< CARTOGRAPHIE DES RISQUES DANS LE CLOUD >

CAMPUS CYBER 2026

< SOMMAIRE >

< 1. INTRODUCTION >

1.1 CONTEXTE & OBJECTIFS

Le présent document traite de la problématique de la détection d'attaques potentielles ou avérées sur un environnement de production numérique hébergé sur le Cloud public, privé ou hybride. Les principales attaques à détecter sont celles relatives à des risques dont l'identification servira de base au développement d'une stratégie de détection efficace, en considérant la spécificité du Cloud.

Pour asseoir cette stratégie, il s'agit de procéder à l'identification des risques et de les relier à des règles de détection de haut niveau pour les intégrer à un système de détection outillé.

Les risques se rattachent aux fonctionnalités spécifiques du Cloud telles que les accès depuis Internet, les environnements virtualisés pouvant être mutualisés, l'externalisation de l'administration et de l'hébergement.

- **Grâce à ce document vous pourrez…**
  Repenser votre stratégie de détection des évènements de sécurité lors de l'usage partiel ou massif des solutions Cloud, que la partie prenante soit l'utilisateur final ou le fournisseur de la solution.

- **Pour utiliser ce document...**
  La liste des risques Cloud est proposée par valeurs métier et par acteurs. Elle permet donc à chacun selon son profil de se focaliser sur les risques de détection auxquels il peut être confronté.
  Sur la base des risques sélectionnés, l'utilisateur des documents va pouvoir retrouver les éléments pour aborder sa stratégie de détection dans le Cloud.

1.2 MÉTHODOLOGIE

L'évaluation des risques dans le cadre de la détection nous amène à réfléchir à trois situations auxquelles tout acteur, opérationnel ou hiérarchique, ne souhaite pas être confronté :

- La première correspond à la **non-détection d'un incident de sécurité** ;
- La deuxième est relative à un **défaut de qualité dans les éléments remontés** ;
- La troisième est **l'incapacité de prendre la bonne décision**.

Dans ce contexte, il nous importe donc de disposer de ressources suffisantes et qualifiées, tant humaines que techniques, pour assurer un déroulement optimal du processus de détection.

Toutefois, la réalité opérationnelle est tout autre et les efforts à consentir pour éviter les situations redoutées identifiées sont conséquents.

Le but de ce livrable est de proposer une démarche qui permet de se focaliser sur l'essentiel en termes de détection et qui se veut progressive.

Les étapes retenues pour arriver à ce résultat ont été :

- L'identification des éléments essentiels, par acteur du Cloud, grâce à une démarche d'analyse de risques ;
- La sélection des risques identifiés par le CESIN associés aux éléments essentiels précédemment définis ;
- La sélection de méthodes d'attaques MITRE en lien avec les risques retenus.

