AYI NEDJIMI Consultants

Forensique Cloud : Analyser les Logs CloudTrail, Azure

Catégorie : Forensics Lecture : 5 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide de forensique cloud : analyse des logs AWS CloudTrail, Azure Activity/Sign-in Logs, GCP Audit Logs, investigation d'incidents et méthodologie.

Architecture de CloudTrail

AWS CloudTrail enregistre chaque appel API effectué dans un compte AWS, qu'il provienne de la console, du CLI, du SDK ou d'un service AWS. Chaque entrée CloudTrail contient l'identité de l'appelant (ARN de l'utilisateur ou du rôle), l'action effectuée (nom de l'API), les paramètres de la requête, la réponse, l'adresse IP source, l'User-Agent et un horodatage précis. CloudTrail distingue trois types d'événements : Guide de forensique cloud : analyse des logs AWS CloudTrail, Azure Activity/Sign-in Logs, GCP Audit Logs, investigation d'incidents et méthodologie. L'investigation numérique exige rigueur et méthodologie. Forensique Cloud : Analyser les Logs CloudTrail, Azure couvre les aspects pratiques que les analystes forensics rencontrent sur le terrain. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Type d'événement	Description	Exemples	Activation
Management Events	Actions sur les ressources AWS (plan de contrôle)	CreateUser, RunInstances, PutBucketPolicy	Activé par défaut
Data Events	Actions sur les données (plan de données)	GetObject (S3), Invoke (Lambda)	Désactivé par défaut (coût)
Insights Events	Détection automatique d'anomalies d'utilisation API	Pic d'appels DeleteObject	Optionnel (payant)

Attention critique : Data Events
Par défaut, CloudTrail n'enregistre PAS les Data Events (accès aux objets S3, invocations Lambda, requêtes DynamoDB). Si un attaquant accède à des données sensibles dans S3 sans que les Data Events soient activés, il n'y aura **aucune trace** de ces accès dans CloudTrail. L'activation des Data Events est indispensable pour la forensique, malgré le coût supplémentaire.

Requêtage avec Amazon Athena

Pour les investigations portant sur de grandes périodes ou des volumes importants de logs, **Amazon Athena** permet de requêter les fichiers CloudTrail stockés dans S3 avec du SQL standard. La première étape consiste à créer une table Athena pointant vers le bucket CloudTrail :

```
-- Création de la table Athena pour CloudTrail
CREATE EXTERNAL TABLE cloudtrail_logs (
    eventVersion STRING,
    userIdentity STRUCT<
        type: STRING,
        principalId: STRING,
        arn: STRING,
        accountId: STRING,
        invokedBy: STRING,
        accessKeyId: STRING,
        userName: STRING,
        sessionContext: STRUCT<
            attributes: STRUCT,
            sessionIssuer: STRUCT
        >
    >,
    eventTime STRING,
    eventSource STRING,
    eventName STRING,
    awsRegion STRING,
    sourceIPAddress STRING,
    userAgent STRING,
    errorCode STRING,
    errorMessage STRING,
    requestParameters STRING,
    responseElements STRING,
    resources ARRAY>
)
ROW FORMAT SERDE 'org.apache.hive.hcatalog.data.JsonSerDe'
LOCATION 's3://mon-bucket-cloudtrail/AWSLogs/123456789012/CloudTrail/'

-- Requête : toutes les actions d'un utilisateur compromis
SELECT eventTime, eventName, sourceIPAddress, userAgent, errorCode
FROM cloudtrail_logs
WHERE userIdentity.arn LIKE '%compromised-user%'
AND eventTime BETWEEN '2026-01-15T00:00:00Z' AND '2026-02-01T00:00:00Z'
ORDER BY eventTime;

-- Requête : connexions depuis des IPs inhabituelles
SELECT sourceIPAddress, COUNT(*) as nb_events,
       MIN(eventTime) as first_seen, MAX(eventTime) as last_seen,
       ARRAY_AGG(DISTINCT eventName) as actions
FROM cloudtrail_logs
WHERE userIdentity.arn LIKE '%admin%'
AND eventTime > '2026-01-01'
GROUP BY sourceIPAddress
ORDER BY nb_events DESC;
```

Sources complémentaires AWS

VPC Flow Logs capturent les métadonnées des flux réseau (IP source/destination, ports, protocole, bytes, action accept/reject) au niveau de l'interface réseau (ENI), du sous-réseau ou du VPC. Ils sont essentiels pour détecter les mouvements latéraux entre instances, les connexions vers des IP de C2 et l'exfiltration de données. Les Flow Logs peuvent être publiés vers CloudWatch Logs, S3 ou Kinesis Data Firehose.

