AYI NEDJIMI Consultants

AWS Security : Les 20 Services Sécurité Essentiels

Catégorie : Cloud Security Lecture : 8 min Publié le : 03/03/2026 Auteur : Ayi NEDJIMI

Découvrez les 20 services de sécurité AWS essentiels pour protéger votre infrastructure cloud : IAM, GuardDuty, Security Hub, KMS et bien plus en.

Résumé exécutif

AWS propose plus de trente services liés à la sécurité. Ce guide sélectionne les vingt les plus critiques, détaille leur configuration optimale et explique comment les orchestrer pour construire une posture de défense en profondeur complète sur AWS.
Lorsque vous ouvrez la console AWS pour la première fois avec des responsabilités sécurité, le catalogue de services peut paraître vertigineux. Entre IAM, GuardDuty, Security Hub, Inspector, Macie, Detective, CloudTrail, Config, KMS, WAF, Shield, Firewall Manager, Network Firewall, VPC Flow Logs, Secrets Manager, Certificate Manager, Systems Manager, Organizations, Control Tower et Artifact, il faut savoir par où commencer et surtout comment ces services s'articulent entre eux. Après avoir déployé et opéré ces services sur des dizaines de comptes AWS en production, je vous propose une cartographie pragmatique qui classe ces vingt services par domaine fonctionnel, détaille les configurations critiques souvent négligées, et fournit un ordre de déploiement réaliste pour une équipe sécurité qui part de zéro ou qui souhaite consolider sa posture existante sur Amazon Web Services.

Comment structurer la gouvernance avec AWS Organizations ?

Tout commence par **AWS Organizations** et **Control Tower**. Organizations permet de créer une hiérarchie d'Organizational Units (OU) pour regrouper vos comptes par fonction : Security, Sandbox, Development, Staging, Production. Chaque OU hérite de Service Control Policies (SCP) qui définissent les gardes-fous infranchissables. Par exemple, une SCP sur l'OU Production peut interdire la suppression de CloudTrail, empêcher la création de ressources hors de certaines régions, ou bloquer l'utilisation de services non approuvés.

Control Tower automatise le provisioning de cette structure avec des guardrails prédéfinis (obligatoires et optionnels). Activez au minimum les guardrails de détection pour CloudTrail, le chiffrement EBS, et la restriction des régions. Les guardrails proactifs, basés sur AWS CloudFormation Hooks, bloquent le déploiement de ressources non conformes avant même leur création. C'est un changement de paradigme par rapport à la détection a posteriori.

Pour les détails sur les risques d'escalade de privilèges dans AWS, référez-vous à notre article sur escalades de privilèges AWS. Les SCP mal configurées sont souvent le premier vecteur exploité.

Quelles configurations IAM sont indispensables ?

AWS IAM reste le service le plus critique et le plus complexe. Les bonnes pratiques fondamentales incluent : éliminer les access keys du compte root, activer le MFA matériel sur le root, utiliser **IAM Identity Center** (ex-SSO) pour la gestion centralisée des accès humains, et privilégier les rôles IAM avec des sessions temporaires pour les accès programmatiques. Au-delà de ces basiques, configurez les *permission boundaries* pour limiter les permissions maximales que les développeurs peuvent s'auto-attribuer via leurs propres policies.

Le service **IAM Access Analyzer** détecte les ressources partagées publiquement ou avec des comptes externes. Activez-le dans chaque région active. Son module de génération de policies analyse les logs CloudTrail pour proposer des policies least-privilege basées sur l'usage réel — un outil puissant pour réduire les permissions excessives héritées de déploiements anciens.

Service	Domaine	Priorité	Coût
IAM + Identity Center	Identité	Critique	Gratuit
CloudTrail	Audit	Critique	S3 storage
GuardDuty	Détection	Critique	Volume analysé
Security Hub	Posture	Haute	Checks/mois
KMS	Chiffrement	Critique	Par clé/requête
Config	Conformité	Haute	Par règle évaluée
WAF	Protection web	Haute	Par règle/requête
Inspector	Vulnérabilités	Haute	Par scan
Macie	Données	Moyenne	Go scannés
Detective	Investigation	Moyenne	Volume ingéré

Mon avis : Trop d'organisations déploient Security Hub sans avoir d'abord correctement configuré CloudTrail et Config. Security Hub agrège les findings de ces services — s'ils sont mal configurés, Security Hub donnera un faux sentiment de sécurité. Respectez l'ordre de déploiement.