1.3 REMERCIEMENTS

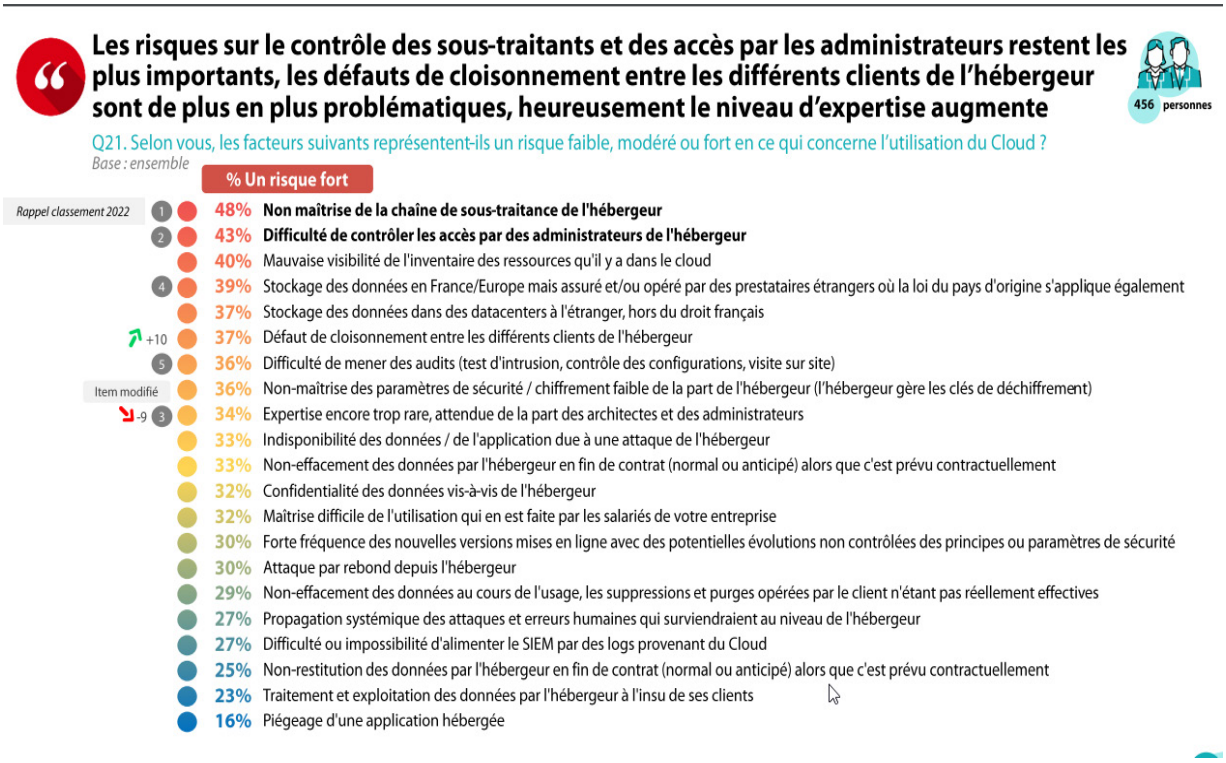
Le Campus Cyber adresse ses sincères remerciements aux contributeurs du Groupe de travail « Cartographie des risques dans le Cloud », rattaché à la Communauté d'Intérêt « Détection dans le Cloud » notamment à Nadège LESAGE (Hexatrust), Timothé PENISSON (Bouygues Télécom), Pierre PARREND (EPITA) et Baptiste CIANCHI (Wavestone).

< 2. IDENTIFICATION DES RISQUES >

La mise en place d'une méthode de recensement des risques ne peut s'affranchir de l'étude de l'existant et des publications produites. En effet, tout domaine d'expertise suppose le consensus entre pairs et à ce titre, il est de bon usage de prendre en considération les directions et les positions déjà explorées. Bien entendu, il ne s'agit pas de reprendre sans analyse cet existant mais bien de l'adapter et de le compléter.

Ainsi, dans le cas de notre groupe de travail, nous avons retenu la production du CESIN en matière de risques Cloud. Ce choix se justifie par le rayonnement de cet organisme et par la qualité de ses réflexions et de ses livrables. Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association de référence qui réunit les responsables de la cybersécurité des grandes organisations françaises afin de partager expertises, retours d'expérience et bonnes pratiques face aux enjeux cyber.

En substance, cette liste positionne de manière hierarchisée les principaux risques auxquels les acteurs du Cloud sont confrontés.



Les risques mis en avant posent la question de la gestion des responsabilités des acteurs du Cloud, de la maîtrise des actions d'administration qui sont réalisées sur les composants du Cloud et de la protection des données gérées dans le Cloud. Comme le résume le CESIN, « les risques sur le contrôle des sous-traitants et des accès par les administrateurs restent les plus importants, les défauts de cloisonnement entre les différents clients de l'hébergeur sont de plus en plus problématiques. Heureusement, le niveau d'expertise augmente. »

De cette liste nous avons extrait les risques qui correspondaient le plus à notre problématique de détection dans le Cloud. Et pour organiser de manière rigoureuse cette sélection, nous avons décidé de reprendre en parallèle une démarche d'analyse de risques sur notre contexte particulier qu'est la détection.

Notre choix pour aborder cette analyse de risques s'est porté sur la méthode EBIOS RM. EBIOS Risk Manager (EBIOS RM) est la méthode française de référence pour l'analyse et le traitement des risques numériques. Publiée par l'ANSSI, elle propose une approche structurée permettant aux organisations de maîtriser leurs risques cyber, d'orienter leurs décisions stratégiques et d'assurer la résilience de leurs activités. Cette méthode permet d'identifier et de comprendre les risques pesant sur les activités critiques, en prenant en compte les cybermenaces propres au périmètre étudié. Cela permet ainsi de définir une stratégie de sécurité cohérente, fondée sur la gestion des risques en priorisant les mesures nécessaires et en justifiant les investissements à consentir.
La méthodologie se fonde sur une approche bâtie autour de cinq ateliers, de la définition du périmètre, des valeurs métier à l'acceptation du risque résiduel en passant par les mises en avant de scénarios stratégiques et opérationnels et de plan de traitement des risques. Par cette approche opérationnelle et concrète, elle s'adapte aux enjeux métiers de manière modulaire et flexible. De plus, elle est en conformité avec la norme ISO/IEC 27005 ,qui définit les principes généraux de gestion des risques de sécurité de l'information et cyber.