S3 Access Logs fournissent un détail des requêtes effectuées sur chaque bucket (méthode HTTP, clé d'objet, statut HTTP, bytes transférés). Ils complètent les Data Events de CloudTrail avec des métadonnées supplémentaires comme le referer et les headers HTTP.

Amazon GuardDuty est un service de détection de menaces qui analyse automatiquement les logs CloudTrail, VPC Flow Logs et DNS pour identifier les comportements suspects. Les findings GuardDuty constituent un point de départ précieux pour l'investigation : chaque finding contient un type de menace, un score de sévérité, les ressources affectées et les détails techniques. Pour la forensique, les findings de type `UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B`, `Exfiltration:S3/MaliciousIPCaller` ou `PrivilegeEscalation:IAMUser/AnomalousBehavior` sont particulièrement pertinents.

Notre avis d'expert
La reconstruction de timeline est l'art le plus sous-estimé de la forensique numérique. Corréler les horodatages entre fichiers système, journaux d'événements, artefacts réseau et traces applicatives permet de reconstituer le scénario exact d'une compromission.

```
// Connexions suspectes : échecs suivis de succès (password spray réussi)
SigninLogs
| where TimeGenerated > ago(30d)
| summarize
    FailedCount = countif(ResultType != "0"),
    SuccessCount = countif(ResultType == "0"),
    DistinctIPs = dcount(IPAddress),
    IPList = make_set(IPAddress)
  by UserPrincipalName
| where FailedCount > 50 and SuccessCount > 0
| sort by FailedCount desc

// Détection de connexion impossible (impossible travel)
SigninLogs
| where ResultType == "0"
| project TimeGenerated, UserPrincipalName, IPAddress, Location
| sort by UserPrincipalName, TimeGenerated
| extend PrevTime = prev(TimeGenerated, 1), PrevLocation = prev(Location, 1), PrevUser =
prev(UserPrincipalName, 1)
| where UserPrincipalName == PrevUser
| extend TimeDiffMinutes = datetime_diff('minute', TimeGenerated, PrevTime)
| where TimeDiffMinutes < 60 and Location != PrevLocation and PrevLocation != ""
| project TimeGenerated, UserPrincipalName, Location, PrevLocation, TimeDiffMinutes,
IPAddress

// Opérations sensibles sur les rôles RBAC
AzureActivity
| where OperationNameValue has_any ("Microsoft.Authorization/roleAssignments/write",
    "Microsoft.Authorization/roleDefinitions/write")
| where ActivityStatusValue == "Success"
| project TimeGenerated, Caller, OperationNameValue, ResourceGroup, Properties
| sort by TimeGenerated desc

// Investigation Key Vault : accès aux secrets
AzureDiagnostics
| where ResourceType == "VAULTS"
| where OperationName in ("SecretGet", "SecretList", "KeyGet", "CertificateGet")
| project TimeGenerated, CallerIPAddress, identity_claim_upn_s, OperationName, id_s
| sort by TimeGenerated desc
```

Microsoft Sentinel pour la forensique

Microsoft Sentinel est le SIEM cloud-native d'Azure qui centralise les logs de l'ensemble de l'écosystème Microsoft (Azure, M365, Entra ID, Defender) et de sources tierces. Pour la forensique cloud, Sentinel offre plusieurs avantages : la corrélation automatique entre les logs Azure et les logs Microsoft 365 (Exchange Online, SharePoint, Teams), les workbooks de visualisation prêts à l'emploi, et les capacités de hunting avec les requêtes KQL. Les tables Sentinel les plus pertinentes pour la forensique sont `SigninLogs`, `AuditLogs`, `AzureActivity`, `SecurityAlert` et `OfficeActivity`.

L'API **Microsoft Graph** complète les sources de logs en donnant accès programmatique aux audit logs d'Entra ID, aux sign-in logs et aux détections Identity Protection. Pour une investigation approfondie, l'API Graph permet de récupérer les détails des applications enregistrées (app registrations), des consentements OAuth accordés et des configurations de service principal -- des éléments essentiels pour comprendre les attaques par abus d'applications.

