



ARCHITECTURE CLOUD ET HYBRIDES



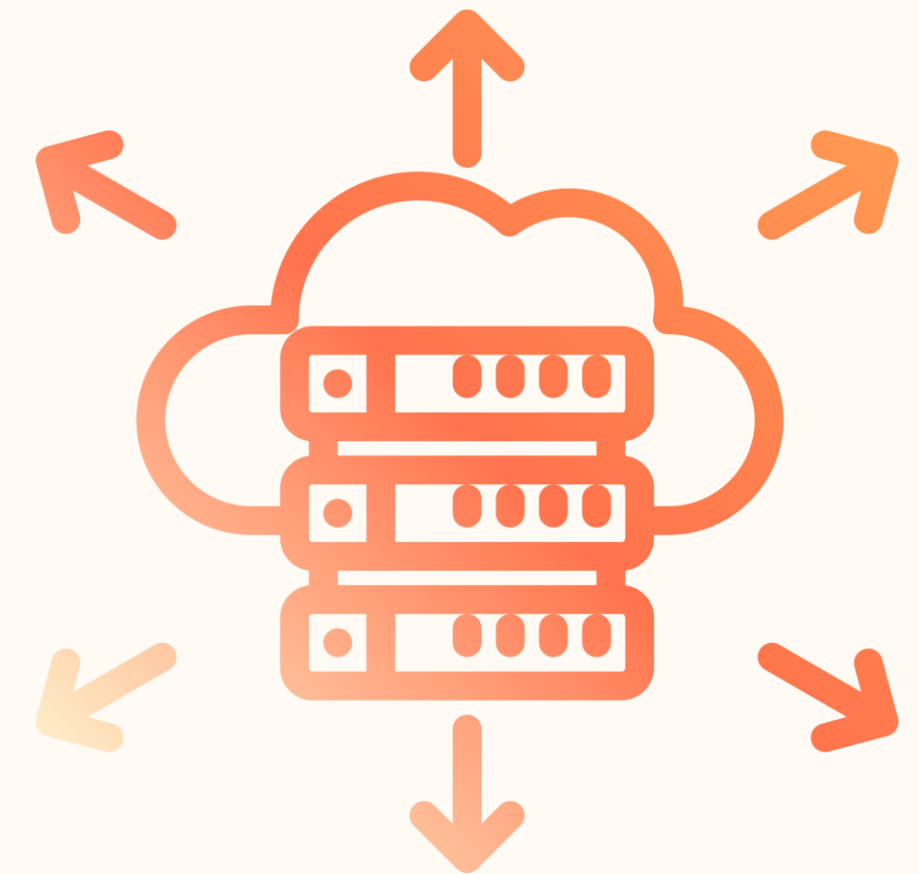
Intervenant : Nathan VIDAL FAGES

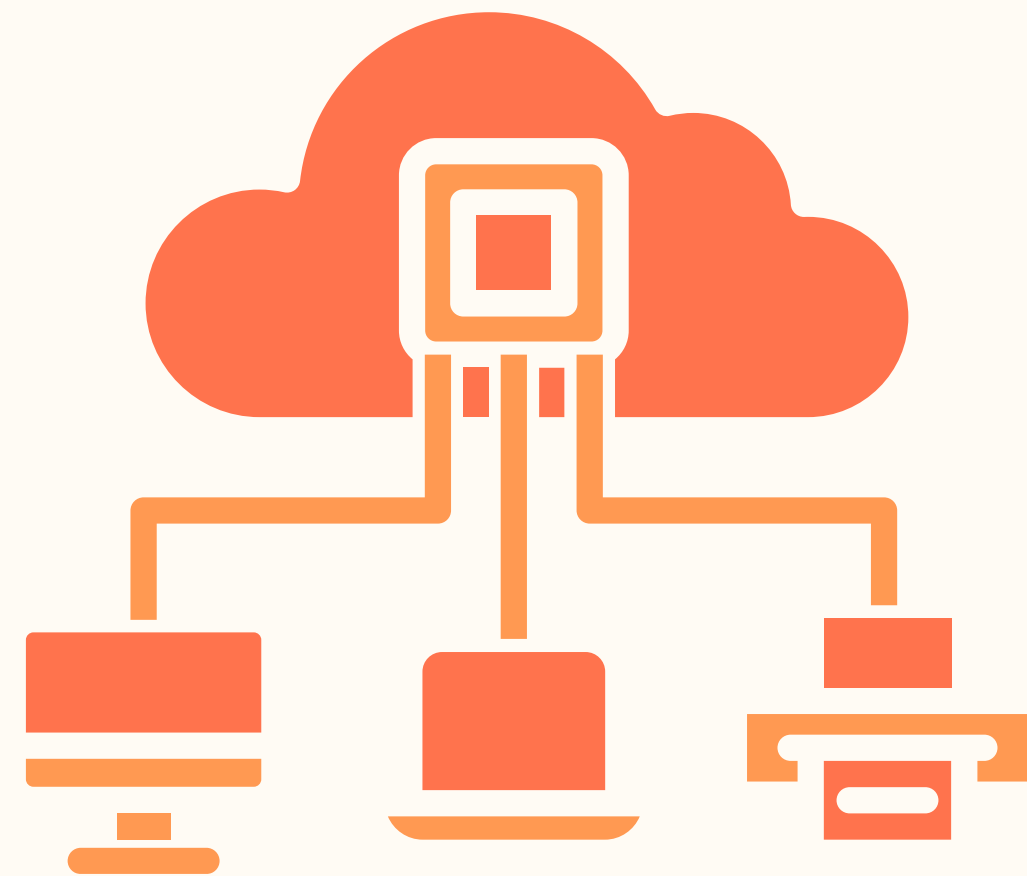




PRÉSENTATION DU MODULE

- Chapitre 1 : Introduction aux architectures Cloud et hybrides
- Chapitre 2 : Gestion des risques liés aux architectures Cloud et hybrides
- Chapitre 3 : Stratégies de protection des données en environnement Cloud
- Chapitre 4 : Stratégies de protection des applications en environnement Cloud
- Chapitre 5 : Mise en pratique à travers des études de cas





CHAPITRE 1 :

INTRODUCTION AUX

ARCHITECTURES

CLOUD ET HYBRIDES





DÉFINITION DU CLOUD COMPUTING


MODÈLES DE
SERVICES





DÉFINITION DU CLOUD COMPUTING

On-site	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

 You manage

 Service provider manages



EVERYTHING AS A SERVICE (XAAS)

MODÈLES DE SERVICES

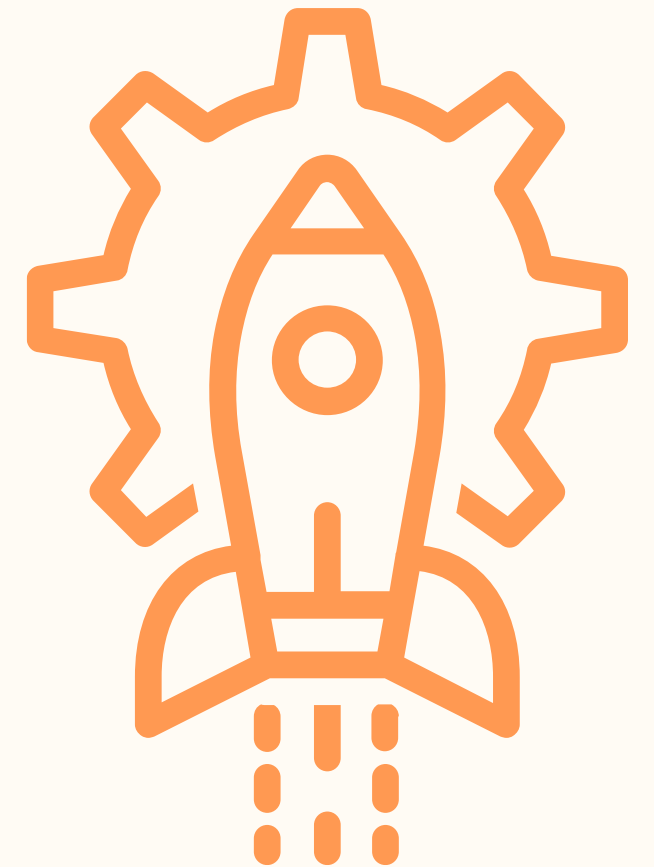
- **DESKTOP AS A SERVICE (DaaS)**
Externalisation d'une solution VDI (Virtual Desktop Infrastructure) dans le Cloud, où l'utilisateur peut accéder directement à un bureau virtuel à distance (une session sur un système d'exploitation).
- **COMMUNICATIONS AS A SERVICE (CAAS)**
Modèle qui fait référence aux services de communication basés sur Internet (téléphonie par Internet, visioconférence, etc.)
- **DATABASE AS A SERVICE (DBaaS)**
Référence à la mise à disposition d'un système de bases de données via le Cloud
- **VPN AS A SERVICE (VPNAAS)**
Lorsque le VPN est proposé sous la forme d'un service
- **RANSOMWARE AS A SERVICE (RAAS)**
Référence à un modèle utilisé par les cybercriminels qui offrent la possibilité de louer un logiciel malveillant de type ransomware et toute l'infrastructure associée.