Dans notre contexte, les parties prenantes retenues sont les clients finaux (usagers d'une solution clé en main de type SaaS, exploitants d'une infrastructure de type PaaS ou administrateurs d'une infrastructure IaaS), les fournisseurs de services (application en SaaS, infrastructure IaaS ou PaaS) et les hébergeurs. Au cours de cette analyse de risques, il a été décidé de prendre les hébergeurs uniquement sous l'angle de la sous-traitance (et non en tant qu'acteur) pour la fourniture des locaux et des services associés tels que la gestion de la sécurité physique, de l'alimentation électrique. Cela évite d'exprimer directement des risques de sécurité physique et permet de les aborder qu'en tant que modalités d'attaque éventuelles.

Pour les valeurs métiers, à savoir les actifs qui sont à protéger car ils représentent les composants numériques essentiels des parties prenantes pour assurer leurs missions, nous avons identifié les données et les processus essentiels aux clients finaux et aux fournisseurs de services tels que les données métiers des clients finaux, les configurations des équipements, les logs métier et les comptes associés à leur secret.

C'est en mettant en relation les valeurs métiers et les parties prenantes, que nous avons remarqué l'absence de pertinence de prendre en considération les valeurs métiers de l'hébergeur, dans le contexte de ce guide. De la sorte, nous n'avons traité à la suite de cette analyse que les risques relatifs aux clients finaux et les fournisseurs de services.

Pour identifier les risques, nous avons repris les critères de sécurité que sont la confidentialité, l'intégrité et la disponibilité. Dans la mesure où nous avions identifié les logs métiers pour les utilisateurs finaux comme pour les fournisseurs de services Cloud, nous ne nous sommes pas attardés sur le critère de sécurité lié à la traçabilité. Et, à chacune des valeurs métiers, nous nous sommes posé la question du risque, du point de vue de la détection, associé à la perte du critère de sécurité. Ainsi, il en est ressorti une liste restreinte et générale de risques à envisager.

Cette liste est présentée ci-après :

1. Actif à protéger : la base de comptes tant utilisateurs qu'administrateurs, de l'utilisateur final (le client) ou des administrateurs (le client sur sa sphère de responsabilité et le fournisseur sur son périmètre de responsabilité)

- **Risque en confidentialité** : vol des comptes et de leur secret pour permettre l'usurpation d'identité par un attaquant depuis Internet ou par une attaque en engineering social, rendant impossible la détection de l'attaque puisque les comptes sont légitimes.
- **Risque en disponibilité** : blocage des comptes par tentatives infructueuses dépassant les seuils autorisés ou par intégration des comptes dans des listes noires (blacklist) par détournement de finalité de fonctions de sécurité.
- **Risque en intégrité** : création de comptes fantômes ou élévation de privilèges sur des comptes existants pour rendre les actions liées à l'attaque indétectable car reposant sur la base de comptes légitimes.

2. Actif à protéger : les données métier appartenant tant à l'utilisateur final (le client, par exemple la base de données qui recense toutes ses ventes réalisées) qu'au fournisseur de solutions Cloud (ex : dossiers d'architecture technique sensible, procédures techniques.

- **Risque en confidentialité** : vol ou fuite de ces données métiers, attaque réalisée par un attaquant interne ou externe à l'organisation ciblée pour répondre à une mission commanditée par un concurrent, par exemple, ou pour obtenir le gain d'une vente illégale sur le darkweb.
- **Risque en disponibilité** : destruction massive de données métier par un attaquant interne ou externe à l'organisation ciblée ou attaque par rançonlogiciel pour monnayer la restitution des données.
- **Risque en intégrité** : modification silencieuse de données métiers pour induire de l'incohérence dans celles-ci et les rendre ainsi non fiables et inutilisables.

