

La Sécurité et le Cloud Computing

SL par Stéphane LARCHER



Les Fondamentaux de la Sécurité Cloud

La Triade CIA (Confidentialité, Intégrité, Disponibilité)



Le Modèle de Responsabilité Partagée

Dans le Cloud, la sécurité est une responsabilité partagée entre le fournisseur et le client :

Responsabilité du fournisseur

Sécurité **DE** l'infrastructure Cloud

- Infrastructure physique
- Réseau
- Hyperviseurs
- Systèmes d'exploitation hôtes

Responsabilité du client

Sécurité **DANS** le Cloud

- Données
- Applications
- Systèmes d'exploitation invités
- Configuration des services

Cette répartition varie selon le modèle de service (IaaS, PaaS, SaaS).

Questions Critiques à se Poser

Avant d'adopter le Cloud, il est essentiel de considérer :



La cybercriminalité

Le Cloud est-il la meilleure réponse pour s'en protéger ?



La responsabilité

Comment établir clairement les responsabilités en cas d'incident ?



Les spécificités de sécurité

- Utilisateurs extérieurs avec accès privilégiés
- Absence de visibilité sur la topologie de l'infrastructure
- Localisation exacte des données inconnue
- Responsabilité partagée avec le prestataire

Les Risques Cachés du Cloud

Risques de Confidentialité

Transfert de données sensibles :

- Emails professionnels et personnels
- Comptes bancaires
- Données d'entreprise confidentielles
- Contacts et informations clients

Problématiques :

- Perte de contrôle sur les données
- Exposition potentielle à des tiers
- Conformité réglementaire (RGPD, etc.)

Risques de Disponibilité et d'Accès

Risques de Disponibilité

Fiabilité du fournisseur :

- Coupures d'accès imprévues
- Arrêt des applications chez le fournisseur
- Dépendance totale au prestataire

Questions à se poser : Le fournisseur est-il plus fiable que notre propre infrastructure ?

Risques d'Accès

Verrouillage de compte :

- Perte d'accès aux données
- Blocage des services critiques
- Dépendance aux politiques du fournisseur

Risques de Vol ou d'Altération

Points d'attention :

- 1 Localisation géographique des données
Les données peuvent être stockées dans différentes juridictions avec des lois variables sur la protection et l'accès.
- 2 Cloisonnement dans les environnements hybrides
Risques liés à l'interconnexion entre infrastructures cloud et on-premise.
- 3 Sécurisation de l'infrastructure de virtualisation
Vulnérabilités potentielles dans les couches d'hyperviseur et de virtualisation.
- 4 Utilisation excessive de services non approuvés (Shadow IT)
Risques liés à l'utilisation de services cloud non contrôlés par la DSI.



Menaces et Vulnérabilités Spécifiques

Définitions Clés

Menace (Threat) :

- Événement ou acteur potentiel pouvant causer un dommage
- Exemples : cyberattaques, pannes, erreurs humaines

Vulnérabilité (Vulnerability) :

- Faiblesse exploitable par une menace
- Exemples : mauvaise configuration, absence de chiffrement

Catégories de Menaces



Vulnérabilités du prestataire

Failles dans la stratégie de sécurité du fournisseur



Attaques inter-clients

Exploitation des faiblesses de l'isolation multi-tenant



Problèmes de disponibilité

Pannes, maintenance, incidents



Problèmes réglementaires

Non-conformité, changements législatifs



Responsabilité

Ambiguïté dans la répartition des responsabilités

Risques Organisationnels

Verrouillage des Données (Vendor Lock-in)

Définition : Dépendance excessive envers un fournisseur unique

Problématiques :

- Difficulté de changer de fournisseur
- Dans le SaaS, intégration des données dans des schémas propriétaires
- Migration complexe et coûteuse

Perte de Gouvernance

Enjeux contractuels :

- Éviter la sous-traitance non contrôlée
- Ne pas privilégier les performances au détriment de la sécurité
- Maintenir le contrôle sur les décisions critiques

Conformité et Certifications

Défis :

