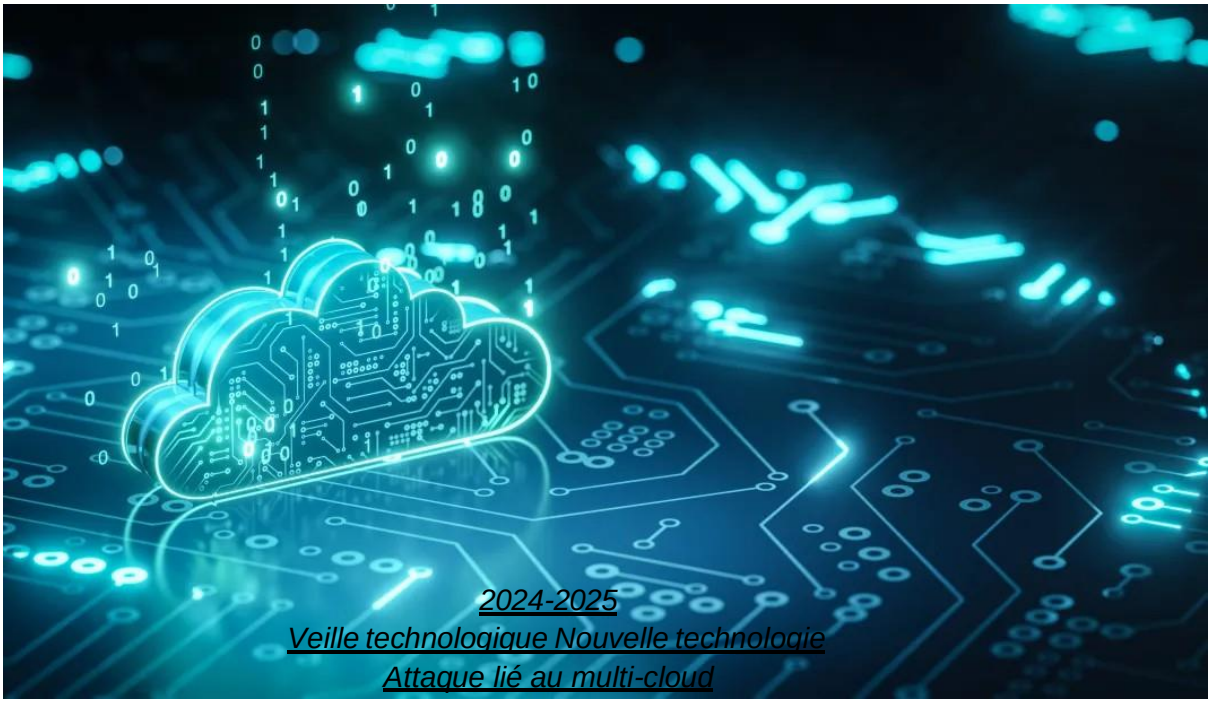
Lucas leclerc vigneron

Journal de bord - La cybersécurité des réseaux dans un environnement multi-cloud



2024-2025

Veille technologique Nouvelle technologie

Attaque lié au multi-cloud

SAINT-ASPAIS MELUN

DATE	Source	Développement
07/01/2025	Owasp	Recherche du sujet
14/01/2025	Youtube	Découverte et choix du sujet via la vidéo "Stratégie de cybersécurité dans un monde multi-cloud : mission impossible ?"
22/01/2025	Youtube	Exploration du concept multi-cloud et ses implications pour les organisations via la vidéo "Le MULTI-CLOUD, pour quoi faire ?"
29/01/2025	Wikipedia	Recherche sur la complexité des systèmes et la gestion des identités dans un environnement multi-cloud
04/02/2025	YouTube/IA	Étude des vulnérabilités spécifiques (attaques DDOS) et aspects de conformité/création onglet portfolio
11/02/2025	OWASP/CISA	Approfondissement des attaque lié au multi-cloud/réorganisation document

Ressources consultées :

- Vidéos YouTube sur la stratégie multi-cloud
- Documentation sur les attaques DDOS
- Articles Wikipedia sur la complexité des systèmes
- Analyses assistées par IA (ChatGPT)

 OWASP (Open Web Application Security Project)

→ Référence en sécurité des applications et API (ex. injection SQL, attaques sur API cloud).