3. Actif à protéger : les configurations de composants critiques sous la responsabilité du fournisseur de solutions Cloud (ex : configuration de composants réseaux ou systèmes critiques, de fonctions de sécurité).

- **Risque en confidentialité :** récupération des paramètres utilisés dans les configurations pour une évaluation par l'attaquant des moyens de contournement et de faiblesse dans le but de faciliter son attaque.

- **Risque en disponibilité** : neutralisation de fonctions de sécurité ou d'un service par un attaquant interne ou externe à l'organisation ciblée.
- **Risque en intégrité :** abaissement du niveau de sécurité d'une fonction de sécurité ou plus généralement d'une configuration par un attaquant interne ou externe à l'organisation ciblée.

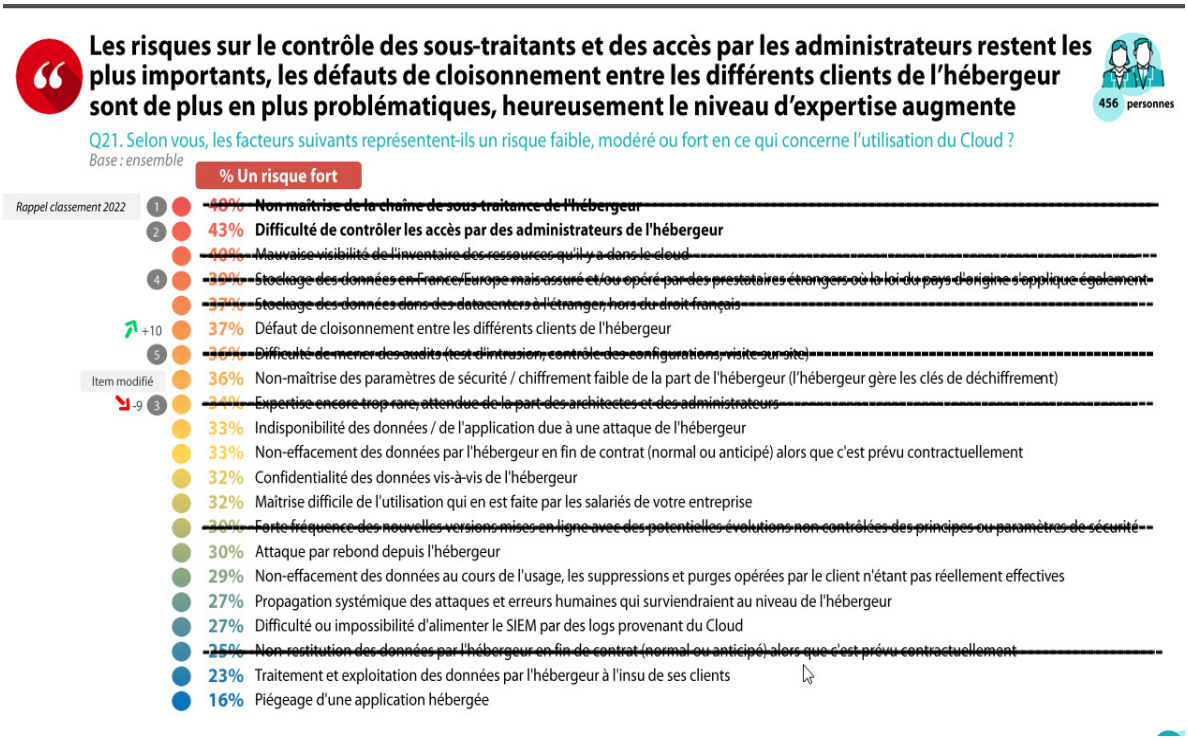
4. Actif à protéger : les logs métier liés aux activités réalisées par l'utilisateur final (le client, par exemple les actions réalisées sur les données de la base de données) ou par le fournisseur de solutions Cloud (ex : logs techniques liées aux activités d'administration, de sauvegardes...).