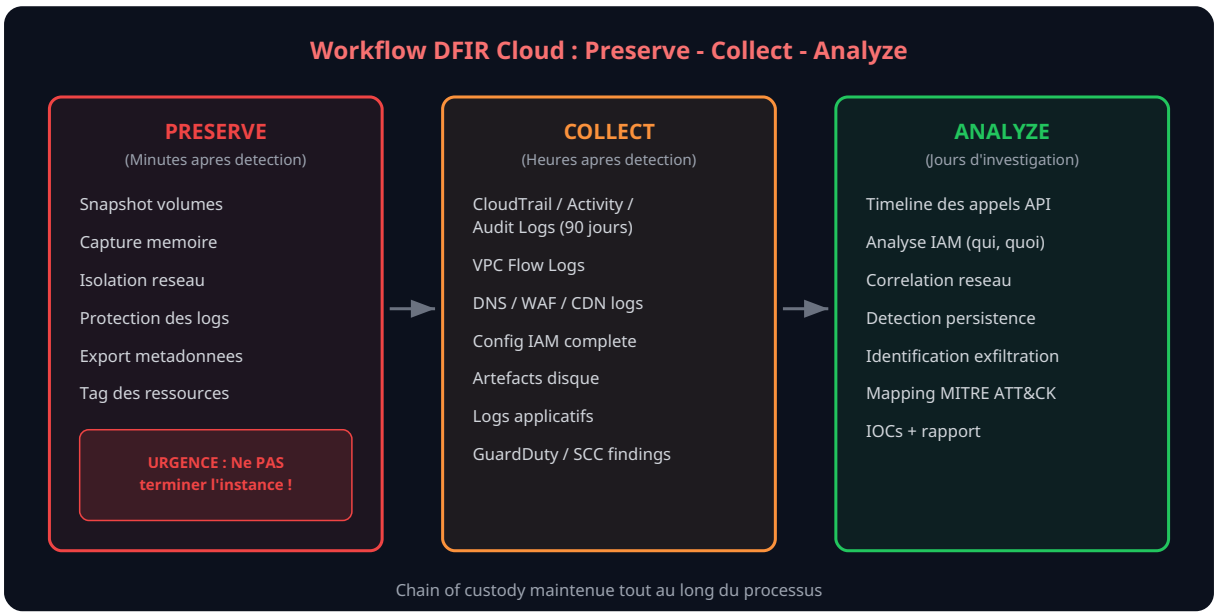
Cas concret
L'analyse de Stuxnet, considéré comme le premier cyberarme étatique, a nécessité des mois de rétro-ingénierie par les équipes de Symantec et Kaspersky. La forensique a révélé un niveau de sophistication sans équivalent : exploitation de 4 zero-days Windows, ciblage de contrôleurs Siemens spécifiques et mécanismes de propagation USB multiples.

La collecte rassemble toutes les données forensiques pertinentes dans un environnement d'analyse sécurisé. Pour la forensique cloud, la collecte couvre trois dimensions :

Logs du cloud provider : exporter les logs CloudTrail, Activity Logs ou Cloud Audit Logs pour la période d'investigation (typiquement, 90 jours avant la détection). Pour AWS, les logs sont déjà dans S3 si un trail est configuré. Pour Azure, il faut exporter le Log Analytics Workspace. Pour GCP, utiliser `gcloud logging read` avec des filtres temporels ou configurer un sink vers BigQuery pour l'analyse.

Artefacts système : à partir des snapshots préservés, créer un volume et le monter sur une instance d'analyse pour extraire les logs système, les configurations, les binaires suspects et les artefacts forensiques classiques (crontab, authorized_keys, bash_history, journalctl).

Configuration et état : collecter l'état actuel de la configuration IAM (politiques, rôles, utilisateurs, clés d'accès), des Security Groups, des bucket policies, des VPC et de tous les éléments de configuration qui auraient pu être modifiés par l'attaquant.