 SANS Institute

→ Rapports détaillés sur les menaces, guides et formations en cybersécurité.

 MITRE ATT&CK

→ Base de données sur les techniques utilisées par les cybercriminels (ex. compromission cloud).

 CISA (Cybersécurité & Infrastructure Security Agency)

→ Alertes et bonnes pratiques pour sécuriser les infrastructures multi-cloud.

</aside>

Stratégie de cybersécurité dans un monde multi-cloud : mission impossible ?

Le MULTI-CLOUD, pour quoi faire ?

Méthode de calcul de la complexité d'un algorithme | Rachid Guerraoui

Comprendre l'attaque DDOS en 4 minutes

Points clés de la recherche

Définition du Multi-Cloud Utilisation simultanée de plusieurs fournisseurs de services cloud pour la gestion des données, applications et services d'une organisation.

Principaux défis de sécurité

- **Complexité de l'infrastructure :** Gestion de différents outils et configurations de sécurité
- **Gestion des identités (IAM) :** Nécessité d'une authentification forte et centralisée
- **Surveillance :** Difficulté de détection des anomalies sur plusieurs plateformes
- **Surface d'attaque :** Multiplication des points d'entrée potentiels
- **Conformité réglementaire :** Respect des normes (RGPD, HIPAA) sur plusieurs plateformes

1. Attaques DDoS (Déni de Service Distribué)

Ces attaques visent à submerger une application, un serveur ou un réseau avec un trafic massif, rendant les services inaccessibles aux utilisateurs légitimes.

Types d’attaques DDoS en multi-cloud :

- **Attaque volumétrique** : Inondation du réseau avec des paquets malveillants (ex. UDP flood, ICMP flood).
- **Attaque de protocole** : Exploitation des faiblesses dans les protocoles réseau (ex. SYN flood, Smurf attack).
- **Attaque applicative**: Ciblage des applications via des requêtes HTTP massives (ex. Slowloris, HTTP Flood).

 Contre-mesures : Solutions de protection DDoS (AWS Shield, Cloudflare, Akamai Kona).

2. Attaques de type "Man-in-the-Middle" (MitM)

Ces attaques permettent à un acteur malveillant d'intercepter et d'altérer la communication entre deux entités.

Exemples de MitM en multi-cloud :

- **Interception de trafic entre les clouds** : Captation des données non chiffrées circulant entre les fournisseurs cloud.
- **Détournement de session (Session Hijacking)** : Exploitation des cookies de session mal protégés.
- **ARP Spoofing / DNS Spoofing** : Redirection du trafic vers un serveur malveillant.

 Contre-mesures : Chiffrement TLS, VPN, Zero Trust Network Access (ZTNA).

3. Exploitation des erreurs de configuration

La complexité du multi-cloud entraîne souvent des erreurs de configuration qui sont une cible privilégiée des attaquants.

Vulnérabilités courantes :

- **Ports ouverts** sur des serveurs mal configurés (ex. MongoDB exposé publiquement).
- **Permissions excessives** sur les identités IAM, facilitant les escalades de privilèges.
- **Stockage non sécurisé** (ex. S3 buckets publics, bases de données non protégées).

 Contre-mesures : Audit de configurations (CSPM), principes du moindre privilège, segmentation des accès.

4. Attaques sur les API Cloud

Les **API mal sécurisées** sont une porte d'entrée pour les attaquants.

Exemples d'attaques sur API multi-cloud :

- **Injection SQL/XSS** via des API vulnérables.
- **Attaques par force brute** sur des endpoints d'authentification.
- **Exfiltration de données** via des appels API non surveillés.

 Contre-mesures : WAF (Web Application Firewall), authentification forte (OAuth 2.0, JWT), surveillance des logs API

5. Ransomware et compromission des données

Les attaques par **ransomware** exploitent souvent les environnements multi-cloud pour se propager rapidement.