La stratégie de déploiement des services de sécurité AWS doit suivre le principe de la défense en profondeur. Chaque service adresse une couche spécifique de la protection : IAM et Organizations couvrent la couche gouvernance et identité, CloudTrail et Config couvrent la couche audit et conformité, GuardDuty et Security Hub couvrent la couche détection et posture, WAF et Shield couvrent la couche protection périmétrique, et Inspector et Macie couvrent la couche protection des workloads et données. L'erreur la plus fréquente est de déployer tous les services simultanément sans comprendre leurs interdépendances, ce qui crée un enchevêtrement de findings redondants et de configurations conflictuelles. Suivez plutôt une approche par paliers en validant le bon fonctionnement de chaque couche avant de passer à la suivante, garantissant une intégration cohérente et une valeur ajoutée mesurable à chaque étape du parcours de maturité sécurité AWS.

Détection des menaces avec GuardDuty et Security Hub

Amazon GuardDuty analyse en continu les logs VPC Flow, DNS, CloudTrail, S3, EKS et Lambda pour détecter les comportements malveillants via du machine learning et des threat intelligence feeds. Activez-le dans toutes les régions, même celles où vous ne déployez pas — un attaquant pourrait utiliser une région inactive pour du cryptomining. Les findings de GuardDuty se classent en trois catégories : **reconnaissance** (port scanning, API enumeration), **compromission d'instance** (communication avec C2, cryptomining) et **exfiltration** (transfert S3 anormal, DNS tunneling).

Security Hub centralise les findings de GuardDuty, Inspector, Macie, Firewall Manager, IAM Access Analyzer et des solutions tierces dans un tableau de bord unifié. Activez les standards CIS AWS Foundations Benchmark et AWS Foundational Security Best Practices. Chaque finding reçoit un score de sévérité normalisé ASFF (AWS Security Finding Format) qui facilite la priorisation. Configurez des actions automatisées via EventBridge pour les findings critiques : isolation d'instance, révocation de credentials, notification PagerDuty.

Les techniques d'escalade documentées dans notre article sur escalade de privilèges IAM cloud génèrent des findings spécifiques dans GuardDuty qu'il faut savoir interpréter. Pour la documentation officielle complète, consultez AWS Security.

Chiffrement et gestion des secrets

AWS KMS gère les clés de chiffrement pour l'ensemble des services AWS. Créez des clés CMK (Customer Managed Keys) pour chaque domaine applicatif avec des key policies restrictives. Activez la rotation automatique annuelle. Pour les données les plus sensibles, utilisez des clés asymétriques RSA-4096 ou ECC stockées dans des *CloudHSM* dédiés (FIPS 140-2 Level 3). **Secrets Manager** stocke et rote automatiquement les credentials de bases de données, clés API et autres secrets. Configurez la rotation Lambda pour chaque secret avec une fréquence de 30 à 90 jours selon la criticité.

AWS Certificate Manager (ACM) automatise le provisioning et le renouvellement des certificats TLS pour CloudFront, ALB et API Gateway. Utilisez des certificats publics ACM pour les endpoints externes et des certificats privés ACM Private CA pour les communications internes service-à-service. La combinaison KMS plus Secrets Manager plus ACM couvre l'ensemble des besoins cryptographiques d'une infrastructure AWS moderne.

Pour auditer la conformité de vos configurations de chiffrement via Terraform, notre guide sur audit Terraform compliance fournit des checklist actionnables.

Protection réseau : WAF, Shield et Network Firewall

AWS WAF protège vos applications web contre les attaques OWASP Top 10 : injection SQL, XSS, SSRF, path traversal. Déployez-le devant CloudFront, ALB ou API Gateway. Utilisez les Managed Rule Groups d'AWS (Core Rule Set, Known Bad Inputs, SQL Database) comme base, puis ajoutez des règles custom pour votre contexte applicatif. **AWS Shield Standard** est inclus gratuitement

et protège contre les attaques DDoS volumétriques de base. Pour les applications critiques, Shield Advanced ajoute la détection DDoS applicative, l'accès au DDoS Response Team et une protection financière contre les surcoûts d'absorption.

AWS Network Firewall est un pare-feu réseau managé qui inspecte le trafic VPC avec des règles Suricata IPS/IDS. Déployez-le dans un subnet dédié du VPC et routez le trafic via des route tables. Il complète les Security Groups et NACLs en offrant une inspection stateful en profondeur, du filtrage par domaine et de la détection d'intrusion basée sur des signatures. Combiné avec **Firewall Manager**, vous pouvez appliquer des politiques WAF, Shield et Network Firewall uniformément à travers tous vos comptes Organizations.

Chez un client e-commerce, nous avons configuré AWS WAF avec des rate-based rules qui bloquent automatiquement les IP dépassant 2000 requêtes par cinq minutes sur les endpoints de login et de paiement. Cette seule mesure a éliminé 94% des tentatives de credential stuffing sans impacter les utilisateurs légitimes. Le coût mensuel du WAF sur un ALB reste inférieur à 50 euros pour un trafic modéré.

Pourquoi AWS Inspector est indispensable en 2026 ?