MODÈLES DE DÉPLOIEMENT

- **CLOUD PUBLIC**
Ressources partagées, opérées par un fournisseur tiers (AWS, Azure, OVH).
- **CLOUD PRIVÉ**
Infrastructure dédiée, interne ou hébergée (VMware, OpenStack).
- **CLOUD HYBRIDE**
Combinaison des deux, permettant flexibilité et optimisation.
- **MULTICLOUD**
Utilisation de plusieurs fournisseurs pour éviter le verrouillage et augmenter la résilience.

MODÈLES DE SERVICES





CAS PRATIQUE

CARTE MENTALE AVANTAGES / DÉFIS



OBJECTIF

IDENTIFIER COLLECTIVEMENT LES AVANTAGES/DÉFIS DU CLOUD.

DÉROULÉ - GROUPES DE 5 ÉTUDIANTS

➤ SUR UNE FEUILLE / TABLEAU COLLABORATIF, DESSINER UNE CARTE AVEC DEUX BRANCHES :

AVANTAGES DU CLOUD

DÉFIS / RISQUES DU CLOUD

CHAQUE GROUPE DOIT TROUVER AU MOINS 5 AVANTAGES ET 5 DÉFIS.



**20
MIN**

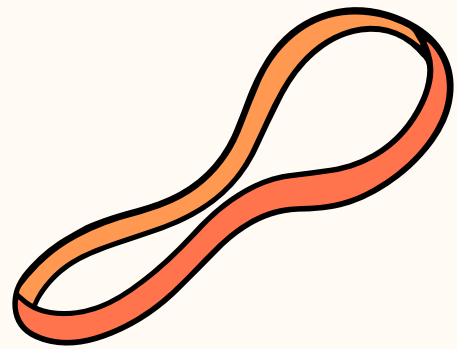
ANALYSE EN GROUPE

**CHAQUE GROUPE PARTAGE 2 AVANTAGES + 2 DÉFIS → COMPILATION EN TABLEAU
COMMUN**

AVANTAGES ET DÉFIS DU CLOUD

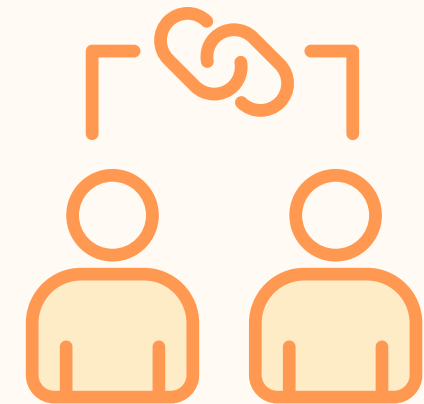
1

AVANTAGES

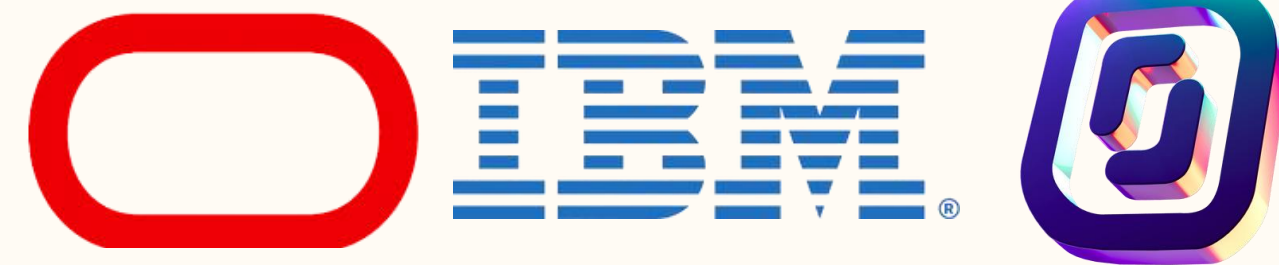
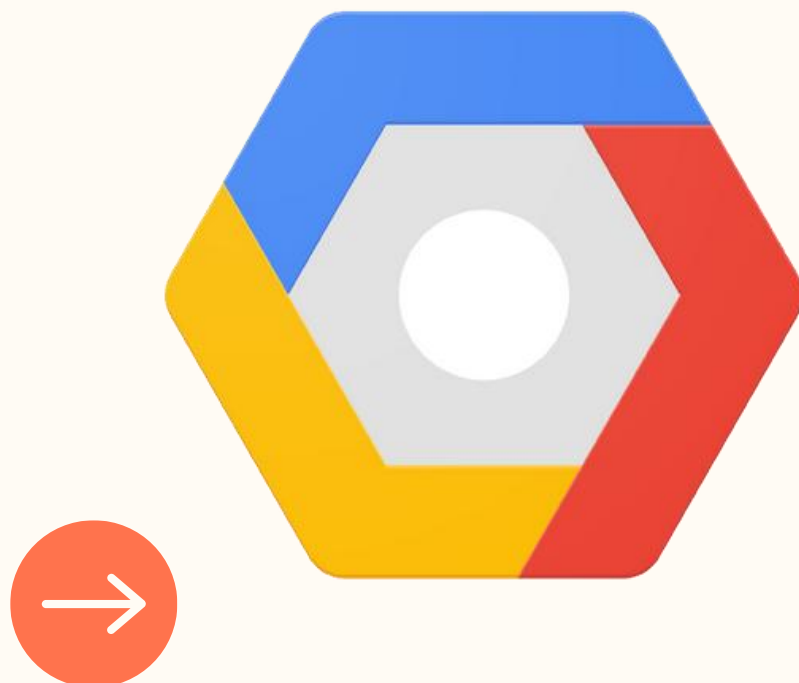


