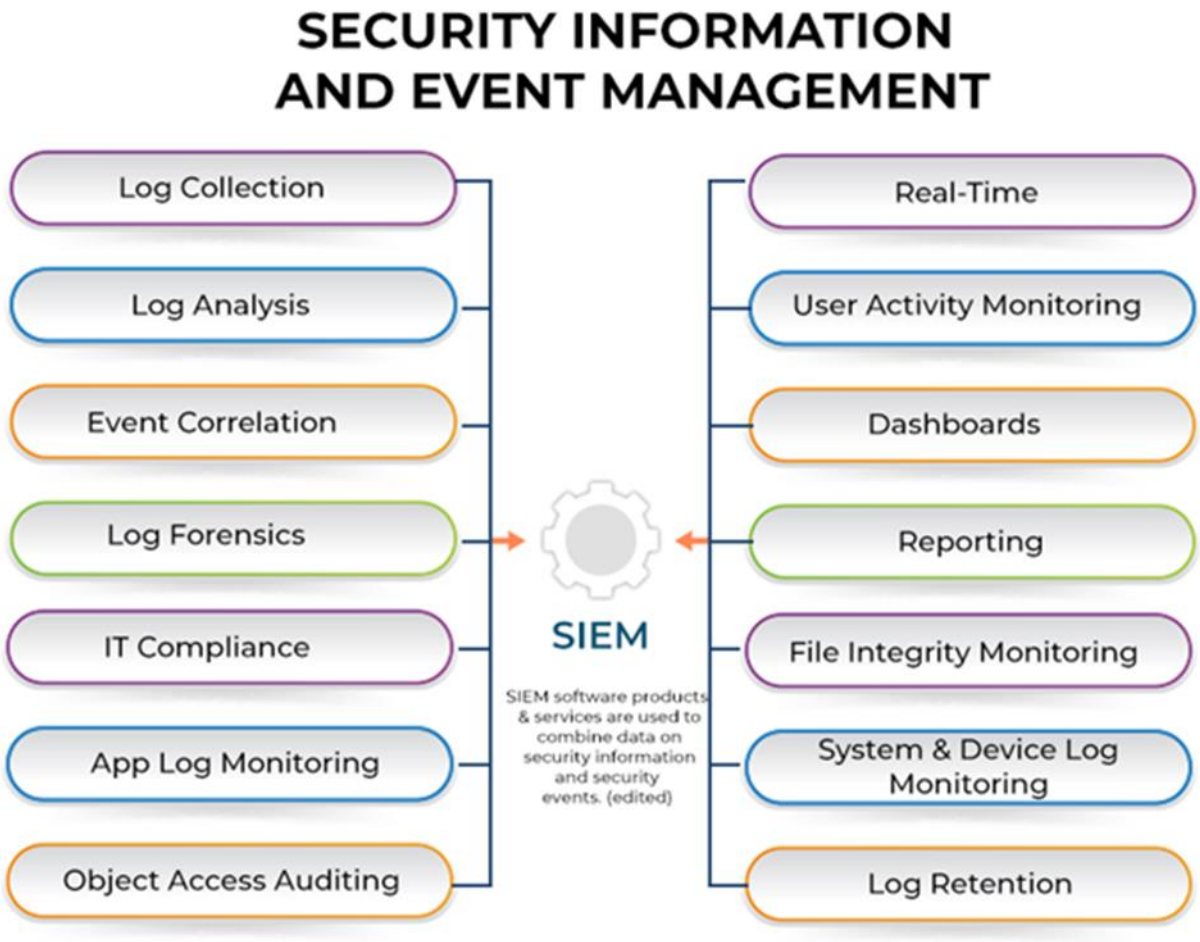


Figure 1 Système de gestion des informations et des événements de sécurité

1.2.2 Histoire du SIEM

1.2.2.1 Origines et Évolution Initiale

Le Security Information and Event Management (SIEM) est apparu il y a plus de vingt ans, répondant aux besoins des entreprises en matière de conformité réglementaire, notamment les normes PCI, SOX et HIPAA. Les premiers systèmes SIEM combinaient la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM). Ces systèmes initiaux se concentraient principalement sur la collecte de logs et la génération d'alertes pour des fins de conformité, avec des capacités limitées en termes de corrélation et d'analyse des données.

1.2.2.2 Phase de Scalabilité et Big Data

Avec l'augmentation exponentielle des volumes de données, les SIEM ont évolué pour mieux gérer les besoins en big data. La deuxième génération de SIEM a introduit des architectures capables de stocker et d'interroger de grandes quantités de données historiques, facilitant ainsi une analyse plus approfondie et une corrélation efficace des événements de sécurité. Des outils

comme Splunk ont révolutionné le marché en facilitant l'indexation et la recherche rapide dans les données brutes, permettant aux entreprises d'analyser leurs données de sécurité de manière plus efficace.

1.2.2.3 Intégration de l'Analytique et de l'Automatisation

Vers 2015, la troisième génération de SIEM a intégré des capacités analytiques avancées et l'apprentissage automatique pour améliorer la détection des menaces. Les systèmes d'analyses comportementales des utilisateurs et des entités (UEBA) ont permis d'établir des baselines comportementales et de détecter les anomalies plus efficacement. De plus, l'intégration de l'automatisation et de l'orchestration de la sécurité (SOAR) a permis une réponse rapide et coordonnée aux incidents de sécurité, réduisant ainsi la charge de travail des analystes.

1.2.2.4 Perspectives Futures

Les SIEM modernes évoluent pour intégrer davantage de capacités de traitement en cloud, offrant une évolutivité rapide et une réduction des coûts de maintenance. Ces solutions se concentrent désormais sur l'amélioration de l'intégration, de la collaboration et de l'automatisation, permettant aux équipes de sécurité de répondre de manière plus efficace aux menaces croissantes. L'utilisation de l'analytique comportementale et de l'intelligence artificielle permet d'offrir des réponses plus rapides et plus précises aux incidents de sécurité, renforçant ainsi la posture de sécurité des organisations.

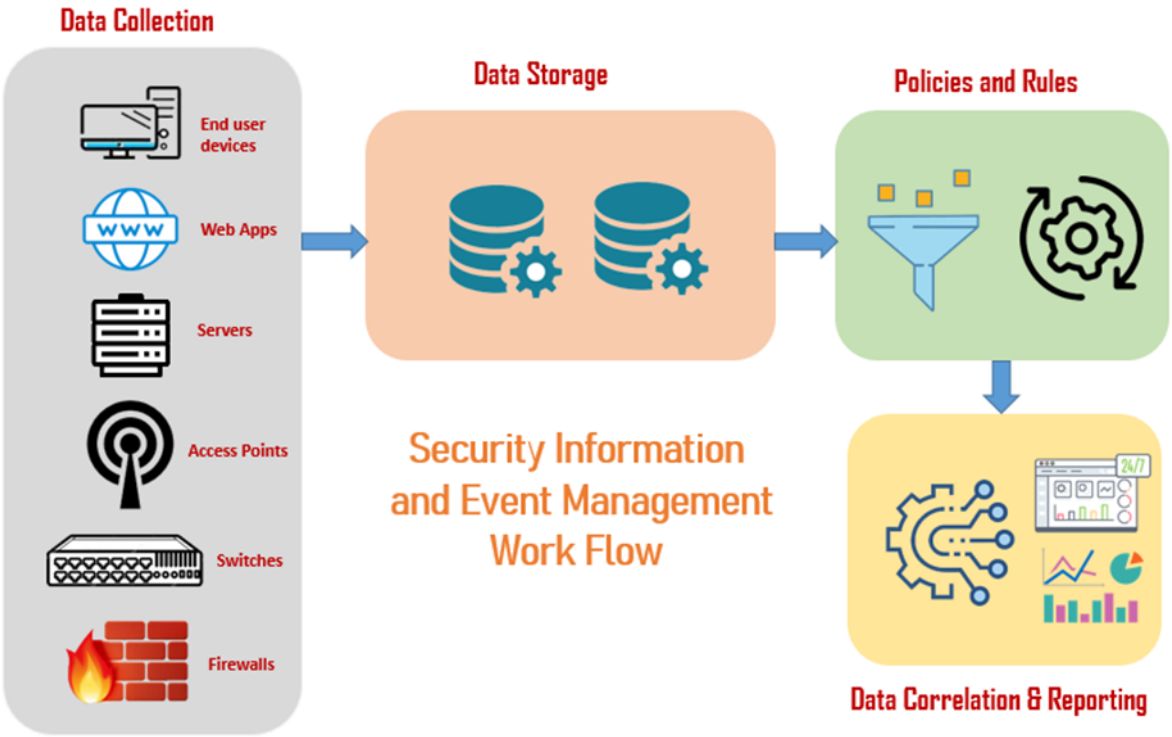


Figure 2: Fonctionnalité SIEM moderne

1.2.2.5 Fonctionnalités Clés des SIEM Modernes

- **Collecte et Agrégation de Logs** : Les SIEM collectent et agrègent des logs provenant de diverses sources telles que les pare-feu, les systèmes d'exploitation et les applications, offrant une visibilité complète sur les activités de sécurité.
- **Analyse en Temps Réel** : Grâce à l'analyse en temps réel, les SIEM peuvent identifier immédiatement les menaces potentielles et générer des alertes appropriées pour une intervention rapide.
- **Corrélation des Événements** : En associant différents événements, les SIEM peuvent détecter des comportements malveillants qui pourraient passer inaperçus si les événements étaient analysés isolément.
- **Gestion des Incidents** : Les SIEM facilitent la réponse aux incidents en permettant aux équipes de sécurité de suivre, d'analyser et de résoudre les incidents de manière efficace.
- **Génération de Rapports de Conformité** : Les SIEM produisent des rapports détaillés pour s'assurer que les organisations respectent les diverses réglementations en vigueur.

Le SIEM a donc évolué pour devenir un outil indispensable en cybersécurité, s'adaptant continuellement aux besoins changeants des infrastructures modernes. Il offre une gestion plus efficace des menaces et une réponse rapide aux incidents, tout en intégrant les dernières avancées technologiques pour renforcer la sécurité des organisations.

1.2.3 Fonctionnement des SIEM

Les systèmes de gestion des informations et des événements de sécurité (SIEM) sont essentiels pour la cybersécurité des entreprises. Ils collectent des données de sécurité de différentes sources, normalisent ces données, détectent des comportements anormaux, corrèlent les événements et automatisent la réponse aux incidents. Leur capacité à surveiller continuellement les environnements cloud améliore la sécurité globale en permettant une réponse proactive aux menaces.

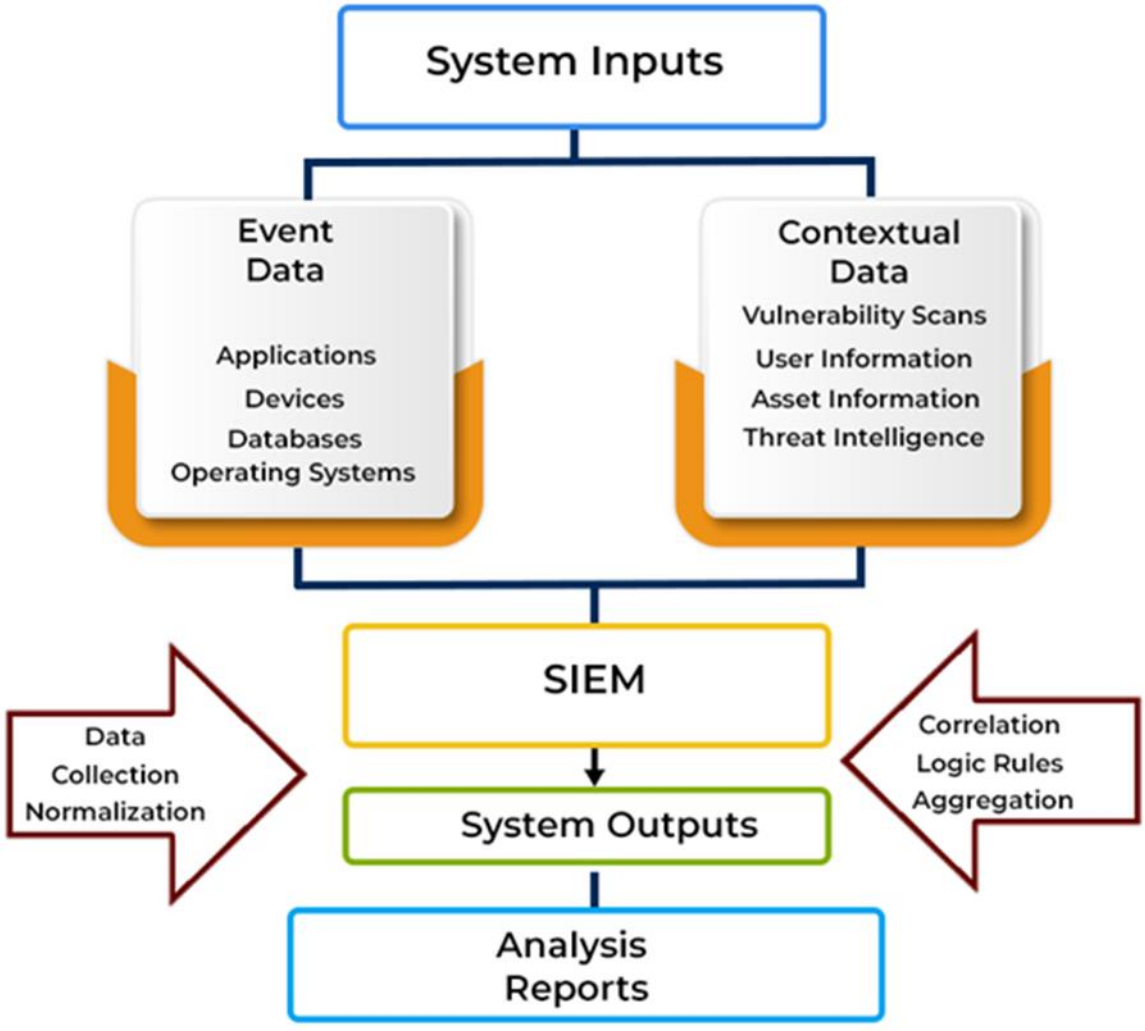


Figure 3: Architecture SIEM

- **Collecte et Agrégation des Données**

Les SIEM recueillent des logs et des événements de sécurité provenant de serveurs, dispositifs réseau, applications et équipements de sécurité. Cette collecte centralisée permet une analyse cohérente des données. La normalisation des données est cruciale pour comparer et combiner des informations de différentes sources.

- **Détection des Comportements Anormaux**

En utilisant des règles prédéfinies et des algorithmes d'apprentissage automatique, les SIEM analysent en temps réel les logs et les événements pour identifier des activités suspectes. Cette détection rapide aide à prévenir les incidents de sécurité avant qu'ils ne causent des dommages.

- **Corrélation des Événements**

La corrélation des événements permet d'associer différents incidents pour identifier des schémas de comportement malveillants. Par exemple, plusieurs tentatives de connexion échouées suivies d'une connexion réussie depuis une adresse IP inconnue peuvent déclencher une alerte. Cette capacité de corrélation est essentielle pour détecter les attaques sophistiquées.

- **Réponse aux Incidents**

Lorsqu'une menace est détectée, les SIEM génèrent des alertes et fournissent des informations détaillées sur l'incident. Les systèmes peuvent automatiser certaines réponses, permettant aux équipes de sécurité de réagir rapidement et efficacement. L'intégration avec des outils d'orchestration et d'automatisation de la sécurité (SOAR) améliore cette capacité.

- **Surveillance Continue dans le Cloud**

Dans les environnements cloud, les SIEM offrent une surveillance continue et une gestion centralisée des incidents de sécurité. Cette surveillance en temps réel permet de détecter rapidement les menaces potentielles et de réagir de manière proactive. En assurant une visibilité complète et en facilitant la gestion des incidents, les SIEM améliorent significativement la sécurité des infrastructures cloud.

Globalement, les SIEM sont des outils indispensables pour la gestion de la cybersécurité. En centralisant la collecte et l'analyse des données de sécurité, en détectant rapidement les comportements anormaux, en corrélant les événements et en automatisant les réponses aux incidents, ils offrent une protection robuste et proactive contre les cybermenaces. Ces systèmes permettent aux organisations de réagir rapidement et efficacement aux incidents de sécurité, renforçant ainsi la sécurité de leurs systèmes informatiques.

1.2.4 Avantages des SIEM dans les Environnements Cloud

Le SIEM (Security Information and Event Management) offre plusieurs avantages pour les organisations cherchant à renforcer leur sécurité informatique. L'un des principaux atouts est la centralisation et la corrélation des événements de sécurité provenant de divers systèmes et applications. Cela permet de détecter rapidement les anomalies et les incidents potentiels, facilitant ainsi la réponse immédiate aux menaces.



Figure 4: Avantages du SIEM

- **Visibilité Complète**

Les systèmes de gestion des informations et des événements de sécurité (SIEM) centralisent les logs et les événements de sécurité provenant de diverses sources cloud. Cette centralisation offre une vue d'ensemble exhaustive de l'infrastructure cloud, permettant aux équipes de sécurité de surveiller efficacement les activités. Cela facilite la détection rapide des comportements anormaux, essentiel pour prévenir les menaces avant qu'elles ne causent des dommages significatifs.

- **Détection Précise des Menaces**

Grâce à des règles de corrélation avancées et à l'analyse en temps réel, les SIEM peuvent identifier des menaces complexes et des attaques en plusieurs étapes, souvent invisibles pour les outils de sécurité traditionnels. Cette capacité à détecter des menaces sophistiquées permet une réponse plus efficace et rapide aux incidents de sécurité.

- **Réponse Rapide aux Incidents**

Les SIEM fournissent des alertes en temps réel et des outils de gestion des incidents, permettant aux équipes de sécurité de réagir rapidement pour minimiser l'impact des incidents. Cette réactivité est particulièrement cruciale dans les environnements cloud, où les attaques peuvent se propager rapidement, nécessitant une intervention immédiate pour contenir et résoudre les problèmes.

- **Conformité Réglementaire**

Les SIEM aident les entreprises à maintenir la conformité avec les réglementations de sécurité en fournissant des rapports détaillés et en documentant les mesures de sécurité mises en place. Cette capacité est essentielle pour les entreprises opérant dans des secteurs réglementés et utilisant des services cloud, car elle démontre le respect des exigences légales et la protection adéquate des données sensibles.

- **Scalabilité et Flexibilité**

  Les solutions SIEM basées sur le cloud offrent une scalabilité et une flexibilité accrue, permettant aux entreprises d'ajuster leurs capacités de sécurité en fonction de leurs besoins. Cette adaptabilité est particulièrement avantageuse pour les organisations en croissance ou celles ayant des besoins de sécurité variables, car elle permet de gérer efficacement les ressources de sécurité sans surcharger les systèmes existants.

En somme, les SIEM apportent de nombreux avantages dans les environnements cloud, de la visibilité complète à la détection précise des menaces, en passant par la réponse rapide aux incidents et la conformité réglementaire. Leur scalabilité et leur flexibilité en font des outils indispensables pour renforcer la sécurité dans un monde de plus en plus numérisé.

1.2.5 Cas d'utilisation d'un SIEM moderne

Les systèmes de gestion des informations et des événements de sécurité (SIEM) sont essentiels pour la cybersécurité. Ils offrent des solutions pour divers cas d'utilisation critiques. Voici une explication détaillée des principaux cas d'utilisation des SIEM modernes.



Figure 5: Composants et capacités SIEM

- **Gestion des Logs**

Les SIEM collectent, stockent et analysent les données de log et les événements créés par les hôtes, les applications et les réseaux d'une entreprise. Cette centralisation des logs permet de conserver des traces détaillées des activités, facilitant ainsi l'analyse en cas d'incident de sécurité. La gestion des logs est une composante clé pour maintenir une visibilité complète sur l'infrastructure IT d'une organisation.

- **Monitoring Continu**

Le monitoring actif aide les analystes à détecter des tendances liées à des anomalies pouvant indiquer une menace. Cela inclut la surveillance des modifications du système, la disponibilité des services et le flux réseau. Cette surveillance continue est cruciale pour identifier rapidement les comportements anormaux et réagir en conséquence. En détectant les anomalies en temps réel, les équipes de sécurité peuvent prévenir les incidents avant qu'ils ne causent des dommages.

- **Détection Avancée**

Les SIEM modernes sont équipés de capacités de détection avancées pour repérer les attaques sophistiquées, comme les malwares et ransomwares. Ils peuvent émettre des alertes sur :

  - Les modifications des identifiants/privilèges d'utilisateur
  - Les comportements anormaux

- Les menaces internes
- L’exfiltration de données

Cette détection avancée permet de prévenir les incidents de sécurité avant qu'ils n'aient un impact significatif sur l'organisation. Les alertes générées aident les équipes de sécurité à prendre des mesures rapides et appropriées pour neutraliser les menaces.

- **Recherche des Menaces**

La recherche proactive des menaces est une activité cruciale qui nécessite un moteur rapide capable de traiter de grandes quantités de données. Cette recherche permet de détecter les menaces cachées et de comprendre les tactiques, techniques et procédures des attaquants. En identifiant proactivement les menaces, les équipes de sécurité peuvent renforcer leur posture défensive et anticiper les attaques potentielles.

- **Réponse aux Incidents**

Lorsqu'un incident de sécurité survient, une réponse coordonnée est nécessaire pour limiter l'impact. Les SIEM offrent des outils pour automatiser et orchestrer cette réponse, garantissant une intervention rapide et efficace. Cela inclut la documentation des incidents, la gestion des alertes et l'exécution de réponses automatisées pour contenir et neutraliser les menaces.

- **Conformité**

Les SIEM aident les entreprises à se conformer aux exigences réglementaires et aux infrastructures applicables. Les exigences de conformité varient selon les secteurs et les régions, incluant :

- RGPD (Règlement général sur la protection des données)
- HIPAA (Health Insurance Portability and Accountability Act)
- SOX (Sarbanes-Oxley Act)
- PCI DSS (Payment Card Industry Data Security Standard)
- SOC 2/3 (Service Organization Control)
- ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)

Ces exigences de conformité sont essentielles pour protéger les données sensibles et éviter les sanctions légales. Les SIEM fournissent des rapports détaillés et documentent les mesures de sécurité en place pour démontrer la conformité.

Les SIEM modernes sont des outils indispensables pour la gestion de la sécurité informatique. Ils permettent de centraliser la collecte et l'analyse des données de sécurité, d'assurer une surveillance continue, de détecter les menaces avancées, de mener des recherches proactives

sur les menaces, de répondre efficacement aux incidents et de maintenir la conformité réglementaire. En combinant ces capacités, les SIEM renforcent la sécurité des infrastructures IT et améliorent la résilience des organisations face aux cybermenaces.

1.2.6 Différence entre le SIEM et le SOAR

- **SIEM (Security Information and Event Management)**

Le SIEM est une technologie qui se concentre sur la collecte, l'analyse et la corrélation des données de sécurité provenant de diverses sources, telles que les systèmes, les réseaux et les applications. Il détecte les incidents de sécurité en temps réel et génère des alertes pour permettre aux équipes de sécurité d'intervenir rapidement. Le SIEM offre également des rapports détaillés et des visualisations pour identifier les motifs et tendances des incidents, améliorant ainsi la posture de sécurité globale.

- **SOAR (Security Orchestration, Automation and Response)**

Le SOAR automatise et orchestre les processus de réponse aux incidents de sécurité. Il intègre divers outils de sécurité pour enrichir les alertes, collecter des renseignements sur les menaces et exécuter des actions automatiques en réponse aux incidents. Cette automatisation permet de rationaliser les réponses aux incidents, de réduire le temps de réaction et de minimiser les erreurs humaines, offrant une gestion proactive et coordonnée des menaces.

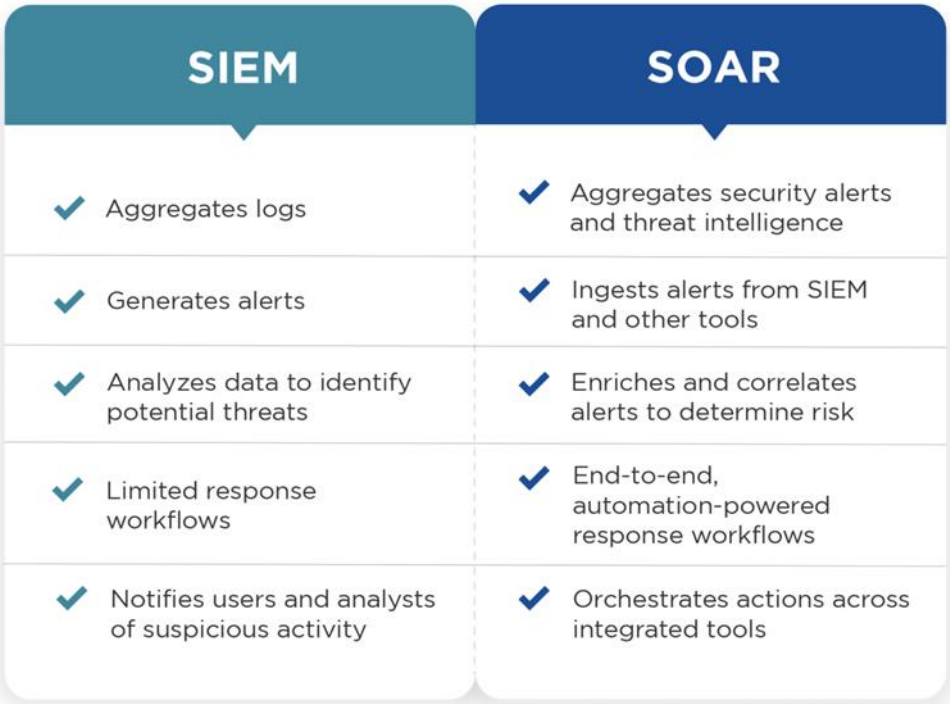


Figure 6: Différence entre SIEM et SOAR

- **Comparaison**
    - **SIEM** : Se concentre sur la détection des menaces par l'analyse et la corrélation des logs. Nécessite une intervention humaine pour enquêter et réagir aux alertes.
    - **SOAR** : Automatise la réponse aux incidents en utilisant des workflows prédéfinis, gérant les menaces de manière plus efficace et autonome, réduisant la dépendance à l'intervention humaine continue.

Pour devenir un véritable "point de surveillance unique" intégrant diverses technologies, le SIEM doit évoluer vers un modèle de développement de sécurité ouvert. Cela signifie que le code et les fonctionnalités des SIEM seront accessibles et améliorables par la communauté. Cette transparence permettra de renforcer la sécurité en facilitant l'identification et la correction rapide des vulnérabilités, améliorant ainsi la collaboration, l'innovation et la résilience globale contre les cybermenaces.

1.3 Spécificités et Défis de la Mise en Place d'un SIEM sur AWS

1.3.1 Spécificités de l'Environnement AWS

L'implémentation d'un système SIEM dans un environnement cloud AWS présente des caractéristiques et des défis uniques. AWS propose une gamme complète de services de sécurité natifs qui peuvent être intégrés dans un SIEM pour améliorer la détection et la réponse aux incidents de sécurité. Nous allons faire une explication détaillée de ces spécificités.

- **Services de Sécurité Natifs**

  Amazon Web Services (AWS) propose une gamme de services de sécurité natifs intégrés aux solutions SIEM pour une meilleure détection et réponse aux incidents de sécurité. Les principaux services comprennent :

  - **AWS GuardDuty** : Surveille et analyse en continu les données pour détecter les activités malveillantes.
  - **AWS Macie** : Utilise l'apprentissage automatique pour découvrir, classer et protéger les données sensibles.
  - **AWS Security Hub** : Centralise et hiérarchise les alertes de sécurité de divers services AWS, facilitant la gestion des incidents.

- **Scalabilité et Évolutivité**

  Les environnements cloud AWS sont réputés pour leur haute scalabilité et leur évolutivité. Cela permet aux entreprises d'ajuster rapidement leurs ressources de sécurité selon les besoins. Les solutions SIEM doivent être capables de gérer efficacement les variations de charge et de volumétrie des données pour maintenir des performances optimales. Cette capacité est essentielle pour gérer les périodes de forte activité sans interruption de service.

- **Automatisation et Orchestration**

  L'automatisation des processus de sécurité est cruciale dans un environnement cloud. AWS offre des services comme **AWS Lambda** pour automatiser les workflows de traitement des données de sécurité et exécuter des réponses automatisées aux incidents. L'utilisation de l'automatisation et de l'orchestration permet de réduire les temps de réaction et d'améliorer l'efficacité des équipes de sécurité en rationalisant les tâches répétitives et en facilitant les réponses coordonnées aux menaces.

L'intégration d'un SIEM dans un environnement AWS exige une compréhension approfondie des services de sécurité natifs, une capacité à gérer la scalabilité et l'évolutivité, ainsi qu'une utilisation efficace de l'automatisation et de l'orchestration. En maîtrisant ces aspects, les entreprises peuvent améliorer significativement leur posture de sécurité et leur capacité à répondre aux menaces dans un environnement cloud dynamique.