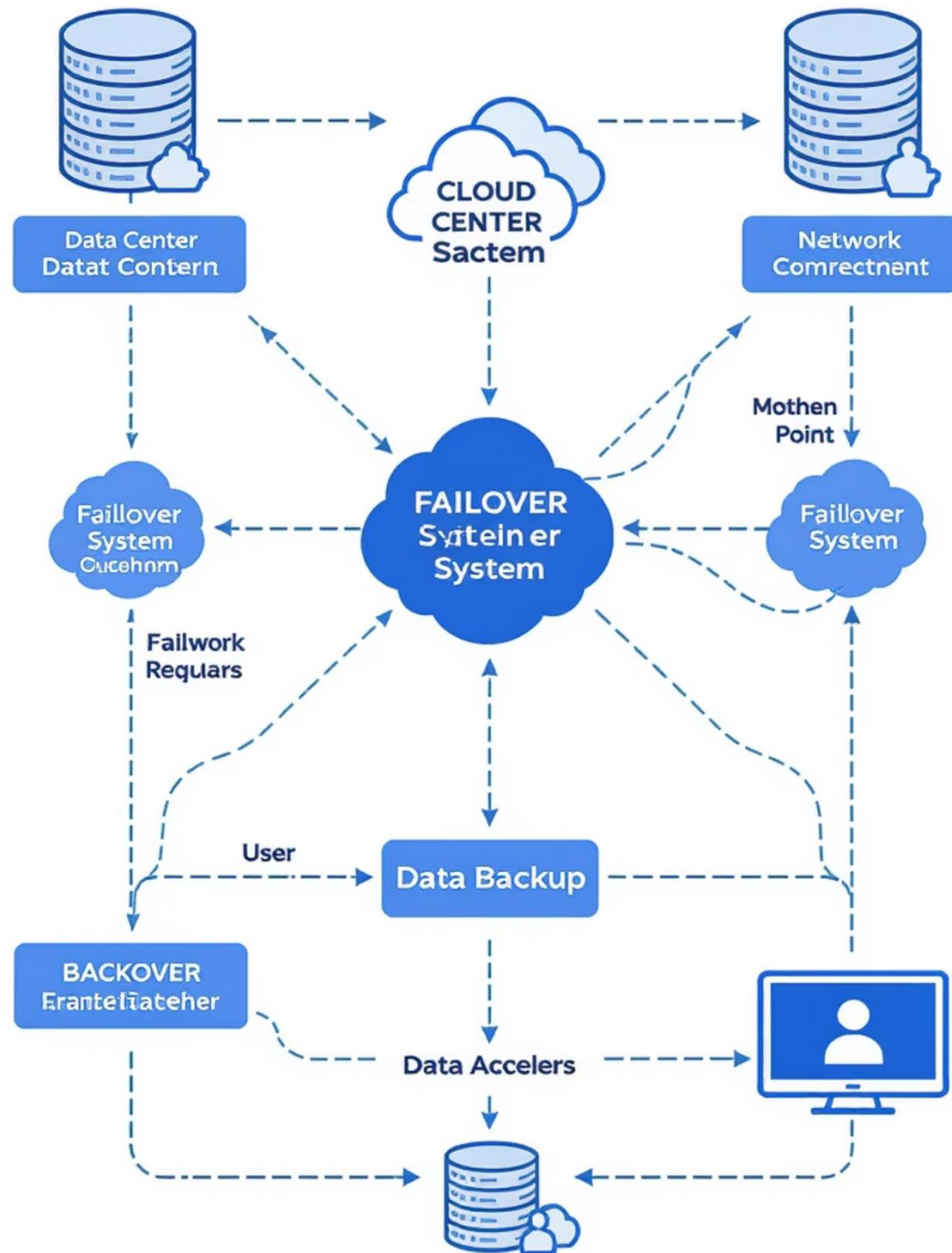
- 1 Maintien des normes de l'entreprise certifiée
Assurer que les services cloud respectent les mêmes standards que l'infrastructure interne.
- 2 Exemple : Hébergement de Données de Santé (HDS)
Conformité aux exigences spécifiques pour les données médicales sensibles.
- 3 Audit continu des pratiques du fournisseur
Vérification régulière que le prestataire maintient ses engagements de conformité.

Risques de Réputation

Causes potentielles :

- Défaillance du prestataire
- Non-conformité découverte
- Impact sur l'image de l'entreprise

Business Continuity



Continuité d'Activité

Scénarios critiques :

- 1 — Arrêt ou défaut de service du prestataire
Interruption soudaine des services cloud critiques pour l'entreprise.
- 2 — Acquisition du prestataire par une autre société
Changement de propriétaire pouvant entraîner des modifications de services ou de conditions.
- 3 — Changement de politique commerciale
Évolution des tarifs, des niveaux de service ou des conditions d'utilisation.