2

DÉFIS



⚡ LES GRANDS ACTEURS DU MARCHÉ





ENJEUX DE SÉCURITÉ SPÉCIFIQUES



➤ MODÈLE DE RESPONSABILITÉ PARTAGÉE

FOURNISSEUR CLOUD

CLIENT

➤ PRINCIPAUX ENJEUX

PROTECTION DES DONNÉES

GESTION DES IDENTITÉS ET DES ACCÈS

SURVEILLANCE ET DÉTECTION

PLAN DE CONTINUITÉ ET REPRISE D'ACTIVITÉ



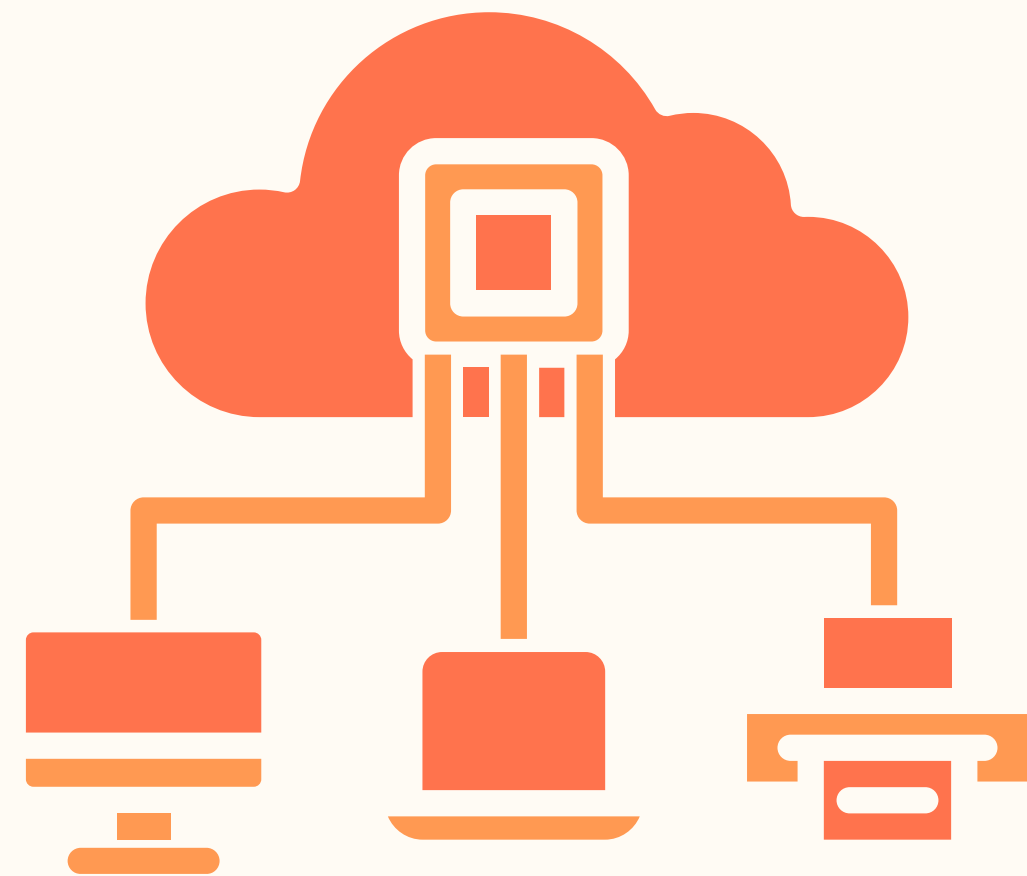
QUIZZ

VRAI / FAUX

- ✓ GOOGLE DRIVE EST UN SERVICE SAAS
- ✗ AMAZON EC2 EST UN SERVICE PAAS.
- ✓ LE CLOUD HYBRIDE COMBINE CLOUD PRIVÉ ET CLOUD PUBLIC.
- ✓ NETFLIX REPOSE SUR AWS.
- ✗ DROPBOX EST UN SERVICE IAAS.
- ✗ UN CLOUD PRIVÉ EST TOUJOURS PLUS SÉCURISÉ QU'UN CLOUD PUBLIC.
- ✗ AVEC LE CLOUD, LA SÉCURITÉ EST 100% GÉRÉE PAR LE FOURNISSEUR.
- ✓ MICROSOFT AZURE EST SURTOUT UTILISÉ POUR LES ENVIRONNEMENTS HYBRIDES.
- ✗ LE CLOUD SUPPRIME TOTALEMENT LE RISQUE DE PERTE DE DONNÉES.
- ✓ SPOTIFY EST UN EXEMPLE DE SAAS.
- ✓ LE MULTICLOUD CONSISTE À UTILISER PLUSIEURS FOURNISSEURS CLOUD POUR UN MÊME SI.
- ✗ SALESFORCE EST UN EXEMPLE DE PAAS

CONCLUSION

- LE CLOUD OFFRE DE NOMBREUX AVANTAGES MAIS NÉCESSITE UNE MAÎTRISE DES MODÈLES DE SERVICE ET DE DÉPLOIEMENT.
- LA SÉCURITÉ N'EST PAS EXTERNALISÉE : LE CLIENT CONSERVE DES RESPONSABILITÉS CLÉS.
- LA COMPRÉHENSION DE CES ENJEUX EST ESSENTIELLE AVANT D'ABORDER LA GESTION PROACTIVE DES RISQUES.



CHAPITRE 2 :

GESTION DES RISQUES LIÉS AUX ARCHITECTURES CLOUD ET HYBRIDES





1. INTRODUCTION À LA GESTION DES RISQUES (CONCEPTS CLÉS)

DÉFINITION DU
RISQUE

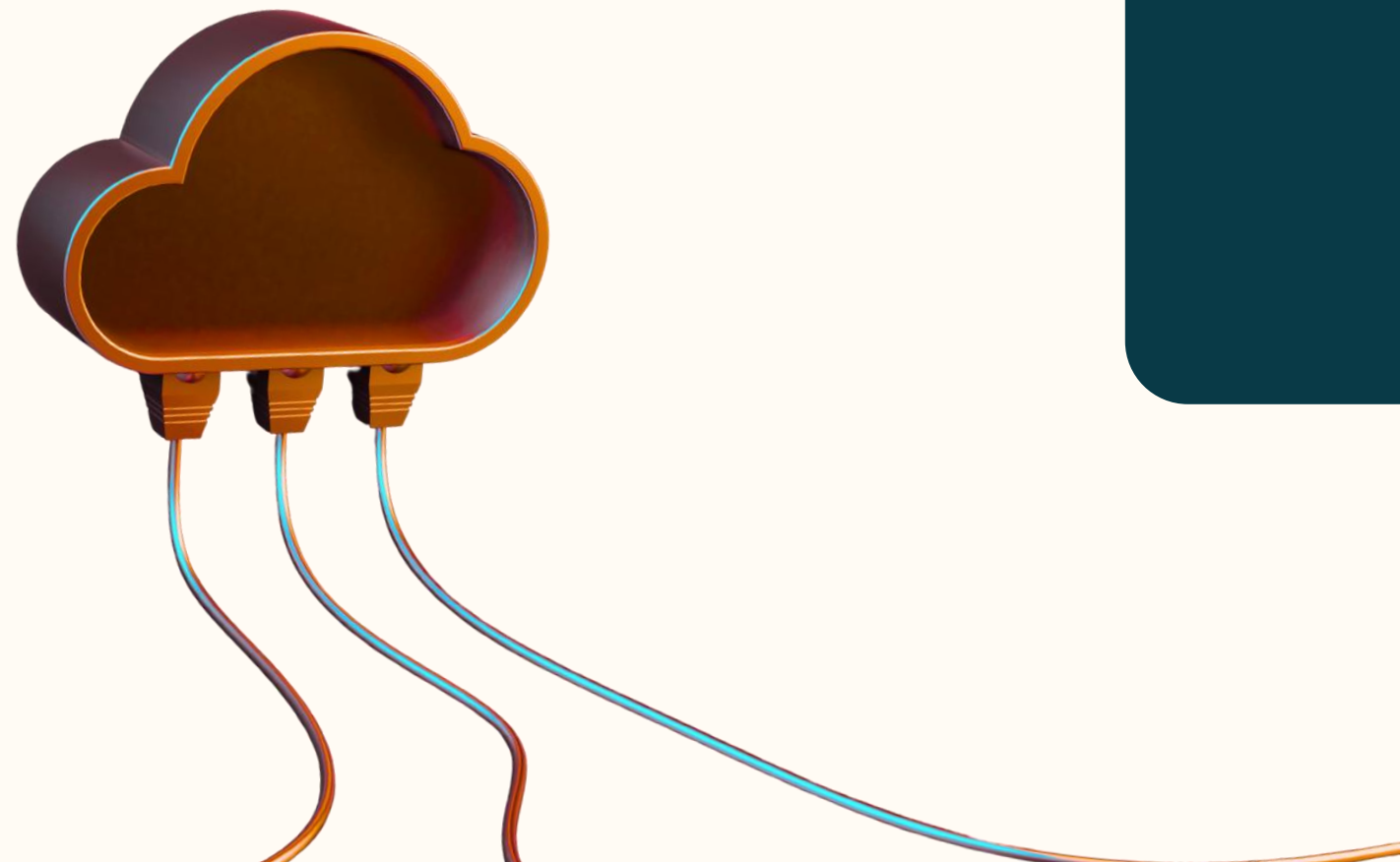
DIFFÉRENCES ENTRE
SI CLASSIQUE ET
SI CLOUD





DÉFINITION DU
RISQUE

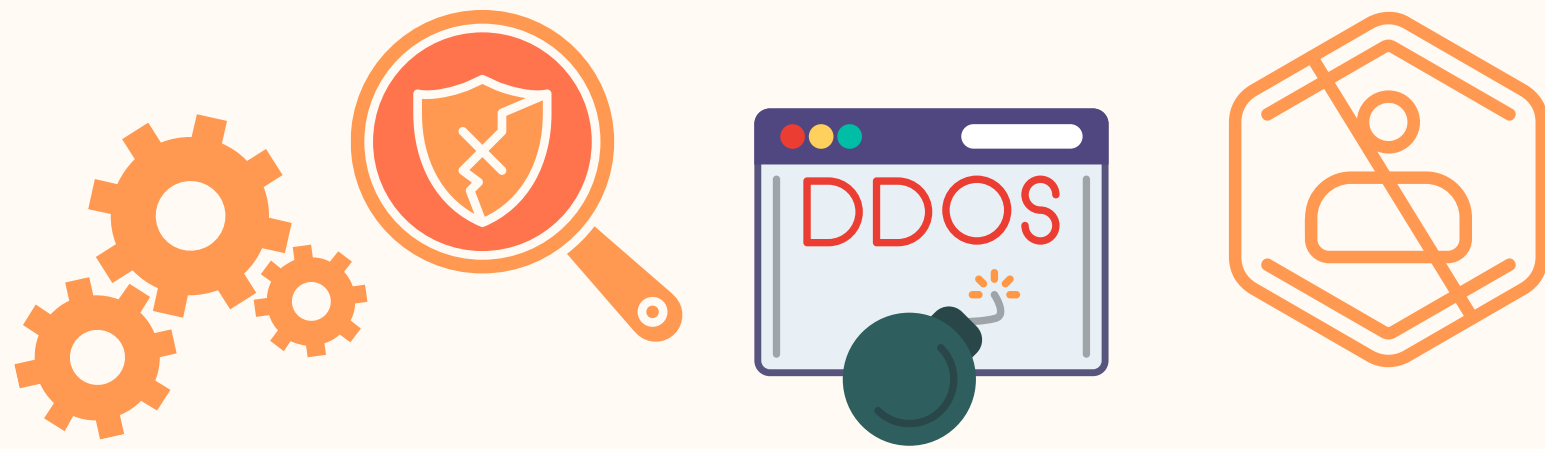
DIFFÉRENCES ENTRE
SI CLASSIQUE ET
SI CLOUD