Amazon Inspector scanne automatiquement les instances EC2, les images de conteneurs ECR et les fonctions Lambda pour détecter les vulnérabilités logicielles et les problèmes de configuration réseau. La version 2 (relancée en 2023) fonctionne en mode agentless via l'intégration SSM Agent — plus besoin d'installer un agent dédié. Inspector évalue les packages installés contre la base NVD et le catalogue des vulnérabilités connues exploitées (KEV) de la CISA. Les findings sont enrichis d'un score CVSS contextualisé qui prend en compte l'exposition réseau de la ressource.

Intégrez Inspector dans votre pipeline CI/CD pour scanner les images Docker avant leur push vers ECR. Bloquez le déploiement de toute image contenant des vulnérabilités critiques ou hautes non patchées. Pour les fonctions Lambda, Inspector analyse les dépendances et signale les bibliothèques vulnérables. Cette couverture étendue fait d'Inspector un pilier de la gestion des vulnérabilités cloud-native. Les recommandations de l'ANSSI complètent cette approche avec un cadre réglementaire français.

Comment exploiter CloudTrail et Config ensemble ?

CloudTrail enregistre chaque appel API dans votre environnement AWS. Configurez un trail organisationnel qui centralise les logs de tous les comptes dans un bucket S3 dédié du compte Security, avec chiffrement KMS, validation d'intégrité des fichiers et une politique de rétention de 365 jours minimum. Activez les Data Events pour S3 et Lambda si votre budget le permet — ils capturent les accès aux objets S3 et les invocations Lambda, essentiels pour la forensique.

AWS Config enregistre en continu la configuration de vos ressources et évalue leur conformité contre des règles prédéfinies ou custom. Les Config Rules détectent les dérives : un Security Group modifié pour autoriser 0.0.0.0/0, un bucket S3 rendu public, un volume EBS non chiffré.

Combiné avec les *Remediation Actions*, Config peut corriger automatiquement les non-conformités via des documents SSM Automation. Cette combinaison CloudTrail plus Config forme le socle d'audit et de conformité de toute infrastructure AWS sérieuse.

Consultez notre article sur secrets sprawl et collecte pour comprendre comment les attaquants tirent parti des secrets mal gérés dans les pipelines CI/CD AWS. De même, les problématiques de segmentation réseau traitées dans segmentation réseau VLAN firewall s'appliquent directement aux architectures VPC AWS.

À retenir : Les 20 services de sécurité AWS ne s'activent pas d'un coup. Commencez par le trio fondamental Organizations plus CloudTrail plus GuardDuty, puis étendez à IAM Identity Center, Security Hub et Config. Les services avancés comme Detective, Macie et Network Firewall viennent dans un second temps selon vos besoins spécifiques.

Faut-il investir dans Macie et Detective ?

Amazon Macie utilise le machine learning pour découvrir et classifier les données sensibles stockées dans S3 : PII, données de santé, informations financières, credentials. Activez un scan initial complet puis des scans récurrents hebdomadaires sur les buckets critiques. Macie est particulièrement utile pour la conformité RGPD et la préparation aux audits. **Amazon Detective** construit automatiquement un graphe de sécurité à partir des logs CloudTrail, VPC Flow Logs et GuardDuty pour faciliter l'investigation des incidents. Au lieu de passer des heures à corréler manuellement des logs, Detective visualise les relations entre les entités suspectes et retrace la chronologie d'un incident.

Parmi ces vingt services, combien en avez-vous réellement activé et correctement configuré dans votre environnement AWS actuel ?

Comment optimiser les coûts de sécurité AWS ?

Les services de sécurité AWS représentent un coût non négligeable qui doit être optimisé. GuardDuty facture au volume de logs analysés — désactivez les sources de données non pertinentes dans les régions peu utilisées. Security Hub facture par check de conformité — désactivez les standards non pertinents pour votre secteur. Config facture par règle évaluée — consolidez les règles redondantes. Macie facture au volume scanné — ciblez uniquement les buckets contenant potentiellement des données sensibles au lieu de scanner l'intégralité de votre parc S3. Inspector facture par scan — optimisez la fréquence selon la criticité des workloads. L'approche la plus rentable consiste à déployer les services gratuits en priorité (IAM Access Analyzer, Trusted Advisor basic, Security Hub free tier) puis à activer progressivement les services payants en mesurant leur valeur ajoutée réelle pour votre contexte spécifique.

Sources et références : CISA · Cloud Security Alliance

Conclusion et feuille de route de déploiement

La sécurité AWS se construit par couches successives. La première semaine, déployez Organizations, CloudTrail et GuardDuty. Le premier mois, ajoutez IAM Identity Center, Security Hub, Config et KMS. Le premier trimestre, complétez avec WAF, Inspector, Secrets Manager et Network Firewall. Ensuite, affinez avec Macie, Detective et les guardrails Control Tower. Cette approche progressive permet de construire une posture solide sans submerger les équipes. Chaque service renforce les autres, créant un écosystème de sécurité intégré et cohérent sur Amazon Web Services.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr