AYI NEDJIMI Consultants

Cloud Forensics Avancée Post-Compromission sur AWS

Catégorie : Cloud Security Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Méthodologie de forensics cloud AWS post-compromission : collecte de preuves, analyse CloudTrail, isolation des ressources et reconstruction de la.

Résumé exécutif

La forensics cloud post-compromission AWS nécessite des méthodologies adaptées à l'éphémérité des ressources cloud. Ce guide technique couvre la collecte de preuves, l'analyse CloudTrail, l'isolation des ressources et la reconstruction de la kill chain.
Trois heures du matin, votre PagerDuty sonne : GuardDuty a détecté une exfiltration de credentials via le metadata service suivi d'appels API suspects sur l'ensemble de vos comptes AWS. L'attaquant est actif, les données sont potentiellement compromises, et chaque minute qui passe est une minute de plus pour l'adversaire et une minute de preuves volatiles perdues. La forensics cloud est fondamentalement différente de la forensics traditionnelle : pas de disque dur à saisir physiquement, pas d'image forensique classique, des preuves réparties entre des dizaines de services managés et des logs qui peuvent être supprimés par l'attaquant s'il dispose des permissions suffisantes. Après avoir conduit des investigations forensiques sur des compromissions AWS majeures affectant des entreprises cotées en bourse, des institutions financières et des acteurs du e-commerce traitant des millions de transactions, je partage la méthodologie structurée que nous appliquons en situation de crise réelle, de la détection initiale à la remédiation complète et la production du rapport forensique final.

Comment structurer la réponse initiale ?

Les trente premières minutes après la détection sont critiques. L'objectif est triple : **contenir** la compromission pour limiter les dégâts, **préserver** les preuves avant qu'elles ne soient altérées ou détruites, et **maintenir** la continuité de service autant que possible. La première action est de *qualifier l'incident* : quel type de compromission (credential theft, ransomware, data exfiltration, cryptomining), quelle est l'étendue (un compte, plusieurs comptes, l'organization), et quelles sont les données potentiellement impactées (PII, données financières, IP).

Activez immédiatement le runbook d'incident response prédéfini. Si l'attaquant a obtenu des credentials IAM, la priorité est de les révoquer sans perdre les logs de ses activités. Ne supprimez jamais un rôle IAM compromis — désactivez-le via une policy deny-all puis analysez ses actions. Les techniques d'escalade IAM documentées dans escalades de privilèges AWS et escalade de privilèges IAM cloud sont les premiers vecteurs à investiguer.

Phase	Actions	Outils	Durée
Triage (0-30 min)	Qualifier, contenir, activer IR team	GuardDuty, CloudTrail	30 min
Préservation (30-120 min)	Sauvegarder logs, snapshots, configs	S3, EBS Snapshot, Config	90 min
Analyse (2-48h)	Reconstruire kill chain, timeline	Athena, Detective, SIEM	Variable
Remédiation (24-72h)	Corriger vulnérabilités, rotation credentials	IAM, Config, SSM	Variable
Rapport (72h-2 sem)	Documenter, lessons learned, améliorer	Documentation	1-2 semaines

Mon avis : La plus grande erreur en forensics cloud est de commencer par remédier avant d'avoir préservé les preuves. J'ai vu des équipes paniquées supprimer les instances compromises, détruisant ainsi les preuves volatiles (processus en mémoire, fichiers temporaires, network connections). Prenez un snapshot EBS AVANT de toucher à quoi que ce soit. La préservation des preuves est juridiquement nécessaire si des poursuites sont envisagées.

Quelles preuves collecter en priorité sur AWS ?

Les preuves cloud se répartissent en **preuves volatiles** (à collecter immédiatement car éphémères) et **preuves persistantes** (disponibles dans les logs et configurations stockés). Les preuves volatiles incluent : **EBS Snapshots** des volumes des instances compromises (capture l'état du disque à l'instant T), **mémoire des instances** via SSM Run Command avec des outils comme LiME ou AVML, **network connections actives** via `ss` ou `netstat`, **processus en cours** via `ps aux` et `/proc`, et les **metadata d'instance** (rôle IAM, Security Groups, user-data).

Les preuves persistantes incluent : **CloudTrail logs** (toutes les actions API), **VPC Flow Logs** (trafic réseau), **S3 Access Logs** (accès aux buckets), **CloudWatch Logs** (logs applicatifs), **AWS Config History** (changements de configuration), **GuardDuty findings** (alertes de sécurité), et les **IAM Credential Reports** (état des credentials au moment de l'incident). Chaque preuve doit être copiée dans un **bucket forensique dédié** dans un compte séparé avec Object Lock pour garantir l'intégrité. L'AWS Security documente les meilleures pratiques de collecte de preuves sur AWS.

Comment analyser les CloudTrail logs efficacement ?

L'analyse CloudTrail est le cœur de la forensics AWS. Utilisez **Amazon Athena** pour requêter les logs CloudTrail stockés dans S3 avec des requêtes SQL. Les requêtes prioritaires incluent : toutes les actions effectuées par le principal compromis (`WHERE userIdentity.arn = 'arn:aws:iam::...'`), les événements d'erreur `AccessDenied` (l'attaquant explore ses permissions), les créations et modifications de ressources IAM, les appels API depuis des IP non reconnues, et les actions de *defense evasion* (StopLogging, DeleteTrail, PutEventSelectors).

Construisez une **timeline** chronologique de toutes les actions du principal compromis, depuis le premier accès jusqu'à la détection. Identifiez le vecteur d'initial access (credentials fuités, SSRF, compromission de compte), les actions de reconnaissance (ListBuckets, DescribeInstances, GetCallerIdentity), l'escalade de privilèges (AttachRolePolicy, CreatePolicyVersion, AssumeRole), le mouvement latéral (cross-account AssumeRole, accès à d'autres services), et l'objectif final (GetObject S3, CreateDBSnapshot, RunInstances pour cryptomining). Les techniques de gestion des secrets via secrets sprawl et collecte aident à comprendre comment les credentials ont pu être compromis initialement.

L'ANSSI recommande une approche structurée de la collecte et conservation des preuves numériques conforme au cadre juridique français.

Lors d'une investigation forensique pour un groupe média, l'analyse CloudTrail a révélé 47 000 événements API sur 72 heures effectués par le principal compromis. En filtrant par IP source, nous avons identifié trois adresses IP distinctes utilisées par l'attaquant, géolocalisées en Russie, au Vietnam et aux Pays-Bas (VPN). La reconstruction de la kill chain a montré : initial access via des credentials IAM trouvés dans un bucket S3 public contenant des backups Terraform (state file non chiffré), reconnaissance pendant 6 heures, création d'un rôle admin backdoor, puis exfiltration de 2.3 To de données client depuis un bucket S3 de production. Le temps entre l'initial access et la détection GuardDuty : 68 heures.

L'utilisation d'**Amazon Detective** accélère considérablement l'investigation forensique en construisant automatiquement un graphe de sécurité à partir des logs CloudTrail, VPC Flow Logs et GuardDuty findings. Au lieu de corréler manuellement des milliers d'événements CloudTrail via des requêtes Athena, Detective visualise les relations entre les entités suspectes et retrace la chronologie d'un incident. Le panneau de profil de chaque entité (user, role, instance, IP) affiche l'historique de ses activités avec des statistiques de baseline permettant d'identifier les anomalies. Les graphes de comportement montrent les interactions entre les entités au fil du temps, révélant les patterns de mouvement latéral et d'escalade de privilèges que l'analyse manuelle des logs bruts prendrait des heures à reconstituer. Detective est particulièrement utile pendant les premières heures critiques de l'incident quand la vitesse d'analyse est primordiale pour contenir la compromission avant qu'elle ne se propage davantage dans l'environnement.

Comment isoler les ressources compromises ?

L'isolation des ressources compromises doit préserver les preuves tout en coupant l'accès de l'attaquant. Pour les **instances EC2** : créez un snapshot EBS (preuve), puis modifiez le Security Group pour n'autoriser que le trafic depuis l'IP de l'équipe forensique sur le port SSH — ne terminez pas l'instance. Pour les **credentials IAM** : attachez une policy inline deny-all au user ou role compromis plutôt que de le supprimer (préserve les logs). Pour les **buckets S3** : ajoutez une bucket policy deny-all sauf pour le compte forensique. Pour les **Lambda functions** : retirez les triggers mais ne supprimez pas la fonction (le code et les variables d'environnement sont des preuves).

L'IaC et les configurations Terraform via audit Terraform compliance permettent de comparer l'état actuel des ressources avec l'état attendu pour identifier les modifications malveillantes. Les techniques GCP forensiques via sécurité offensive GCP complètent cette méthodologie pour les environnements multi-cloud.

Quelles leçons tirer pour améliorer la posture ?

Chaque incident forensique doit se conclure par un **post-mortem structuré** qui documente : la cause racine (root cause), la chronologie complète de l'incident, les facteurs qui ont permis ou facilité la compromission, les facteurs qui ont limité les dégâts, et les actions correctives classées par priorité. Les améliorations typiques incluent : renforcement des configurations IAM (least privilege, SCP), activation de services de détection manquants (GuardDuty dans toutes les régions), amélioration de la rétention et de la protection des logs, formation des équipes aux procédures d'incident response, et tests réguliers du plan de réponse aux incidents.