2. TYPOLOGIE DES RISQUES SPÉCIFIQUES AU CLOUD

1

TECHNIQUES



3

CONTRACTUELS / JURIDIQUE



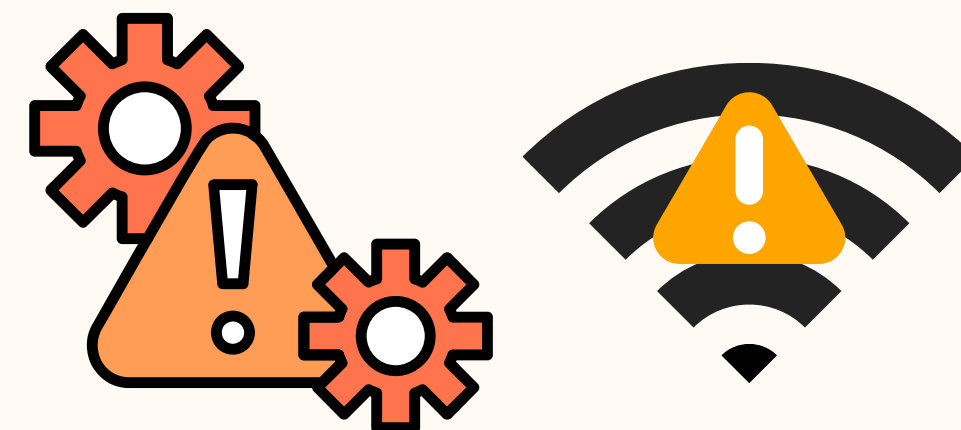
2

ORGANISATIONNEL



4

OPÉRATIONNELS



3. ÉVALUATION DE L'IMPACT DES RISQUES

MÉTHODOLOGIE SIMPLE (UTILISABLE EN COURS)

- IDENTIFIER LES RISQUES.
- DÉTERMINER LEUR PROBABILITÉ (FAIBLE, MOYENNE, FORTE).
- DÉTERMINER LEUR IMPACT (FAIBLE, MOYEN, FORT).
- COMBINER POUR OBTENIR UN NIVEAU DE CRITICITÉ.

MÉTHODES AVANCÉES

- EBIOS RISK MANAGER (ANSSI) / ISO 27005 / FAIR



EXERCICE



40 MIN

ANALYSE EN
GROUPE

MATRICE DE CRITICITÉ

OBJECTIF

- LISTE DE RISQUES : FUITE S3, PANNE AZURE RÉGIONALE, PIRATAGE COMPTE ADMIN, SHADOW IT, DDOS
- CHAQUE GROUPE DOIT PLACER CES RISQUES DANS UNE MATRICE 2×2 (PROBABILITÉ FAIBLE/FORTE × IMPACT FAIBLE/FORT).
- EXPLIQUER UN CHOIX “CRITIQUE” ET COMMENT Y RÉPONDRE.

LIVRABLE ATTENDU

- MATRICE DES RISQUES SUR FEUILLE / MAIL : esn@vidalfages.fr



◀ 4. MESURES DE PRÉVENTION ET DE DÉTECTION

PRÉVENTION



DÉTECTION

CORRECTION
ET RÉPONSE

5. GOUVERNANCE ET CONFORMITÉ

➤ RÈGLEMENTATIONS



➤ NORMES & CERTIFICATIONS





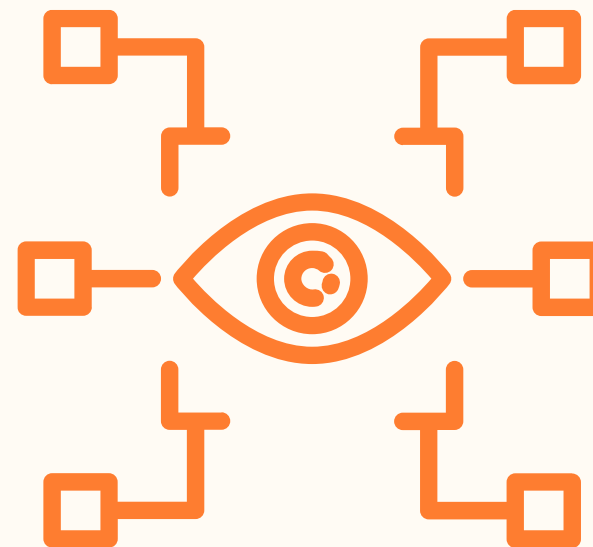
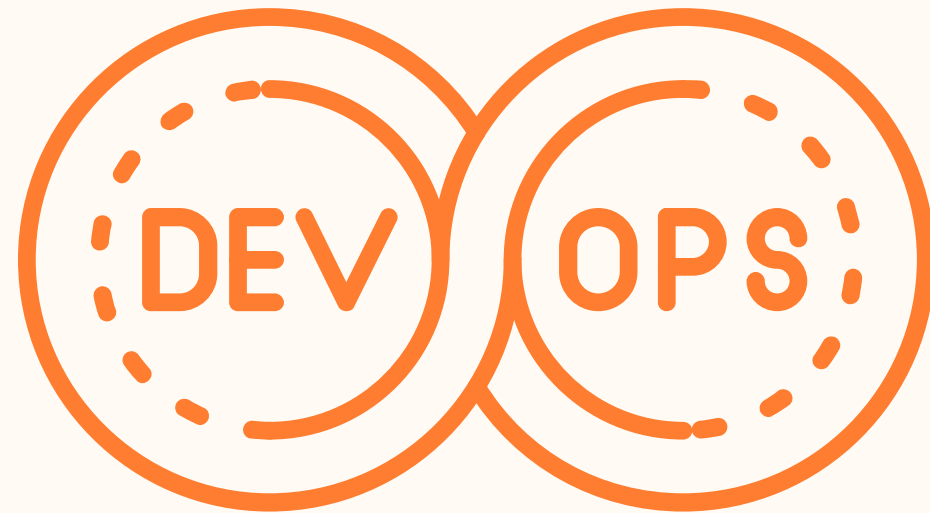
ENJEUX DE SÉCURITÉ SPÉCIFIQUES



- MODÈLE DE RESPONSABILITÉ PARTAGÉE
- PRINCIPAUX ENJEUX



6. APPROCHE PROACTIVE





45 MIN

ANALYSE EN GROUPE

CAS PRATIQUE 1



SCÉNARIO

UNE ENTREPRISE A MIGRÉ UNE PARTIE DE SON SI VERS AZURE (CRM + ERP). ELLE CONSERVE UN DATACENTER INTERNE (HYBRIDE).

➤ UN BUCKET DE STOCKAGE CONTIENT DES DONNÉES INTERNES SENSIBLES.

TRAVAIL DEMANDÉ (EN SOUS-GROUPES)

- IDENTIFIER LES RISQUES CONCRETS LIÉS À CETTE APPLICATION.
- ÉVALUER LEUR CRITICITÉ
- PROPOSER UNE MESURE DE PRÉVENTION
- PROPOSER UNE MESURE DE DÉTECTION
- DÉCRIRE UNE RÉPONSE EN CAS DE FUITE CONFIRMÉE.