- **Risque en confidentialité :** récupération de données sensibles (ex : géolocalisation, données à caractère personnel, comptes...) présentes dans les logs métiers pour faciliter la conduite d'une attaque d'ampleur par un attaquant interne ou externe à l'organisation ciblée ou pour obtenir le gain de la vente illégale de ces données sur le darkweb.
- **Risque en disponibilité :** Suppression de logs métier pour anéantir tout moyen d'analyse ou d'investigation et rendre l'organisation ciblée non conforme à ses obligations légales (ex : RGPD, HDS, traçabilité des connexions...).
- **Risque en intégrité :** destruction de logs métier pour effacer des traces d'une attaque interne ou externe ou pour détériorer la qualité des logs métier et détruire ainsi leur caractère de preuve probante (ex : logs de connexion à des fins d'imputabilité des actions).

Le guide de l'ANSSI portant sur "l'état de la menace informatique" dans le contexte du Cloud Computing, publié en février 2025, complète et précise notre analyse de risques sous l'angle de menace.

En résumé, nous pouvons retenir que les environnements cloud sont devenus une cible de choix pour les cybercriminels, les groupes de menaces avancées et les acteurs malveillants. Les attaques décrites dans le guide de l'ANSSI, illustrent l'ampleur et la diversité du niveau de menace contre les infrastructures cloud. Ces attaquent révèlent les vulnérabilités critiques des infrastructures et de l'organisation qui les entoure, et illustrent les techniques sophistiquées utilisées par les attaquants pour compromettre les systèmes cloud.

En synthèse de cette première partie, nous vous proposons de revenir sur la liste des risques du CESIN pour exhiber les risques que nous retenons dans le cadre de notre problématique de détection. Ainsi, il s'agirait de couvrir, tout ou partie des risques identifiés grâce à une détection efficace.



< 3. DES RISQUES AUX RÈGLES DE DÉTECTION >

L'analyse de risque présentée permet de prioriser les actions de protection et de supervision de l'environnement Cloud. Chaque risque correspond à une action malveillante qui peut être réalisée par l'attaquant.

Le cadre de référence pour le recensement de ces actions malveillantes possibles est la matrice d'analyse MITRE ATT&CK, qui identifie les tactiques et techniques d'attaques, c'est à dire la raison d'exécution d'une action, le « pourquoi» d'une part, et les implémentations de ces attaques, le « comment » d'autre part.

Cette matrice permet de positionner les techniques d'attaques à l'intérieur de la chaine d'attaque ('Cyber Kill Chain'), telle que définie par Lockheed Martin : accès initial, exécution, persistance, escalade de privilège, évasion des défenses, vol de crédentiels, découverte de l'infrastructure, mouvement latéral, collecte de donnée, exfiltration (mise à mal de la confidentialité), et impact (mise à mal de l'intégrité et de la disponibilité).

Pour notre environnement cible, nous nous référons à la matrice MITRE > ENTERPRISE > CLOUD[1]. Elle intègre 1 matrice principale et 4 matrices secondaires pour 4 fonctions principales du Cloud : Traitement de texte/office, Fournisseur d'Identité, SaaS (Software as a Service), IaaS (Infrastructure as a Service).

Ce référentiel assure la cohérence des analyses menées, ainsi que la traçabilité dans les outils automatisés de détection et de suivi des attaques. Comme outil d'analyse manuelle, MITRE propose un environnement web qui permet de naviguer entre les tactiques (entêtes de colonnes), les techniques (entrées individuelles dans les colonnes) et les procédures : c'est le référentiel TTP.

Pour chaque technique, les procédures, mais également les contre-mesures et les stratégies de détections, sont nommées. Par exemple, pour la tactique 'exfiltration', la technique 'Transfert de données vers un stockage Cloud' liste des malwares ayant pratiqué ce type de vol de données, donne quatre familles de contre-mesures : prévention de la perte de données, filtrage du trafic réseau, configuration logicielle, et gestion des comptes utilisateurs ; ainsi qu'une famille d'approche pour la détection : 'détection cross-plate-forme de transfert de données vers des comptes Cloud'.

1. MITRE ATT&CK. (2026). Cloud Matrix. Disponible sur : https://attack.mitre.org/matrices/enterprise/cloud/

3.1 EXEMPLES D'INCIDENTS MAJEURS

Les environnements cloud sont devenus une cible de choix pour les cybercriminels, les groupes de menaces avancées et les acteurs malveillants. Les incidents majeurs, tels que ceux subis par Capital One, Tesla et Uber, illustrent l'ampleur et la diversité des attaques contre les infrastructures cloud.