1.3.2 Défis de l'Intégration des SIEM sur AWS

L'intégration des systèmes de gestion des informations et des événements de sécurité (SIEM) sur Amazon Web Services (AWS) présente plusieurs défis uniques.

- **Gestion de la Volumétrie des Données**

  Les environnements cloud génèrent une énorme quantité de logs et d'événements de sécurité provenant de sources diverses comme les instances EC2, les conteneurs, les bases de données et les services réseau. Gérer cette volumétrie est un défi majeur pour les SIEM, qui doivent collecter, stocker et analyser ces données en temps réel . Cela nécessite des capacités de stockage élevées et des mécanismes efficaces pour traiter et analyser les logs sans ralentir les performances du système. La capacité d'un SIEM à ingérer de grandes quantités de données en temps réel est cruciale pour garantir une détection rapide et précise des menaces potentielles.

- **Optimisation des Performances**

  Assurer une performance optimale du SIEM est essentiel pour une détection rapide et précise des incidents de sécurité. Cela inclut l'optimisation des requêtes d'analyse des logs, la gestion de l'utilisation des ressources (CPU, mémoire, stockage) et la réduction de la latence des alertes. Les SIEM doivent être configurés pour fonctionner efficacement avec les ressources disponibles dans le cloud. L'utilisation de services comme AWS Lambda peut aider à automatiser et à accélérer les processus, garantissant ainsi que les incidents de sécurité sont détectés et traités rapidement.

- **Maîtrise des Coûts**

  Les coûts associés à la collecte, au stockage et à l'analyse des logs de sécurité peuvent rapidement augmenter dans un environnement cloud. Les entreprises doivent trouver un équilibre entre la couverture de sécurité et la maîtrise des coûts, en utilisant des stratégies comme l'archivage des logs anciens, l'échantillonnage des données et l'utilisation de services de stockage à bas coût comme Amazon S3 . Il est essentiel de surveiller régulièrement les dépenses liées aux services cloud et d'ajuster les configurations pour éviter des coûts inutiles. Les entreprises doivent également explorer des options de stockage et d'analyse plus économiques sans compromettre la sécurité.

- **Complexité de l'Intégration**

  L'intégration des divers services de sécurité AWS avec un SIEM peut être complexe, nécessitant une configuration minutieuse et une orchestration cohérente des workflows de sécurité. Les entreprises doivent s'assurer que tous les composants du SIEM sont correctement configurés pour travailler ensemble de manière harmonieuse et efficace. Les équipes de sécurité doivent posséder une expertise approfondie pour configurer et maintenir un SIEM dans un environnement AWS. Cela inclut la connaissance des services AWS et la capacité à intégrer ces services dans le SIEM pour maximiser la sécurité et l'efficacité opérationnelle.

1.3.3 Solutions pour Surmonter les Défis

Surmonter les défis de l'intégration des SIEM sur AWS nécessite une approche stratégique et bien planifiée. Voici quelques solutions clés pour aborder ces problèmes :

- **Utilisation de Services Gérés**

  AWS offre des services gérés qui simplifient la gestion des logs et la détection des menaces, comme AWS CloudWatch pour la surveillance des performances et Amazon OpenSearch Service pour l'analyse des logs. Ces services peuvent être intégrés avec le SIEM pour réduire la complexité et améliorer l'efficacité. L'utilisation de services gérés permet de déléguer une partie de la gestion des logs et de l'analyse à AWS, réduisant ainsi la charge sur les équipes internes et améliorant la rapidité et la précision des réponses aux incidents de sécurité.

- **Automatisation des Processus**

  L'utilisation d'AWS Lambda pour automatiser les workflows de traitement des logs et la réponse aux incidents permet de réduire la charge manuelle et d'améliorer la rapidité et la fiabilité des réponses. L'automatisation aide également à gérer la volumétrie des données en temps réel et à optimiser les performances du SIEM . L'automatisation permet de standardiser les réponses aux incidents, réduisant ainsi les erreurs humaines et accélérant les temps de réponse. Les processus automatisés peuvent inclure des tâches telles que l'analyse des logs, la génération d'alertes et l'exécution de scripts de réponse.

- **Optimisation des Configurations**

  Les entreprises doivent régulièrement surveiller et ajuster les configurations de leur SIEM et des services AWS pour maximiser l'efficacité et minimiser les coûts. Cela inclut l'optimisation des règles de corrélation, l'ajustement des seuils d'alerte et l'utilisation de stratégies de stockage efficaces pour les logs. L'optimisation continue des configurations permet de s'assurer que le SIEM fonctionne de manière optimale, offrant une détection rapide des menaces tout en contrôlant les coûts. Les entreprises doivent également rester à jour sur les meilleures pratiques et les nouvelles fonctionnalités pour améliorer constamment leur posture de sécurité.

1.4 Objectifs du Mémoire

L'objectif principal est d'analyser en profondeur les avantages l'intégration d'un SIEM dans un environnement AWS :

- **Avantages :**

- **Visibilité accrue :** En offrant une vue centralisée des événements de sécurité, les équipes peuvent surveiller efficacement les activités suspectes et réagir rapidement.
- **Détection Améliorée des Menaces :** Grâce à la corrélation et à l'analyse avancée, les SIEM peuvent identifier des menaces complexes qui pourraient passer inaperçues avec des outils de sécurité traditionnels.
- **Automatisation des réponses :** En automatisant les tâches répétitives et les réponses aux incidents, les SIEM réduisent la charge manuelle et améliorent la rapidité des réponses, permettant aux équipes de se concentrer sur des tâches plus stratégiques.

- **Inconvénients :**
  - **Complexité de mise en place :** L'intégration des divers services de sécurité AWS avec un SIEM peut être complexe et nécessite une configuration minutieuse pour assurer une cohérence et une efficacité optimales.
  - **Coûts élevés :** La collecte, le stockage et l'analyse des logs de sécurité peuvent entraîner des coûts importants. Il est crucial de trouver un équilibre entre la couverture de sécurité et la maîtrise des coûts.
  - **Gestion de la Volumétrie des Données :** Les SIEM doivent être capables de traiter efficacement de grandes quantités de données en temps réel, ce qui peut être difficile sans compromettre les performances.

- **Méthodologie de Mise en Place d'un SIEM sur AWS**

Ce mémoire vise également à fournir une méthodologie détaillée pour la mise en place d'un SIEM sur AWS :

- **Configuration initiale des Services AWS :** Activer et configurer des services comme GuardDuty, Macie et Security Hub pour la collecte et l'analyse des logs de sécurité. Cela comprend la définition des paramètres de sécurité et l'intégration avec d'autres outils de sécurité.
- **Intégration des Services :** Décrire comment intégrer ces services avec un SIEM pour créer une solution de sécurité centralisée. L'objectif est de garantir une communication fluide entre les différents composants de la solution de sécurité.
- **Automatisation des Workflows :** Utiliser AWS Lambda et d'autres outils pour automatiser les processus de collecte, d'analyse et de réponse aux incidents. Cela inclut la création de scripts et de workflows pour automatiser les tâches courantes.

- **Évaluation de la Performance et de l'Efficacité du Système**

Un autre objectif est d'évaluer la performance et l'efficacité du SIEM intégré avec les services AWS :

- **Temps de Détection et de Réponse :** Mesurer le temps nécessaire pour détecter et répondre aux incidents de sécurité afin de déterminer l'efficacité du SIEM à réagir aux menaces en temps réel.
- **Précision des Alertes :** Évaluer la précision des alertes générées par le SIEM pour minimiser les faux positifs et s'assurer que les alertes pertinentes sont priorisées.
- **Impact sur les Ressources :** Analyser l'impact de l'intégration des services AWS sur les ressources (CPU, mémoire, stockage) et les coûts associés pour optimiser l'utilisation des ressources et contrôler les dépenses.

Les objectifs de ce mémoire sont d'analyser les bénéfices et les limitations d'un SIEM sur AWS, de fournir une méthodologie détaillée pour sa mise en place, et d'évaluer sa performance et son efficacité. Ces objectifs permettront de fournir des recommandations pratiques et des meilleures pratiques pour les entreprises cherchant à améliorer leur posture de sécurité dans des environnements cloud complexes.

CHAPITRE 2 : *Connaissances Fondamentales*

2.1 Concepts de base du Cloud Computing et de la sécurité du cloud.

2.1.1 Définition et Principes Fondamentaux

Le cloud computing, ou informatique en nuage, est un modèle de fourniture de services informatiques via Internet. Ce modèle permet aux utilisateurs d'accéder à des ressources informatiques partagées telles que des serveurs, du stockage, des bases de données et des logiciels. Les principaux principes du cloud computing incluent la mutualisation des ressources, l'accès à la demande, la scalabilité et le paiement à l'usage.

Le cloud computing a changé la manière dont nous stockons et partageons les données. Plutôt que de les sauvegarder sur des disques durs ou des serveurs locaux, le cloud permet de gérer les données en ligne, les rendant accessibles depuis n'importe où avec une connexion Internet.

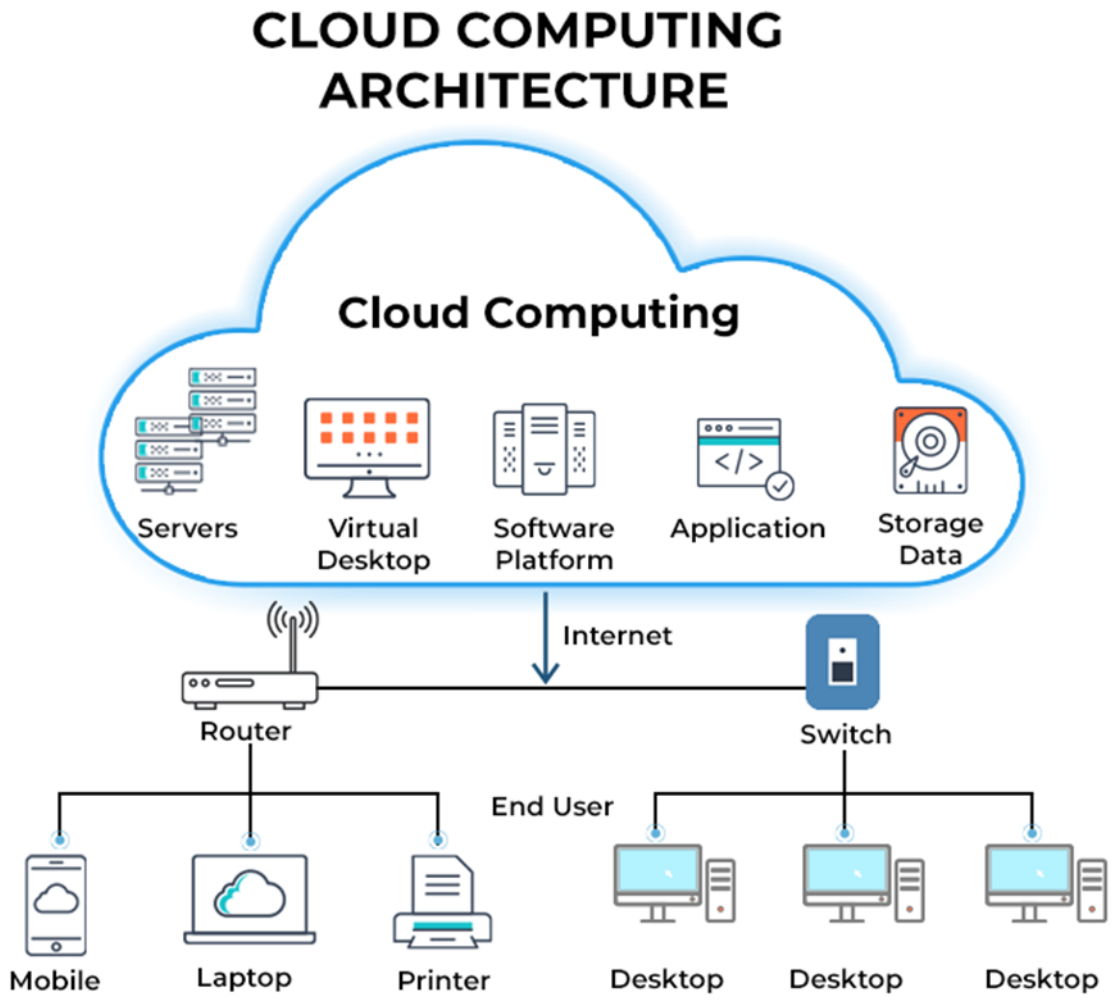


Figure 7: Architecture du cloud computing

Autrefois, nous sauvegardions nos photos, documents et musiques sur des supports physiques comme des disques durs externes ou des clés USB. Aujourd'hui, ces données sont sauvegardées dans le cloud. Les entreprises ont suivi cette évolution, transférant leurs données de serveurs sur site vers le cloud, rendant ainsi cette technologie omniprésente.

Les entreprises adoptent le cloud pour répondre à divers besoins. Cette technologie facilite le développement d'applications, réduit les coûts, soutient le télétravail et offre une grande flexibilité dans le déploiement de produits. Le cloud computing est une solution économique et efficace pour répondre aux exigences des données modernes.

Cependant, le cloud computing comporte des risques de sécurité. Les entreprises collaborent souvent avec des fournisseurs de cloud, confiant ainsi des données sensibles à des tiers. Par conséquent, la sécurité des données dans le cloud nécessite une attention particulière.

Le cloud computing existe sous différentes formes, chacune présentant ses propres risques et responsabilités pour les utilisateurs et les fournisseurs. Les meilleures pratiques de sécurité doivent être intégrées aux procédures, politiques et technologies des entreprises.

La sécurité du cloud inclut des processus, stratégies et outils pour protéger les données et réduire les risques associés à l'utilisation du cloud. Avec de nombreuses entreprises reposant sur des services cloud, la sécurité du cloud est devenue indispensable.

En choisissant de stocker leurs données via Internet, les entreprises bénéficient de meilleures performances et d'une collaboration accrue, mais s'exposent aussi à des problèmes de sécurité qu'il est essentiel de résoudre.

La sécurité du cloud regroupe les processus, stratégies et outils utilisés pour protéger et sécuriser les données tout en réduisant les risques liés à l'utilisation du cloud computing par les entreprises. Étant donné que la majorité des entreprises s'appuient sur des services cloud, assurer la sécurité du cloud est crucial. Bien que le stockage de données via Internet offre de nombreux avantages, il expose également à des problèmes de sécurité qu'il est impératif de résoudre pour garantir la protection des informations sensibles et assurer la continuité des activités.

2.1.2 Les Principales Formes de Cloud Computing et Modèle de responsabilité partagée

2.1.2.1 Les Principales Formes de Cloud Computing

Le cloud computing se décline en trois principales catégories : l'infrastructure en tant que service (IaaS), la plateforme en tant que service (PaaS) et le logiciel en tant que service (SaaS). Chaque modèle offre des capacités uniques adaptées à des besoins spécifiques.

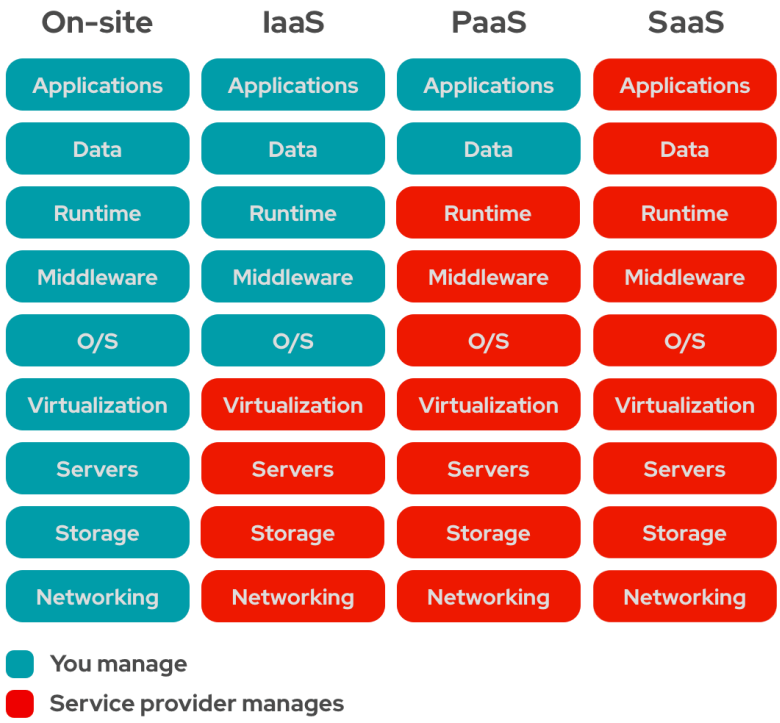


Figure 8: services du cloud computing

- **Infrastructure as a Service (IaaS)**

IaaS offre une infrastructure informatique virtuelle comprenant des serveurs, des réseaux et du stockage. Les utilisateurs peuvent installer et gérer leurs propres systèmes d'exploitation et applications, offrant ainsi un contrôle complet sur leur environnement informatique tout en bénéficiant de la flexibilité du cloud. Exemples : Amazon EC2, Google Compute Engine .

  - **Responsabilités de Sécurité :**
    - **Fournisseur Cloud :** Responsable de la sécurité des infrastructures, y compris les centres de données physiques, le stockage et la virtualisation.
    - **Client :** Responsable de la gestion des systèmes d'exploitation, des applications et des données .

- **Platform as a Service (PaaS)**

PaaS fournit un environnement de développement et de déploiement complet dans le cloud. Les développeurs peuvent créer et déployer des applications sans se soucier de la gestion de l'infrastructure sous-jacente. Ce modèle permet une innovation rapide et une réduction des coûts de développement. Exemples : Google App Engine, AWS Elastic Beanstalk.

  - **Responsabilités de Sécurité :**

    - **Fournisseur Cloud :** Responsable de la sécurité de la plateforme, y compris les systèmes d'exploitation, les bases de données et les outils de développement.
    - **Client :** Responsable du développement, de la mise à jour et de la sécurisation des applications déployées sur la plateforme.

- **Software as a Service (SaaS)**

Saas propose des applications logicielles accessibles via Internet. Les utilisateurs accèdent aux applications via un navigateur web, et le fournisseur gère l'infrastructure, la maintenance et la sécurité. Ce modèle est pratique pour les entreprises cherchant à minimiser les tâches de gestion technique. Exemples : Google Workspace, Microsoft Office 365.

  - **Responsabilités de Sécurité :**

    - **Fournisseur Cloud :** Responsable de la gestion et de la sécurité complètes de l'application, de l'infrastructure sous-jacente et des données stockées.
    - **Client :** Responsable de la gestion des accès utilisateurs et de la protection contre le phishing et autres attaques sociales.

2.1.2.2 Modèle de responsabilité partagée

Le modèle de responsabilité partagée dans le cloud computing est essentiel pour garantir la sécurité et la gestion des données. Il divise les tâches de sécurité entre le fournisseur de services cloud et le client, chaque partie ayant des responsabilités spécifiques.

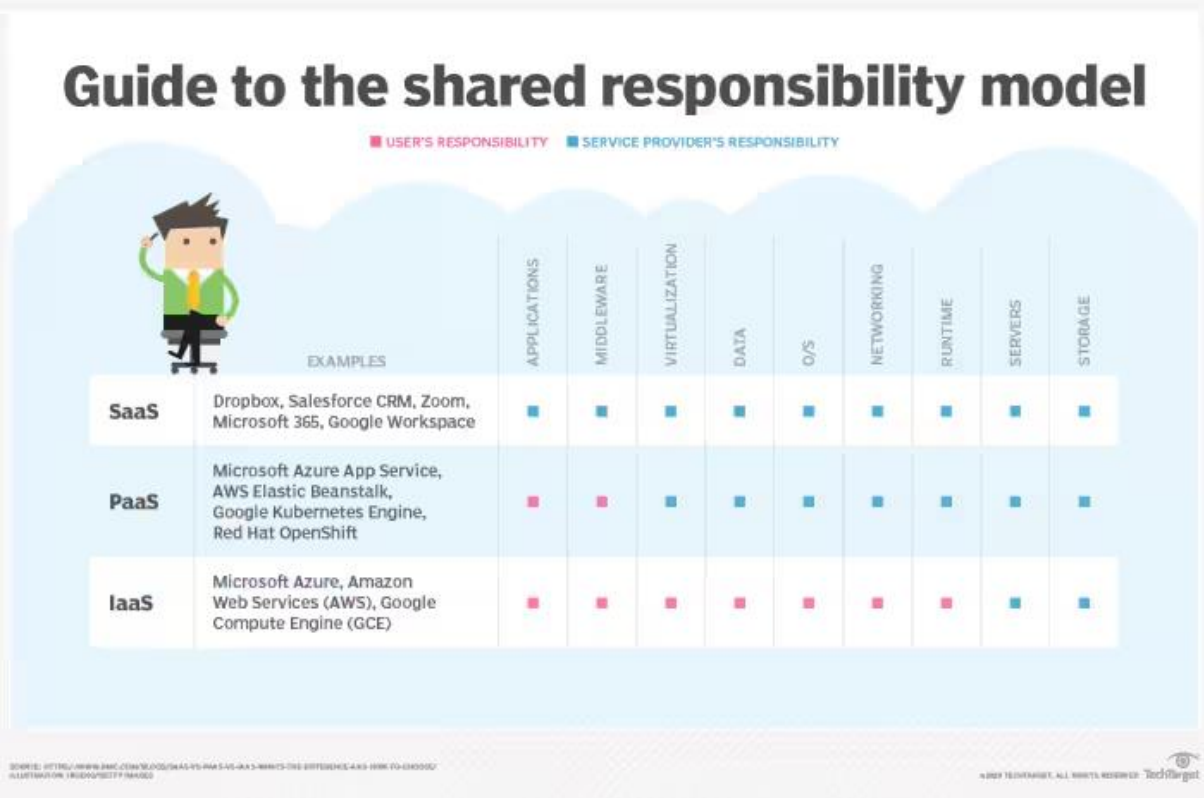


Figure 9: Modèle de responsabilité partagée

- **Responsabilités du fournisseur de services cloud :**

Les fournisseurs, comme AWS, Microsoft Azure et Google Cloud, prennent en charge la sécurité de l'infrastructure sous-jacente. Cela inclut la protection des centres de données physiques, la sécurité du matériel et des réseaux, et la maintenance de la couche de virtualisation. Ils s'assurent également que l'infrastructure est régulièrement mise à jour avec les derniers correctifs de sécurité.

- **Responsabilités du client :**

Le client est responsable de la gestion des données qu'il héberge dans le cloud, de la configuration des accès aux ressources, et de la sécurité des applications qu'il déploie. Cela inclut des tâches telles que le chiffrement des données, la gestion des identités et des accès, et la surveillance des activités pour détecter toute activité suspecte. Le client doit également s'assurer que ses pratiques sont conformes aux régulations pertinentes, comme le GDPR ou le HIPAA, en fonction de la nature des données traitées .

- **Partage des responsabilités :**

Certaines responsabilités sont partagées. Par exemple, bien que le fournisseur assure la sécurité de l'infrastructure, le client est responsable de la configuration des services de sécurité supplémentaires, comme les pare-feu. Cela nécessite une bonne compréhension et

une coopération entre les deux parties pour garantir une sécurité optimale et la protection des données.

Le modèle de responsabilité partagée exige une collaboration étroite entre le fournisseur et le client pour assurer la sécurité des environnements cloud.

2.1.2.3 Modèle de responsabilité partagée selon AWS

Le modèle de responsabilité partagée est une structure essentielle qui répartit les tâches de sécurité entre AWS et ses clients. Ce cadre clarifié qui est responsable de quoi, assurant une protection complète des données et des infrastructures.

- **Responsabilité d'AWS (sécurité du cloud) :**

  AWS est responsable de la sécurité de l'infrastructure de base, y compris la sécurité physique des centres de données, le matériel, les logiciels, les réseaux, et la couche de virtualisation. Cela signifie que AWS gère la maintenance des serveurs, la gestion des mises à jour de sécurité pour l'infrastructure et la protection contre les intrusions physiques. En assurant ces fonctions, AWS crée un environnement sécurisé pour l'hébergement des services cloud.

- **Responsabilité du client (sécurité dans le cloud) :**

  Les clients, quant à eux, sont responsables de la sécurité de leurs données et applications dans le cloud. Cela inclut la gestion des systèmes d'exploitation invités, l'installation des mises à jour et des correctifs de sécurité, et la configuration des paramètres de sécurité, comme les groupes de sécurité (pare-feu). Par exemple, avec Amazon EC2, les clients doivent gérer eux-mêmes la sécurité des systèmes d'exploitation et des applications qu'ils utilisent. Pour des services tels qu'Amazon S3 ou DynamoDB, AWS gère l'infrastructure, mais les clients sont responsables de la gestion des accès aux données et de l'application des stratégies de sécurité appropriées, comme le chiffrement des données .

- **Partage des responsabilités :**

  Ce partage des responsabilités peut varier selon le type de service utilisé. Dans les services IaaS (Infrastructure as a Service) comme EC2, le client a une plus grande part de responsabilité en matière de configuration et de sécurité des systèmes d'exploitation et des applications. Dans les services PaaS (Platform as a Service) ou SaaS (Software as a Service), AWS gère davantage d'éléments de sécurité, offrant ainsi aux clients une expérience plus gérée. Cette différenciation permet une flexibilité et un contrôle adaptés aux besoins spécifiques des clients, leur offrant la possibilité de sécuriser leur environnement selon leurs propres critères.

En comprenant et en respectant ces responsabilités partagées, les entreprises peuvent s'assurer que leurs environnements cloud sont sécurisés et conformes, tout en bénéficiant de la flexibilité et de l'évolutivité du cloud AWS.

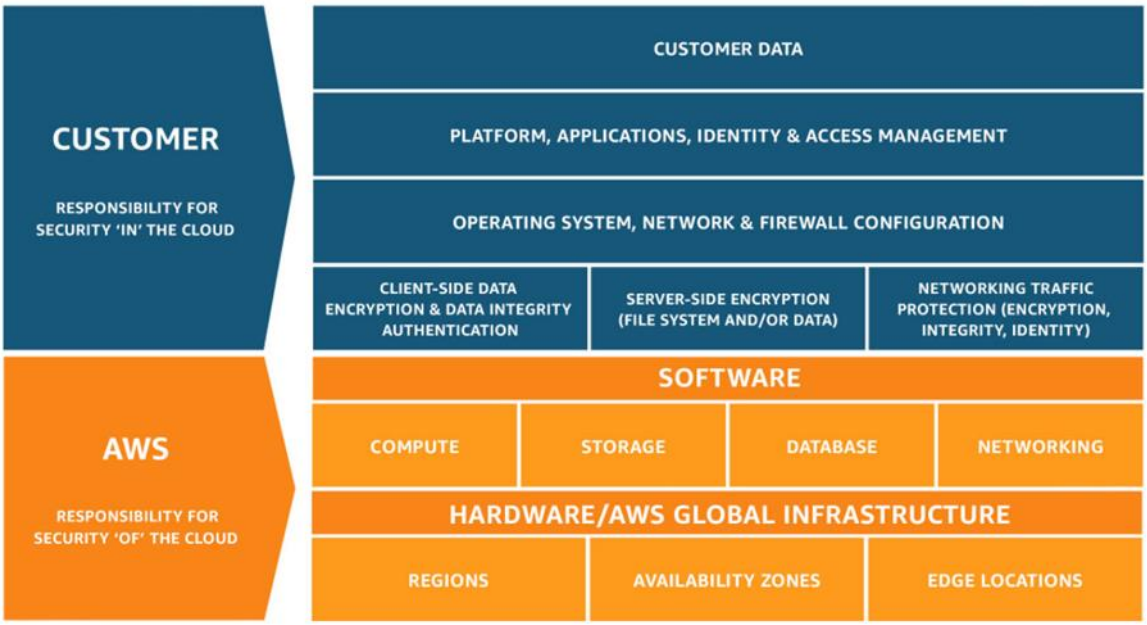


Figure 10: Modèle de responsabilité partagée sur AWS

Le modèle de responsabilité partagée est une pierre angulaire de la sécurité et de la conformité dans le cloud, répartissant les tâches entre AWS et ses clients. Ce modèle assure une gestion efficace des infrastructures et des applications, tout en clarifiant les rôles de chacun.

- **Contrôles acquis :**

  Les clients bénéficient de la sécurité physique des centres de données et des environnements fournis par AWS. Cela inclut la protection contre les intrusions physiques et les catastrophes naturelles, garantissant ainsi que l'infrastructure de base est toujours sécurisée .