RESTITUTION SUR FEUILLE / MAIL : esn@vidalfages.fr



CAS PRATIQUE 1



➤ Identification des risques concrets :

Catégories	Risques	Description
Confidentialité	Fuite de données depuis le bucket	Mauvaise configuration des permissions (accès public, clé partagée, compte compromis)
Intégrité	Altération ou suppression de données sensibles	Mauvais contrôle d'accès, absence de versioning, ransomware Cloud
Disponibilité	Indisponibilité du service CRM/ERP hébergé sur Azure	Dépendance réseau entre le site local et Azure (panne VPN, latence, erreur DNS)
Conformité / RGPD	Stockage de données personnelles hors UE ou sans clause contractuelle adaptée	Non-respect des exigences de localisation et de sous-traitance
Shadow IT / Gouvernance	Utilisation non maîtrisée de comptes Azure ou buckets personnels	Absence de gouvernance et de politique Cloud
Authentification / IAM	Compromission d'un compte administrateur Azure	MFA absent, mots de passe faibles ou partagés
Réseau hybride	Tunnel VPN ou ExpressRoute mal configuré	Fuite de trafic ou interception possible entre les environnements
Sauvegarde / Restauration	Absence de sauvegarde régulière des données du bucket	Perte définitive de données en cas de corruption ou suppression



CAS PRATIQUE 1



➤ Évaluation de la criticité :

		Impact		
		Important	Moyen	Faible
Probabilité	Important	Fuite de données sensibles (bucket)		Shadow IT
	Moyen	Compromission de compte Azure Admin	Altération de données / ransomware Absence de sauvegarde Cloud	
	Faible	Indisponibilité CRM/ERP (réseau ou panne Azure) Non-conformité RGPD		



CAS PRATIQUE 1



➤ Mesures de prévention

Risque	Mesure de prévention
Fuite de données	Chiffrement au repos (SSE-KMS) et en transit (TLS) ; configuration des ACL strictes sur le bucket (principe du moindre privilège).
Compromission de compte	Activation du MFA sur tous les comptes administrateurs ; gestion centralisée via Azure AD / Entra ID ; rotation des clés d'accès.
Indisponibilité	Mise en place d'un plan de continuité d'activité (PCA) et réplication géographique sur Azure.
Non-conformité RGPD	Vérification du lieu d'hébergement des données et des clauses contractuelles (DPA) ; documentation des traitements.
Altération / ransomware	Sauvegardes immuables (Object Lock / versioning) et contrôle d'accès basé sur rôle (RBAC) .
Shadow IT	Mise en place d'une gouvernance Cloud (Cloud Policy / Azure Blueprint) avec suivi des déploiements.
Absence de sauvegarde	Déploiement de sauvegardes automatiques (Azure Backup / Blob Snapshot) .



CAS PRATIQUE 1



➤ Mesures de détection

Objectif	Mesure de détection
Activité suspecte sur le bucket	Azure Defender for Storage / CloudTrail / Log Analytics : détection d'accès inhabituels ou IP suspectes
Compromission de comptes	Audit Azure AD et alertes sur connexions anormales
Altération de données	Activation du versioning + journalisation des accès
Fuite réseau	IDS/IPS sur la liaison VPN / ExpressRoute
Conformité	Rapports automatiques via Azure Compliance Manager / Security Center



Réponse

CAS PRATIQUE 1



Étape	Action	Objectif
Identification	Identifier la source de la fuite (compte compromis, bucket public, clé exposée) via les logs Azure	Déterminer l'origine et la portée
Blocage	Révoquer les clés / tokens, isoler le bucket ou le compte compromis	Empêcher la propagation
Restauration	Restaurer les données à partir des sauvegardes immuables	Revenir à un état sûr
Communication	Notifier les utilisateurs et la CNIL (sous 72h si RGPD concerné)	Respect de la conformité
Analyse post-incident	Réaliser un rapport d'incident (type RCA – Root Cause Analysis) et renforcer les politiques IAM / logs / sécurité réseau	Prévenir la récurrence



45 MIN

ANALYSE DE GROUPE

CAS PRATIQUE 2

“LA BASE DE DONNÉE ACCESSIBLE EN PUBLIQUE”



SCÉNARIO

UNE START-UP UTILISE UNE BASE DE DONNÉE SAAS POUR SON SITE E-COMMERCE AVEC COMME DONNÉES:

- IMAGES PRODUITS (NON SENSIBLES).
- LOGS CLIENTS (EMAILS, NUMÉROS DE CARTE PARTIELS).

TRAVAIL DEMANDÉ (EN SOUS-GROUPES)

- IDENTIFIER LES RISQUES CONCRETS LIÉS À CETTE APPLICATION.
- ÉVALUER LEUR CRITICITÉ
- PROPOSER UNE MESURE DE PRÉVENTION
- PROPOSER UNE MESURE DE DÉTECTION
- DÉCRIRE UNE RÉPONSE EN CAS DE FUITE CONFIRMÉE.

RESTITUTION SUR FEUILLE / MAIL : esn@vidalfages.fr



CAS PRATIQUE 2



➤ Identification des risques concrets :

Catégorie	Risque concret	Description
Confidentialité	Fuite ou exposition des logs clients	Mauvaise configuration du stockage SaaS (bucket public, clé API exposée, partage externe non maîtrisé)
Intégrité	Altération ou suppression des logs	Mauvaise gestion des rôles / API ou injection SQL si interface exposée
Disponibilité	Indisponibilité de la base SaaS	Panne du fournisseur, attaque DDoS ou absence de plan de secours
Conformité / RGPD	Données personnelles exposées ou mal pseudonymisées	Logs contenant emails et fragments de CB = données personnelles
Authentification / IAM	Compromission du compte administrateur SaaS	Absence de MFA, mots de passe faibles, partage de compte
API / Exposition	Exploitation d'API publiques mal sécurisées	Endpoint non protégé ou trop permissif
Sauvegarde / Rétention	Perte de logs en cas d'incident ou purge automatique non maîtrisée	Pas de sauvegarde externe ou de rétention adaptée



CAS PRATIQUE 2

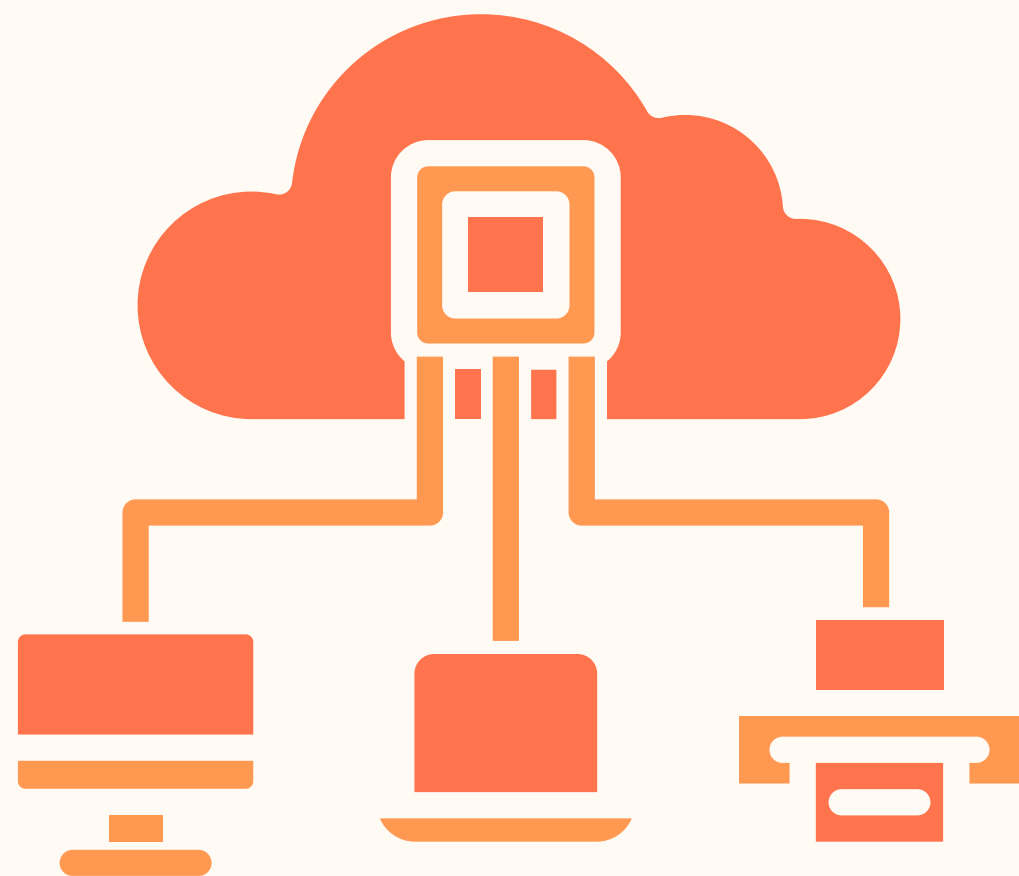
➤ Évaluation de la criticité :



		Impact		
		Important	Moyen	Faible
Probabilité	Important	Fuite des logs clients		Perte de logs
	Moyen	Compromission de compte Azure Admin - Non-conformité RGPD	Altération de données / ransomware Absence de sauvegarde Cloud	Perte ou vol d'image
	Faible	Indisponibilité du service		

CONCLUSION

- LA GESTION DES RISQUES CLOUD EST MULTIDIMENSIONNELLE (TECHNIQUE, ORGANISATIONNELLE, JURIDIQUE).
- PRÉVENTION, DÉTECTION ET CORRECTION DOIVENT ÊTRE INTÉGRÉES EN CONTINU.
- LA GOUVERNANCE ET LA CONFORMITÉ (RGPD, ISO, SECNUMCLOUD) SONT DES PILIERS INDISPENSABLES.