Ces scénarios nécessitent des plans de continuité d'activité robustes et des stratégies de sortie clairement définies.

Risques Techniques

Sur-Allocation des Ressources

Définition : Attribution excessive de ressources virtuelles par rapport aux ressources physiques

Conséquences :

- Choix incorrect du fournisseur
- Mauvaise gestion des services et de leur disponibilité
- Défauts de délivrance de services (performance dégradée)
- Compromission du système d'accès
- Pertes financières (violation de SLA, défauts en cascade)

Resource Allocation Monitor



Bonnes Pratiques pour la Sur-Allocation

Bonnes pratiques :



Attention aux ressources allouées par contrat

Vérifier les garanties de ressources dans les SLA et les conditions de service.



Capacity planning rigoureux

Anticiper les besoins en ressources et planifier les évolutions de capacité.



Monitoring continu des performances

Surveiller en temps réel l'utilisation des ressources et les performances des services.

Défaut d'Isolation

Problématique : Partage des ressources entre différents clients

Risques :

- Fuite d'informations entre tenants
- Attaques par canaux auxiliaires
- Propagation de vulnérabilités

Autres Risques Techniques

- **Malveillance du fournisseur** : Accès non autorisé aux données
- **Compromission de l'interface de gestion** : Point unique de défaillance
- **Interception des données en transit** : Man-in-the-middle





Risques Techniques Supplémentaires

1 Suppression des données non certifiées

Perte irréversible de données sans confirmation de suppression sécurisée.

2 Gestion des clés de chiffrement

Risque de perte des clés entraînant l'impossibilité d'accéder aux données chiffrées.

3 Perte de contrôle physique

Accès aux datacenters par des personnes non autorisées, compromettant la sécurité physique.

Déni de Service (DoS)

DDoS (Distributed Denial of Service)

Définition : Attaque visant à rendre un service indisponible par saturation

Spécificités Cloud :

- Élasticité peut amplifier l'impact
- Coûts associés à la consommation de ressources

EDoS (Economic Denial of Service)

Définition : Attaque visant à générer des coûts excessifs

Mécanisme :

- Exploitation de la facturation à l'usage
- Consommation massive de ressources
- Factures astronomiques



Autres Formes de DoS

1 Utilisation de sondes malveillantes

Scans intensifs des infrastructures cloud pour identifier les vulnérabilités, pouvant entraîner une dégradation des performances.

2 Conflits client-fournisseur

Blocage de service suite à des désaccords contractuels ou des litiges entre le client et le fournisseur cloud.

3 Perte de contrôle physique

Accès non autorisé aux infrastructures physiques pouvant entraîner des interruptions de service délibérées.

Risques Réglementaires

Changement de Juridiction

Problématiques :

- Données hébergées dans différents pays
- Application de lois contradictoires
- Souveraineté des données

Risques liés aux Licences

Enjeux :

- Conformité des licences logicielles
- Audit de licences dans le Cloud
- Modèles de licensing adaptés

Protection des Données

Cadres réglementaires :

- RGPD (Règlement Général sur la Protection des Données)
- CCPA (California Consumer Privacy Act)
- Lois sectorielles (santé, finance)

Risques Réseau

Coupures de réseau :

- Perte de connectivité
- Isolation des services

Gestion du réseau :

- Congestion
- Défaut de connexion
- Utilisation non optimale
- Modification du trafic

Risques Humains

Ingénierie sociale :

- Phishing ciblé
- Usurpation d'identité
- Manipulation psychologique

Risques sur les Données

Journaux et logs :

- Perte ou compromission des journaux opérationnels
- Manipulation des preuves
- Absence de traçabilité

Risques Physiques

Accès non autorisés :

- Intrusion dans les datacenters
- Vol d'équipement informatique

Sauvegardes :

- Media perdus ou volés
- Corruption des sauvegardes
- Restauration impossible

Sinistres naturels :