À retenir : La forensics cloud AWS repose sur un principe fondamental : préserver d'abord, analyser ensuite. Les preuves volatiles (mémoire, processus, connections) disparaissent en minutes si l'instance est redémarrée ou terminée. Les preuves persistantes (CloudTrail, Flow Logs) peuvent être supprimées par un attaquant avec les bonnes permissions. Protégez vos logs dans un compte dédié avec Object Lock et des SCP qui empêchent leur suppression — c'est votre assurance forensique.

Faut-il externaliser la forensics cloud ?

La forensics cloud nécessite des compétences pointues rarement disponibles en interne : expertise AWS IAM profonde, maîtrise des outils de requêtage (Athena, jq, Python), connaissance des techniques d'attaque cloud, expérience de la gestion de crise et des aspects juridiques (préservation de preuves, chaîne de custody, collaboration avec les forces de l'ordre). Pour les organisations sans équipe DFIR (Digital Forensics and Incident Response) dédiée, un contrat de retainer avec un prestataire spécialisé garantit une disponibilité sous 4 heures en cas d'incident. Le coût d'un retainer annuel (10-30k€) est négligeable comparé au coût d'une investigation improvisée par des équipes non formées qui risquent de détruire des preuves et de prolonger l'incident.

La **chaîne de custody** (chain of custody) des preuves numériques cloud est essentielle si des poursuites judiciaires sont envisagées. Chaque preuve collectée doit être documentée avec : qui l'a collectée, quand, comment (commande exacte), où elle est stockée, et son hash SHA-256 pour vérifier l'intégrité. Les preuves stockées dans S3 avec Object Lock en mode Compliance fournissent une garantie d'immuabilité vérifiable. Conservez un journal d'investigation chronologique détaillant chaque action de l'équipe forensique, chaque preuve consultée et chaque conclusion tirée. Ce journal est admissible en tribunal et démontre le sérieux et la rigueur de l'investigation, protégeant votre organisation en cas de litige avec des clients ou des partenaires affectés par l'incident de sécurité.

Si vous découvrez demain matin que vos credentials AWS root ont été utilisés depuis une IP inconnue il y a trois jours, disposez-vous d'un runbook documenté et testé pour les trente premières minutes de réponse ?

Comment constituer une équipe de réponse aux incidents cloud ?

L'équipe de réponse aux incidents cloud (CSIRT Cloud) doit combiner des compétences techniques et organisationnelles spécifiques. Le **noyau technique** comprend : un analyste CloudTrail expert en requêtes Athena et reconstitution de timelines, un spécialiste IAM capable de comprendre les permissions effectives et les chemins d'escalade, un ingénieur réseau cloud maîtrisant les VPC Flow Logs et les architectures réseau AWS, Azure et GCP, et un analyste forensique traditionnel formé aux spécificités du cloud. Le **noyau organisationnel** inclut : un incident commander qui coordonne la réponse et les communications, un liaison juridique qui valide la préservation des preuves et les obligations de notification, et un communicant qui gère les notifications aux parties prenantes internes et externes.

L'équipe doit disposer de **runbooks pré-validés** pour les scénarios de compromission les plus fréquents : compromission de credentials IAM, ransomware cloud avec chiffrement de données S3, cryptomining sur instances EC2 ou Lambda, exfiltration de données via des API publiques, et compromission d'un pipeline CI/CD. Chaque runbook détaille les étapes de containment, de préservation des preuves, d'analyse et de remédiation avec les commandes AWS CLI ou les scripts Python exacts à exécuter. Les runbooks sont testés lors d'exercices tabletop trimestriels et mis à jour après chaque incident réel pour intégrer les leçons apprises et les nouvelles techniques d'attaque observées dans le paysage des menaces cloud en constante évolution.

Sources et références : CISA · Cloud Security Alliance

Conclusion : préparer la forensics avant l'incident

La forensics cloud efficace se prépare avant l'incident, pas pendant. Activez CloudTrail dans toutes les régions avec des Data Events pour S3 et Lambda. Centralisez les logs dans un compte forensique dédié avec Object Lock. Documentez les runbooks d'isolation et de collecte de preuves. Formez votre équipe aux outils Athena et Detective. Testez votre plan d'incident response via des exercices tabletop trimestriels simulant des scénarios de compromission AWS réalistes. Cette préparation transforme une situation de crise chaotique en une réponse structurée et efficace qui limite les dégâts, préserve les preuves et accélère le retour à la normale.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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