CHAPITRE 3 :

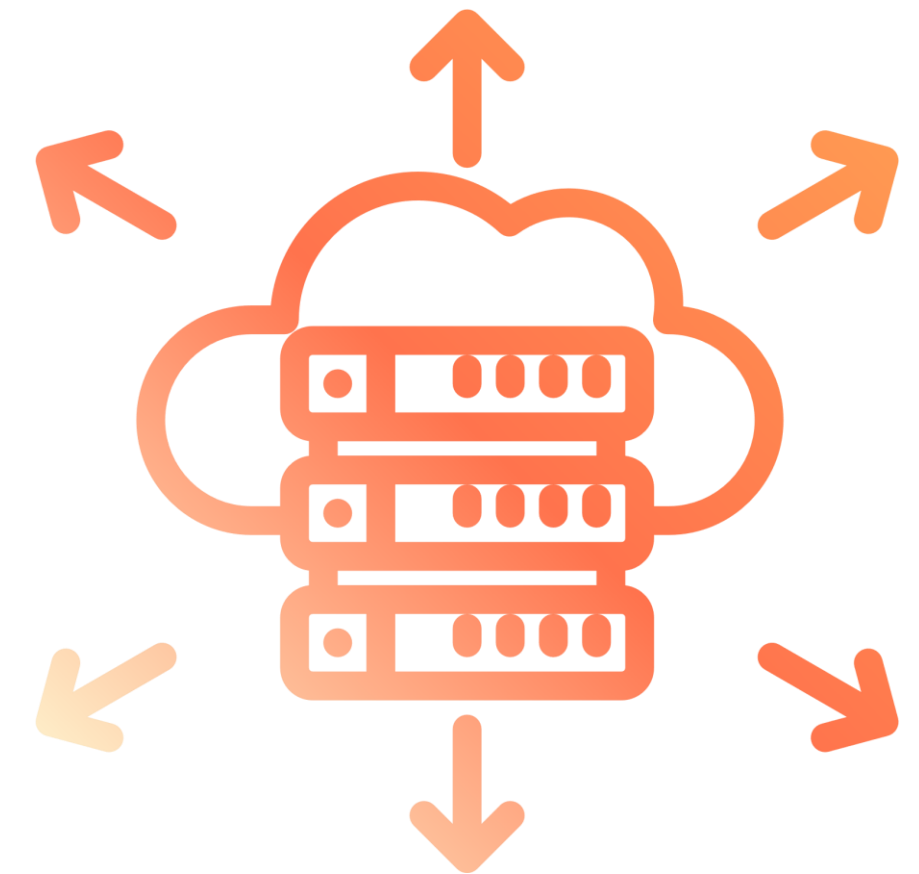
Stratégies de protection des données





Objectif

- **Confidentialité** : empêcher tout accès non autorisé (chiffrement, IAM)
- **Intégrité** : garantir que les données n'ont pas été altérées,
- **Disponibilité** : garantir l'accès aux données en cas d'incident,
- **Traçabilité** : assurer la journalisation et la détection d'anomalies





1. CONTEXTE ET
ENJEU

2. CHIFFREMENT
DES DONNÉES



1. CONTEXTE ET
ENJEU

2. Les types de chiffrement

➤ Chiffrement au repos

- Données stockées sur disques, snapshots, bases de données, etc.
- Objectif : protéger contre le vol physique ou la compromission d'un support.
- Exemples : AWS S3 Server-Side Encryption (SSE-S3, SSE-KMS)
 Azure Storage Encryption



1. CONTEXTE ET ENJEU

2. Les types de chiffrement

SSE-KMS (SERVER-SIDE ENCRYPTION – AWS KEY MANAGEMENT SERVICE)

- Chiffrement géré par **AWS KMS (Key Management Service)**.
Permet d'utiliser :
 - Soit une clé KMS par défaut gérée par AWS,
 - Soit une clé KMS personnalisée (CMK – Customer Managed Key).
- Offre un contrôle plus fin :
 - Droits IAM sur l'usage de la clé,
 - Journalisation CloudTrail de toutes les requêtes de chiffrement/déchiffrement,
 - Rotation automatique ou manuelle des clés.
- Usage typique : pour les environnements sensibles, réglementés ou audités (RGPD, ISO 27001...).



1. CONTEXTE ET ENJEU

2. Les types de chiffrement

SSE-S3 (SERVER-SIDE ENCRYPTION – S3 MANAGED KEYS)

- Chiffrement géré entièrement par AWS S3.
- Les clés sont **créées, stockées et gérées automatiquement** par S3.
L'utilisateur **n'a aucune action à faire** pour la rotation ou la gestion des clés.
- Chiffrement réalisé avec **AES-256**.
Pas de journalisation fine des accès aux clés.
- Usage typique : pour les données standards sans exigence réglementaire forte.



1. CONTEXTE ET
ENJEU

2. Les types de chiffrement

➤ Chiffrement en transit

- Protection des flux entre client et serveur.
- **Outils** : HTTPS, TLS 1.2+, SSH, VPN IPSec
- **Cas typique** : communication entre une appli web et son backend API via HTTPS.



1. CONTEXTE ET
ENJEU

2. Les types de chiffrement

➤ Chiffrement applicatif

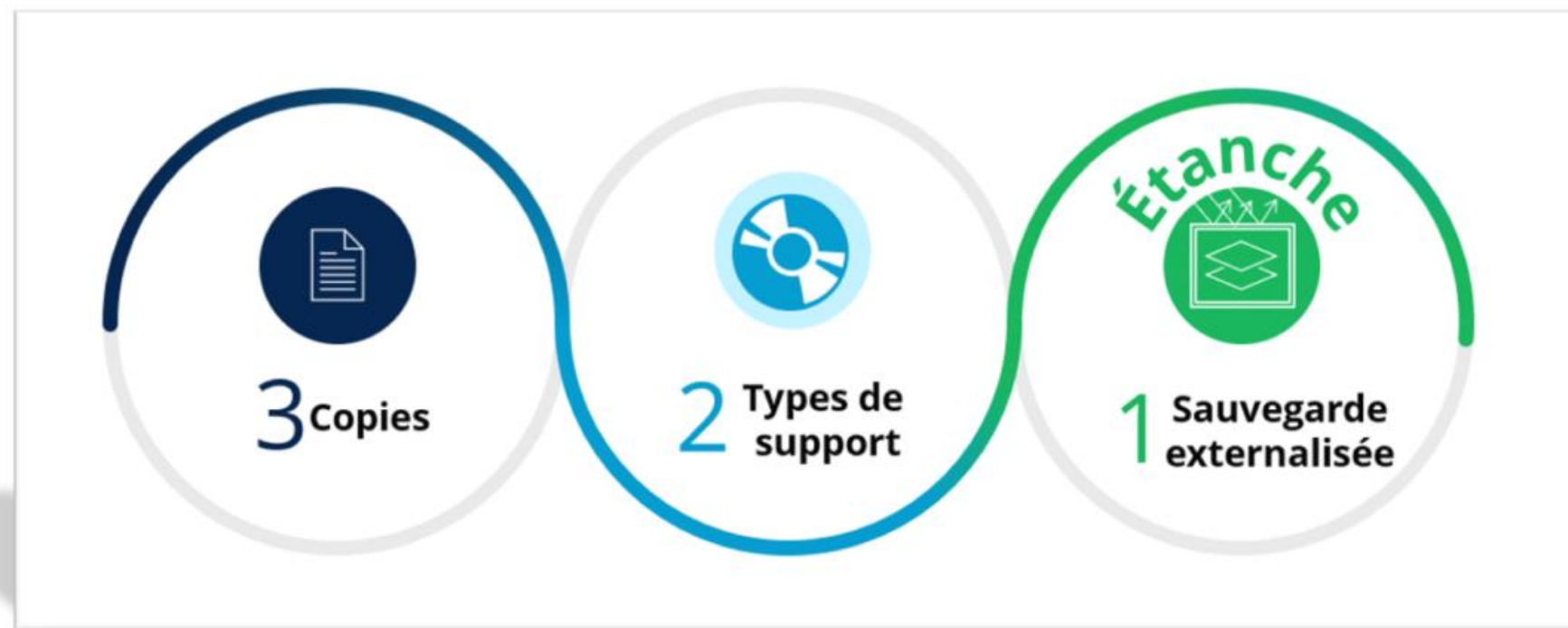
- Le chiffrement est géré directement par l'application.
- Exemple : les mots de passe utilisateurs stockés en hash (bcrypt, Argon2).
- Avantage : l'app reste sécurisée même si le stockage Cloud est compromis.