- Inondations
- Tremblements de terre
- Incendies

Matrice de Risques Cloud

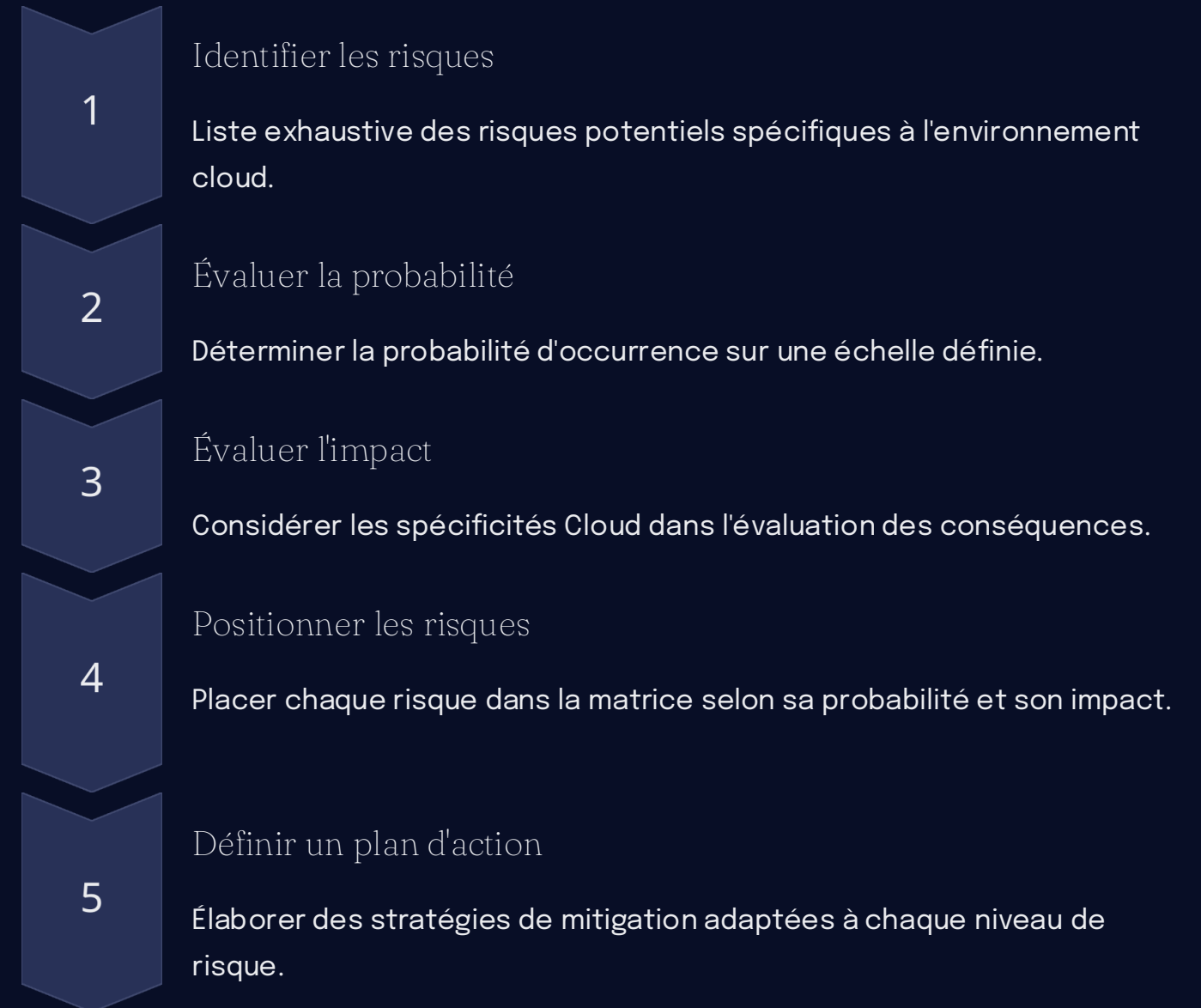
Concept de Matrice de Risques

Définition : Outil visuel permettant d'évaluer et prioriser les risques selon leur probabilité et leur impact

Axes :

- **Probabilité** : Likelihood d'occurrence
- **Impact** : Gravité des conséquences

Méthodologie d'Évaluation



Exemples de Menaces Cloud



Fuite de données

Buckets S3 mal configurés exposant des données sensibles publiquement.



Pannes majeures

Rupture de service régionale affectant de nombreux clients simultanément.



Erreurs de configuration

Exposition de clés d'accès dans des référentiels de code publics.