- **Contrôles partagés :**

  Ces contrôles sont divisés entre AWS et le client, avec des responsabilités spécifiques pour chaque partie. Par exemple :

  - **Gestion des correctifs** : AWS se charge de la mise à jour et de la correction des défauts de l'infrastructure, tels que les serveurs et les réseaux. En revanche, le client doit gérer les mises à jour de sécurité et les correctifs pour ses systèmes d'exploitation et applications hébergés sur les instances AWS.
  - **Gestion de la configuration** : Tandis qu'AWS s'assure que ses infrastructures sont configurées et sécurisées, les clients doivent configurer et sécuriser leurs systèmes d'exploitation et applications. Cela inclut des tâches telles que l'installation de logiciels de sécurité, la configuration des pare-feu et la gestion des accès utilisateurs.

- **Connaissance et formation** : AWS forme ses propres employés pour gérer l'infrastructure cloud, mais les clients doivent former leurs équipes à l'utilisation sécurisée des services AWS et à la gestion des systèmes qu'ils y déploient.

- **Spécificité client :**

Certains contrôles sont exclusivement sous la responsabilité des clients, en fonction des services et applications spécifiques utilisés. Par exemple, pour des applications nécessitant des mesures de sécurité spéciales, comme des routages sécurisés ou des protocoles de communication particuliers, les clients doivent mettre en place ces configurations supplémentaires pour protéger leurs données sensibles.

Ce modèle permet aux clients de bénéficier d'une infrastructure sécurisée tout en conservant le contrôle et la responsabilité de leurs propres données et configurations. En comprenant bien ce partage des responsabilités, les entreprises peuvent mieux sécuriser leurs environnements cloud et répondre efficacement aux exigences de conformité.

2.1.3 Modèles de Déploiement Cloud

Les environnements cloud offrent divers types de déploiement. Pour les entreprises, il est crucial de comprendre comment accéder au cloud et utiliser les données qui s'y trouvent. Chaque type de déploiement possède ses propres spécificités. Il est essentiel de travailler avec votre fournisseur de services cloud pour déterminer celui qui convient le mieux à votre entreprise.

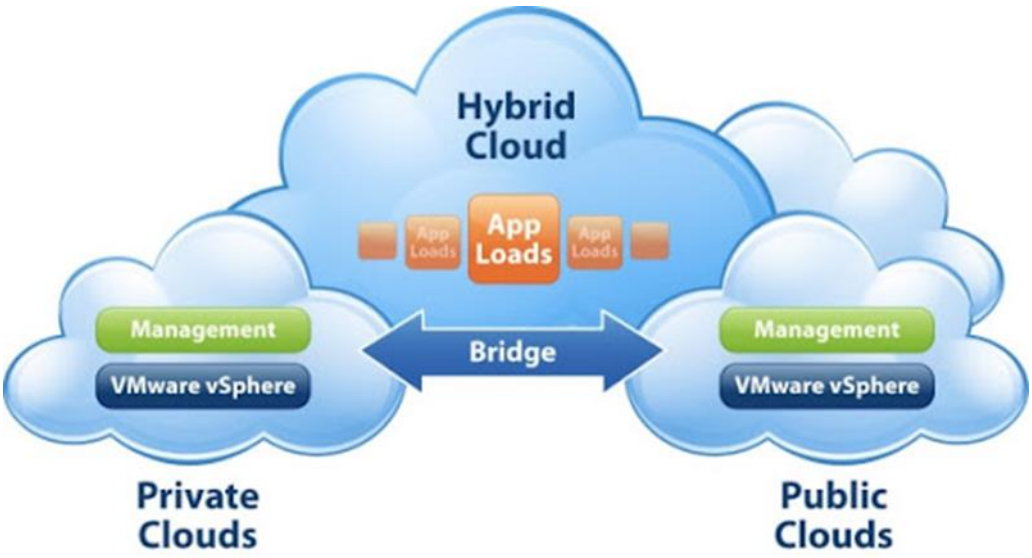


Figure 11: Types de cloud computing

- **Cloud public :** Ce modèle repose sur une infrastructure partagée, fournie par des géants du secteur comme Amazon Web Services (AWS), Microsoft Azure ou Google Cloud. Les services offerts sont accessibles à tous, généralement via un abonnement ou un système de paiement à l'usage. Il est idéal pour les entreprises cherchant une solution économique et flexible, avec un déploiement rapide. Cependant, l'infrastructure partagée peut poser des défis en matière de sécurité et de performance, notamment en cas de surcharge par d'autres utilisateurs.

- **Cloud privé :** Le cloud privé est dédié à une seule organisation, offrant un contrôle total sur l'infrastructure et une sécurité renforcée. Cette configuration est particulièrement adaptée aux données sensibles ou aux applications nécessitant une conformité stricte. La gestion peut être assurée en interne ou par un fournisseur tiers. Bien que les coûts soient généralement plus élevés en raison des besoins en matériel et gestion, ce modèle offre une personnalisation et un contrôle inégalés.

- **Cloud hybride :** Ce modèle combine les avantages des clouds public et privé. Il permet de garder les données critiques et les applications sensibles dans un environnement privé, tout en utilisant des ressources publiques pour des tâches moins critiques. Cela offre une flexibilité et une évolutivité accrues, tout en maîtrisant les coûts et la sécurité. Le cloud hybride convient particulièrement aux entreprises avec des besoins variables et des exigences spécifiques en matière de sécurité.

- **Multicloud :** Le modèle multicloud implique l'utilisation de plusieurs services cloud de différents fournisseurs, permettant ainsi de diversifier les risques et d'optimiser les performances. Cela permet aux entreprises de choisir les meilleurs services pour chaque tâche spécifique, évitant ainsi une dépendance excessive à un seul fournisseur. Bien que cette approche offre une grande flexibilité, elle peut également poser des défis en termes de gestion et de sécurité, en raison de la complexité accrue des opérations.

Ces différents types de déploiement cloud offrent chacun des solutions adaptées à des besoins spécifiques, permettant aux entreprises de choisir en fonction de leurs priorités en termes de coûts, de sécurité et de flexibilité.

2.1.4 Avantages et Défis du Cloud Computing

Le cloud computing offre une multitude d'avantages essentiels pour les entreprises modernes, tout en présentant certains défis qu'il est crucial de comprendre et de gérer efficacement.

- **Avantages :**
    - **Flexibilité :** Le cloud permet une grande adaptabilité, donnant aux entreprises la possibilité d'accéder à des ressources variées selon leurs besoins. Cela inclut la capacité de développer de nouvelles applications, de tester des idées ou de répondre à des pics de demande sans investissements massifs en infrastructures supplémentaires.
    - **Scalabilité :** Les entreprises peuvent ajuster leurs ressources en fonction des besoins, augmentant ou réduisant leur capacité selon l'activité. Cette flexibilité aide à optimiser les coûts et à gérer les ressources de manière efficiente.
    - **Réduction des coûts :** Grâce au modèle de paiement à l'usage, les entreprises ne paient que pour les services utilisés. Cela élimine les coûts initiaux élevés et réduit les dépenses opérationnelles, ce qui est particulièrement avantageux pour les startups et les PME.
    - **Accessibilité :** Le cloud permet aux employés d'accéder aux données et applications de n'importe où, facilitant le télétravail et la collaboration internationale. Cette accessibilité est cruciale pour une flexibilité optimale du lieu de travail.
    - **Innovation rapide :** Les entreprises peuvent adopter rapidement de nouvelles technologies via le cloud, leur permettant de rester compétitives et d'innover sans les délais et coûts associés à l'achat de nouveaux matériels.

- **Défis :**
    - **Sécurité :** Il est crucial de protéger les données sensibles et de gérer les risques de sécurité, en particulier contre les cyberattaques et les violations de données.
    - **Conformité :** Les entreprises doivent respecter des réglementations et des normes de sécurité spécifiques à leur secteur, telles que le GDPR, le PCI-DSS et le HIPAA, pour garantir la protection des données.
    - **Gestion de la Complexité :** L'intégration et la gestion des services cloud provenant de différents fournisseurs nécessitent des compétences spécialisées et des outils de gestion adaptés.
    - **Fiabilité :** La dépendance à l'égard de la connectivité Internet et des performances des fournisseurs de services cloud peut affecter la disponibilité et les performances des services. Les interruptions ou les pannes peuvent avoir un impact significatif sur les opérations des entreprises.
    - **Contrôle :** Les entreprises peuvent perdre le contrôle sur certains aspects de l'infrastructure et des données. Il est donc essentiel de mettre en place des

accords de niveau de service (SLA) rigoureux pour garantir la performance et la sécurité des services fournis, et de s'assurer que les fournisseurs de cloud respectent les politiques de sécurité et de gestion des données appropriées.

En adoptant une approche stratégique, les entreprises peuvent tirer le meilleur parti du cloud tout en minimisant les risques associés.

2.2 Concepts de Cybersécurité

2.2.1 Aperçu des Principes et Techniques de Base

La cybersécurité englobe la protection des réseaux, des systèmes, des appareils et des informations sensibles contre les menaces et les accès non autorisés. Ce processus est essentiel pour préserver l'intégrité et la confidentialité des données, ainsi que pour assurer la disponibilité des systèmes. Il s'agit d'une approche globale qui nécessite une collaboration étroite entre les équipes, les processus et les technologies. Pour cela, les experts en cybersécurité déploient diverses stratégies, notamment l'utilisation de pare-feux, de systèmes de détection et de prévention des intrusions, et de protocoles de chiffrement. Ces mesures sont conçues pour protéger non seulement les actifs de l'entreprise, mais aussi les employés, les clients et les utilisateurs finaux contre les cybermenaces.

La cybersécurité consiste à protéger les systèmes, les réseaux et les données contre les cyberattaques. Les principes de base de la cybersécurité incluent :

- **Confidentialité** : Garantir que les informations ne sont accessibles qu'à ceux qui sont autorisés à y accéder. Cela implique des contrôles d'accès stricts et l'utilisation de techniques de cryptage pour protéger les données sensibles.
- **Intégrité** : Assurer que les informations sont exactes et complètes, et qu'elles n'ont pas été altérées de manière non autorisée. Les techniques telles que les hash et les signatures numériques sont couramment utilisées pour vérifier l'intégrité des données.
- **Disponibilité** : Garantir que les informations et les ressources sont disponibles pour les utilisateurs autorisés lorsqu'ils en ont besoin. Cela implique la mise en place de mesures de redondance, de sauvegarde et de plans de reprise après sinistre pour assurer la continuité des opérations.
- **Authentification** : Vérifier l'identité des utilisateurs, des appareils et des systèmes avant de leur permettre d'accéder aux ressources. Les mécanismes d'authentification incluent les mots de passe, les certificats numériques et l'authentification multifactorielle (MFA).
- **Autorisation** : Déterminer les permissions d'accès des utilisateurs, définissant ce qu'ils sont autorisés à faire avec les ressources auxquelles ils ont accès. Les modèles

d'autorisation incluent le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC).

- **Audit et Surveillance** : Suivre et enregistrer les activités dans le système pour détecter les anomalies, les violations de sécurité et pour assurer la conformité avec les politiques de sécurité. Les journaux de sécurité, les systèmes de détection d'intrusion (IDS), et les systèmes de gestion des informations et des événements de sécurité (SIEM) sont des outils clés pour la surveillance et l'audit.

2.2.2 Techniques de Cybersécurité

La cybersécurité couvre une large gamme de types et de techniques, chacune adaptée à des aspects spécifiques de la protection des systèmes d'information et des données. Voici un aperçu détaillé de certaines catégories clés :

- **Security Information and Event Management(SIEM) :** Les systèmes SIEM combinent la gestion des informations de sécurité et des événements de sécurité pour offrir une vue d'ensemble des activités de sécurité. Ils collectent, analysent et interprètent les logs et les données d'événements pour détecter les menaces et assurer la conformité réglementaire. Ces systèmes alertent les équipes de sécurité en cas d'anomalies, facilitant ainsi une réponse rapide aux incidents.
- **Sécurité aux points de terminaison :** Cette catégorie concerne la protection des dispositifs individuels tels que les ordinateurs et les smartphones. Les solutions incluent les systèmes de détection et de prévention des intrusions (IDS/IPS), le chiffrement des données et la gestion des appareils mobiles, visant à prévenir les infections par des malwares et à sécuriser les données stockées sur ces dispositifs.
- **Sécurité du cloud :** Avec l'essor des services cloud, la sécurité du cloud est essentielle pour protéger les données et les applications hébergées. Cela implique la gestion des configurations de sécurité, la surveillance continue des menaces et l'application de contrôles de sécurité spécifiques aux environnements cloud.
- **Security Orchestration, Automation, and Response (SOAR) :** Les solutions SOAR automatisent et orchestrent les réponses aux incidents de sécurité, intégrant divers outils pour coordonner les réponses et réduire le temps de réaction. Elles permettent d'automatiser les réponses aux incidents via des playbooks, aidant ainsi les équipes à se concentrer sur les menaces critiques.
- **Sécurité des applications :** Ce domaine se concentre sur la protection des applications contre les vulnérabilités, qu'elles soient dans le cloud ou sur des serveurs sur site. Il inclut des tests de sécurité, l'intégration de mesures de sécurité dès la phase de développement et la surveillance continue pour détecter et corriger les failles.

- **Sécurité réseau :** Cette catégorie vise à protéger l'infrastructure réseau contre les abus et les accès non autorisés, en utilisant des pare-feu, des VPN et d'autres technologies pour sécuriser les communications et contrôler l'accès.
- **Sécurité IoT :** Avec l'augmentation des dispositifs connectés, la sécurité IoT vise à protéger ces dispositifs contre les cyberattaques, en sécurisant les communications et les données échangées.
- **Gestion des identités et des accès (IAM) :** IAM gère les identités numériques et les accès des utilisateurs, incluant l'authentification multifactorielle et la gestion des accès privilégiés, garantissant que seules les personnes autorisées accèdent aux informations sensibles.
- **Zero Trust :** Ce modèle de sécurité ne fait jamais confiance par défaut à aucun utilisateur, exigeant une vérification stricte de toutes les entités avant d'accorder l'accès aux ressources réseau, particulièrement pertinent avec le travail à distance.
- **Sécurité mobile :** Avec l'utilisation croissante des appareils mobiles, cette catégorie protège ces dispositifs contre les pertes de données et les accès non autorisés, incluant la gestion des politiques de sécurité et le contrôle des applications.

2.2.3 Types de menaces de cybersécurité

Les menaces de cybersécurité sont variées et représentent un défi croissant pour les entreprises et les organisations. Voici un aperçu détaillé de certains types courants de menaces :

- **Malwares**
  Les malwares, ou logiciels malveillants, sont conçus pour endommager ou perturber les systèmes informatiques, voler des informations ou accéder sans autorisation. Ils incluent les virus, les vers, les chevaux de Troie et les logiciels espions, souvent distribués via des e-mails contenant des liens ou des pièces jointes infectées.

- **Ransomwares**
  Les ransomwares chiffrent les données d'une victime et exigent une rançon pour les déchiffrer. Ce type d'attaque peut paralyser les opérations d'une entreprise en rendant les systèmes ou les fichiers critiques inaccessibles jusqu'à ce que la rançon soit payée.

- **Phishing**
  Le phishing utilise des e-mails, SMS ou sites Web frauduleux pour inciter les victimes à divulguer des informations sensibles, comme des identifiants de connexion ou des numéros de carte de crédit. Ces attaques peuvent paraître provenir de sources légitimes telles que des banques ou des collègues.

- **Menaces internes**

Ces menaces proviennent de personnes ayant un accès autorisé aux systèmes d'une organisation, comme des employés ou des sous-traitants. Elles peuvent, intentionnellement ou non, compromettre la sécurité en divulguant des informations sensibles ou en facilitant l'accès à des tiers.

- **Ingénierie sociale**

  L'ingénierie sociale manipule les gens pour qu'ils révèlent des informations confidentielles ou prennent des mesures compromettantes, souvent en exploitant des aspects psychologiques pour tromper les victimes.

- **Menaces persistantes avancées (APT)**

  Les APT sont des attaques ciblées et prolongées menées par des groupes organisés, cherchant à obtenir des informations sensibles ou à perturber des opérations critiques. Elles peuvent rester non détectées pendant de longues périodes, permettant aux attaquants de recueillir des données précieuses.

- **Exploits IoT**

  Les cybercriminels ciblent les appareils de l'Internet des objets (IoT), qui peuvent être des points d'entrée pour accéder à des réseaux plus larges. Ces appareils, souvent mal sécurisés, peuvent être utilisés pour lancer des attaques ou obtenir des informations.

- **Attaques par déni de service (DDoS)**

  Les attaques DDoS submergent un système de requêtes pour le rendre inaccessible aux utilisateurs légitimes. Elles utilisent souvent des réseaux de dispositifs compromis pour générer un trafic énorme, perturbant ainsi les opérations normales.

Ces menaces illustrent la complexité croissante de la cybersécurité et soulignent l'importance de mettre en place des mesures de défense solides pour protéger les actifs numériques.

2.2.4 Cas d'utilisation de la cybersécurité

La cybersécurité est essentielle pour protéger les entreprises contre les cybermenaces toujours croissantes. Voyons comment différentes stratégies peuvent être appliquées pour renforcer la sécurité numérique de manière plus accessible.

- **Monitoring continu**

  Imaginer le monitoring continu comme un système de sécurité à plusieurs niveaux pour votre maison, avec des caméras, des alarmes, et des gardiens surveillant constamment. En cybersécurité, cela se traduit par l'utilisation de systèmes de détection d'intrusion

(IDS) et l'analyse des journaux pour surveiller en permanence les réseaux et les systèmes. Le but est de détecter rapidement toute activité suspecte pour intervenir avant que des dommages ne se produisent.

- **Protection contre les menaces**

  Penser à la protection contre les menaces comme à des serrures solides et des systèmes d'alarme sophistiqués qui empêchent les intrus d'entrer. Les entreprises utilisent des pare-feu, des antivirus et des systèmes de prévention des intrusions pour se protéger contre les malwares et autres cybermenaces. Ces mesures visent à bloquer les attaques avant qu'elles ne pénètrent dans les systèmes.

- **Examen et réponse aux incidents**

  Avoir un plan pour les urgences, comme un plan d'évacuation en cas d'incendie, est crucial. En cybersécurité, cela signifie disposer de procédures pour enquêter sur les incidents et y répondre rapidement. Les outils automatisés de réponse aux incidents aident à gérer les alertes, enquêter sur les problèmes et minimiser les impacts des attaques

- **Recherche des menaces**

  La recherche des menaces, c'est comme avoir des détectives spécialisés qui cherchent activement les failles avant qu'elles ne soient exploitées. Cette approche proactive permet d'identifier et de neutraliser les menaces avant qu'elles ne causent des dommages. Les équipes de sécurité analysent les comportements anormaux et les signes de compromission pour rester en avance sur les cybercriminels.

Ces pratiques sont essentielles pour construire une défense robuste contre les menaces numériques et protéger les données sensibles des entreprises. En adoptant ces stratégies, les entreprises peuvent non seulement se protéger contre les attaques, mais aussi améliorer leur résilience face aux menaces future.

2.3 Présentation de AWS GuardDuty, Macie, et Security Hub

2.3.1 Amazon GuardDuty

Amazon GuardDuty est un service de sécurité dans le cloud, conçu pour détecter les menaces et surveiller en continu les activités suspectes dans les environnements AWS. Ce service utilise une combinaison de machine learning, d'intelligence sur les menaces et d'analyse de logs pour identifier les activités potentiellement malveillantes ou non autorisées.

2.3.1.1 Fonctionnement

Amazon GuardDuty est un service de détection des menaces qui surveille en continu les comptes et ressources AWS pour identifier les activités malveillantes ou non autorisées. Voici comment il fonctionne :

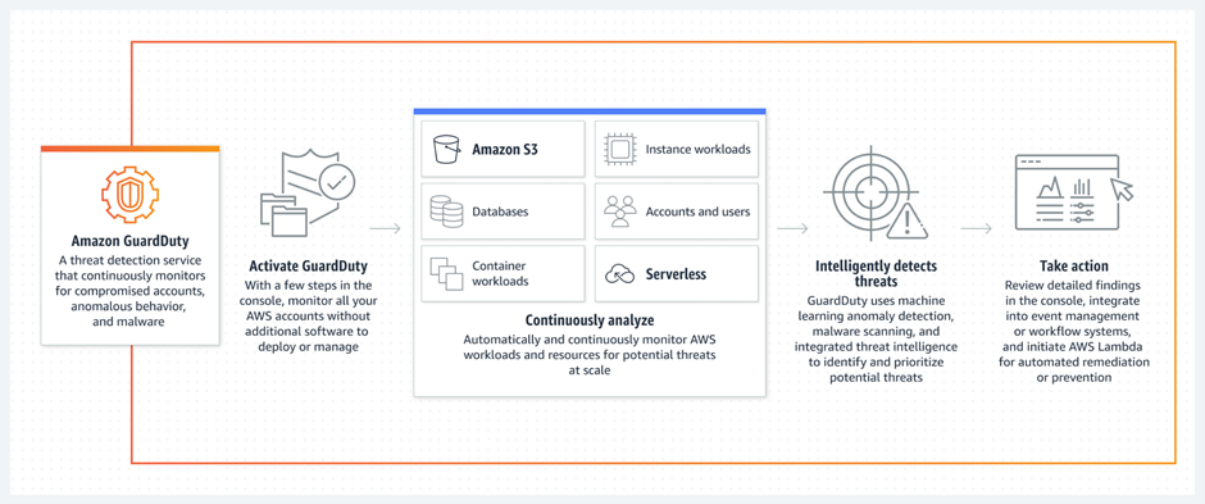


Figure 12: Architecture Amazon GuardDuty

- **Surveillance des Logs et des Activités**

  GuardDuty analyse les journaux de plusieurs sources, notamment AWS CloudTrail, VPC Flow Logs et les logs DNS. En utilisant ces données, il peut détecter des comportements suspects, tels que des tentatives de connexion inhabituelles ou des appels d'API anormaux.

- **Utilisation de l'Intelligence sur les Menaces et du Machine Learning**

  Le service s'appuie sur des flux d'intelligence sur les menaces et des modèles de machine learning pour identifier les activités potentiellement malveillantes. Par exemple, il peut repérer des connexions depuis des adresses IP malveillantes ou des tentatives de désactivation de la journalisation CloudTrail. GuardDuty est aussi capable de détecter des activités comme l'extraction de cryptomonnaies sur des instances EC2 compromises.

- **Classification et Gestion des Incidents**

  Les menaces détectées sont classées par niveau de gravité (faible, moyen, élevé), permettant aux équipes de sécurité de prioriser leur réponse. GuardDuty peut être intégré avec d'autres outils AWS, tels que AWS Lambda, pour automatiser

les réponses aux incidents en temps réel. Par exemple, il peut isoler immédiatement des ressources compromises pour limiter les dommages.

Amazon GuardDuty offre une surveillance continue et une détection des menaces dans les environnements AWS, utilisant des techniques avancées de machine learning et des renseignements sur les menaces pour protéger contre les activités malveillantes. C'est un outil essentiel pour renforcer la sécurité des infrastructures cloud sur AWS.

2.3.1.2 **Avantages de GuardDuty**

Amazon GuardDuty offre de nombreux avantages pour renforcer la sécurité des environnements AWS :

- **Détection Avancée et Précise des Menaces**

  GuardDuty utilise des modèles de machine learning et des flux de renseignement sur les menaces pour identifier rapidement les comportements suspects. Par exemple, il peut détecter des connexions provenant d'adresses IP malveillantes ou des tentatives d'escalade de privilèges. Cette technologie avancée permet de repérer non seulement les menaces connues, mais aussi les activités anormales indiquant des attaques nouvelles ou en cours.

- **Surveillance Continue et Réactive**

  Le service offre une surveillance 24/7 des comptes et ressources AWS, analysant les logs de CloudTrail, les VPC Flow Logs et les logs DNS. Cette surveillance continue permet de détecter rapidement les incidents de sécurité, de les classer par gravité et d'automatiser les réponses nécessaires, réduisant ainsi les risques de dommages.

- **Évolutivité et Flexibilité**

  GuardDuty s'adapte facilement aux besoins des entreprises, que ce soit pour des petites start-ups ou des grandes entreprises. Il peut évoluer avec les charges de travail sans nécessiter une infrastructure de sécurité supplémentaire, permettant ainsi aux entreprises de se concentrer sur leurs activités principales sans se soucier de la gestion de la sécurité.

- **Coût-Efficacité**

  En s'intégrant de manière fluide avec les services AWS existants, GuardDuty minimise les coûts liés à l'infrastructure de sécurité. Le service est facturé à

l'utilisation, permettant aux entreprises de payer uniquement pour les ressources consommées, ce qui en fait une solution abordable même pour les budgets limités.

- **Rapidité et Efficacité dans la Réponse aux Incidents**

  GuardDuty fournit des alertes en temps réel et des recommandations sur les actions à entreprendre en cas d'incident. Cette capacité à réagir rapidement aux menaces aide à minimiser les interruptions de service et à protéger les données sensibles contre les accès non autorisés.

Ces caractéristiques font de GuardDuty un outil précieux pour les entreprises souhaitant sécuriser efficacement leurs environnements AWS.

2.3.1.3 **Protection de la Charge de Travail avec GuardDuty pour AWS**

Amazon GuardDuty joue un rôle crucial dans la sécurisation des charges de travail sur AWS, utilisant des technologies avancées pour détecter et répondre aux menaces potentielles. Voici un aperçu détaillé de ses capacités et avantages :

- **Surveillance Continue et Analyse Avancée**

  GuardDuty surveille en permanence les logs et événements provenant de sources telles que AWS CloudTrail, VPC Flow Logs et les logs DNS. Grâce à l'utilisation de modèles de machine learning et de flux de renseignement sur les menaces, il identifie des activités anormales, comme des tentatives de connexion depuis des IP malveillantes ou des modifications suspectes des configurations de sécurité. Cette surveillance aide à détecter des comportements inhabituels, tels que des transferts de données anormaux ou des accès inhabituels aux ressources, qui peuvent signaler une compromission.

- **Détection des Compromissions et des Malwares**

  GuardDuty excelle dans la détection des instances EC2 compromises pouvant être utilisées pour des activités malveillantes, telles que le minage de cryptomonnaies ou l'hébergement de malwares. Le service surveille également les charges de travail des conteneurs et les fichiers stockés dans Amazon S3 pour détecter la présence de malwares. Cette capacité de détection étendue permet de réagir rapidement aux menaces avant qu'elles ne causent des dommages significatifs.

- **Protection contre les Menaces Internes**

  En plus des menaces externes, GuardDuty peut détecter les menaces internes en surveillant les activités suspectes des utilisateurs ayant accès aux ressources

AWS. Par exemple, il peut identifier des comportements inhabituels, comme des tentatives de modification des politiques de mots de passe ou des accès non autorisés à des données sensibles. Cette surveillance aide à prévenir les abus de privilèges et à protéger les données critiques de l'entreprise.

En combinant une surveillance continue, une analyse avancée des menaces et des capacités de réponse rapide, Amazon GuardDuty offre une protection robuste pour les charges de travail AWS. Il aide les entreprises à se défendre contre une large gamme de menaces, internes et externes, et assure une réponse rapide et efficace aux incidents de sécurité.

2.3.1.4 Cas d'utilisation de GuardDuty

- **Détection des activités suspectes dans les charges de travail d'IA générative**

  GuardDuty surveille les activités anormales liées aux systèmes d'intelligence artificielle, comme Amazon Bedrock et SageMaker. Il détecte les utilisations non autorisées des API et les tentatives de fraude avec des credentials. En identifiant ces activités, GuardDuty aide à prévenir les accès non autorisés et les manipulations des systèmes d'IA, garantissant ainsi la sécurité des données et des processus critiques.

- **Accélération des enquêtes et automatisation des mesures correctives**

  GuardDuty fournit des résultats détaillés et contextuels, incluant des métadonnées et des informations sur les ressources affectées. En intégrant avec Amazon Detective, il permet de rapidement identifier la cause première des incidents de sécurité. Les résultats peuvent être envoyés à AWS Security Hub et Amazon EventBridge pour automatiser les réponses, ce qui permet de gagner du temps et de réduire les risques en prenant des mesures correctives rapides et coordonnées.

- **Protection contre les rançongiciels et autres logiciels malveillants**

  GuardDuty analyse les volumes Amazon EBS et surveille les chargements vers Amazon S3 pour détecter les logiciels malveillants, y compris les rançongiciels, les chevaux de Troie et les programmes de minage de cryptomonnaies. En surveillant ces menaces, GuardDuty aide à protéger les données et les ressources contre les attaques potentielles.

- **Centralisation de la détection des menaces pour les environnements de conteneurs AWS**

GuardDuty fournit un point centralisé pour la gestion des menaces dans les environnements de conteneurs AWS, tels qu'Amazon EKS et ECS. Cette fonctionnalité permet aux équipes de sécurité de détecter, profiler et gérer les menaces de manière plus efficace, simplifiant ainsi le processus de sécurisation des charges de travail conteneurisées et des infrastructures associées.