Question :

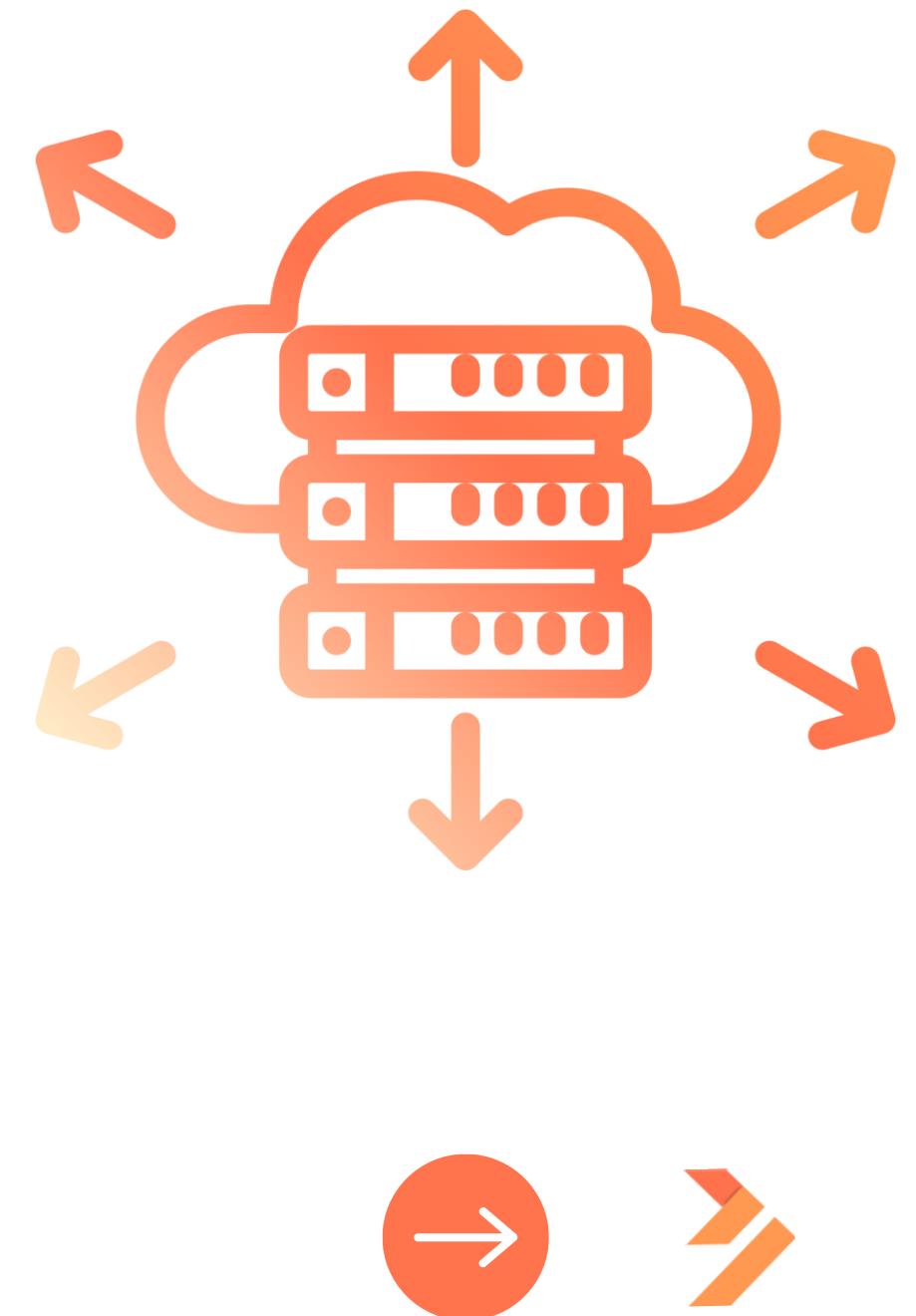
Pourquoi le chiffrement applicatif peut-il être préférable à un chiffrement natif Cloud ?

SAUVEGARDE ET RESTAURATION

- Objectif : garantir la continuité de service (BCP/DRP).
- Stratégies :
 - Sauvegarde complète, différentielle, incrémentale.
 - Rétention : définir le temps de conservation des sauvegardes.
 - Test de restauration obligatoire (ne jamais se fier à la sauvegarde seule).



Exemples : AWS Backup, Azure Recovery Services Vault, GCP Backup for GKE.



SAUVEGARDE ET RESTAURATION

➤ RTO – RECOVERY TIME OBJECTIVE (OBJECTIF DE TEMPS DE RÉTABLISSEMENT)

C'est le **temps maximal acceptable** pour restaurer un service ou une application après un incident.

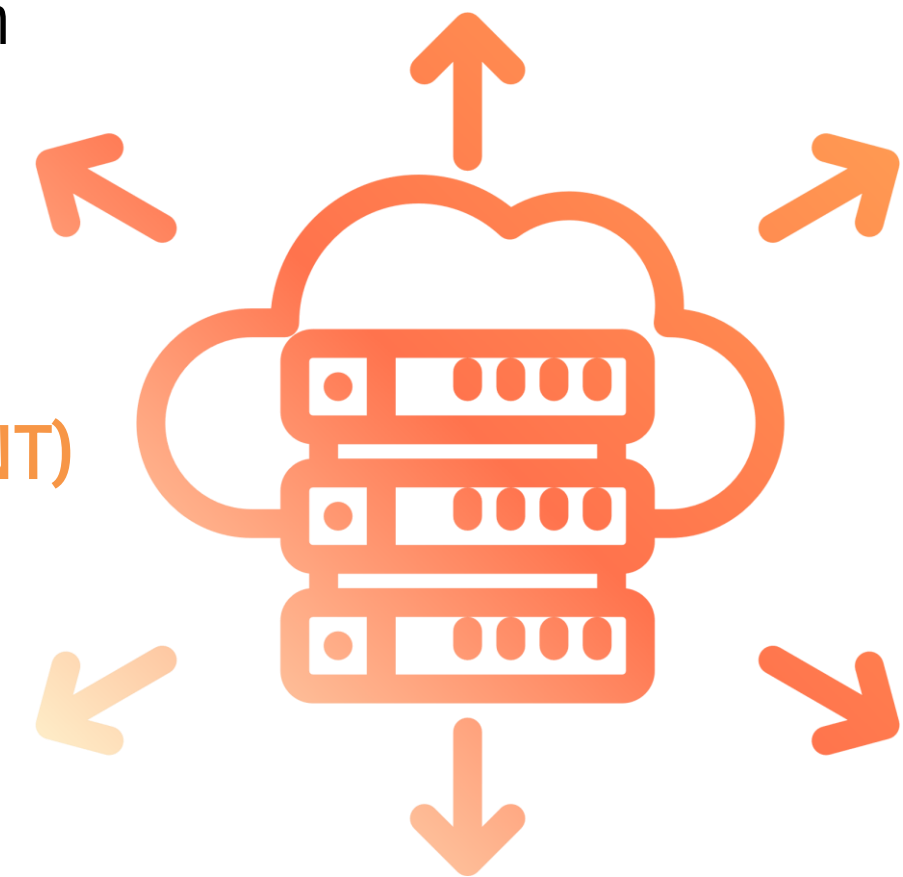
Combien de **temps maximum** peut-on rester en panne avant que cela ait un impact critique sur l'activité ?

Si ton RTO est de **2 heures**, cela signifie que ton système doit être opérationnel **au plus tard 2 h après la panne**.

➤ RPO – RECOVERY POINT OBJECTIVE (OBJECTIF DE POINT DE RÉTABLISSEMENT)

C'est la **quantité maximale de données** que l'on peut se permettre de perdre, exprimée en temps entre la dernière sauvegarde et la panne.