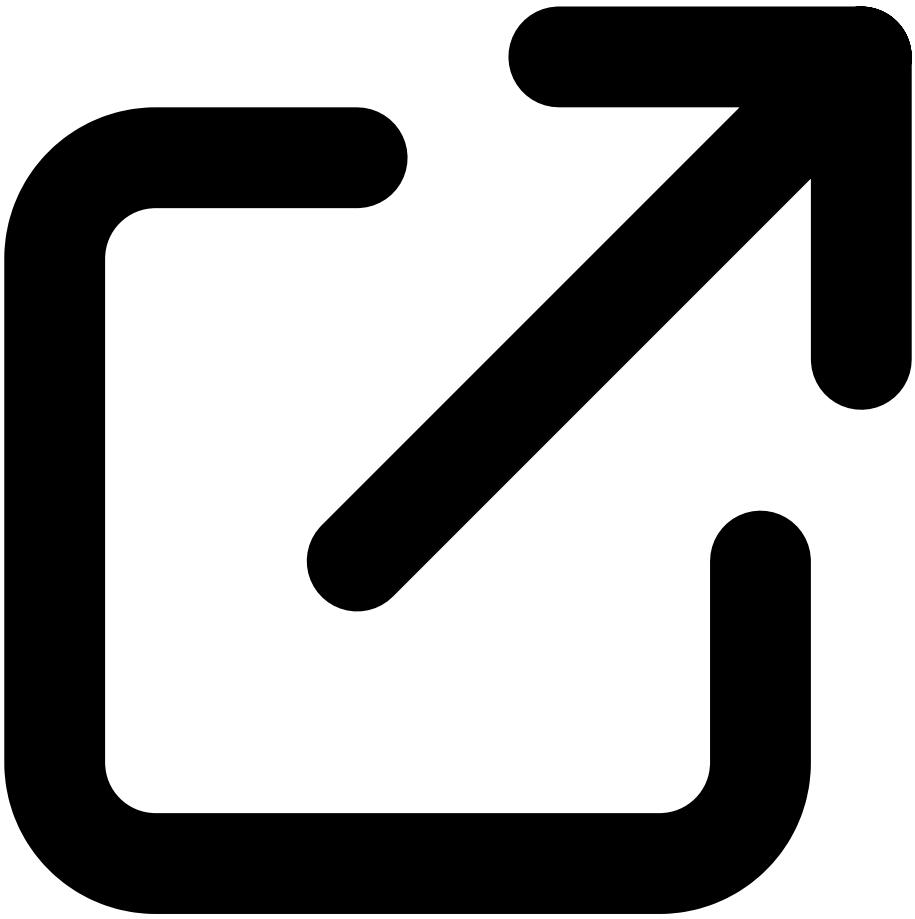
Cet article vous a été utile ? Partagez-le avec votre réseau professionnel !