- **Répondre aux exigences de conformité**

  GuardDuty facilite la conformité avec des normes de sécurité comme PCI DSS, en assurant une surveillance continue et une détection des intrusions. Cette capacité permet aux entreprises de démontrer leur engagement en matière de sécurité et de conformité, renforçant la confiance des partenaires et des régulateurs.

Ces cas d'utilisation illustrent l'importance de GuardDuty dans la protection des environnements AWS contre une variété de menaces et dans l'automatisation des réponses pour une gestion plus efficace de la sécurité.

2.3.2 Amazon Macie

Amazon Macie est un service de sécurité basé sur le cloud qui aide les entreprises à protéger leurs données sensibles sur Amazon Web Services (AWS). Il utilise l'apprentissage automatique et l'intelligence artificielle pour identifier, classer et protéger les informations sensibles stockées dans Amazon S3.

2.3.2.1 Fonctionnement de Amazon Macie

Amazon Macie est un service de sécurité avancé conçu pour identifier et protéger les données sensibles stockées dans le cloud AWS. Son fonctionnement repose sur plusieurs composants clés qui permettent une gestion proactive des informations sensibles.

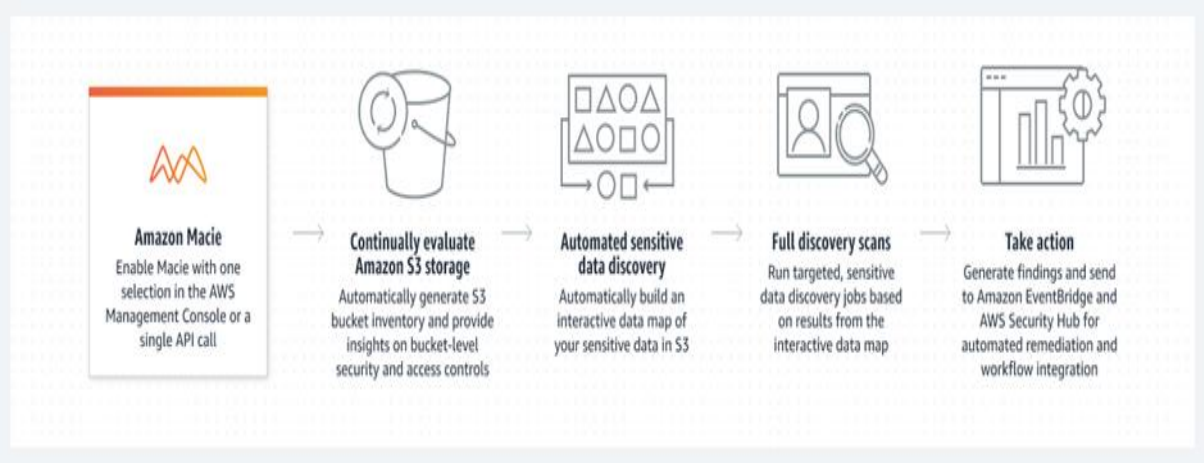


Figure 13: Architecture Am52azon Macie

- **Identification et Classification des Données**
  Amazon Macie utilise des algorithmes de machine learning pour analyser les données stockées dans Amazon S3. Grâce à ces algorithmes, Macie est capable de :

  - **Identifier automatiquement les informations sensibles**, telles que les numéros de carte de crédit, les numéros de sécurité sociale et d'autres données personnelles identifiables (PII).
  - **Classer ces données** selon leur niveau de sensibilité, ce qui aide les entreprises à localiser précisément leurs informations sensibles et à évaluer les risques associés à leur stockage.

  Cette fonction de classification automatique est cruciale pour la gestion des données, car elle permet aux organisations de comprendre où se trouvent leurs informations sensibles et comment elles sont protégées.

- **Surveillance des Comportements et des Accès**
  Amazon Macie surveille en continu les accès aux données stockées et les comportements des utilisateurs pour détecter des activités inhabituelles. Les fonctionnalités incluent :

  - **Détection des tentatives d'accès non autorisées** et des configurations de sécurité incorrectes. Par exemple, Macie peut générer une alerte si une personne tente d'accéder à des données sensibles sans les autorisations appropriées.
  - **Analyse des comportements anormaux**, tels que des tentatives de téléchargement massif de données ou des modifications inhabituelles des configurations de sécurité.

Cette surveillance proactive est essentielle pour prévenir les violations de données et garantir que les informations sensibles restent protégées contre les menaces internes et externes.

- **Intégration avec d'autres services AWS et Rapports**

  Amazon Macie s'intègre de manière transparente avec d'autres services AWS, tels que AWS CloudTrail, AWS Security Hub et divers outils de sécurité, pour offrir une visibilité complète sur les activités de sécurité. Les principales caractéristiques de cette intégration incluent :

  - **Rapports détaillés** sur les types de données sensibles détectées, les événements de sécurité et les recommandations d'actions.
  - **Aide à la conformité** en fournissant des informations et des alertes qui permettent aux équipes de sécurité de répondre rapidement aux incidents et de se conformer aux exigences réglementaires.

Amazon Macie est un outil essentiel pour les entreprises utilisant AWS, leur offrant une solution complète pour la gestion et la protection des données sensibles. Il aide non seulement à prévenir les fuites de données, mais aussi à répondre aux défis de conformité, en fournissant une vue d'ensemble claire des données sensibles et des mesures de sécurité nécessaires.

2.3.2.2 Cas d'utilisation de Amazon Macie

Amazon Macie est un service essentiel pour les entreprises cherchant à sécuriser leurs données sensibles dans le cloud AWS. Voici des cas d'utilisation concrets où Macie peut être particulièrement utile :

- **Renforcement de la Sécurité des Données**

  Amazon Macie agit comme un détective numérique, parcourant les compartiments S3 pour identifier et classer les informations sensibles, telles que les numéros de carte de crédit, les numéros de sécurité sociale et d'autres données personnelles. Cette visibilité accrue permet aux entreprises de repérer rapidement les données sensibles et de prendre les mesures nécessaires pour les protéger contre les fuites potentielles. Par exemple, une entreprise de commerce électronique pourrait utiliser Macie pour s'assurer que les informations de paiement de ses clients sont stockées de manière sécurisée et conformes aux normes de sécurité.

- **Conformité et Gestion des Données Sensibles**

  Pour les entreprises soumises à des réglementations strictes comme le RGPD (Règlement Général sur la Protection des Données) ou la loi HIPAA (Health Insurance Portability and Accountability Act), Macie est un outil précieux. Il automatise la détection des données sensibles et fournit des rapports détaillés qui facilitent la démonstration de la conformité lors des audits. Cela aide les entreprises

à éviter des amendes coûteuses et à maintenir une bonne réputation en matière de protection des données. Par exemple, une société de services financiers peut utiliser Macie pour assurer la conformité avec les régulations en surveillant les données sensibles et en fournissant des rapports réguliers aux régulateurs.

- **Protection des Données pendant la Migration**

Lorsqu'une entreprise migre ses données vers le cloud AWS, la sécurité des informations sensibles est une préoccupation majeure. Macie surveille ces processus de migration pour détecter toute exposition involontaire de données sensibles et s'assurer que les informations restent protégées tout au long du transfert. Par exemple, une entreprise du secteur de la santé pourrait utiliser Macie pour garantir que les dossiers médicaux des patients sont transférés de manière sécurisée, sans risque de violation.

- **Surveillance Continue des Données Sensibles**

Amazon Macie fournit une surveillance continue des données stockées, détectant tout comportement suspect ou toute configuration de sécurité incorrecte. Par exemple, si un employé ou un cybercriminel tente d'accéder à des données sensibles sans autorisation, Macie peut générer une alerte, permettant une intervention rapide pour éviter une violation de données. Cette surveillance en temps réel est essentielle pour la protection proactive des informations sensibles et la prévention des incidents de sécurité.

Amazon Macie est un outil polyvalent pour la protection des données sensibles, offrant aux entreprises non seulement une meilleure sécurité mais aussi une assistance précieuse pour la conformité réglementaire et la gestion proactive des risques.

2.3.2.3 Fonctionnalités d'Amazon Macie

- **Automatisation de la découverte des données sensibles**

Imaginez qu'Amazon Macie soit un détective numérique pour vos données. Il explore vos compartiments Amazon S3 pour découvrir automatiquement des informations sensibles, comme des numéros de carte de crédit ou des PII (informations personnelles identifiables). En configurant des tâches spécifiques, Macie peut effectuer des analyses approfondies, vous aidant à comprendre où se trouvent vos données sensibles et comment elles sont protégées.

- **Large variété de données détectables**

Macie n'est pas limité à une seule région ou type de données. Il utilise des critères intégrés et personnalisables pour détecter divers types de données sensibles dans le monde entier. Cela inclut les données financières, les informations d'identification, et bien plus encore. Vous pouvez même créer vos propres règles pour identifier des

données spécifiques à votre entreprise, assurant une couverture complète et adaptée à vos besoins.

- **Surveillance et contrôle des accès**

Macie ne se contente pas de découvrir les données sensibles, il surveille également les accès à ces données. Il génère des rapports et des alertes en cas de problèmes potentiels, comme des configurations de sécurité incorrectes ou des accès publics non intentionnels. Ces rapports sont essentiels pour prévenir les violations de données et garantir que seules les personnes autorisées ont accès à des informations critiques.

- **Revue et gestion des signalements**

Les signalements dans Macie sont comme des diagnostics médicaux pour vos données. Chaque signalement fournit des détails sur les données sensibles ou les problèmes de sécurité détectés, avec des évaluations de gravité. Vous pouvez explorer ces signalements pour comprendre l'étendue du problème et prendre des mesures correctives appropriées, que ce soit via la console Macie ou l'API pour une intégration plus profonde avec d'autres outils de sécurité.

- **Gestion centralisée des comptes**

Pour les organisations avec plusieurs comptes AWS, Macie permet une gestion centralisée. Cela signifie qu'un administrateur peut superviser la sécurité des données de tous les comptes depuis un seul tableau de bord. Que vous utilisiez AWS Organizations ou des invitations directes, Macie facilite la surveillance et la gestion des données sensibles à grande échelle.

Ces fonctionnalités font d'Amazon Macie un allié précieux pour protéger les données sensibles, renforcer la sécurité et assurer la conformité dans le cloud AWS.

2.3.3 AWS Security Hub

AWS Security Hub est une plateforme centrale qui vous aide à gérer la sécurité de vos ressources dans le cloud AWS c'est-à-dire automatiser les contrôles de sécurité AWS et centraliser les alertes de sécurité. Imaginez que c'est comme un poste de commandement pour toutes vos opérations de sécurité. Security Hub regroupe et organise les données de sécurité provenant de différents services AWS et de solutions de partenaires. Par exemple, il intègre les résultats de services comme Amazon GuardDuty, AWS Macie, et d'autres outils de sécurité, pour offrir une vue d'ensemble de votre posture de sécurité.

Ce service est particulièrement utile pour surveiller la conformité de votre environnement avec des normes de sécurité reconnues, comme le CIS AWS Foundations Benchmark. En

rassemblant ces informations, Security Hub vous permet de prioriser les incidents de sécurité les plus critiques et d'automatiser les réponses grâce à des intégrations avec des services comme AWS Lambda. Cela signifie que vous pouvez configurer des actions automatiques pour répondre rapidement aux menaces, rendant la gestion de la sécurité plus efficace et proactive.

2.3.3.1 Fonctionnement de AWS Security Hub

AWS Security Hub agit comme un centre névralgique pour la gestion de la sécurité dans les environnements AWS. AWS Security Hub est un service de gestion de la posture de sécurité dans le cloud (CSPM) qui effectue des vérifications de bonnes pratiques, regroupe les alertes et permet l'utilisation de la correction automatisée.

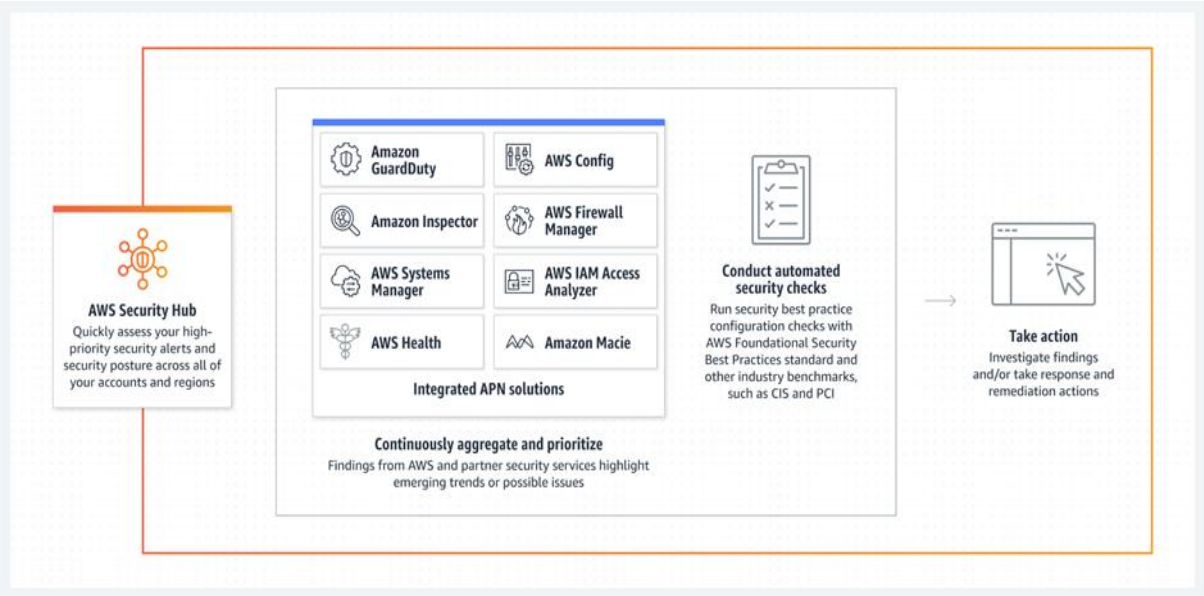


Figure 14: Architecture AWS Security Hub

- **Agrégation des Résultats de Sécurité**

Imaginez AWS Security Hub comme un tableau de bord de contrôle pour la sécurité. Il centralise et organise les informations provenant de divers services AWS et outils tiers, tels que Amazon GuardDuty et AWS Macie. Cela permet d'avoir une vue d'ensemble de toutes les menaces potentielles et des vulnérabilités, triées par niveau de gravité. Ainsi, il est plus facile de prioriser les actions à entreprendre pour renforcer la sécurité.

- **Surveillance Continue et Analyse des Comportements**

Security Hub ne dort jamais. Il surveille en continu les activités sur vos comptes AWS, détectant les comportements inhabituels ou les configurations de sécurité à risque. Par exemple, il peut repérer des configurations S3 incorrectes qui exposeraient des données sensibles au public. Cette surveillance proactive aide à identifier rapidement les problèmes, permettant de réagir avant qu'ils ne deviennent critiques.

- **Vérification de la Conformité**

Pour les entreprises qui doivent se conformer à des réglementations spécifiques, Security Hub compare l'état de leur infrastructure aux normes de sécurité reconnues, comme le CIS AWS Foundations Benchmark. Il génère des rapports de conformité, soulignant les écarts et suggérant des améliorations pour respecter les standards de sécurité. Cela facilite la gestion de la conformité et aide à prévenir les amendes et autres sanctions.

- **Automatisation des Réponses**

L'un des grands avantages de Security Hub est sa capacité à automatiser les réponses aux incidents. En cas de détection d'un problème, il peut déclencher des actions prédéfinies, comme l'activation de fonctions AWS Lambda pour remédier rapidement à la situation. Cela réduit le temps de réponse et assure une gestion efficace des incidents, limitant les impacts potentiels sur les opérations.

En utilisant AWS Security Hub, les entreprises peuvent centraliser la gestion de la sécurité, surveiller en temps réel les activités suspectes, vérifier leur conformité aux normes, et automatiser les réponses aux menaces, renforçant ainsi leur posture de sécurité globale.

2.3.3.2 Les Avantages de AWS Security Hub

- **Surveillance Continue**

AWS Security Hub assure une surveillance continue de votre environnement AWS, détectant rapidement les écarts par rapport aux meilleures pratiques de sécurité. Par exemple, il peut identifier des configurations incorrectes ou des comportements suspects, tels que des tentatives d'accès non autorisées, permettant de prévenir les incidents de sécurité avant qu'ils ne deviennent critiques .

- **Agrégation des Résultats de Sécurité**

Le service centralise et normalise les résultats de divers outils de sécurité, y compris ceux de services AWS comme Amazon GuardDuty et AWS Macie. Cela offre une vue consolidée des vulnérabilités et menaces, facilitant ainsi la priorisation et la gestion des risques de sécurité. L'agrégation des données permet aux équipes de sécurité de se concentrer sur les problèmes les plus urgents et d'optimiser leur réponse.

- **Lancement de Réponses Automatisées**

Grâce à l'intégration avec AWS Lambda et Amazon EventBridge, Security Hub peut automatiser les réponses aux incidents de sécurité. Par exemple, en cas de détection d'une menace, des actions automatiques telles que l'isolation des ressources affectées ou la notification des administrateurs peuvent être déclenchées, réduisant ainsi le temps de réponse et limitant l'impact des incidents.

- **Visualisation du Niveau de Sécurité**

Security Hub offre un tableau de bord intuitif qui visualise le niveau de sécurité de votre infrastructure AWS. Ce tableau de bord affiche des statistiques et des alertes critiques, aidant les administrateurs à surveiller l'état de sécurité et à prendre des décisions éclairées pour renforcer la sécurité de l'organisation. Cette vue d'ensemble est également utile pour les audits de conformité et pour démontrer la sécurité à des parties prenantes externes.

Ces avantages font d'AWS Security Hub un outil précieux pour gérer et améliorer la sécurité des environnements AWS, en fournissant une surveillance proactive, une réponse rapide aux incidents et une vue claire de la posture de sécurité.

2.3.3.3 Cas d'utilisation de AWS Security Hub

- **Gestion de la Posture de Sécurité dans le Cloud (CSPM)**

AWS Security Hub simplifie l'évaluation de la sécurité en automatisant les vérifications de conformité par rapport à des standards comme le CIS ou PCI DSS. Cela permet aux entreprises de repérer rapidement les vulnérabilités et d'améliorer leur posture de sécurité en suivant des recommandations précises.

- **Orchestration, Automatisation et Réponse de Sécurité (SOAR)**

Security Hub, en s'intégrant avec Amazon EventBridge, permet d'automatiser les réponses aux incidents de sécurité. Par exemple, lorsqu'une menace est détectée, des actions automatiques telles que la correction ou l'envoi de notifications peuvent être déclenchées, optimisant ainsi le processus de gestion des incidents .

- **Simplification des Intégrations et Réduction des Coûts**

Le service centralise les intégrations entre les différents outils de sécurité, simplifiant l'ingestion des données et l'intégration avec des systèmes SIEM ou des gestionnaires de tickets. Cette centralisation améliore l'efficacité et réduit les coûts opérationnels associés à la gestion des incidents de sécurité.

- **Visualisation des Résultats de Sécurité**

Security Hub fournit un tableau de bord détaillé qui permet de visualiser et de prioriser les incidents de sécurité par compte et par ressource. Cela aide les équipes à comprendre rapidement les problèmes de sécurité et à réagir de manière appropriée, en optimisant les ressources et les efforts de sécurité.

Ces cas d'utilisation montrent comment AWS Security Hub peut être un atout précieux pour les entreprises cherchant à renforcer leur sécurité dans le cloud.

2.3.3.4 **Fonctionnalités AWS Security Hub**

❖ **Contrôles de Sécurité et Conformité**

- **Vérifications Automatisées des Meilleures Pratiques de Sécurité**

AWS Security Hub intègre la norme AWS Foundational Security Best Practices, qui inclut des contrôles de sécurité validés par des experts. Ces contrôles sont continuellement mis à jour pour couvrir de nouvelles menaces, permettant aux entreprises de maintenir une posture de sécurité proactive. Chaque contrôle est associé à une gravité, aidant à prioriser les efforts de remédiation en fonction du risque identifié .

- **Normes de Sécurité Alignées sur les Cadres de Conformité**

Security Hub offre des normes de sécurité alignées avec des cadres réglementaires tels que PCI DSS et CIS AWS Foundations Benchmark. Ces normes comprennent des contrôles automatisés qui aident les organisations à évaluer leur conformité et à s'assurer qu'elles respectent les exigences légales et sectorielles. Cela simplifie la gestion de la conformité en unifiant plusieurs cadres en une vue consolidée.

- **Évaluation de la Posture de Sécurité avec le Score de Sécurité**

Le score de sécurité fourni par Security Hub, allant de 0 à 100, permet aux organisations de visualiser et d'évaluer leur posture de sécurité. Ce score est basé sur le ratio de contrôles réussis par rapport aux contrôles échoués, offrant une mesure claire de la sécurité globale. Cette évaluation est utile pour identifier les domaines nécessitant des améliorations et pour les audits de conformité.

- **Personnalisation des Contrôles CSPM**

Security Hub permet de personnaliser les contrôles de sécurité en fonction des besoins spécifiques de chaque organisation. Les administrateurs peuvent ajuster des paramètres tels que les politiques de mot de passe ou les délais avant qu'une ressource ne soit considérée comme non utilisée. Cette personnalisation centralisée facilite la gestion des contrôles sans nécessiter de mises à jour manuelles pour chaque compte ou région, tout en maintenant une conformité rigoureuse aux politiques internes.

- **Visualisation des Données de Sécurité**

Le tableau de bord de Security Hub offre une vue d'ensemble des résultats de sécurité, permettant de visualiser les menaces, vulnérabilités et tendances. Les administrateurs peuvent personnaliser les filtres et widgets pour se concentrer sur les informations les plus pertinentes, facilitant ainsi la prise de décisions éclairées et l'amélioration continue de la posture de sécurité de l'organisation.

❖ Gestion des Alertes de Sécurité avec AWS Security Hub

- **Agrégation des Résultats Inter-Régions**

AWS Security Hub permet de centraliser les alertes de sécurité de plusieurs régions en utilisant une région principale appelée "région agrégatrice". Cette région collecte et synchronise les résultats de sécurité de toutes les régions liées, offrant ainsi une vue unifiée des menaces et vulnérabilités. Cela simplifie l'intégration avec des outils de gestion des incidents et autres systèmes, centralisant les données dans un seul endroit pour une gestion plus efficace.

- **Collecte des Résultats des Services AWS et Intégrations Partenaires**

Security Hub collecte les résultats de divers services AWS tels qu'Amazon GuardDuty, Amazon Inspector, et Amazon Macie, ainsi que des partenaires intégrés via l'AWS Partner Network. Ces résultats incluent des informations sur la détection des intrusions, les analyses de vulnérabilité, et la configuration de la sécurité. Ces données sont conservées pendant 90 jours, fournissant une vue continue et approfondie des risques de sécurité potentiels.

- **Consolidation et Visualisation des Résultats de Contrôle**

Le système consolide les résultats des alertes de sécurité selon plusieurs normes, facilitant le triage et la résolution des problèmes. Il offre une vue d'ensemble des contrôles activés et de leur état de conformité, ainsi qu'un résumé des réussites et échecs. Cette consolidation permet de mieux comprendre les zones à risque et de prioriser les actions correctives nécessaires.

- **Standardisation des Données avec le Format ASFF**

Security Hub utilise le format AWS Security Findings Format (ASFF) pour normaliser les résultats des alertes de sécurité. Ce format assure une présentation cohérente des données, y compris les ressources identifiées, les niveaux de gravité et les horodatages. Cela simplifie l'analyse et la gestion des données, rendant le processus plus efficace et moins sujet aux erreurs.

- **Prise en Charge des Comptes Multiples et AWS Organizations**

Avec AWS Organizations, Security Hub peut gérer plusieurs comptes AWS, offrant une vue centralisée des alertes de sécurité. Cela permet une gestion cohérente et centralisée des politiques de sécurité, tout en permettant aux propriétaires de comptes individuels de voir uniquement les résultats pertinents pour leur propre compte. Cette fonctionnalité est essentielle pour une surveillance et une gestion efficaces dans les grandes organisations .

❖ Automatisation et Réponse

- **Mise à jour Automatique des Résultats**

AWS Security Hub propose des règles d'automatisation permettant de gérer les résultats de sécurité. Ces règles peuvent être configurées pour mettre à jour automatiquement des attributs tels que la gravité des menaces ou l'état du workflow des résultats, en fonction de critères spécifiques. Par exemple, lorsqu'un nouveau résultat de sécurité est détecté, la gravité peut être ajustée automatiquement selon les politiques définies par l'entreprise. Cette fonctionnalité assure que les données de sécurité sont constamment à jour et facilite la priorisation des réponses.

- **Actions de Réponse et de Remédiation Automatisées**

Grâce à l'intégration avec Amazon EventBridge, Security Hub peut automatiser les réponses aux incidents de sécurité. Les résultats sont envoyés à EventBridge, où des règles prédéfinies déclenchent des actions correctives, comme l'exécution de fonctions AWS Lambda ou l'activation de runbooks AWS Systems Manager Automation. Cette automatisation réduit le temps de réponse aux incidents et améliore l'efficacité globale des opérations de sécurité.

- **Intégrations avec Outils de Sécurité**

Security Hub supporte l'intégration avec divers outils de gestion des incidents, de billetterie, et de SIEM, facilitant la centralisation des alertes et la gestion des menaces. Ces intégrations permettent aux équipes de sécurité d'avoir une vue unifiée des incidents, simplifiant ainsi la coordination et l'investigation des menaces. Cela rend le processus de gestion des incidents plus fluide et efficace .

❖ Optimisation des Coûts avec AWS Security Hub

- **Période d'Essai Gratuite de 30 Jours**

AWS Security Hub offre une période d'essai gratuite de 30 jours, permettant aux utilisateurs de tester l'ensemble des fonctionnalités disponibles. Cette période inclut les vérifications des meilleures pratiques de sécurité et offre un aperçu des coûts mensuels potentiels si le service est maintenu. De plus, le service propose un niveau gratuit perpétuel pour l'ingestion de jusqu'à 10 000 résultats par compte et par région chaque mois.

- **Tarifs en Fonction du Volume**

Le modèle de tarification de Security Hub est basé sur trois facteurs : le nombre de contrôles de sécurité, le nombre de résultats ingérés, et le nombre d'évaluations de règles traitées par mois. Ce système permet aux entreprises de payer uniquement pour les services qu'elles utilisent, offrant une flexibilité et une adaptation aux besoins spécifiques. En utilisant AWS Organizations, les entreprises peuvent connecter plusieurs comptes et bénéficier d'une tarification par paliers, réduisant ainsi les coûts pour les grandes structures.

- **Coût Unique pour les Contrôles de Sécurit**

Pour les vérifications des meilleures pratiques, Security Hub applique un coût unique pour chaque contrôle, même s'il est utilisé dans plusieurs normes. Cela signifie que les utilisateurs ne paient qu'une fois pour les contrôles identiques, même s'ils sont appliqués à différentes normes, ce qui optimise les coûts tout en assurant une couverture complète des contrôles de sécurité.

2.4 Intégration des Services AWS avec SIEM

L'intégration des services AWS avec un SIEM nécessite une planification minutieuse et l'adoption de meilleures pratiques pour assurer une efficacité maximale. Voici quelques techniques et meilleures pratiques pour cette intégration :

❖ **Collecte des Logs**

Pour intégrer efficacement les services AWS avec un SIEM, il est crucial de centraliser les logs provenant de sources telles que AWS CloudTrail, VPC Flow Logs, et les logs d'application via AWS CloudWatch Logs. Cette centralisation permet d'analyser les données en profondeur, d'identifier les comportements suspects et d'assurer une détection proactive des menaces. Les logs sont essentiels pour tracer l'historique des activités et faciliter les enquêtes post-incidents.

❖ **Automatisation des Processus**

L'automatisation joue un rôle clé dans la gestion des incidents de sécurité. AWS Lambda peut être utilisé pour automatiser les workflows de réponse, en exécutant des actions telles que l'envoi de notifications ou l'application de scripts de remédiation lorsque des anomalies sont détectées. Cela réduit le temps de réponse et permet de gérer les menaces de manière efficace et proactive.

❖ **Analyse et Corrélation des Événements**

Configurer des règles de corrélation dans le SIEM permet de détecter des comportements anormaux, tels que des tentatives de connexion suspectes ou des accès non autorisés. En intégrant des services comme Amazon GuardDuty et AWS Macie, les entreprises peuvent enrichir leurs données de sécurité, améliorant ainsi la précision des détections et la capacité à identifier les menaces en temps réel.

❖ **Surveillance Continue et Alertes**

La surveillance continue est cruciale pour détecter rapidement les anomalies. Security Hub et d'autres services AWS permettent de surveiller en permanence les logs et de générer des alertes en cas d'incidents critiques. Cela assure une réactivité immédiate, limitant les impacts potentiels des incidents sur l'organisation.