Techniques utilisées :

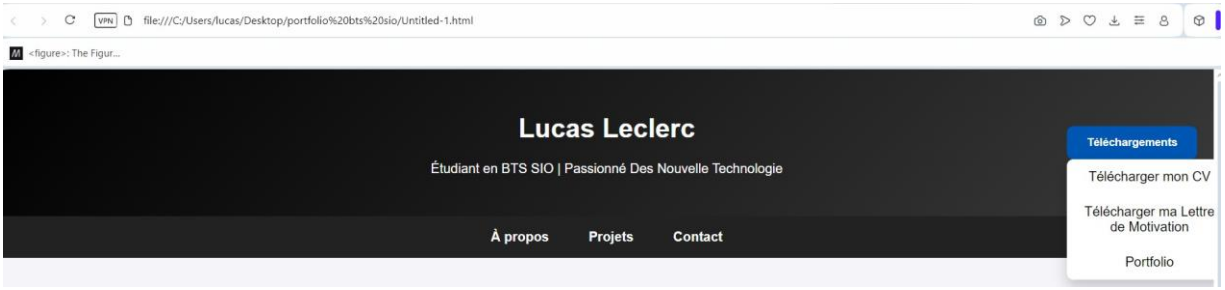
- **Phishing ciblé** (compromission des comptes admin cloud).
- **Exploitation de vulnérabilités** pour chiffrer les fichiers cloud.
- **Double extorsion** : vol + chiffrement des données.

 Contre-mesures : Backups immuables, détection des accès anormaux, solutions EDR/XDR.

ONGLET PORTFOLIO

→ Après la création de mon portfolio j'ai créé un onglet afin d'avoir accès à ma veille technologique préalablement fait dans se PDF

voila le screen ci-dessous :



Point important

1. **Complexité & visibilité** — Les environnements multi-cloud créent des « blind spots » : ressources éphémères et configurations disparates rendent la visibilité difficile et augmentent le risque d'erreurs menant à des compromissions. La majorité des incidents cloud viennent de **mauvaises configurations**. (CSPM = pratique clé). wiz.io+1

2. **Gestion des identités (IAM)** — Les identités et permissions mal gérées (permissions excessives, comptes admin non protégés) sont un vecteur majeur d'attaque dans le cloud ; centraliser l'IAM et appliquer le principe du **moindre privilège** sont essentiels. attack.mitre.org

3. **Risques liés aux API** — Les API mal protégées (authentification faible, injections, manque de validation) exposent les services cloud ; OWASP détaille les risques et bonnes pratiques pour sécuriser les API. OWASP

4. **DDoS & résilience réseau** — Le multi-cloud n'empêche pas les attaques volumétriques ; il faut des protections dédiées (AWS Shield, Cloudflare, Google Cloud Armor, Akamai…) et une architecture résiliente pour absorber/mitiger les pics malveillants. blog.ogwilliam.com+1

5. **Surveillance & tactiques adversaires** — Utiliser des référentiels tactiques (MITRE ATT&CK Cloud) pour mapper les techniques adverses et prioriser la détection et la réponse. attack.mitre.org

Sources clés (onglet veille)

- OWASP — API Security / Top 10 (risques & mitigations). OWASP+1
- CISA — Cloud security technical reference & directives (conseils de gouvernance). cisa.gov
- MITRE ATT&CK — Cloud matrix (tactiques et techniques pour la détection). attack.mitre.org
- Microsoft / Docs — CSPM et Defender for Cloud (importance de la posture et visibilité multi-cloud). Microsoft Learn
- Comparatifs & guides DDoS — Cloudflare, AWS Shield, GCP Armor (choix de protection DDoS). blog.ogwilliam.com+1

Synthèse — La cybersécurité des réseaux dans un environnement multicloud

(pour le portfolio de Lucas Leclerc — journal de bord résumé et enrichi)

Résumé rapide

Le **multi-cloud** consiste à exploiter simultanément plusieurs fournisseurs de cloud (AWS, Azure, GCP, etc.) pour héberger données, applications et services. Cette stratégie apporte résilience et flexibilité, mais multiplie les points d'exposition, la complexité opérationnelle et le risque d'erreurs de configuration