Ces incidents révèlent les vulnérabilités critiques et les techniques sophistiquées utilisées par les attaquants pour compromettre les systèmes cloud. Voici un aperçu global des menaces cloud basées sur ces incidents :

1. Exploitation des Configurations Incorrectes

- Capital One (2019) : Exploitation d'un pare-feu mal configuré permettant l'accès non autorisé aux métadonnées des services cloud.
- Tesla (2018) : Utilisation de clés API exposées pour accéder aux serveurs Kubernetes et miner des cryptomonnaies.

--> TTPs : T1190, T1580

2. Phishing et Vol d'Identifiants

- Uber (2016) : Utilisation de clés AWS trouvées dans un référentiel GitHub public pour accéder aux infrastructures cloud.

--> TTPs : T1566, T1003

4. Utilisation de Comptes Valides et Accès Persistant

- Jenkins (2018) : Compromission de serveurs Jenkins mal configurés pour des activités de cryptojacking.

--> TTPs : T1078, T1543

6. Ransomware et Cryptojacking

- Tesla (2018) : Utilisation des ressources cloud pour miner des cryptomonnaies, exploitant des serveurs Kubernetes compromis.

--> TTPs : T1486, T1496

Au-delà de ces incidents majeurs, de nombreux rapports de CTI[2] nous permettent d'établir une cartographie MITRE Att&ck précise de la menace qui pèse sur les environnements Cloud. Pour chaque catégorie d'actifs, les parties prenantes sont identifiées, ainsi que l'impact (confidentialité, disponibilité ou intégrité), le risque associé, et la technique spécifique susceptible d'être mise en oeuvre par l'attaquant.

2. **La Cyber Threat Intelligence (CTI)** désigne la collecte et l'analyse d'informations sur les menaces informatiques (attaques, acteurs malveillants, vulnérabilités) afin d'anticiper et de prévenir les cyberattaques.

3.2 SYNTHÈSE DE L'ANALYSE DES RISQUES

Actifs	Parties-prenantes	CID	Risques	TTP MITRE ATT&CK
Comptes	Clients / Fournisseurs	Confidentialité	Usurpation d'identité	**T1078.004 :** Valid Accounts : Clouds Accounts
		Disponibilité	Blocage définitif des comptes	**T1098 :** Account Manipulation
		Intégrité	Création de comptes fantômes ou élévation de privilèges	**T1136.003 :** Create Account : Cloud Accounts
Données métiers	Clients	Confidentialité	Vol / fuite de données	**T1530 :** Data from Cloud Storage **T1537 :** Transfer Data to Cloud Account **T1567 :** Exfiltration Over Web Service **T1048 :** Exfiltration Over Alternative Protocol
		Disponibilité	Contrôle totale sur la disponibilité des données	**T1485 :** Data Destruction **T1486 :** Data Encrypted for Impact
		Intégrité	Modification silencieuse de données	**T1565 :** Data Manipulation
Configurations	Fournisseurs	Confidentialité	Identification des chemins d'attaque potentielle	**T1580 :** Cloud Infrastructure Modification silencieuse de données **T1526 :** Cloud Service Discovery **T1619 :** Cloud Storage Object Discovery **T1087.004 :** Account Discovery: Cloud Account

		Disponibilité	Neutralisation de fonction de sécurité	**T1548.005 :** Abuse Elevation Control Mecha-nism: Temporary Elevated Cloud Access **T1562.007 :** Impair Defenses: Disable or Modify Cloud Firewall **T1562.008 :** Impair Defenses: Disable or Modify Cloud Logs
		Intégrité	Abaissement du niveau des fonc-tions de sécurité	**T1548.005 :** Abuse Elevation Control Mecha-nism: Temporary Elevated Cloud Access **T1562.007 :** Impair Defenses: Disable or Modify Cloud Firewall **T1578 :** Modify Cloud Compute
Logs métiers	Clients / Fournisseurs	Confidentialité	Fuite de données	**T1654 :** Log Enu-meration
		Disponibilité	Neutralisation de l'auditabilité	**T1562.008 :** Impair Defenses: Disable or Modify Cloud Logs
		Intégrité	Effacement des traces	**TT1562.008 :** Impair Defenses: Disable or Modify Cloud Logs

A noter : pour l'altération de l'intégrité de données clients par modification silencieuse de données, la technique associée, T1558, est définie dans la matrice MITRE ATT&CK Enterprise, et n'est pas spécifique aux environnements Cloud.