❖ Évaluation de la Conformité

AWS Security Hub peut être utilisé pour effectuer des évaluations continues de la conformité aux normes de sécurité telles que PCI DSS. Les résultats peuvent être intégrés dans le SIEM, offrant une vue d'ensemble de la posture de sécurité de l'entreprise et aidant à identifier les domaines nécessitant des améliorations.

❖ Optimisation des Ressources

Il est essentiel de surveiller l'utilisation des ressources AWS pour maximiser les performances et contrôler les coûts. AWS Cost Explorer permet de suivre les dépenses et d'optimiser l'allocation des ressources de sécurité, garantissant une utilisation efficace des services disponibles .

Ces pratiques permettent aux entreprises de renforcer leur posture de sécurité tout en optimisant leurs opérations et leurs coûts. La compréhension des concepts de base du cloud computing et des services natifs AWS tels que GuardDuty, Macie et Security Hub est essentielle pour mettre en place une solution de sécurité efficace dans un environnement cloud. Ces services fournissent des capacités avancées de détection des menaces, de classification des données et de gestion centralisée des alertes, renforçant ainsi la sécurité des infrastructures cloud. En combinant les principes fondamentaux de la cybersécurité avec les avantages des services cloud, les entreprises peuvent améliorer leur posture de sécurité, gérer les risques de manière proactive et assurer la conformité avec les réglementations en vigueur.

CHAPITRE 3 : *Architecture et Étapes de Mise en Place*

3.1 Architecture du SIEM sur AWS

La mise en place d'un système de gestion des informations et des événements de sécurité (SIEM) sur AWS implique l'intégration de plusieurs services natifs AWS pour créer une infrastructure sécurisée, évolutive et performante. Voici les principaux composants de cette architecture :

- **AWS GuardDuty**

GuardDuty est un service de détection des menaces qui surveille de manière continue les comptes et ressources AWS pour identifier toute activité suspecte ou malveillante. Il analyse les logs de CloudTrail, les VPC Flow Logs, et les DNS logs pour détecter des anomalies comme les accès non autorisés ou les comportements inhabituels. Ce service est essentiel pour fournir une visibilité approfondie sur les menaces potentielles et permettre une réponse rapide aux incidents.

- **AWS Macie**

Utilisant des techniques avancées de machine learning, AWS Macie aide à découvrir, classer et protéger les données sensibles. Il analyse les données stockées dans Amazon S3 pour identifier les informations personnelles et autres données sensibles. Lorsqu'un risque de sécurité ou de conformité est détecté, Macie génère des alertes pour aider à protéger les informations critiques contre les accès non autorisés et autres menaces.

- **AWS Security Hub**

AWS Security Hub est une plateforme centralisée qui agrège, organise et hiérarchise les alertes de sécurité provenant de divers services AWS et de partenaires de sécurité tiers. Elle fournit une vue d'ensemble complète de la posture de sécurité d'une organisation, en intégrant les résultats de services comme GuardDuty, Macie, et d'autres. Security Hub aide à identifier et à prioriser les menaces, et offre des recommandations pour atténuer les risques détectés.

- **Amazon S3**

Amazon S3 est utilisé pour centraliser et stocker les logs de sécurité. Ce service de stockage d'objets permet de conserver de grandes quantités de données, telles que les journaux générés par GuardDuty, Macie, et d'autres services AWS. Les logs sont stockés dans des "buckets" S3, permettant une analyse détaillée et une conservation à long terme.

- **AWS Lambda**

AWS Lambda est un service de calcul sans serveur qui joue un rôle clé dans l'automatisation des processus d'extraction, de transformation et de chargement (ETL) des logs de sécurité. Lambda permet de mettre en place des workflows automatiques pour traiter les données de sécurité en temps réel, contribuant ainsi à une réponse plus rapide et plus efficace aux incidents.

❖ **Amazon OpenSearch Service**

Anciennement connu sous le nom d'Elasticsearch, Amazon OpenSearch Service est utilisé pour l'indexation, l'analyse et la visualisation des logs de sécurité. Ce service permet de créer des visualisations et des tableaux de bord détaillés, facilitant la surveillance continue et l'investigation des incidents de sécurité. Les entreprises peuvent ainsi rapidement identifier les menaces et analyser les tendances de sécurité sur leurs réseaux.

Ensemble, ces composants constituent une architecture SIEM sur AWS qui est non seulement sécurisée et évolutive, mais également capable de répondre efficacement aux défis complexes de la gestion de la sécurité informatique.

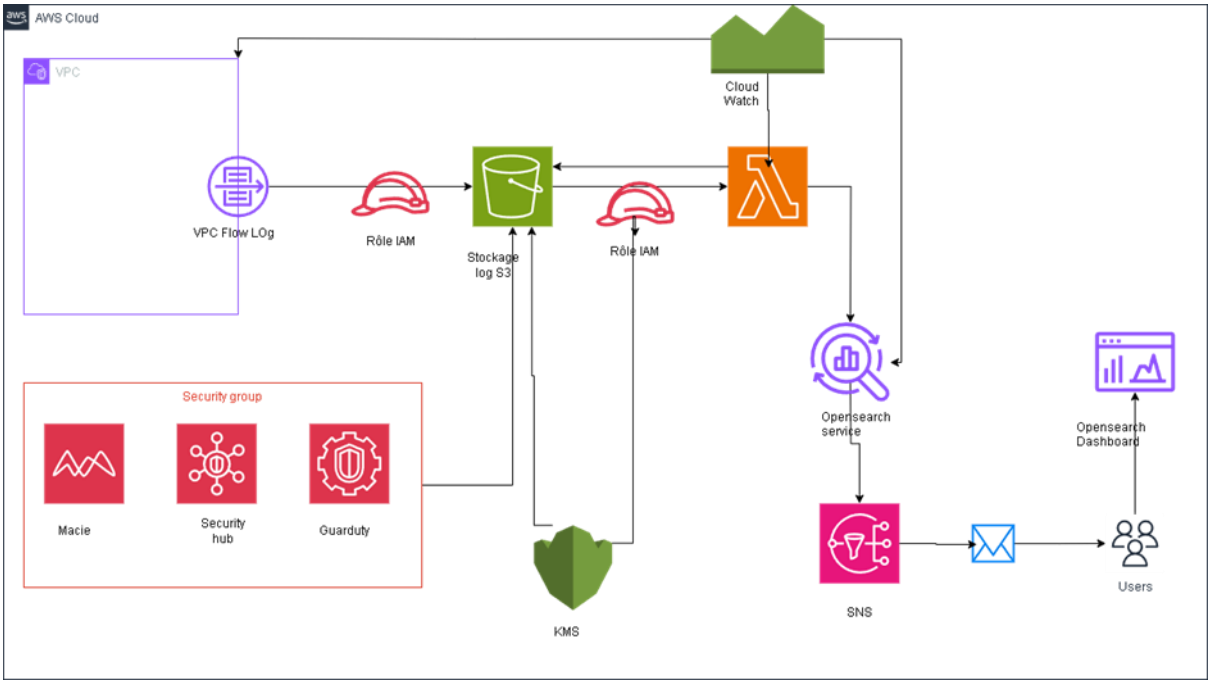


Figure 15: Architecture d'implémentation du SIEM

3.1.1 Intégration des Services AWS

L'intégration des services AWS dans un SIEM (Security Information and Event Management) est une démarche stratégique pour renforcer la sécurité et l'efficacité de l'infrastructure. Voici une explication approfondie des interactions et des rôles de chaque composant :

❖ **Collecte des Logs**

La première étape consiste à collecter les logs de sécurité provenant de diverses sources. AWS GuardDuty est un acteur clé, surveillant en continu les logs de CloudTrail, les VPC Flow Logs,

et les DNS logs pour identifier des activités suspectes. Parallèlement, AWS Macie analyse les données stockées dans Amazon S3, détectant et classifiant les informations sensibles. Ces logs sont ensuite centralisés dans Amazon S3, assurant une gestion uniforme et une disponibilité pour les analyses ultérieures.

- **Analyse et Détection des Menaces**

Une fois les logs collectés, GuardDuty les analyse pour repérer des comportements anormaux, tels que des tentatives d'accès non autorisées ou des activités malveillantes. Les alertes générées, ainsi que celles provenant de Macie concernant les données sensibles, sont envoyées à AWS Security Hub. Ce hub centralise les alertes, les organise et les hiérarchise en fonction de leur gravité, offrant ainsi une vue consolidée de la sécurité globale.

- **Automatisation des Workflows**

AWS Lambda joue un rôle crucial dans l'automatisation des réponses aux incidents. Lorsqu'une alerte est déclenchée, Lambda peut exécuter des fonctions spécifiques, telles que l'envoi de notifications, le déclenchement de processus de remédiation ou l'enrichissement des logs avant leur analyse. Cette automatisation permet une réponse rapide et efficace aux incidents de sécurité, minimisant ainsi les risques potentiels.

- **Indexation et Visualisation des Logs**

Pour faciliter l'analyse des données, les logs centralisés dans Amazon S3 sont indexés par Amazon OpenSearch Service. Ce service offre des capacités de recherche avancées et permet de créer des visualisations et des Dashboard personnalisés. Ces outils sont essentiels pour la surveillance en temps réel des incidents de sécurité et pour l'investigation approfondie des anomalies détectées. OpenSearch Dashboard fournit une interface intuitive pour explorer les logs et comprendre les tendances de sécurité.

- **Gestion Centralisée des Alertes**

Enfin, AWS Security Hub assure une gestion centralisée des alertes, consolidant les données provenant de GuardDuty, Macie et d'autres services AWS. Cette centralisation permet aux équipes de sécurité de prioriser les incidents, de coordonner les réponses et de prendre des mesures correctives rapidement. Security Hub fournit également des recommandations basées sur les meilleures pratiques de sécurité, aidant les organisations à améliorer continuellement leur posture de sécurité.

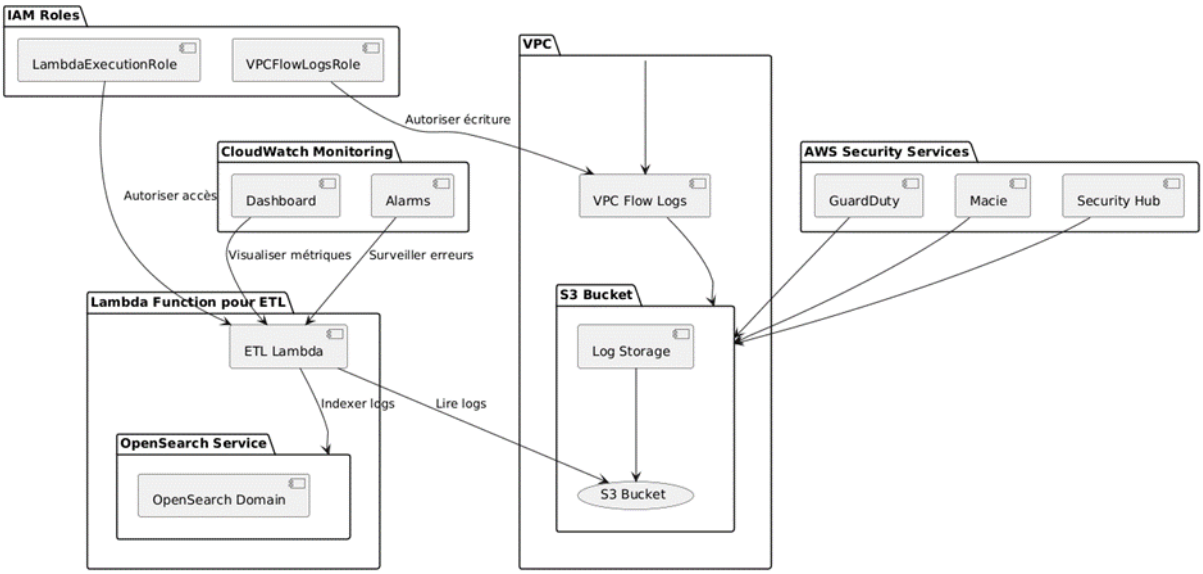


Figure 16: Diagramme illustrant l'implémentation

L'architecture d'un SIEM sur AWS repose sur l'intégration de plusieurs services natifs pour offrir une solution de sécurité complète et efficace. Chaque service joue un rôle crucial dans la collecte, l'analyse et la gestion des logs de sécurité, permettant une détection rapide des menaces et une réponse coordonnée aux incidents. Cette approche intégrée assure une visibilité complète sur l'ensemble de l'infrastructure cloud et aide les entreprises à maintenir une posture de sécurité robuste tout en optimisant l'utilisation des ressources et en maîtrisant les coûts.

3.2 Étapes de Mise en Place

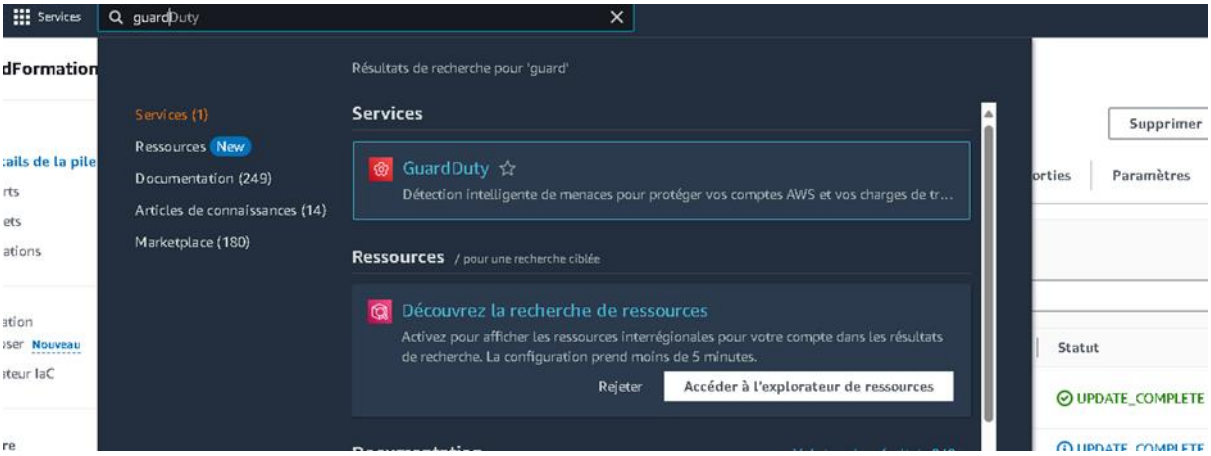
3.2.1 Configuration Initiale des Services AWS

La mise en place d'un SIEM (Security Information and Event Management) sur AWS est une étape cruciale pour renforcer la sécurité des données et des systèmes. Voici une explication détaillée de la configuration et de l'activation des services essentiels :

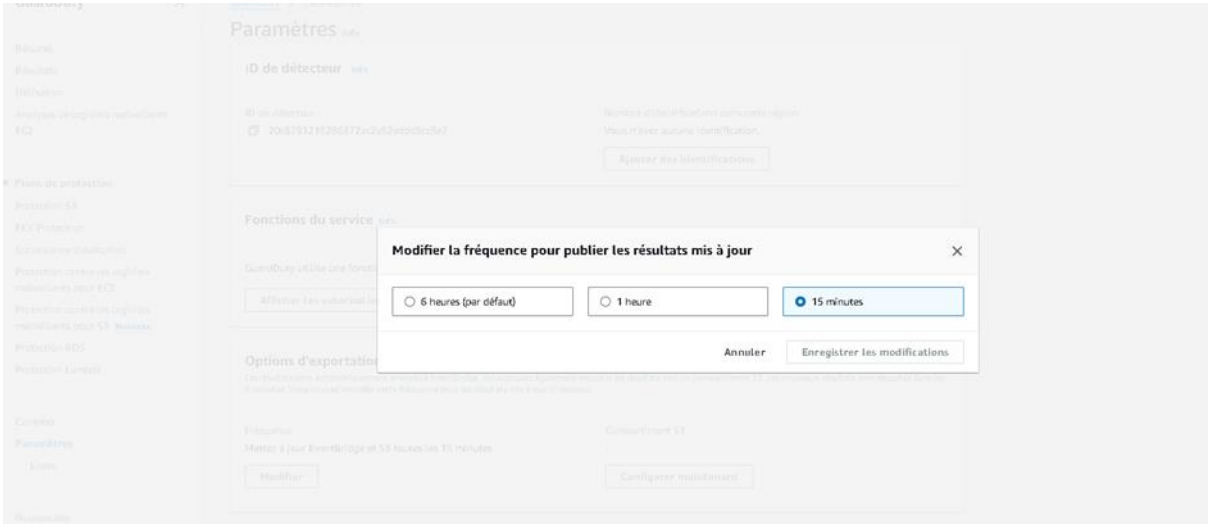
3.2.1.1 Activer AWS GuardDuty

GuardDuty est un service de surveillance et de détection des menaces qui analyse les activités suspectes et les anomalies dans votre environnement AWS. Pour le configurer :

- **Accès à la console AWS** :
  - Activez GuardDuty dans les régions où vous souhaitez surveiller les activités. Cela implique l'analyse des logs provenant de sources telles que AWS CloudTrail, VPC Flow Logs et DNS logs.
- **Connexion à la Console AWS** :
  - Accédez à la console AWS et connectez-vous à la console GuardDuty.

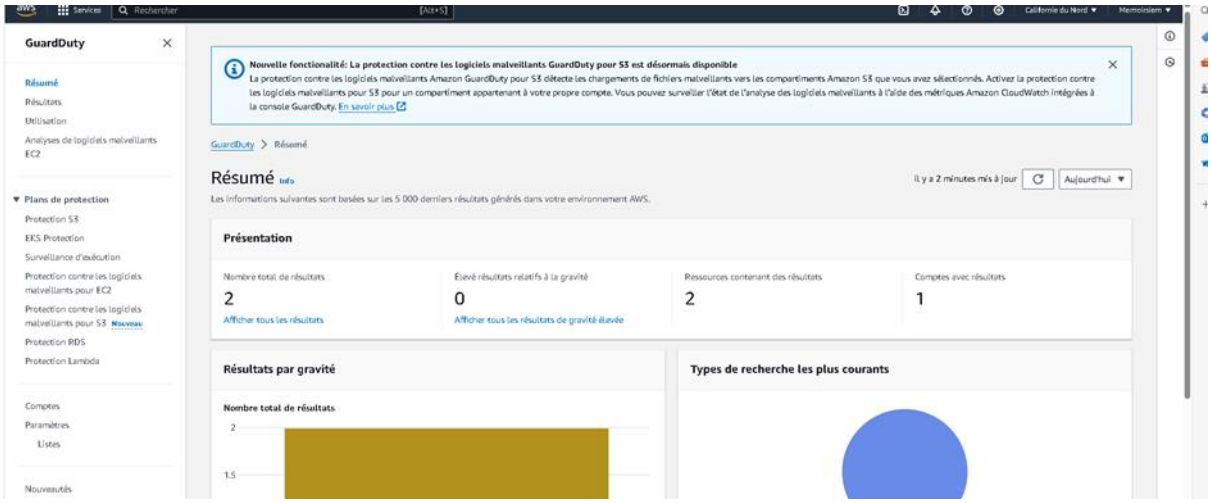


- **Accéder aux Paramètres** :
  - Dans le menu de gauche, sélectionnez "Settings" (Paramètres).
- **Configurer l'Exportation des Résultats** :
  - Dans la section "Findings export options" (Options d'exportation des résultats), choisissez la fréquence de mise à jour **"[Update CWE and S3 every 15 minutes]**" (Mettre à jour CWE et S3 toutes les 15 minutes) et cliquez sur "Save" (Enregistrer)



- **Configuration du Bucket S3** :
  - Cliquez sur "Configure now" (Configurer maintenant) pour le bucket S3. Cochez "Existing bucket in your account" (Bucket existant dans votre compte), sélectionnez le bucket approprié (par exemple, "[aes-siem-381492175502-log]"), en remplaçant "123456789012" par votre identifiant de compte AWS. Laissez le préfixe du fichier journal vide, activez le chiffrement KMS en choisissant une clé de votre compte, et sélectionnez "[aes-siem-key]" pour l'alias de la clé. Enregistrez les paramètres.

- **Configuration des alertes** :
    - Personnalisez les paramètres d'alerte pour recevoir des notifications spécifiques lorsque des activités suspectes sont détectées. GuardDuty utilise des modèles de machine learning et des données de renseignement sur les menaces pour identifier les comportements anormaux .

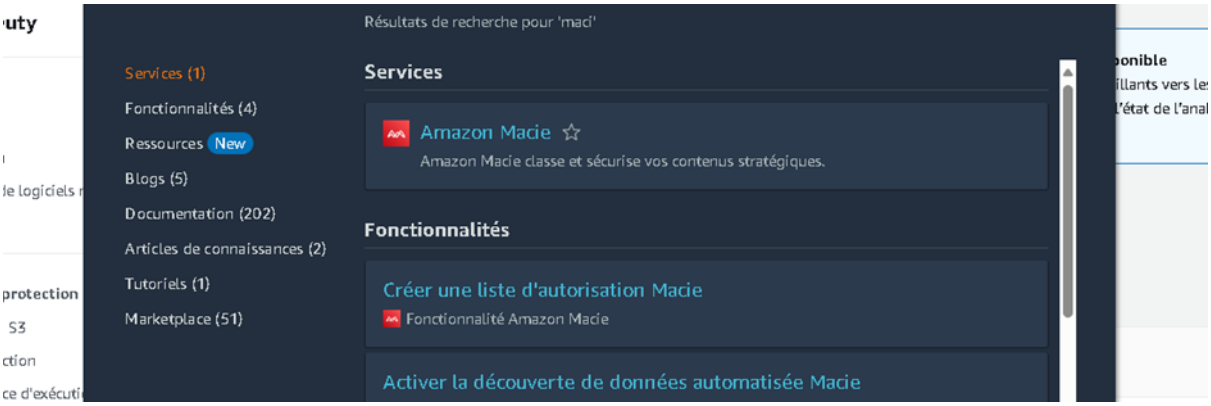


3.2.1.2 Configurer AWS Macie

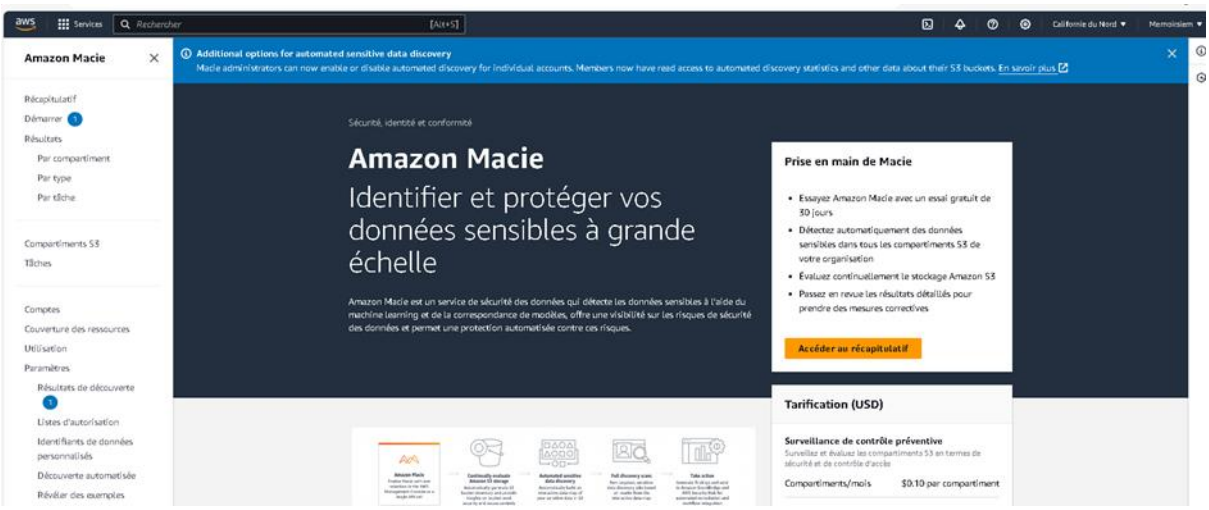
AWS Macie se concentre sur la protection des données sensibles. Il utilise le machine learning pour découvrir, classifier et protéger les données sensibles stockées dans Amazon S3 :

1. Activation de Macie

- **Connectez-vous à la Console AWS** : Accédez à la console AWS, puis à la section Macie.



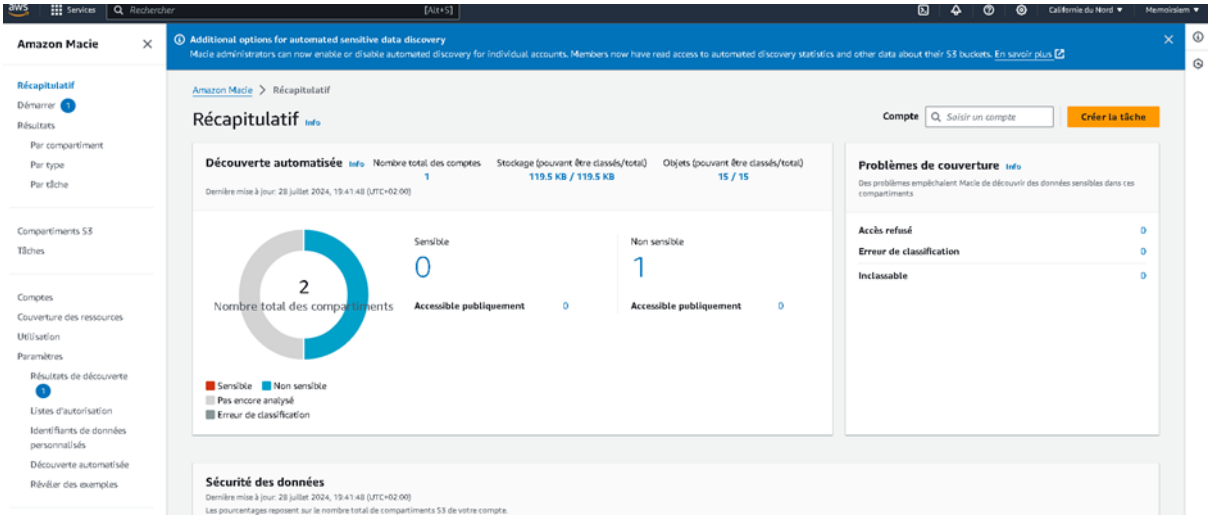
- **Activation** : Activez Macie pour commencer à analyser les données. Cette activation permet de découvrir automatiquement les buckets S3 et de les préparer pour l'analyse des données sensibles.



- **Sélection des Buckets** : Vous pouvez choisir les buckets spécifiques que Macie analysera pour identifier des informations sensibles, comme des PII (informations personnelles identifiables). Cette sélection est cruciale pour s'assurer que toutes les données sensibles sont couvertes.

2. Détection des Anomalies

- **Configurer les Règles de Détection** : Définissez des règles pour que Macie vous alerte lorsqu'il détecte des données sensibles stockées de manière non sécurisée ou des accès suspects. Ces règles aident à identifier rapidement les risques de sécurité potentiels, tels que les accès non autorisés ou le partage public accidentel de données sensibles.
- **Surveillance Continue** : Macie surveille en permanence les données pour garantir une détection rapide des anomalies. Les alertes générées peuvent être intégrées à AWS Security Hub pour une gestion centralisée, permettant une réaction rapide aux menaces détectées et une amélioration continue des mesures de sécurité.



3.2.1.3 **Activer AWS Security Hub**

Security Hub offre une vue unifiée de la posture de sécurité en consolidant les alertes de différents services AWS :

1. Activer AWS Security Hub

- **Accès à la Console AWS** : Connectez-vous à la console AWS et accédez à Security Hub.



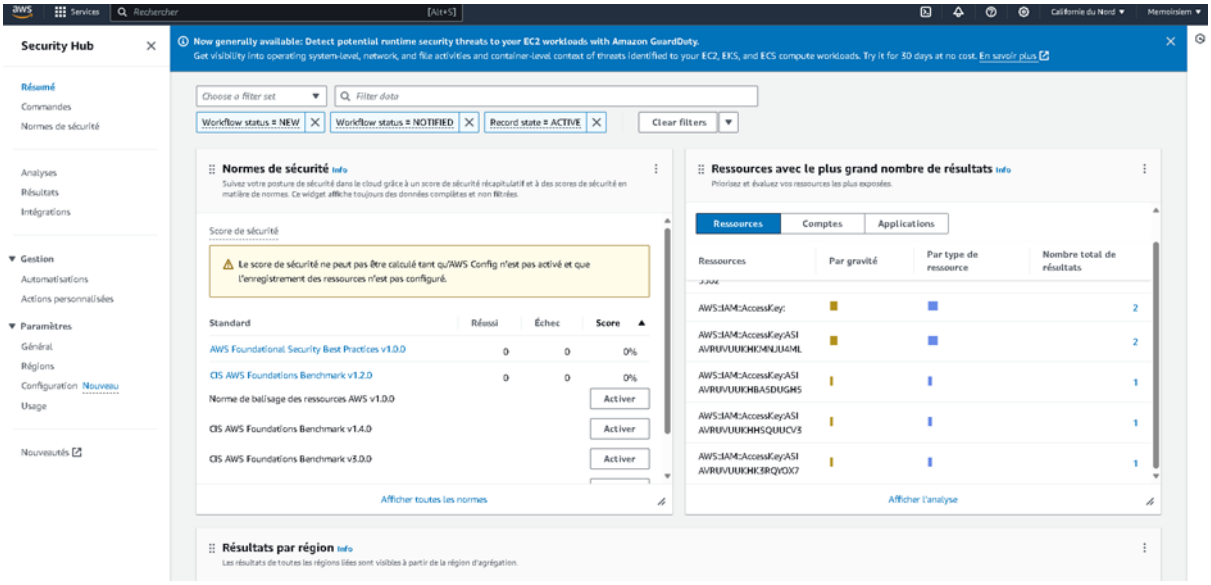
- **Activer le Service** : Cliquez sur "Commencer" ou "Activer Security Hub" et suivez les instructions.

2. Intégration des Services

- **Intégration de GuardDuty et Macie** : Intégrez des services comme AWS GuardDuty, AWS Macie, et AWS Inspector dans Security Hub. Cette intégration permet de centraliser les logs et les alertes provenant de ces services, offrant une vue unifiée des incidents de sécurité.

3. Agrégation et Hiérarchisation des Alertes

- **Classement des Alertes** : Security Hub agrège les alertes et les classe selon leur gravité. Cela aide les équipes de sécurité à prioriser les incidents les plus critiques et à coordonner les réponses de manière efficace.
- **Recommandations de Sécurité** : Utilisez les recommandations fournies par Security Hub pour améliorer la posture de sécurité globale. Ces recommandations sont basées sur les meilleures pratiques de sécurité et aident à atténuer les risques détectés.

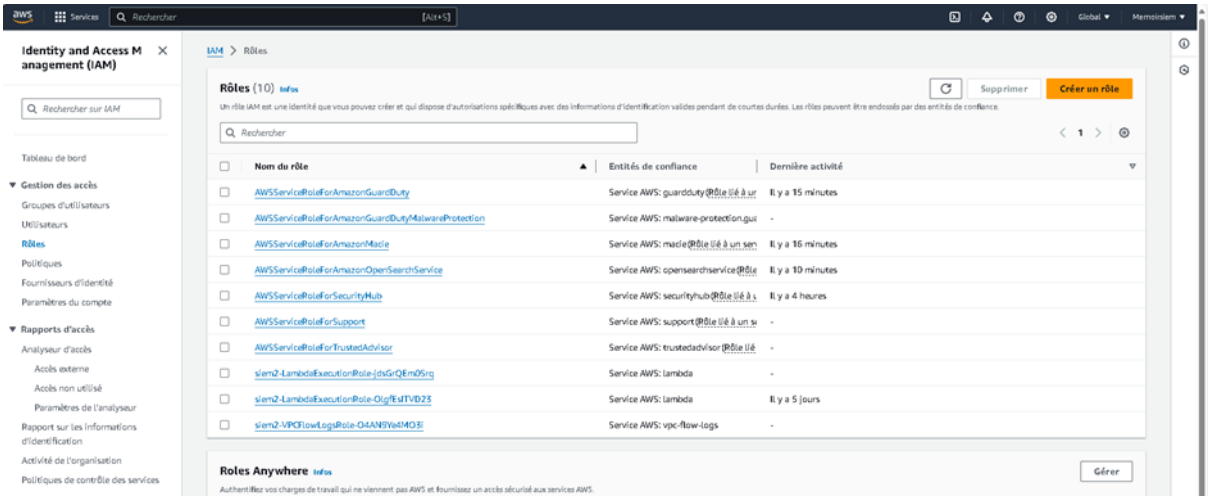


3.2.2 Intégration et Automatisation des Workflows

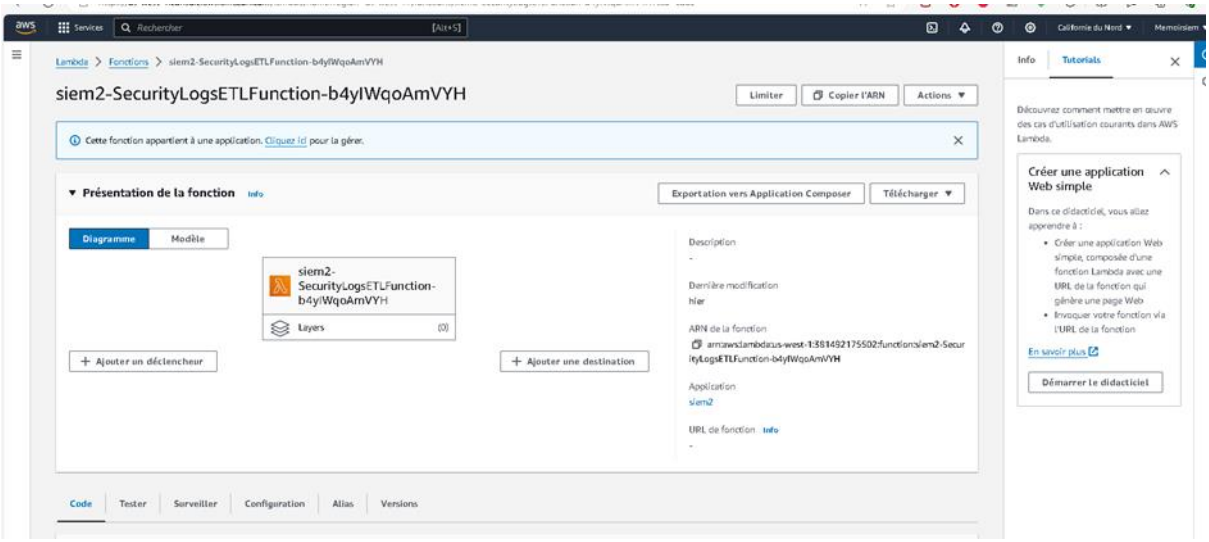
L'intégration des services AWS et l'automatisation des workflows sont essentielles pour une gestion centralisée et efficace des logs de sécurité. Voici une explication détaillée de cette étape :

3.2.2.1 Utilisation de AWS Lambda pour ETL

- **Créer un rôle IAM pour la fonction Lambda:**
  - Dans la console IAM, créez un rôle avec les permissions nécessaires:
  - Accès à S3 pour lire les objets (s3:GetObject sur le bucket aes-siem-381492175502-log).
  - Accès à OpenSearch pour indexer les documents (es:ESHttpPost).



- **Fonctions Lambda pour ETL** : AWS Lambda automatise le processus d'Extraction, Transformation et Chargement (ETL) des logs de sécurité. En utilisant Lambda, les logs collectés depuis différents services comme CloudTrail ou VPC Flow Logs peuvent être transformés en formats standardisés et stockés dans des buckets S3 dédiés pour une analyse ultérieure.
    - Allez dans la console Lambda et cliquez sur "Créer une fonction".
    - Donnez un nom à la fonction, par exemple **SecurityLogsETLFunction**.
    - Choisissez Python 3.8 comme runtime.
    - Collez le code fourni dans le template dans l'éditeur de code intégré.
    - Ajoutez les variables d'environnement nécessaires, par exemple, **ES_HOST** pour l'endpoint OpenSearch.
    - Attribuez le rôle IAM créé précédemment



- **Déclencheurs d'Événements** : Configurez des déclencheurs basés sur les événements pour automatiser le traitement des données en temps réel. Par exemple, dès qu'un

nouveau log est généré, une fonction Lambda peut être déclenchée pour l'analyser immédiatement, garantissant une détection rapide des anomalies et des incidents de sécurité.

```python
import json
import boto3
from requests_aws4auth import AWS4Auth
from opensearchpy import OpenSearch, RequestsHttpConnection
import gzip
import os
from datetime import datetime

s3 = boto3.client('s3')
region = os.getenv('AWS_REGION', 'us-west-1')
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
session_token=credentials.token)

host = os.getenv('ES_HOST')
es = OpenSearch(
    hosts=[{'host': host, 'port': 443}],
    http_auth=awsauth,
    use_ssl=True,
    verify_certs=True,
    connection_class=RequestsHttpConnection
)

def handler(event, context):
    for record in event['Records']:
        bucket = record['s3']['bucket']['name']
        key = record['s3']['object']['key']

        try:
            obj = s3.get_object(Bucket=bucket, Key=key)
            gzipped_body = obj['Body'].read()
            body = gzip.decompress(gzipped_body).decode('utf-8')
            logs = json.loads(body)

            if "eventName" in logs[0]:  # CloudTrail logs
                index_name = "cloudtrail-logs-" + datetime.now().strftime("%Y-%m-%d")
            elif "severity" in logs[0]:  # GuardDuty logs
                index_name = "guardduty-logs-" + datetime.now().strftime("%Y-%m-%d")
            elif "classificationDetails" in logs[0]:  # Macie logs
                index_name = "macie-logs-" + datetime.now().strftime("%Y-%m-%d")
            elif "Finding" in logs[0]:  # Security Hub logs
                index_name = "securityhub-logs-" + datetime.now().strftime("%Y-%m-%d")
            elif "version" in logs[0] and "account-id" in logs[0]:  # VPC Flow Logs
                index_name = "vpcflow-logs-" + datetime.now().strftime("%Y-%m-%d")
            else:
                index_name = "unknown-logs-" + datetime.now().strftime("%Y-%m-%d")

            for log in logs:
                response = es.index(
                    index=index_name,
                    body=log
                )
                print(f"Indexed document: {response}")

        except Exception as e:
            print(f"Error processing file from bucket: {bucket}, key: {key}, error: {str(e)}")

    return {
        'statusCode': 200,
        'body': json.dumps('Indexing complete')
    }
```

Figure 17: Code de la fonction Lambda

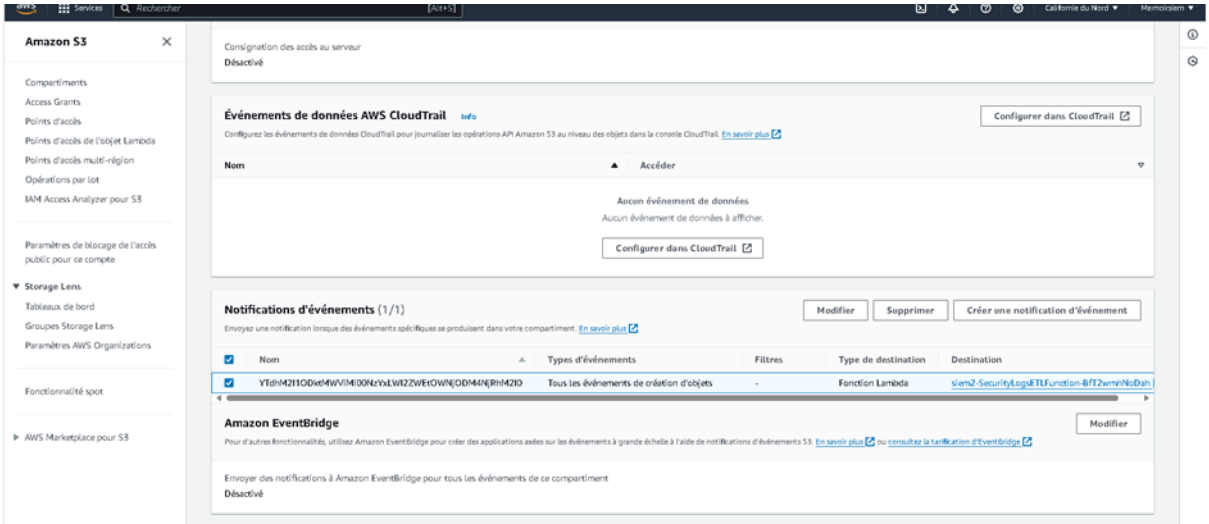
3.2.2.2 Configuration de Amazon S3

- **Création et Sécurisation des Buckets S3** : Créez des buckets spécifiques pour le stockage des logs provenant de différents services AWS. Par exemple, vous pouvez avoir un bucket pour les logs de CloudTrail et un autre pour les journaux de flux VPC. Assurez-vous que chaque bucket est sécurisé avec des politiques de sécurité appropriées, incluant des règles de chiffrement via AWS KMS et des politiques d'accès strictes .

- **Configuration du Bucket S3 pour la collecte des logs**
    - Allez dans la console S3 et créez un bucket nommé aes-siem-381492175502-log.



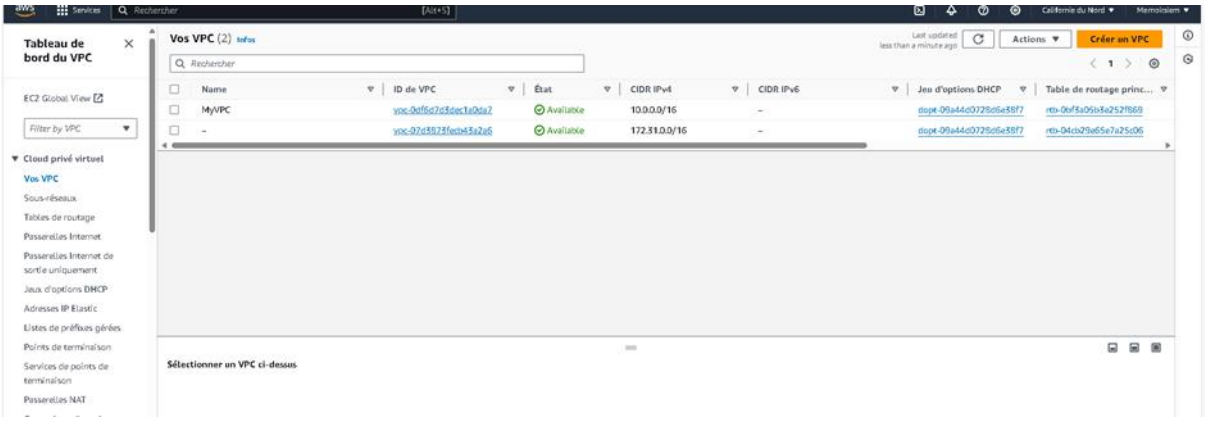
- Accédez à la configuration des événements pour ce bucket.
- Ajoutez une notification pour les événements **s3:ObjectCreated:*** en sélectionnant la fonction Lambda **SecurityLogsETLFunction** comme destination.



3.2.2.3 **Création du VPC et des Journaux de Flux VPC**

- **Création du VPC** : Dans la console AWS, créez un VPC (Virtual Private Cloud) en spécifiant un bloc CIDR, par exemple 10.0.0.0/16. Configurez les paramètres DNS pour activer le support DNS et les noms d'hôtes DNS. Cela crée un réseau isolé pour segmenter et sécuriser les ressources AWS.

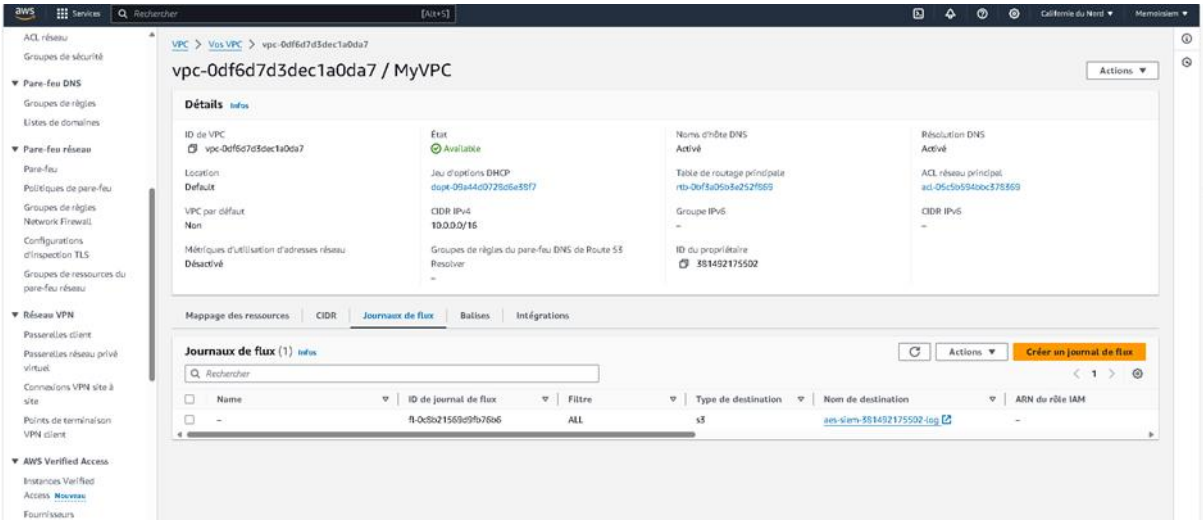
    - Allez dans la console AWS et recherchez "VPC".
    - Cliquez sur "Créer un VPC".
    - Entrez un nom pour le VPC, par exemple "MonVPC".
    - Configurez le bloc CIDR, par exemple **10.0.0.0/16.**
    - Activez les options DNS (DNS support et DNS hostname).
    - Cliquez sur "Créer VPC".



- **Rôle IAM pour les Journaux de Flux VPC** : Créez un rôle IAM dédié qui permet à AWS de publier les logs des journaux de flux VPC dans le bucket S3 configuré. Ce rôle doit inclure les permissions nécessaires comme **s3:PutObject** pour permettre l'enregistrement des logs.
- Recherchez "IAM" dans la console AWS et allez dans "Rôles".
    - Cliquez sur "Créer un rôle" et sélectionnez "VPC Flow Logs" comme service.
    - Ajoutez une politique IAM permettant **s3:PutObject** sur le bucket S3:
- Utilisez la politique gérée ou créez une politique personnalisée :
    - Donnez un nom au rôle, par exemple "**VPCFlowLogsRole**", et créez le rôle



- **Configuration des Journaux de Flux VPC** : Dans la console VPC, activez les journaux de flux pour capturer les données de trafic réseau. Sélectionnez le VPC à surveiller, définissez le type de trafic (par exemple, "Tous"), et spécifiez le bucket S3 de destination ainsi que le rôle IAM créé.
    - Toujours dans la console VPC, sélectionnez "Journaux de flux" dans le menu latéral.
    - Cliquez sur "Créer un journal de flux".
    - Sélectionnez le VPC que vous avez créé.
    - Choisissez "Tous" pour le type de trafic.
    - Sélectionnez "S3" pour le type de destination et entrez l'ARN du bucket aes-siem-381492175502-log.
    - Sélectionnez le rôle IAM que vous avez créé ("**VPCFlowLogsRole**").

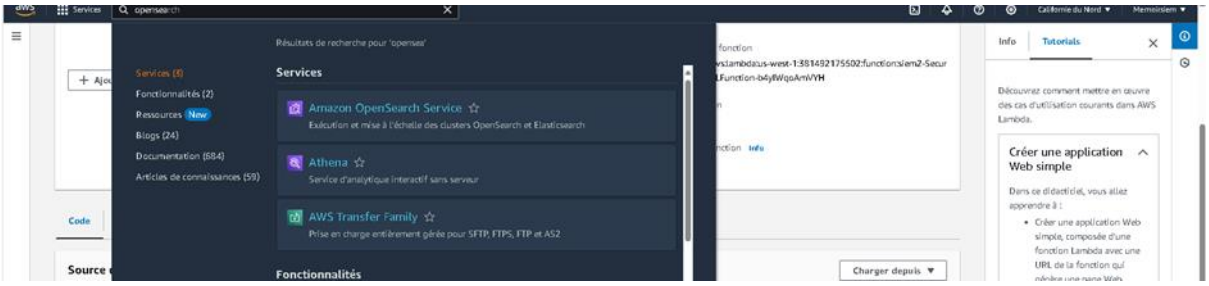


3.2.3 **Analyse et Visualisation des Logs**

Pour assurer une gestion efficace des données de sécurité, il est crucial de mettre en œuvre des solutions d'analyse et de visualisation robustes. Voici une description détaillée de cette étape :

3.2.3.1 **Déploiement d'Amazon OpenSearch Service**

- **Créer un domaine OpenSearch :**
    - Recherchez "OpenSearch Service" et accédez à la console



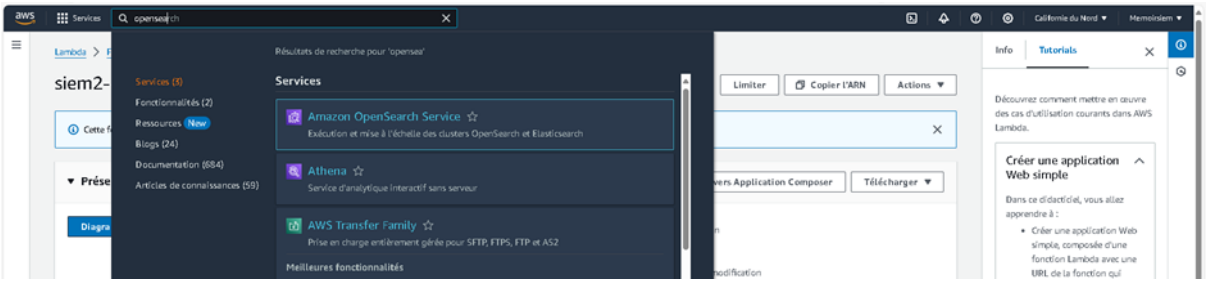
    - Cliquez sur "Créer un domaine".
    - Entrez un nom pour le domaine, par **exemple my-opensearch-domain**.
    - Configurez le moteur (OpenSearch 1.0), le type et le nombre d'instances (par exemple, **t3.small.search**.
    - Activez le chiffrement au repos et entre nœuds, ainsi que HTTPS obligatoire.
    - Configurez les options de sécurité avancées, y compris un utilisateur maître.
    - Spécifiez les politiques d'accès nécessaires.

- **Indexation et Analyse des Logs** : Amazon OpenSearch Service est utilisé pour indexer les logs de sécurité collectés, permettant une recherche et une analyse approfondies. Commencez par créer des index pour différents types de logs tels que ceux provenant de CloudTrail, des VPC Flow Logs, et d'AWS GuardDuty. L'utilisation de templates de mapping standardisés est recommandée pour structurer les données, ce qui facilite leur interprétation et analyse.

3.2.3.2 Création de Dashboards et Visualisations

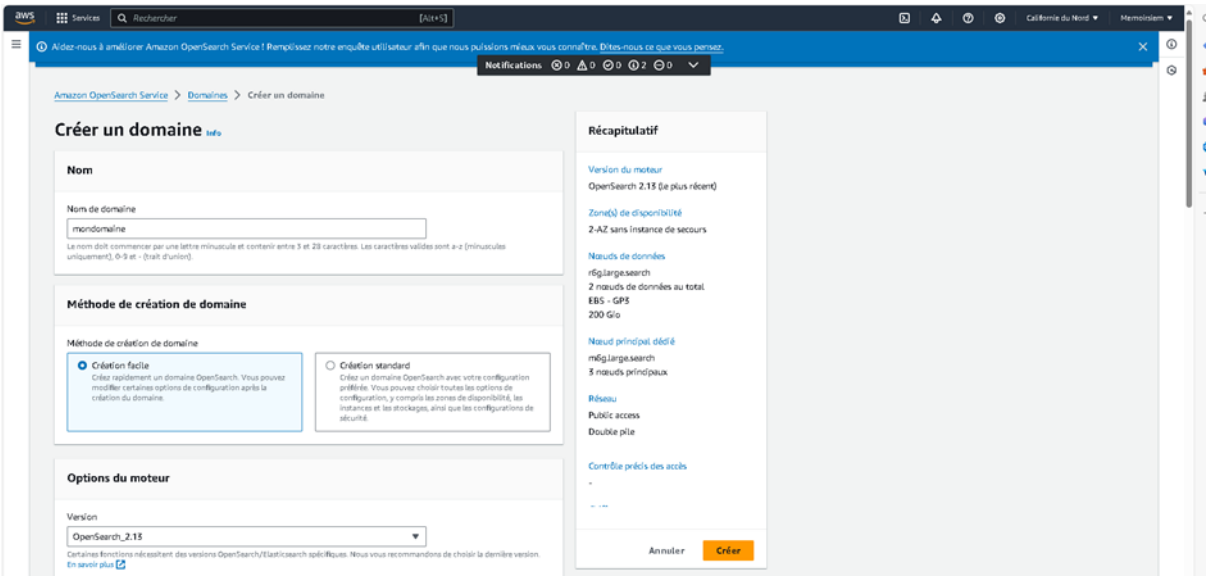
- **OpenSearch Dashboard** : OpenSearch Dashboard offre des outils pour créer des visualisations interactives et des Dashboard personnalisés. Ces visualisations permettent une surveillance en temps réel des activités de sécurité, comme les tentatives de connexion échouées ou les anomalies détectées. Les Dashboard fournissent une vue d'ensemble des données, facilitant l'identification des tendances et des incidents potentiels.

    - Recherchez "OpenSearch Service" et accédez à la console.

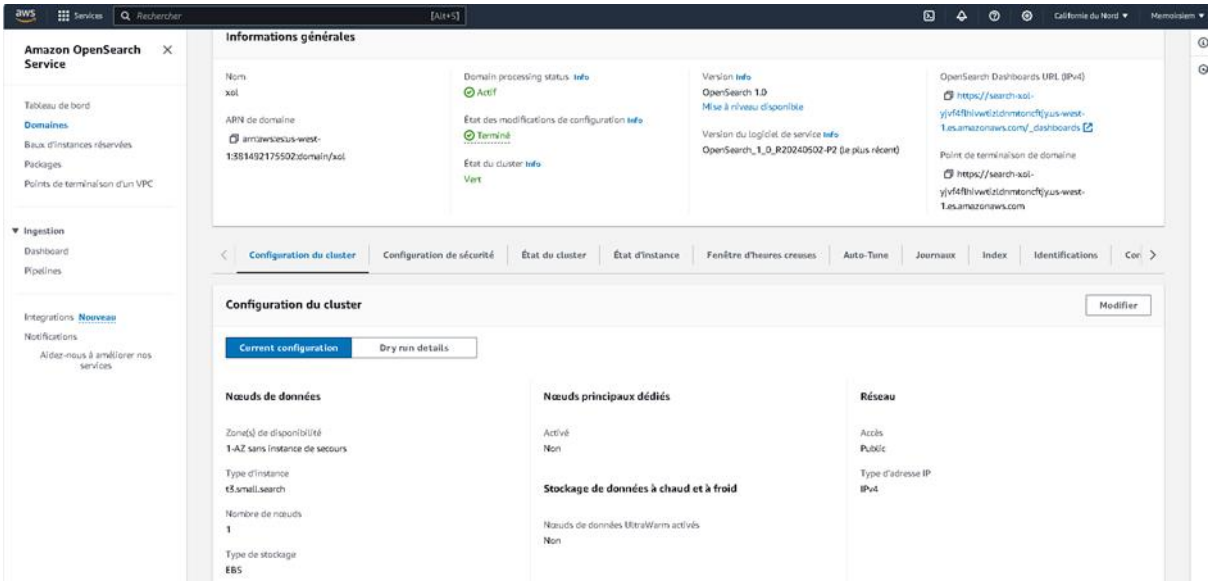


    - Cliquez sur "Créer un domaine".

    - Entrez un nom pour le domaine, par exemple **mondomaine**.



- Configurez le moteur (OpenSearch 1.0), le type et le nombre d'instances (par exemple, **t3.small.search** .
- Activez le chiffrement au repos et entre nœuds, ainsi que HTTPS obligatoire.
- Configurez les options de sécurité avancées, y compris un utilisateur maître.
- Spécifiez les politiques d'accès nécessaires.