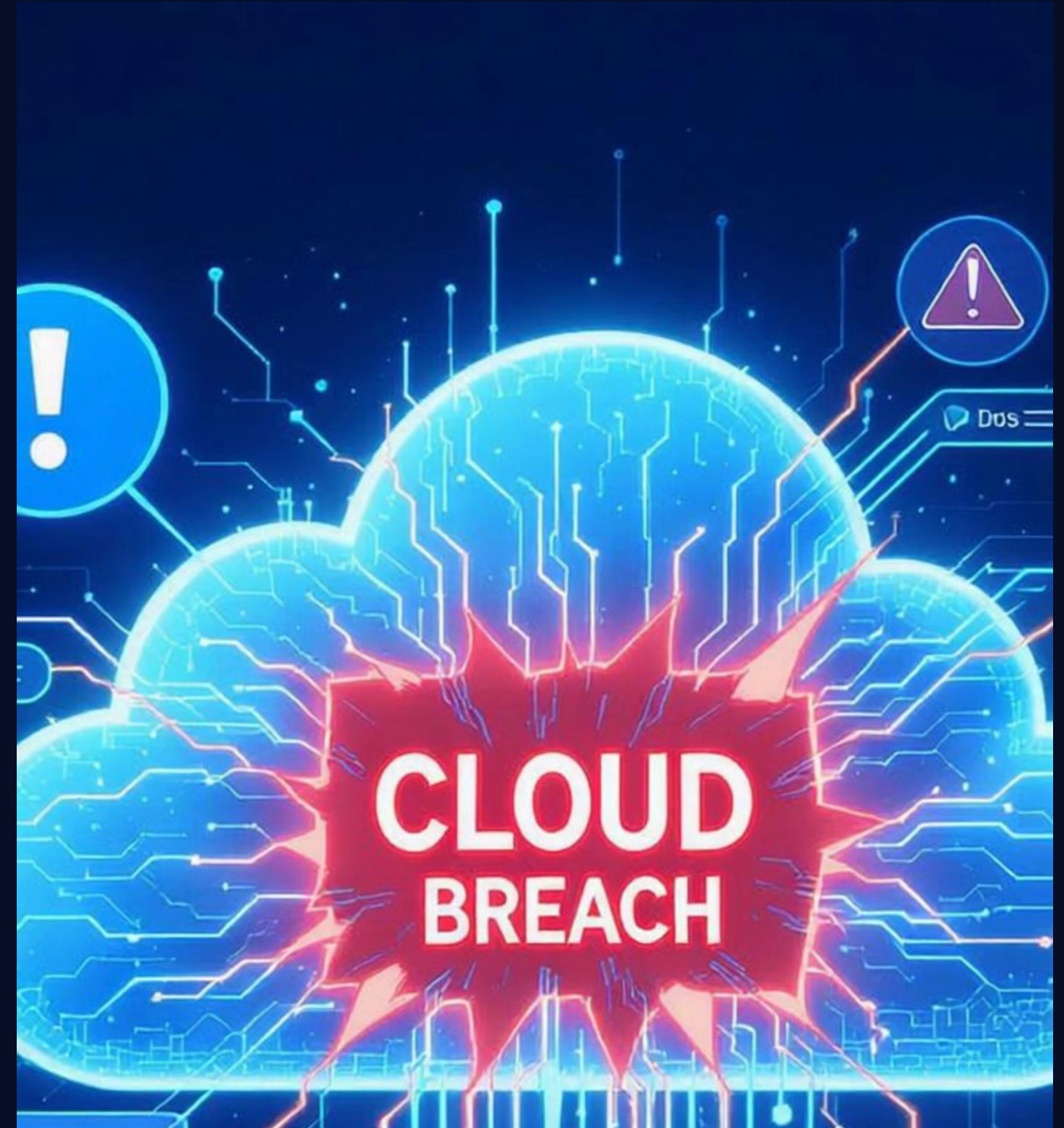
Attaques DDoS

Saturation des endpoints publics rendant les services inaccessibles.



Escalade de coûts

Factures imprévues dues à une mauvaise gestion des ressources élastiques.



Bonnes Pratiques de Sécurité Cloud

Principes Fondamentaux



La sécurité dans le Cloud est un défi complexe nécessitant une approche holistique. La réussite repose sur la compréhension des risques, la responsabilité partagée, une approche multicouche, l'amélioration continue et une culture de sécurité impliquant tous les acteurs.

Le Cloud offre des opportunités exceptionnelles, mais nécessite une vigilance constante et une gestion proactive des risques pour en tirer pleinement parti tout en maintenant un niveau de sécurité approprié.