< 4. COUVERTURE DES RÈGLES DE DÉTECTION >

4.1 STRATÉGIE

La couverture des risques cloud identifiés repose sur une combinaison de mesures préventives et d'outils de surveillance.

En pratique, les organisations doivent durcir leurs configurations cloud et déployer des solutions de détection alignées sur les techniques MITRE ATT&CK identifiées dans la partie 2. Les mesures préventives, comme l'application de configurations sécurisées et la correction des vulnérabilités connues, permettent d'éliminer en amont de nombreux chemins d'attaque. De même, l'exécution de scanners de vulnérabilités cloud (externes et internes) permet de mettre en évidence des services exposés ou des faiblesses afin de les corriger avant que des attaquants ne les exploitent.

Une fois ces bases en place, l'attention se porte sur les outils de supervision et de détection capables d'identifier les comportements menaçants en temps réel et de déclencher une réponse.

4.2 OUTILS ET PLATEFORMES DE SUPERVISION

Une variété d'outils de surveillance cloud peuvent aider à détecter et à atténuer les menaces. Voici les principales catégories d'outils permettant de couvrir les techniques MITRE ATT&CK.

1. Services de sécurité natifs des fournisseurs cloud

Les principaux fournisseurs cloud proposent des services intégrés de détection de menaces et de journalisation, faciles à activer. Par exemple, AWS GuardDuty, Microsoft Defender for Cloud et GCP Security Command Center fournissent une surveillance prête à l'emploi pour des schémas d'attaque cloud courants.

Ces services analysent l'activité cloud (appels API, journaux de flux réseau, etc.) à la recherche d'événements suspects tels que des connexions depuis des emplacements inhabituels, des élévations de privilèges, des activités malveillantes ou de l'exfiltration de données. S'appuyer sur ces outils natifs permet aux équipes d'augmenter rapidement le niveau de sécurité de leur environnement avec un effort de déploiement minimal.

Ils couvrent de nombreux TTP connus, spécifiques à chaque plateforme cloud (par exemple, AWS GuardDuty peut détecter des comportements anormaux sur des instances EC2). Pour un déploiement mono-cloud ou au début d'un parcours cloud, ces outils natifs constituent un gain rapide pour une couverture basique des menaces.

2. Le Security Information and Event Management (SIEM)

Un SIEM joue un rôle central en agrégeant les alertes et les journaux provenant de multiples outils et en permettant la création de règles de détection personnalisées.

En pratique, un SIEM ou une plateforme XDR maîtrisant les environnements cloud peut détecter des techniques d'attaque complexes (par exemple, identifier un attaquant qui pivote d'une instance cloud compromise vers une autre) en corrélant des événements disparates.
Pour couvrir les menaces, il existe des initiatives qui fournissent des règles SIEM prêtes à l'emploi, comme :

- MITRE Cyber Analytics Repository (CAR) – base de connaissances d'analyses développées par le MITRE, fondée sur le modèle d'adversaire MITRE ATT&CK. CAR définit un modèle de données utilisé dans son pseudocode et fournit des implémentations ciblant directement certains outils (par ex. Splunk, EQL).
- SigmaHQ/sigma – principal dépôt de règles Sigma, proposant une liste en croissance continue de règles de détection.
- Rulezet-core – plateforme web open source pour partager, évaluer, améliorer et gérer des règles de détection (YARA, Sigma, Suricata, etc.).

Ces ressources peuvent être exploitées pour implémenter le modèle de menace identifié dans les parties précédentes de l'article.
Le lecteur pourra s'appuyer sur le MITRE Cyber Analytics Repository (CAR) pour décliner opérationnellement les TTP MITRE ATT&CK identifiées en partie 2 du document. Par exemple, pour le TTP T1098 : Account manipulation, le CAR propose un pseudo-code sous differ.

3. Cloud-Native Application Protection Platforms (CNAPP)

Avec la maturité croissante des outils de sécurité cloud, une tendance importante est l'unification des capacités ci-dessus au sein d'une plateforme intégrée.