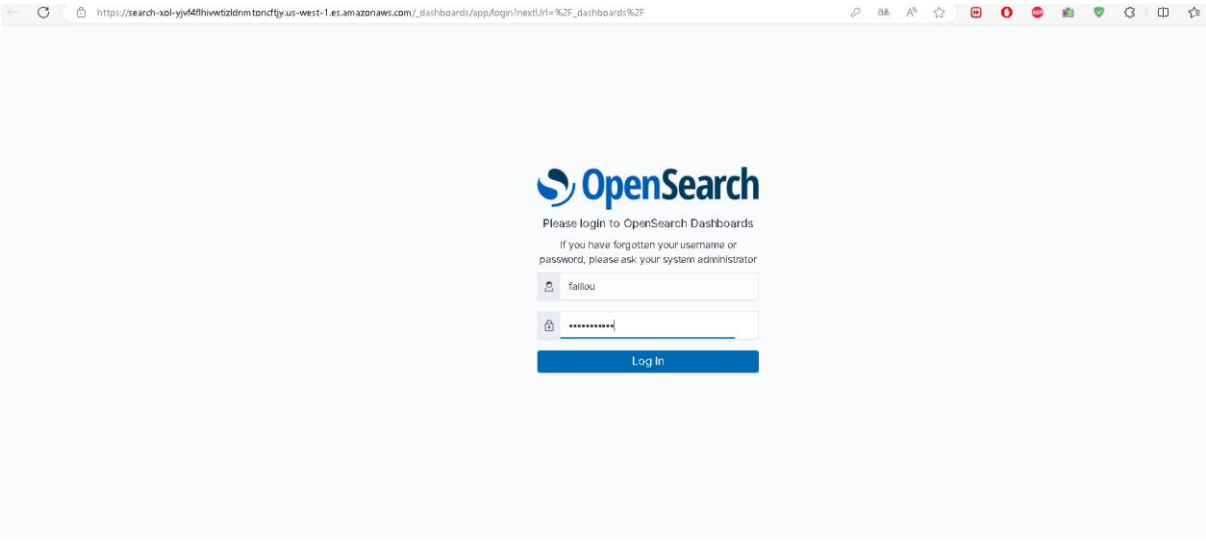


3.2.3.3 **Alertes et Notifications**

Configurez des alertes pour être informé des événements critiques. Par exemple, vous pouvez recevoir des notifications pour des anomalies significatives dans les logs de sécurité. Ces alertes peuvent être configurées pour déclencher des actions spécifiques, comme l'envoi de notifications via Amazon SNS ou l'intégration avec des systèmes de gestion des incidents.

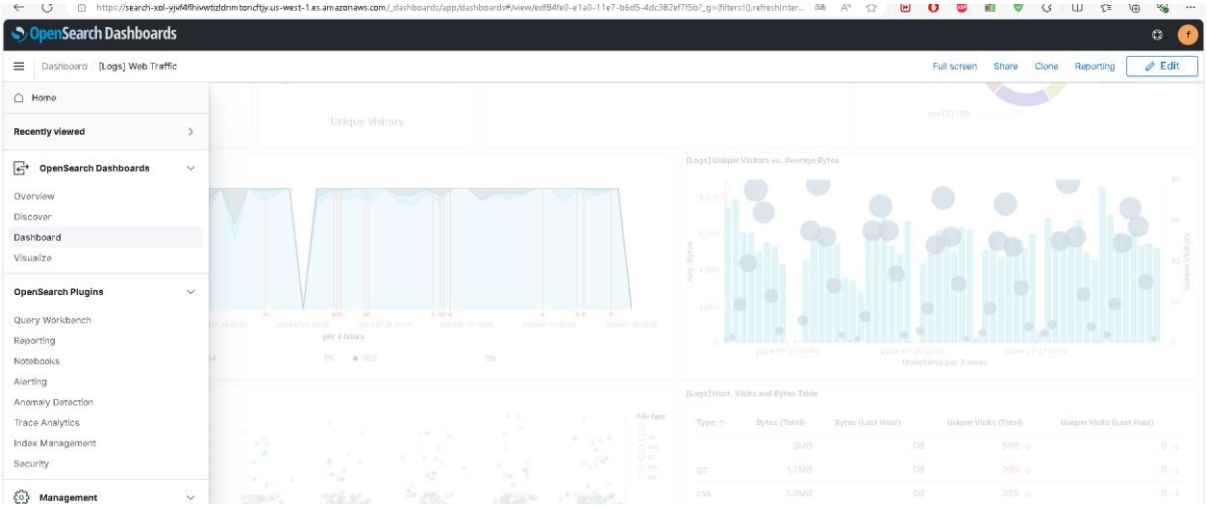
1. Accéder à la Section Alerting dans OpenSearch Dashboards

- **Ouvrir OpenSearch Dashboards** : Accédez à votre instance OpenSearch Dashboards.



- **Navigation vers Alerting** : Dans le menu de gauche, sélectionnez "Alerting" pour accéder à la gestion des alertes.

2. Configurer une Destination d'Alerte



- **Ajouter une Destination** : Dans l'onglet "Destinations", cliquez sur "Add destinations". Remplissez les champs nécessaires :
    - **Nom** : Par exemple, "aes-siem-alert-destination".
    - **Type** : Sélectionnez "Amazon SNS".

- **ARN de l'Alerte SNS** : Entrez l'ARN correspondant, comme arn:aws:sns:<AWS-REGION>:<111111111111>:aes-siem-alert. Remplacez <AWS-REGION> et <111111111111> par vos valeurs spécifiques.
- **IAM Role ARN** : Fournissez l'ARN du rôle IAM avec les permissions appropriées, par exemple, arn:aws:iam::<111111111111>:role/aes-siem-sns-role.

3. Définir les Critères d'Alerte

- **Sélectionner les Critères de Surveillance** : Spécifiez les logs et événements à surveiller, tels que les échecs d'authentification ou les accès non autorisés.
- **Configurer les Conditions d'Alerte** : Utilisez des conditions basées sur les données des logs, par exemple, déclencher une alerte pour un nombre élevé d'échecs de connexion sur une courte période.
- **Actions de Notification** : Définissez les actions à entreprendre en réponse aux alertes, comme l'envoi de notifications par email ou l'intégration avec des systèmes de gestion des incidents.

4. Créer un Moniteur : Dans l'onglet "Monitors", choisissez "Create monitor".

- **Nom** : "Authentication failed"
- **Méthode de définition** : Choisissez "Define using extraction query"
- **Indices** : cloudtrail-logs-* (saisie manuelle)
- **Définir une requête d'extraction** : Entrez une requête qui cible les échecs d'authentification, en utilisant les champs @timestamp et event.ingested pour gérer les décalages de temps entre l'occurrence du log et sa réception par le SIEM.

5. Spécifier les Conditions et Actions : Définissez les conditions précises pour lesquelles

Une alerte doit être déclenchée, comme un nombre excessif d'échecs de connexion. Associez ces conditions à des actions spécifiques, telles que l'envoi de notifications par SNS pour alerter les administrateurs en temps réel.

```
{
    "query": {
```

```
            "bool": {
                "filter": [
                {"term": {"eventSource": "signin.amazonaws.com"}},
                {"term": {"event.outcome": "failure"}},
                {"range": {
                    "event.ingested": {
                    "from": "{{period_end}}||-20m",
                    "to": "{{period_end}}"}}
                    }
                ]
            }
        }
}
```

Indiquez les paramètres suivants pour configurer le moniteur : Vérification : Toutes les 3 minutes

Cliquez sur Créer pour enregistrer le moniteur.

- **Configuration du Trigger pour Envoyer des Emails via Amazon SNS**

Pour configurer le déclenchement des alertes par email via Amazon SNS, procédez comme suit :

1. **Accéder à l'onglet Monitors** : Dans OpenSearch Dashboards, sélectionnez "Monitors" et cliquez sur "Create trigger".
2. **Nom du Trigger** : Entrez "Authentication failed trigger" pour identifier cette alerte.
3. **Condition de déclenchement** : Laissez la condition par défaut qui déclenche l'alerte lorsque le nombre de résultats est supérieur à 0.

- **Créer le Trigger**

1. **Sélectionner "Create trigger"** : Dans l'onglet "Monitors", cliquez sur "Create trigger".
2. **Nom du Trigger** : Entrez "Authentication failed trigger" pour identifier cette alerte.
3. **Configurer les Conditions de Déclenchement** : Le trigger sera activé si le nombre de résultats est supérieur à 0, indiquant un échec d'authentification.

❖ **Configurer les Actions de Notification**

1. **Nom de l'Action** : Saisissez "Authentication failed action".
2. **Destination** : Choisissez "aes-siem-alert-destination" comme destination pour Amazon SNS.
3. **Sujet du Message** : Entrez "(SIEM) Auth failure alert" pour l'objet du message.
4. **Action Throttling** : Activez l'option "Enable action throttling" et configurez-la pour que l'action ne se déclenche qu'une fois toutes les 10 minutes.
5. **Contenu du Message** : Copiez et collez le message suivant dans le champ de texte.



```
Monitor ctx.monitor.name just entered alert status. Please investigate the issue.
Trigger: ctx.trigger.name
Severity: ctx.trigger.severity
@timestamp: ctx.results.0.hits.hits.0._source.@timestamp
event.action: ctx.results.0.hits.hits.0._source.event.action
error.message: ctx.results.0.hits.hits.0._source.error.message
count: ctx.results.0.hits.total.value
source.ip: ctx.results.0.hits.hits.0._source.source.ip
source.geo.country_name: ctx.results.0.hits.hits.0._source.source.geo.country_name
```

6. **Tester le Message** : Après avoir configuré le message, choisissez "Send test message" pour vérifier que vous pouvez recevoir l'email de test.

3.3 Automatisation du Déploiement de l'Architecture avec AWS CloudFormation

AWS CloudFormation permet de déployer et de gérer les ressources AWS de manière automatisée et reproductible. En définissant les configurations de votre architecture SIEM dans des templates CloudFormation, vous pouvez automatiser l'ensemble du processus de déploiement, réduisant ainsi les erreurs humaines et accélérant la mise en place de l'infrastructure.

3.3.1 Fonctionnement

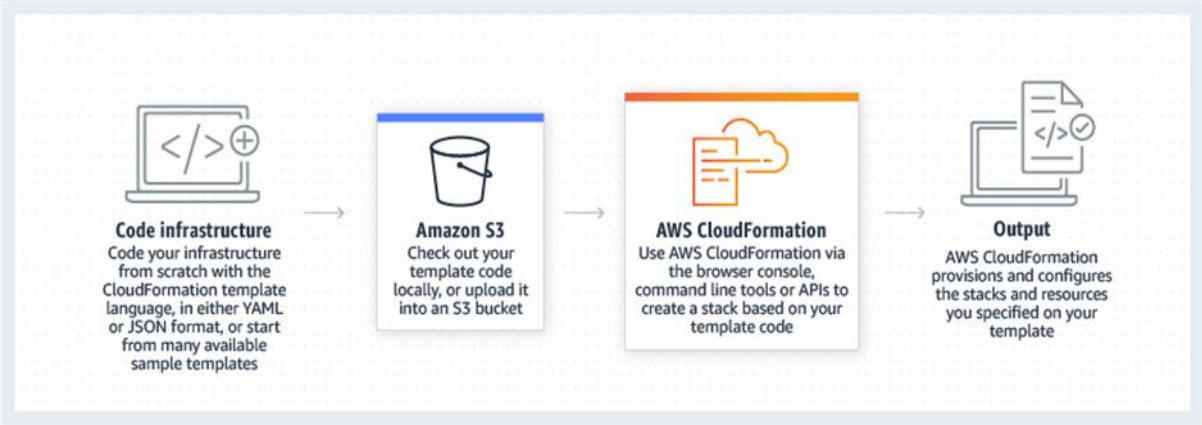


Figure 18: Fonctionnement de AWS CloudFormation

1. Modélisation des Ressources

CloudFormation utilise des modèles (templates) écrits en JSON ou YAML pour décrire les ressources AWS et leurs configurations. Ces modèles définissent tous les composants nécessaires pour une application, y compris les instances EC2, les bases de données RDS, les réseaux et bien plus encore.

2. Création et Déploiement de Stacks

Un *stack* est une collection de ressources AWS que vous pouvez gérer comme une seule unité. Lors de la création d'un stack, CloudFormation interprète le modèle, provisionne les ressources et configure ces ressources pour qu'elles fonctionnent ensemble selon les spécifications.

3. Gestion et Mise à Jour

CloudFormation facilite également la mise à jour et la gestion des ressources. Vous pouvez modifier les configurations de votre infrastructure en mettant à jour les modèles, puis en réappliquant le stack. CloudFormation gère les modifications de manière sûre et efficace, minimisant les interruptions.

4. Automatisation et Contrôle

Les modèles CloudFormation permettent une automatisation complète de la gestion des infrastructures, ce qui aide à maintenir la cohérence, à réduire les erreurs humaines et à standardiser les déploiements.

3.3.2 Cas d'Utilisation

Si vous souhaitez déployer un SIEM sur OpenSearch Service, vous pouvez utiliser un modèle CloudFormation pour créer toutes les ressources nécessaires, comme les instances EC2, les buckets S3 pour le stockage des logs, et les rôles IAM pour les permissions. Une fois le stack déployé, CloudFormation facilite l'administration continue, y compris les mises à jour et la suppression des ressources.

- **Gestion de l'infrastructure avec DevOps**

Apprenez à automatiser, tester et déployer vos infrastructures en utilisant les outils d'intégration et de livraison continues (CI/CD). Ces outils facilitent l'automatisation des tâches courantes, ce qui vous permet d'améliorer l'efficacité et la fiabilité de vos déploiements. En intégrant ces pratiques dans votre workflow, vous pourrez adapter et optimiser vos environnements de production en fonction des besoins.

- **Scalabilité des systèmes**

Comprenez comment adapter vos ressources en fonction de vos besoins, que vous gériez une simple instance Amazon Elastic Compute Cloud (EC2) ou une application complexe répartie sur plusieurs régions. Apprenez les principes de la scalabilité pour pouvoir ajuster vos systèmes afin de répondre aux variations de la demande sans compromettre la performance.

- **Partage des meilleures pratiques**

Découvrez comment configurer facilement des sous-réseaux avec Amazon Virtual Private Cloud (VPC) ou utiliser des services tels qu'AWS OpsWorks et Amazon Elastic Container Service (ECS). Ces outils vous permettent de mettre en place des infrastructures robustes et efficaces en suivant les meilleures pratiques de l'industrie. En vous familiarisant avec ces services, vous serez mieux équipé pour concevoir et gérer des solutions cloud optimisées.

3.3.3 Création de Templates CloudFormation

- **Déploiement**

1. **Définition des Ressources** : Créez un template CloudFormation en définissant les ressources nécessaires pour votre architecture SIEM, y compris les instances EC2, les buckets S3, les fonctions Lambda, les configurations de GuardDuty, Macie et Security Hub, ainsi que les clusters OpenSearch Service.

2. **Configuration des Dépendances** : Spécifiez les dépendances entre les différentes ressources. Par exemple, assurez-vous que les buckets S3 sont créés avant que les fonctions Lambda ne soient déployées pour traiter les logs de sécurité.

3. **Automatisation des paramètres** : Utilisez les paramètres CloudFormation pour rendre le template flexible et réutilisable. Cela permet de personnaliser les déploiements selon les environnements (développement, test, production) sans modifier le template de base.

4. **Exécution des Stack CloudFormation** : Déployez le template CloudFormation en créant une stack via la console AWS, l'interface en ligne de commande (CLI) ou les SDK AWS. La stack provisionne et configure automatiquement toutes les ressources définies dans le template.

❖ **Gestion des Mises à Jour et du Cycle de Vie**

1. **Mises à Jour des Stacks** : Utilisez CloudFormation pour mettre à jour les stacks existantes lorsque des modifications ou des améliorations sont nécessaires dans l'architecture SIEM. CloudFormation applique les modifications de manière contrôlée, en minimisant les interruptions.

2. **Surveillance et Journalisation** : CloudFormation intègre des capacités de surveillance et de journalisation, permettant de suivre l'état des stacks et d'identifier rapidement les problèmes lors des déploiements.

3. **Rollback Automatique** : En cas d'erreur lors du déploiement ou de la mise à jour, CloudFormation permet de revenir automatiquement à l'état précédent, assurant ainsi la continuité des opérations sans impact majeur.

Pour déployer le modèle CloudFormation en utilisant la console de gestion AWS, vous devez suivre une série d'étapes détaillées. Ce modèle met en place une solution complète de surveillance de la sécurité, intégrant des services tels que GuardDuty, Macie, Security Hub, VPC Flow Logs, et OpenSearch pour l'analyse des logs :

Étape 1 : Préparer le modèle CloudFormation

1. **Enregistrer le modèle** : Copiez l'ensemble du modèle YAML que vous avez fourni et enregistrez-le dans un fichier texte avec une extension.yaml, par exemple, security-monitoring-stack.yaml.

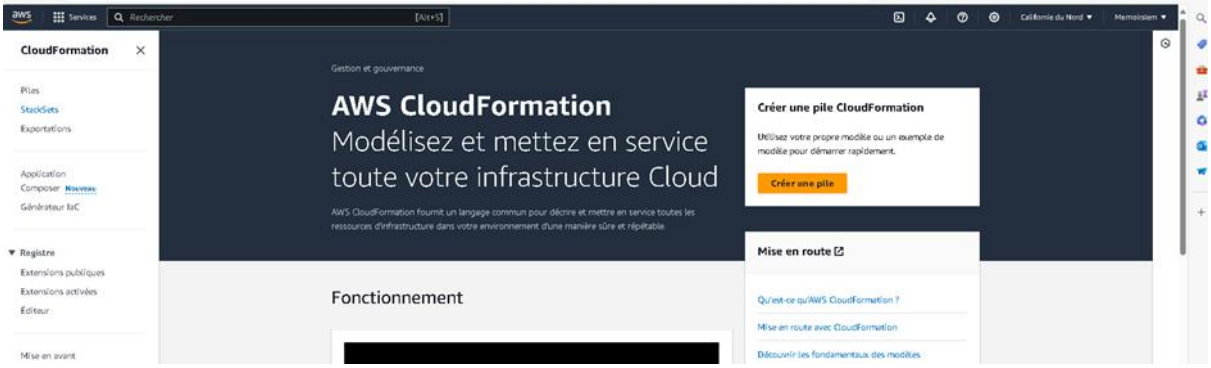
Étape 2 : Se connecter à la console de gestion AWS

1. **Ouvrir la console AWS** : Allez sur la console de gestion AWS.

2. **Se connecter** : Entrez les informations d'identification de votre compte AWS pour vous connecter.

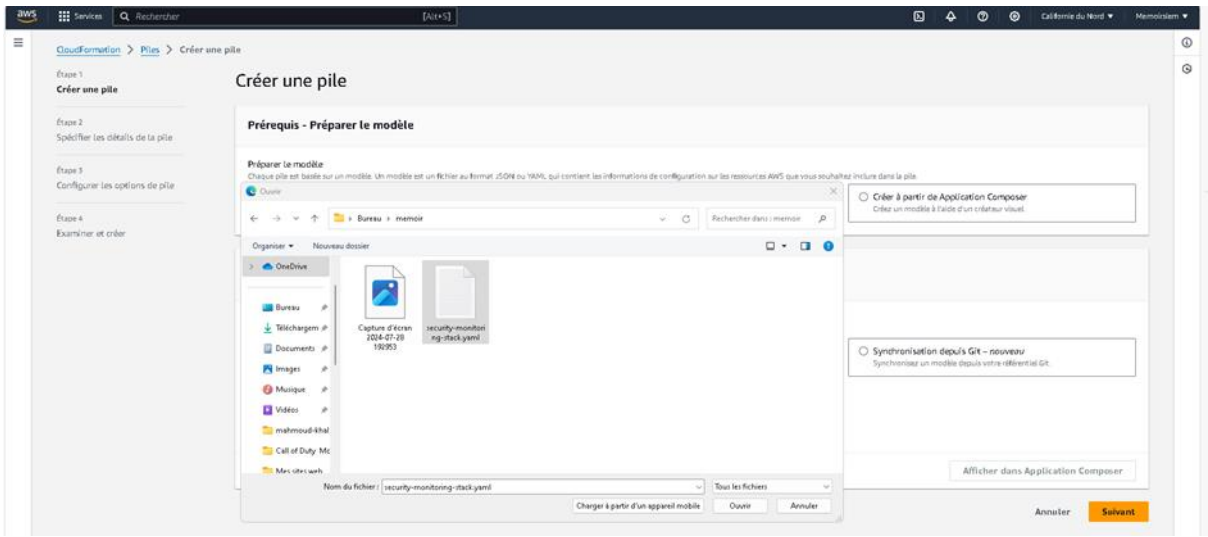
Étape 3 : Accéder à CloudFormation

Ouvrir CloudFormation : Dans la console AWS, utilisez la barre de recherche pour trouver et sélectionner **CloudFormation**.



Étape 4 : Créer une nouvelle pile (stack)

1. **Créer une pile (stack)** : Cliquez sur **"Creer stack"** dans le tableau de bord de CloudFormation.
2. **Choisir un modèle** : Sélectionnez **"Avec nouveaux ressources (standard)"** pour créer une nouvelle pile avec de nouvelles ressources.



1. **Télécharger un fichier de modèle** :
    - Choisissez l'option **"Upload un fichier"**.
    - Cliquez sur **"Choisir un fichier"** et téléchargez le fichier security-monitoring-stack.yaml que vous avez enregistré précédemment.



```yaml
AWSTemplateFormatVersion: '2010-09-09'
Description: Configuration de GuardDuty, Macie, Security Hub, VPC Flow Logs avec Lambda et OpenSearch Service
pour le traitement et l'analyse des logs de sécurité, avec surveillance CloudWatch.

Parameters:
  OpenSearchDomainName:
    Description: Nom du domaine OpenSearch.
    Type: String
  OpenSearchInstanceType:
    Description: Type d'instance OpenSearch.
    Type: String
    Default: t3.small.search
  OpenSearchInstanceCount:
    Description: Nombre d'instances OpenSearch.
    Type: Number
    Default: 1
  OpenSearchMasterUserName:
    Description: OpenSearch Master User Name
    Type: String
    NoEcho: true
  OpenSearchMasterUserPassword:
    Description: OpenSearch Master User Password
    Type: String
    NoEcho: true

Resources:
  # VPC
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsSupport: true
      EnableDnsHostnames: true
      Tags:
        - Key: Name
          Value: MyVPC

  # IAM Role for VPC Flow Logs
  VPCFlowLogsRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: vpc-flow-logs.amazonaws.com
            Action: sts:AssumeRole
      Policies:
        - PolicyName: VPCFlowLogsPolicy
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action: s3:PutObject
                Resource: arn:aws:s3:::aes-siem-881492175502-log/*

  # VPC Flow Log
  VPCFlowLog:
    Type: AWS::EC2::FlowLog
    Properties:
      ResourceId: !Ref VPC
      ResourceType: VPC
      TrafficType: ALL
      LogDestinationType: s3
      LogDestination: arn:aws:s3:::aes-siem-881492175502-log

  # Lambda Permission for S3 Bucket
  LambdaInvokePermission:
    Type: AWS::Lambda::Permission
    Properties:
      Action: lambda:InvokeFunction
      FunctionName: !GetAtt SecurityLogsET
```

Figure 19: Code du modèle Cloudformation en YAML

Étape 5 : Spécifier les détails de la pile

1. **Nom de la pile** : Entrez un nom pour votre pile, par exemple SecurityMonitoringStack.
2. **Paramètres** : Remplissez les paramètres requis :
    - **OpenSearchDomainName** : Entrez un nom pour votre domaine OpenSearch.
    - **OpenSearchInstanceType** : Spécifiez le type d'instance pour OpenSearch (par défaut **t3.small.search**).
    - **OpenSearchInstanceCount** : Spécifiez le nombre d'instances (par défaut 1).
    - **OpenSearchMasterUserName** : Entrez le nom d'utilisateur maître pour OpenSearch.
    - **OpenSearchMasterUserPassword** : Entrez le mot de passe utilisateur maître pour OpenSearch.

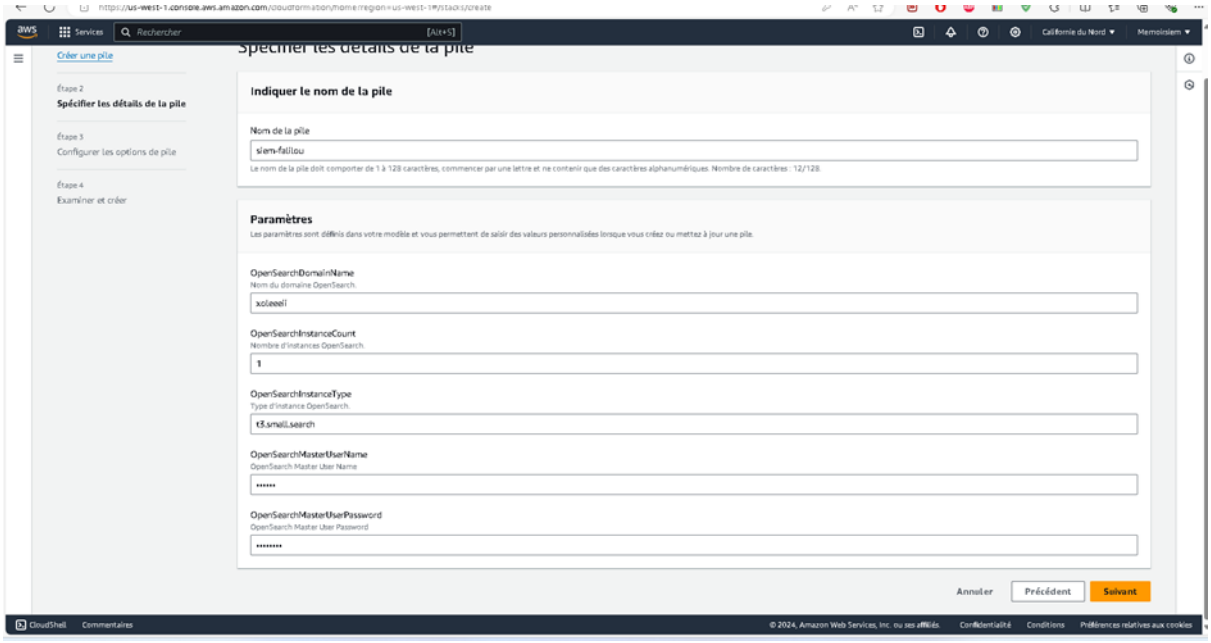


Figure 20: Spécification des détails sur le déploiement avec Cloudformation

Étape 6 : Surveiller la création de la pile

1. **Afficher les événements** : Surveillez la progression de la création de la pile dans la console. Vous pouvez cliquer sur l'onglet **"Events"** pour voir les étapes de création des ressources.

2. **Attendre la finalisation** : Patientez jusqu'à ce que le statut de la pile indique **"CREATE_COMPLETE"**. Cela signifie que toutes les ressources ont été créées avec succès.

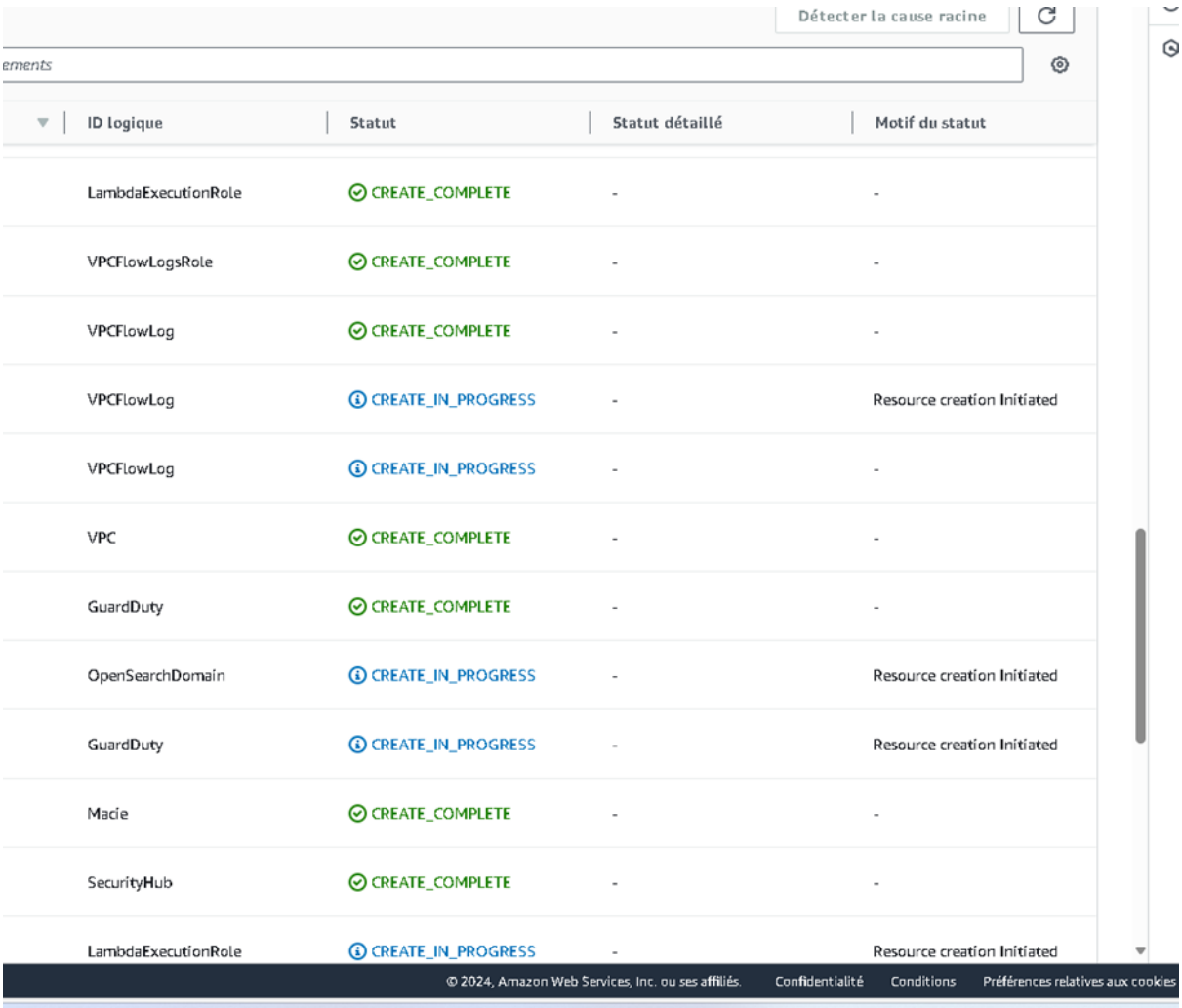


Figure 21: Evénement lors de la création du pile

Étape 7 : Vérifier les ressources créées

1. **Consulter les sorties** : Une fois la pile créée, allez à l'onglet **"Outputs"** pour voir les détails importants tels que les ARN des ressources et les points d'accès de domaine.
2. **Tester les services** : Assurez-vous que les services comme GuardDuty, Macie, Security Hub, et OpenSearch fonctionnent correctement. Vérifiez que les logs de sécurité sont collectés et analysés.