Partager sur X

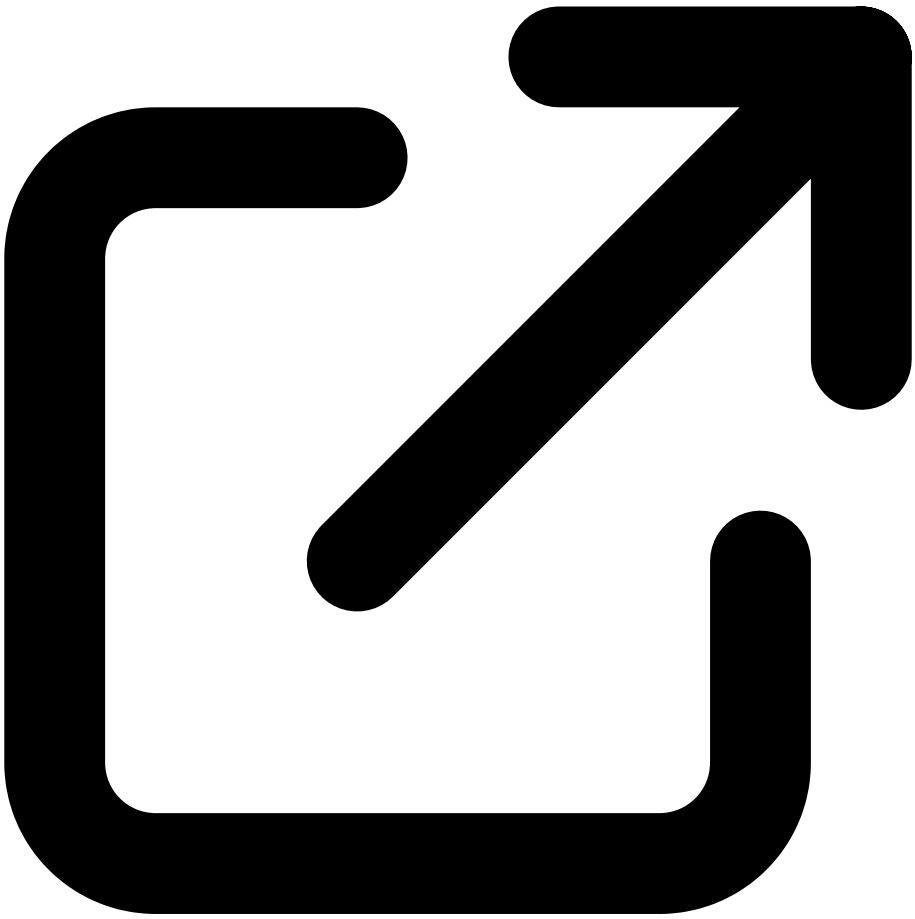
Partager sur LinkedIn

Ressources & Références Officielles

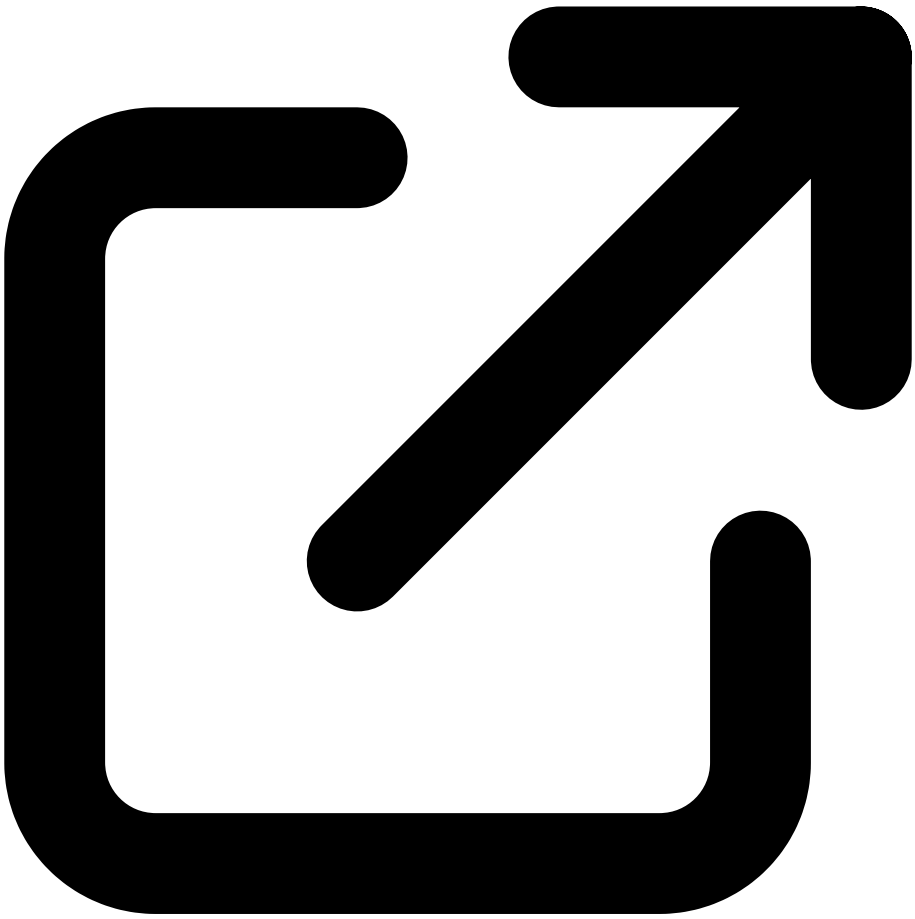
Documentations officielles et outils de la communauté DFIR cloud



AWS CloudTrail Documentation
docs.aws.amazon.com



Azure Monitor & Sentinel
learn.microsoft.com



Prowler - Cloud Security Tool
github.com/prowler-cloud

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Références et ressources externes

- AWS CloudTrail User Guide — Documentation officielle AWS CloudTrail
- Azure Activity Log — Documentation officielle Azure Monitor
- GCP Cloud Audit Logs — Documentation officielle Google Cloud Logging
- Prowler — Outil open source d'audit de sécurité cloud multi-provider
- Invictus IR — Framework open source de réponse à incident cloud

Sources et références : SANS SIFT · MITRE ATT&CK

Articles connexes

- DFIR Cloud : Investigation Logs AWS CloudTrail en 2026
- Mobile Forensics : Extraction et Analyse iOS/Android
- LNK & Jump Lists : Strategies de Detection et de Remediation
- Memory Forensics : Strategies de Detection et de Remediation

FAQ

Qu'est-ce que Forensique Cloud ?

Forensique Cloud désigne l'ensemble des concepts, techniques et méthodologies abordés dans cet article. Les fondamentaux sont détaillés dans les premières sections du guide.

Pourquoi forensique cloud cloudtrail azure gcp est-il important ?

La maîtrise de forensique cloud cloudtrail azure gcp est devenue essentielle pour les équipes de sécurité. Les enjeux et le contexte opérationnel sont développés tout au long de l'article.

Comment appliquer ces recommandations en entreprise ?

Chaque section de cet article propose des méthodologies et des outils directement utilisables. Les recommandations tiennent compte des contraintes d'environnements de production réels.

> Points clés à retenir
>
> • Forensique Cloud : Analyser les Logs CloudTrail, Azure

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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