L'objectif est d'offrir une couverture de sécurité holistique pour les applications cloud natives, depuis le développement (contrôles « shift-left ») [3] jusqu'à la protection en production, via une interface unifiée. De nombreux éditeurs de sécurité commercialisent désormais des solutions CNAPP qui promettent une couverture étendue des techniques MITRE ATT&CK sur les workloads et services cloud.
Par exemple, un CNAPP peut signaler qu'un conteneur vulnérable connu s'exécute sur une machine virtuelle dotée d'un rôle IAM [4] trop permissif et disposant d'un accès à un datastore sensible : une combinaison de facteurs qui, considérés ensemble, indique un risque élevé. En consolidant plusieurs fonctions au sein d'un seul outil, les CNAPP visent à supprimer les angles morts entre outils en silo et à assurer une protection cloud continue de bout en bout.

3. **Le « shift-left control »** consiste à intégrer les contrôles de sécurité et de conformité dès les premières phases du développement logiciel plutôt qu'à la fin.
4. **L'Identity and Access Management (IAM)** désigne l'ensemble des processus et outils permettant de gérer les identités numériques et de contrôler l'accès aux ressources d'un système d'information.

Toutefois, ces plateformes peuvent être complexes à déployer et à exploiter, d'où la nécessité d'un effort de priorisation.

4.3 PRIORISATION DU DÉPLOIEMENT DES OUTILS

Face à la multitude d'outils disponibles, les organisations doivent prioriser les solutions à déployer en premier. Une approche utile consiste à évaluer les outils selon deux axes :

- Étendue de la couverture des TTP MITRE ATT&CK que fournit l'outil (nombre de techniques ou de scénarios de menace qu'il permet de détecter ou de mitiger) ;
- Complexité ou effort de déploiement nécessaires pour mettre l'outil en production.

En positionnant les outils sur une matrice Couverture vs Complexité, on peut identifier les gains à fort impact et éviter les projets très coûteux à faible valeur.

1. Commencer petit

Les fonctionnalités de sécurité natives des fournisseurs cloud permettent de démarrer avec des outils offrant une large couverture pour un effort relativement faible (forte couverture, faible complexité).

2. Tirer parti des outils existants

Ensuite, il convient d'examiner les outils déjà en place et de voir comment les étendre. Si votre organisation dispose déjà d'un SIEM ou d'une solution de sécurité des terminaux (EDR), intégrer les journaux cloud dans le SIEM ou déployer des agents EDR sur les hôtes cloud peut améliorer significativement la visibilité sur les menaces sans acquérir une nouvelle plateforme complète. Cela s'inscrit dans une zone de couverture modérée pour une complexité modérée, en tirant parti des outils existants (effort incrémental réduit) tout en améliorant la détection de nombreuses tactiques (Persistance, Mouvement latéral, etc., via la corrélation de journaux et la télémétrie endpoint).

3. Etudier l'opportunité d'un CNAPP

Les solutions avancées, comme le déploiement complet d'un CNAPP, se situent dans le quadrant forte couverture mais forte complexité. Elles peuvent traiter un large éventail de techniques d'attaque à travers la pile cloud (des risques de supply chain aux menaces runtime), mais nécessitent des investissements importants en matière de déploiement, d'intégration et de formation des équipes. L'adoption d'un CNAPP est souvent un choix stratégique pour les organisations disposant d'opérations cloud matures ou de contextes multi-cloud, où la couverture unifiée l'emporte sur la complexité. En d'autres termes, si votre empreinte cloud est vaste et diversifiée (nombreux services, comptes, voire plusieurs fournisseurs), la couverture globale d'un CNAPP peut s'avérer pertinente. Il faut cependant être prêt à mobiliser des ressources pour gérer la plateforme et adapter les processus (gouvernance, workflows de réponse à incident) autour d'elle.

< 5. CONCLUSION >

Le travail collégial qui a été réalisé a montré la complexité du sujet tant en termes de périmètre à couvrir que de technologies et de compétences à maîtriser. La détection suppose la collecte et l'analyse d'évènements aux sources plurielles et à un niveau de détail pertinent. Cela induit une étude approfondie des journaux d'événements à mettre en place, leur niveau de verbosité et leur durée de rétention.

Le fait de se focaliser sur les risques les plus évidents permet d'assurer le minimum de détection possible sans toutefois garantir la totale étanchéité des données dans le Cloud et la détection de toute attaque.

Le présent guide offre des pistes de réflexion sur les événements à recueillir, les techniques d'attaque fréquemment surveillées et sur les technologies à mettre en place.

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX

CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT
DANS LE CADRE DU PROGRAMME D'INVESTISSEMENTS D'AVENIR