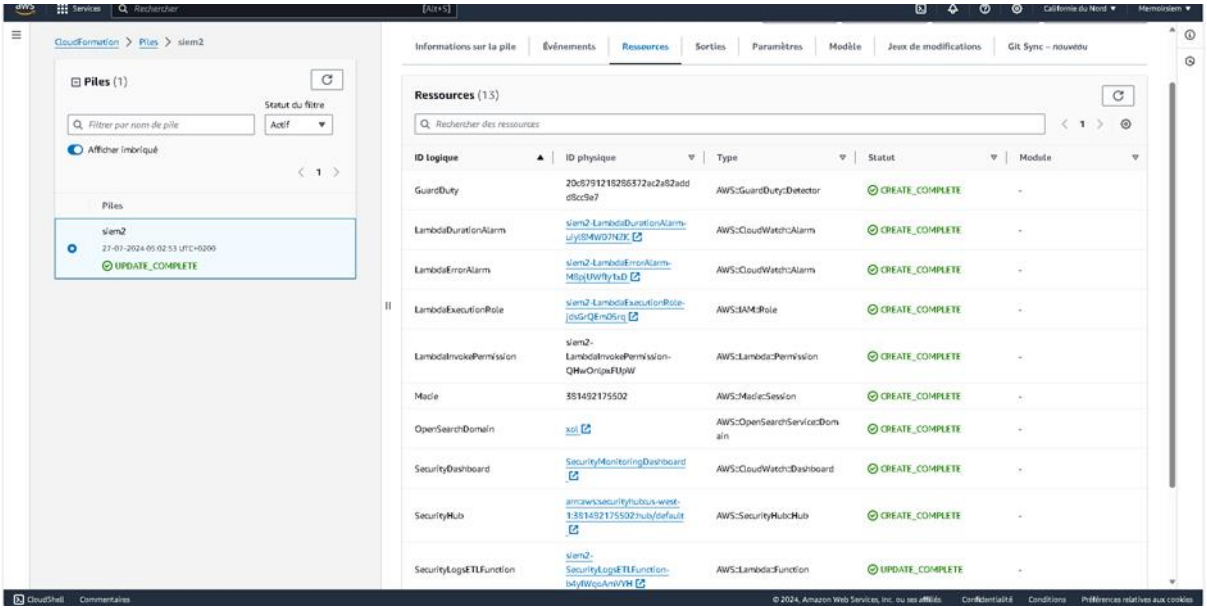


Figure 22: Vérification des ressources

Ces étapes permettent de déployer votre modèle CloudFormation et de mettre en place votre infrastructure de surveillance de la sécurité sur AWS. Si vous avez des questions ou des problèmes pendant le processus, n'hésitez pas à demander des conseils supplémentaires.

CHAPITRE 4 : *Conclusion et Perspectives*

4.1 Résumé des Résultats

L'intégration des services natifs AWS avec un SIEM offre une solution de sécurité robuste et évolutive pour les environnements cloud. Les tests effectués ont montré que l'utilisation combinée de services tels que GuardDuty, Macie et Security Hub permet de :

- **Détection Rapide des Incidents de Sécurité** : Grâce à la surveillance continue et à l'analyse des logs en temps réel, les incidents sont détectés rapidement, ce qui permet une réponse plus rapide et mieux ciblée. Les services comme GuardDuty offrent des alertes en temps réel qui aident à identifier les activités malveillantes dès qu'elles se produisent.
- **Amélioration de la Précision des Alertes** : L'intégration des différents services permet de corréler les événements de sécurité et de réduire le taux de faux positifs, améliorant ainsi la précision des alertes et réduisant les interruptions inutiles. Macie, par exemple, peut identifier des données sensibles et générer des alertes précises en cas de risques de sécurité.
- **Optimisation de l'Utilisation des Ressources** : L'automatisation des workflows avec AWS Lambda et l'utilisation de services scalables comme Amazon S3 et OpenSearch Service permettent une gestion efficace des ressources et une réduction des coûts globaux. Cela assure que les performances du SIEM restent optimales tout en contrôlant les dépenses.
- **Facilitation de la Conformité et de la Gestion de la Posture de Sécurité** : Security Hub centralise les insights de sécurité et facilite la conformité avec les normes de sécurité telles que CIS et PCI-DSS, offrant une vue d'ensemble claire et des recommandations pour améliorer continuellement la posture de sécurité.

4.2 Recommandations

Pour maximiser l'efficacité et l'efficience du SIEM sur AWS, plusieurs recommandations peuvent être formulées :

- **Automatisation des Processus** : Utiliser AWS Lambda pour automatiser les workflows de traitement des logs et la réponse aux incidents, réduisant ainsi la charge manuelle et améliorant l'efficacité opérationnelle. L'automatisation permet également de gérer la volumétrie des données en temps réel.
- **Configuration des Alertes Précises** : Établir des règles de détection et des critères d'alerte dans GuardDuty et Security Hub pour minimiser les faux positifs et garantir une réponse rapide aux incidents critiques. Cela aide à concentrer les ressources sur les véritables menaces et à réduire les interruptions inutiles.

- **Optimisation des Ressources** : Surveiller régulièrement l'utilisation des ressources et ajuster les configurations pour maximiser les performances tout en contrôlant les coûts. Utiliser AWS Cost Explorer pour suivre les dépenses et optimiser les ressources allouées aux services de sécurité .
- **Formation des Équipes de Sécurité** : Assurer une formation continue pour les équipes de sécurité sur l'utilisation des outils AWS et les meilleures pratiques en matière de cybersécurité cloud. Une formation adéquate garantit que les équipes sont préparées à gérer les incidents de sécurité de manière efficace.
- **Utilisation de Services Gérés** : Tirer parti des services gérés proposés par AWS, tels que AWS CloudWatch pour la surveillance des performances et Amazon OpenSearch Service pour l'analyse des logs, afin de simplifier la gestion et d'améliorer l'efficacité des processus de sécurité.
- **Automatisation des Processus de Sécurité** : Mettre en œuvre des scripts et des fonctions Lambda pour automatiser les processus de réponse aux incidents, la mise à jour des politiques de sécurité, et la gestion des configurations, afin de réduire les erreurs humaines et d'accélérer les temps de réponse

4.3 Perspectives Futures

- **Expansion des Capacités d'IA et de ML** : Intégrer davantage de capacités d'intelligence artificielle et d'apprentissage automatique pour améliorer la détection des menaces et la réponse automatisée aux incidents. Par exemple, utiliser Amazon SageMaker pour développer des modèles de détection des anomalies personnalisés

- **Intégration avec d'autres Services de Sécurité** : Explorer l'intégration avec d'autres services AWS et outils de sécurité tiers pour renforcer davantage la posture de sécurité et offrir une vue d'ensemble plus complète des menaces potentielles. L'utilisation de solutions tierces peut apporter des perspectives supplémentaires et des outils spécialisés .
- **Recherche Continue** : Poursuivre la recherche sur l'optimisation des configurations SIEM et sur les nouvelles techniques de détection et de réponse aux incidents pour s'adapter aux menaces en constante évolution dans les environnements cloud. La recherche et le développement continu permettent d'améliorer la résilience face aux nouvelles formes de cyberattaques.
- **Adoption de Meilleures Pratiques** : Continuer à adopter et à partager les meilleures pratiques en matière de sécurité cloud, en participant à des forums industriels, des conférences et des groupes de travail collaboratifs pour rester à la pointe de la cybersécurité. L'échange de connaissances et d'expériences peut aider à renforcer la communauté de la sécurité informatique dans son ensemble.

L'intégration des services natifs AWS dans un système SIEM offre une solution de sécurité puissante et adaptable pour les environnements cloud. En combinant la détection avancée des menaces, la gestion centralisée des alertes et l'automatisation des workflows, les entreprises peuvent améliorer significativement leur posture de sécurité et leur capacité à répondre rapidement et efficacement aux incidents de sécurité. Les recommandations et perspectives futures fournies dans ce mémoire offrent des orientations pratiques pour continuer à améliorer la sécurité des infrastructures cloud et à protéger les données sensibles contre les menaces en constante évolution.

Glossaire

AWS (Amazon Web Services) *: Fournisseur de services cloud offrant une infrastructure informatique à la demande via Internet.*

SIEM (Security Information and Event Management) *: Système de gestion des informations et des événements de sécurité, utilisé pour détecter, analyser et répondre aux incidents de sécurité.*

IaaS (Infrastructure as a Service) *: Modèle de cloud computing fournissant une infrastructure informatique virtuelle.*

PaaS (Platform as a Service) *: Modèle de cloud computing offrant une plateforme complète pour le développement et le déploiement d'applications.*

SaaS (Software as a Service) *: Modèle de cloud computing fournissant des applications logicielles accessibles via Internet.*

VPC (Virtual Private Cloud) *: Réseau cloud privé virtuel permettant de lancer des ressources AWS dans un réseau virtuel isolé.*

DNS (Domain Name System) *: Système de noms de domaine, traduisant les noms de domaine en adresses IP.*

EC2 (Elastic Compute Cloud) *: Service AWS permettant de lancer et de gérer des instances de serveurs virtuels.*

S3 (Simple Storage Service) *: Service de stockage d'objets AWS permettant de stocker et de récupérer des données à grande échelle.*

IDS (Intrusion Detection System) *: Système de détection d'intrusion, surveillant le réseau pour détecter des activités suspectes.*

IPS (Intrusion Prevention System) *: Système de prévention d'intrusion, détectant et empêchant les activités malveillantes.*

RBAC (Role-Based Access Control) *: Modèle de contrôle d'accès basé sur les rôles, définissant les permissions en fonction des rôles des utilisateurs.*

ABAC (Attribute-Based Access Control) *: Modèle de contrôle d'accès basé sur les attributs, définissant les permissions en fonction des attributs des utilisateurs et des ressources.*

GDPR (General Data Protection Regulation) *: Règlement général sur la protection des données, visant à protéger les données personnelles des citoyens de l'UE.*

HIPAA (Health Insurance Portability and Accountability Act) *: Loi américaine sur la portabilité et la responsabilité en matière d'assurance maladie, régissant la protection des informations médicales.*

MFA (Multi-Factor Authentication) *: Authentification multi-facteurs, utilisant plusieurs méthodes de vérification pour sécuriser l'accès.*

ETL (Extract, Transform, Load) *: Processus d'extraction, de transformation et de chargement des données pour l'analyse.*

CLI (Command Line Interface) *: Interface en ligne de commande, permettant d'interagir avec le système via des commandes textuelles.*

KMS (Key Management Service) *: Service de gestion des clés AWS, permettant de créer et de contrôler les clés de chiffrement.*

SNS (Simple Notification Service) *: Service de notification AWS, permettant l'envoi de messages de notification.*

SLA (Service Level Agreement) *: Accord de niveau de service, définissant les attentes en matière de performance et de disponibilité des services.*

CloudTrail *: Service AWS qui permet de surveiller et d'auditer les appels d'API dans les comptes AWS.*

CloudWatch *: Service AWS de surveillance et de gestion des journaux, des métriques et des alarmes des ressources AWS.*

OpenSearch Service *: Service AWS de recherche et d'analyse des données basé sur le projet open source OpenSearch.*

Lambda *: Service AWS de calcul sans serveur permettant d'exécuter du code en réponse à des événements sans gérer de serveurs.*

Security Hub *: Service AWS centralisant les alertes de sécurité et fournissant des recommandations de conformité.*

Macie *: Service AWS utilisant l'apprentissage automatique pour découvrir, classer et protéger les données sensibles.*

GuardDuty *: Service AWS de détection des menaces utilisant des algorithmes de machine learning pour surveiller les activités malveillantes.*

IAM (Identity and Access Management) *: Service AWS permettant de gérer l'accès aux services et ressources AWS en définissant des politiques et des rôles.*

Inspector *: Service AWS d'évaluation automatique de la sécurité des applications pour identifier les vulnérabilités et les déviations par rapport aux bonnes pratiques.*

Bibliographie

Livres

1. **[Ryl19]** Ryan M., Lucifredi F., *AWS: guide de l'administrateur système*, traduit par Olivier Engler, First, 2019
2. . **[Mat24]** Mathieu L., *Mastering AWS Security: Strengthen your cloud environment using AWS security features coupled with proven strategies*, Packt Publishing, April 26, 2024. Kindle Edition.

Rapports et Documents Techniques

3. **Amazon Web Services** (2021). *AWS Security Best Practices*

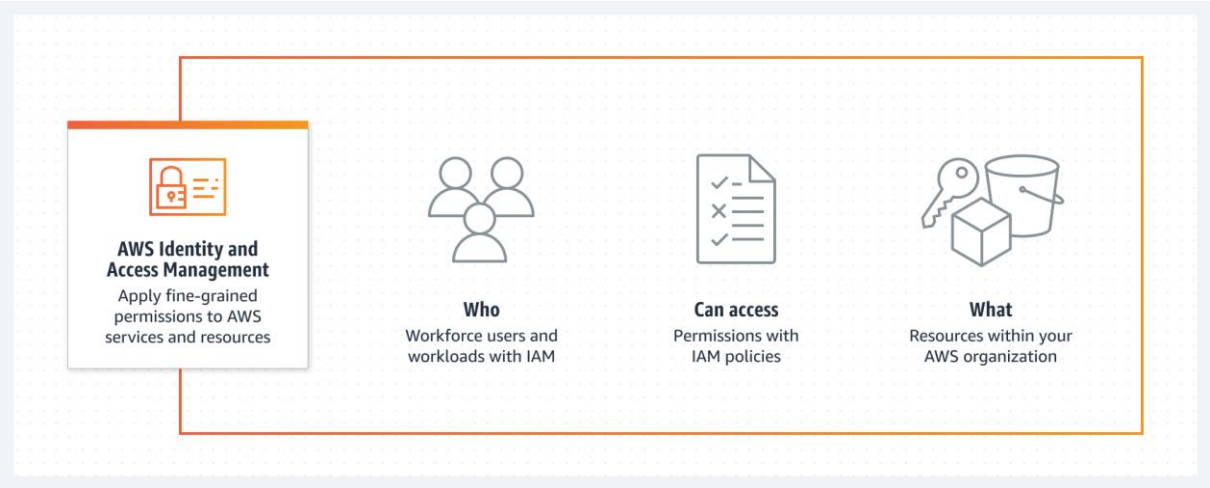
Sites Web et Blogs

4. **AWS Documentation**. (2024). " Documentation de tous les services aws" Amazon Web Services.
5. A Brief History of SIEM - Cybersecurity Magazine (cybersecurity-magazine.com)
6. https://www.fortinet.com/resources/cyberglossary/what-is-siem
7. https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html
8. https://securityintelligence.com/posts/what-is-siem-how-does-siem-work/
9. https://www.microsoft.com/en-us/security/business/security-101/what-is-siem
10. Accès aux guides complets proposés par le centre de formation d'Elastic | Elastic
11. Security information and event management solutions in AWS Marketplace (amazon.com)
12. IaaS vs. PaaS vs. SaaS (redhat.com)
13. How to master the shared responsibility model for cloud security (tenable.com)
14. The Shared Responsibility Model for Security in The Cloud (IaaS, PaaS & SaaS) | Splunk

Annexes

Annexe A: Presentation AWS IAM (Identity and Access Management

AWS Identity and Access Management (IAM) vous offre la capacité de réguler l'accès aux services et aux ressources au sein d'Amazon Web Services (AWS). Grâce à IAM, vous pouvez centraliser la gestion des autorisations de manière précise, accorder des droits spécifiques aux utilisateurs et aux rôles, et analyser les accès pour optimiser et affiner les autorisations selon les exigences de sécurité et opérationnelles.



Contrôle de l'accès

IAM centralise la gestion des autorisations, définissant précisément qui peut accéder à quoi dans votre compte AWS. Cela permet une surveillance continue et des ajustements nécessaires pour maintenir la sécurité des accès.

Gestion des Identités et des Accès

- **Identités** : Lors de la création d'un compte AWS, vous obtenez une identité principale, appelée utilisateur root. Il est recommandé de créer des utilisateurs IAM distincts pour les tâches quotidiennes afin de sécuriser les identifiants root. Ces utilisateurs reçoivent des permissions spécifiques définies par des politiques d'accès.
- **Autorisations** : Les utilisateurs IAM se connectent avec leurs informations d'identification. Une fois authentifiés, ils peuvent demander l'accès aux ressources AWS. Les politiques d'autorisations déterminent si ces demandes sont acceptées ou refusées.

Authentification et Autorisation

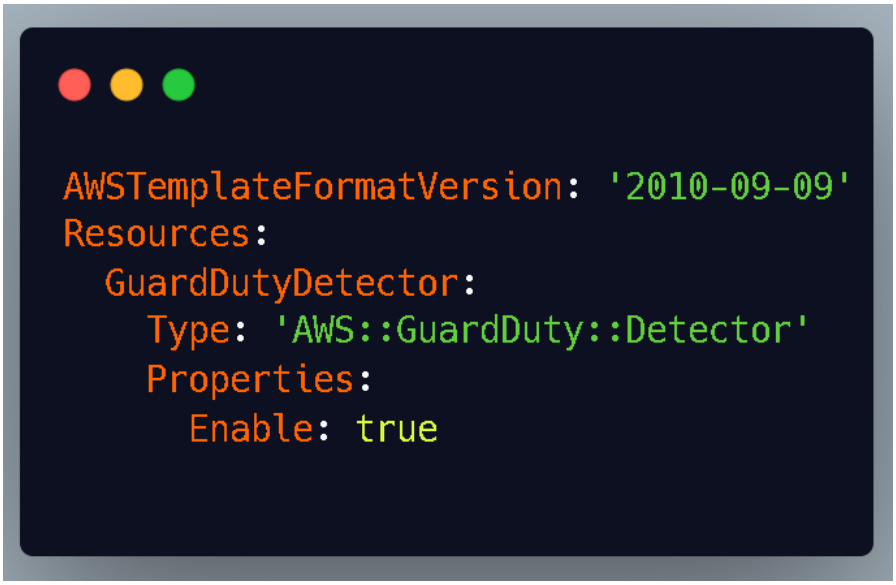
- **Authentification**: L'utilisateur se connecte en utilisant son ID et son mot de passe. IAM vérifie ces informations pour permettre à l'utilisateur d'envoyer des demandes à AWS.
- **Autorisation**: IAM évalue les politiques d'autorisations pour déterminer si l'utilisateur a les droits nécessaires pour effectuer l'action demandée. Une autorisation explicite permet l'action, tandis qu'un refus explicite bloque l'action, même si d'autres politiques la permettent.

Avantages d'IAM

- **Contrôles d'accès détaillés** : IAM permet de définir des permissions précises basées sur les attributs des utilisateurs, comme le département ou le rôle, grâce au contrôle d'accès basé sur les attributs (ABAC).
- **Analyse et validation des politiques** : IAM aide à créer des politiques de moindre privilège, à vérifier les accès externes et inutilisés, et à ajuster les autorisations en continu pour une sécurité optimale.
- **Gestion centralisée** : IAM permet de gérer les identités et les autorisations sur un seul compte AWS ou de connecter centralement les identités à plusieurs comptes, facilitant une gestion cohérente et sécurisée des accès.

Annexe B : Exemple Templates CloudFormation

- **Template de Base pour AWS GuardDuty** :
  - **Description** : Code de configuration pour l'activation de GuardDuty et la configuration des notifications d'alertes.
  - Code :



```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  GuardDutyDetector:
    Type: 'AWS::GuardDuty::Detector'
    Properties:
      Enable: true
```

- **Template pour la Configuration d'AWS Security Hub** :
    - **Description** : Code de configuration pour activer Security Hub et intégrer les services de sécurité associés.
    - **Code**:



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateDetector",
        "guardduty:UpdateDetector",
        "guardduty:DeleteDetector",
        "guardduty:ListDetectors",
        "guardduty:GetFindings",
        "guardduty:ListFindings"
      ],
      "Resource": "*"
    }
  ]
}

      Enable: true
```

Annexe C : Exemples Scripts Lambda

- **Script pour l'Automatisation des Alertes** :
    - **Description** : Script AWS Lambda pour automatiser l'envoi de notifications en cas de détection de menace par GuardDuty.
    - **Code**:



```python
import boto3

def lambda_handler(event, context):
    sns = boto3.client('sns')
    message = "Alerte de sécurité détectée par GuardDuty"
    sns.publish(TopicArn='arn:aws:sns:region:account-id:topic-
name', Message=message)
```

- **Script pour l'Automatisation de la Réponse aux Incidents** :
    - **Description** : Script AWS Lambda pour automatiser les actions de remédiation en réponse aux incidents détectés.
    - **Code:**



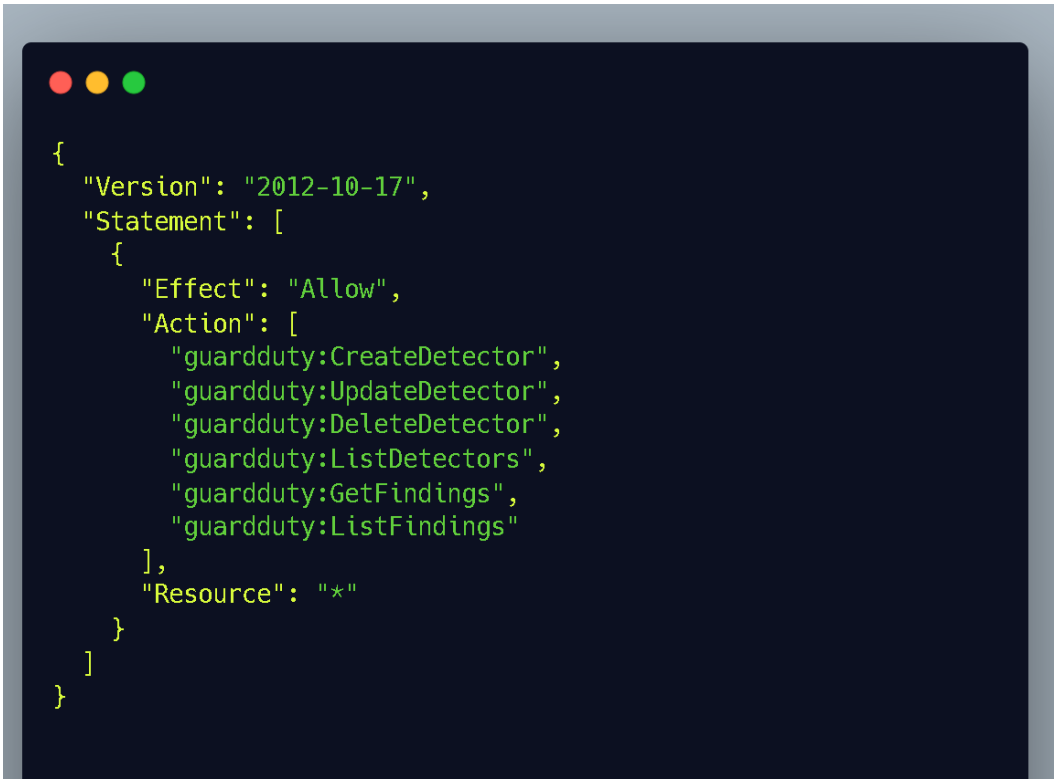
```python
import boto3

def lambda_handler(event, context):
    ec2 = boto3.client('ec2')
    response = ec2.describe_instances(Filters=[
        {'Name': 'instance-state-name', 'Values': ['running']}
    ])
    for reservation in response['Reservations']:
        for instance in reservation['Instances']:
            ec2.stop_instances(InstanceIds=
[instance['InstanceId']])
```

Annexe D : Exemples de Politiques IAM

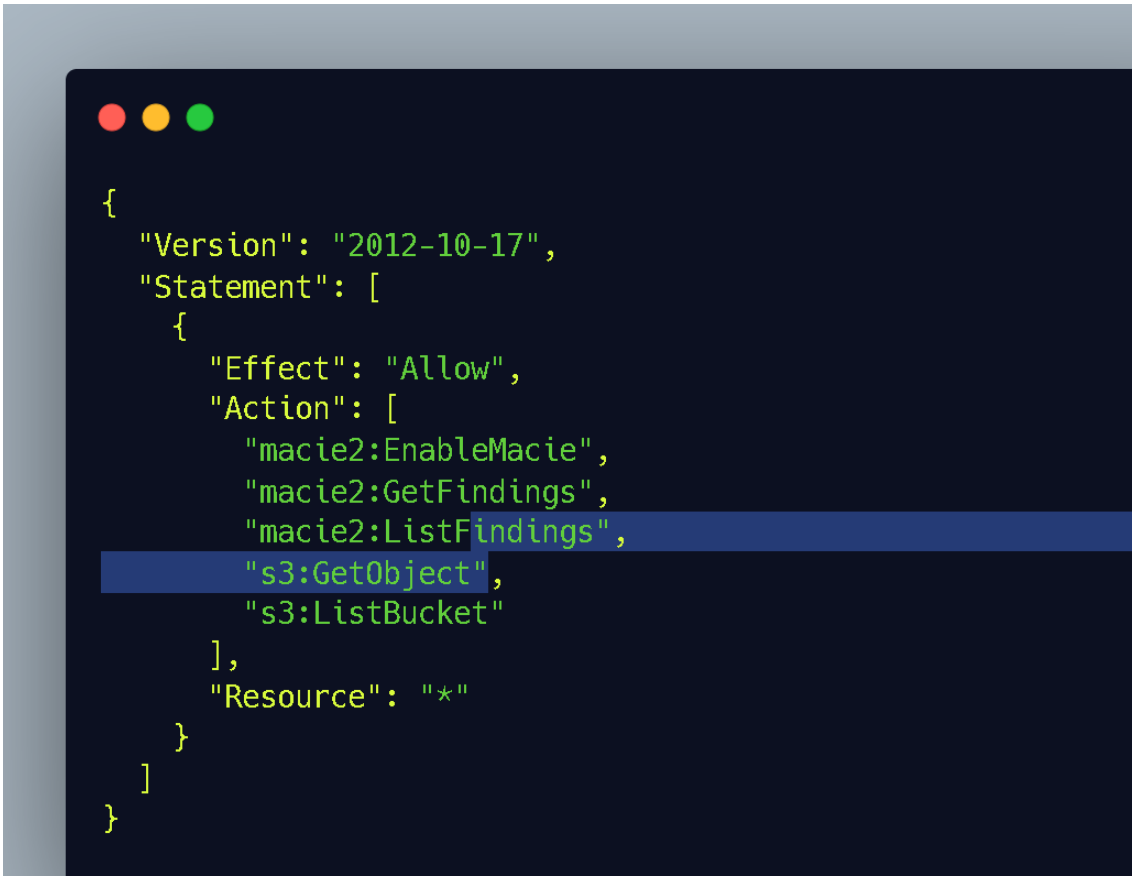
- **Politique IAM pour GuardDuty** :
    - **Description** : Politique d'accès IAM permettant à GuardDuty d'accéder aux logs nécessaires et de générer des alertes.

- **Politique**:



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateDetector",
        "guardduty:UpdateDetector",
        "guardduty:DeleteDetector",
        "guardduty:ListDetectors",
        "guardduty:GetFindings",
        "guardduty:ListFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

- **Politique IAM pour Macie** :
    - **Description** : Politique d'accès IAM permettant à Macie de scanner les buckets S3 et de générer des alertes.
    - **Politique:**


{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"macie2:EnableMacie",
"macie2:GetFindings",
"macie2:ListFindings",
"s3:GetObject",
"s3:ListBucket"
],
"Resource": "*"
}
]
}