Quelle **ancienneté maximale** des données peut-on accepter après un incident ?
Exemple : Si ton RPO est de 15 minutes, cela veut dire qu'en cas de panne, tu peux perdre au maximum 15 min de données.



Exemples : AWS Backup, Azure Recovery Services Vault, GCP Backup for GKE.



Gestion des accès et conformité

- **IAM (Identity & Access Management) :**
 - Politique du moindre privilège. (zero trust)
 - Groupes et rôles (plutôt qu'utilisateurs individuels).
- **Audit de conformité :**
 - RGPD (Europe), ISO 27018 (Cloud privacy), SOC 2 Type II (contrôles internes).
 - CloudTrail, Azure Monitor, GCP Audit Logs.
- **Journalisation et alerte :**
 - Détection d'anomalies (ex. : connexion depuis un pays inhabituel).



ACTIVITÉ PRATIQUE



SCÉNARIO

Une PME migre son serveur de fichiers local vers un espace de stockage AWS (S3 Bucket) et une base de donnée AWS (RDS).

Elle stocke des données clients et RH sensibles.

- Identifier les risques.
- Proposer une stratégie complète : chiffrement, clés, sauvegarde.



ACTIVITÉ PRATIQUE



Solution :

Risques :

- Fuite de données
- Mauvaise configuration IAM / S3
- Compromission des clés AWS (IAM ou KMS)
- Perte de données

Stratégie de chiffrement :

En transit : Forcer **TLS/HTTPS** sur toutes les communications vers S3 et RDS.

Stockage S3 : activer le **chiffrement côté serveur SSE-KMS**
(CloudTrail activé)

Pour les fichiers RH : ajouter un chiffrement applicatif avant l'envoi au bucket (niveau champ ou fichier ZIP chiffré).



ACTIVITÉ PRATIQUE



Solution :

- Activer le chiffrement RDS via KMS dès la création de l'instance.
- Chiffrer aussi les snapshots et réplicas.
- Empêcher le stockage credentials en clair dans le code ou les scripdests.

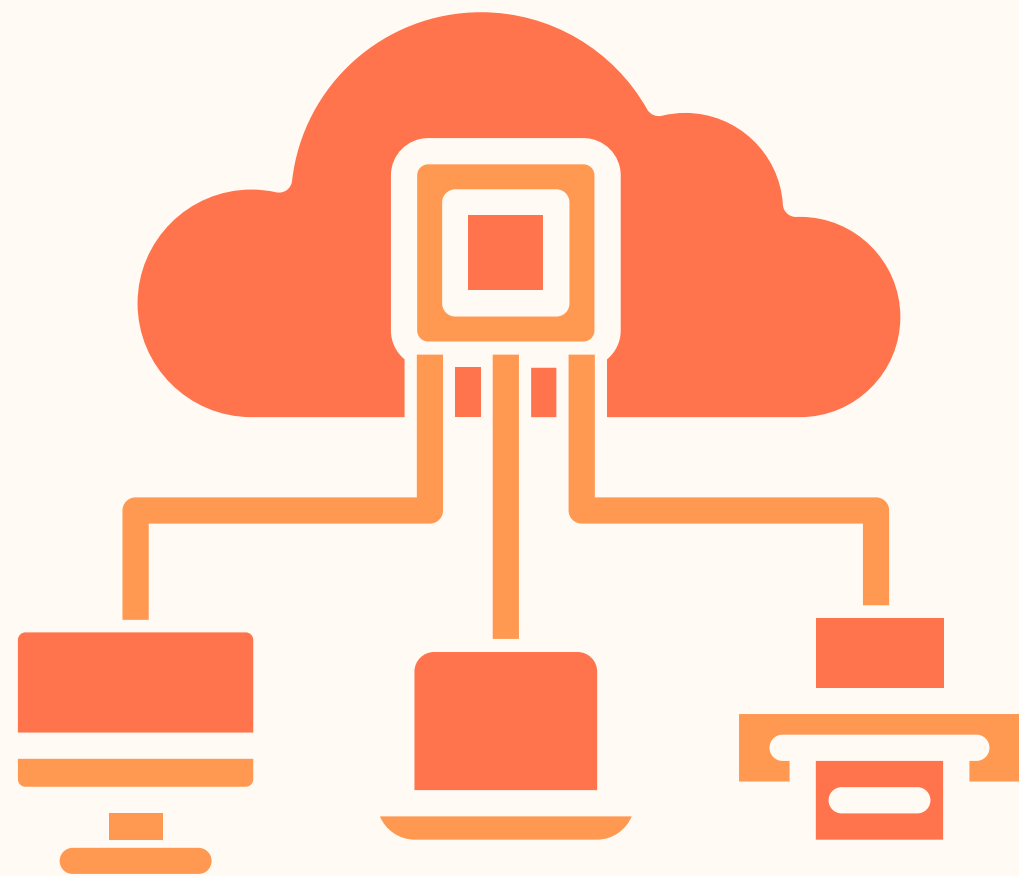
STRATÉGIE DE SAUVEGARDE ET RESTAURATION

RTO (Recovery Time Objective) : ≤ 2 heures

RPO (Recovery Point Objective) ≤ 15 minutes

Snapshot et versionning tous les 15 minutes

Sauvegarde complète tous les jours externalisée :



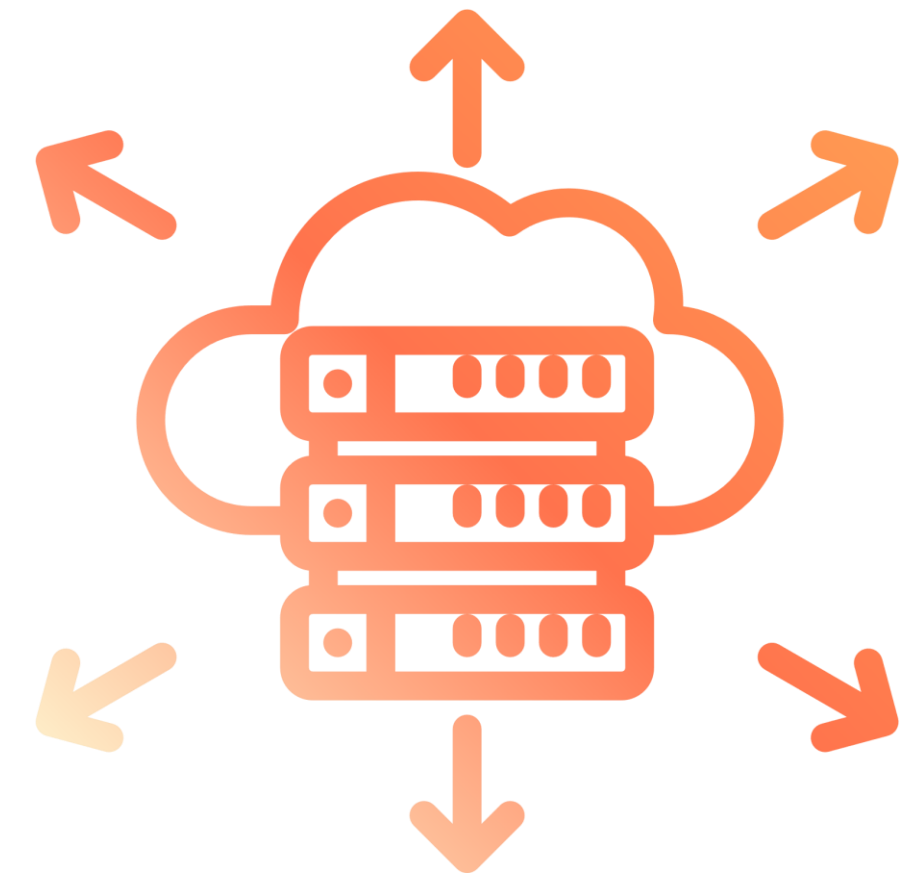
CHAPITRE 4 :

STRATÉGIES DE PROTECTION DES APPLICATIONS EN ENVIRONNEMENT CLOUD



OBJECTIF

- Identifier les risques applicatifs liés à la migration ou au développement dans le Cloud.
- Mettre en œuvre des **mécanismes d'authentification et d'autorisation** adaptés.
- Gérer les **identités, accès et permissions** de manière granulaire
- Intégrer la **sécurité dans le cycle DevOps (DevSecOps)**.
- Mettre en place des outils de **détection, réponse et amélioration continue**.





COMPRENDRE LES RISQUES APPLICATIFS DANS LE CLOUD

Comprendre la surface d'attaque d'une application Cloud

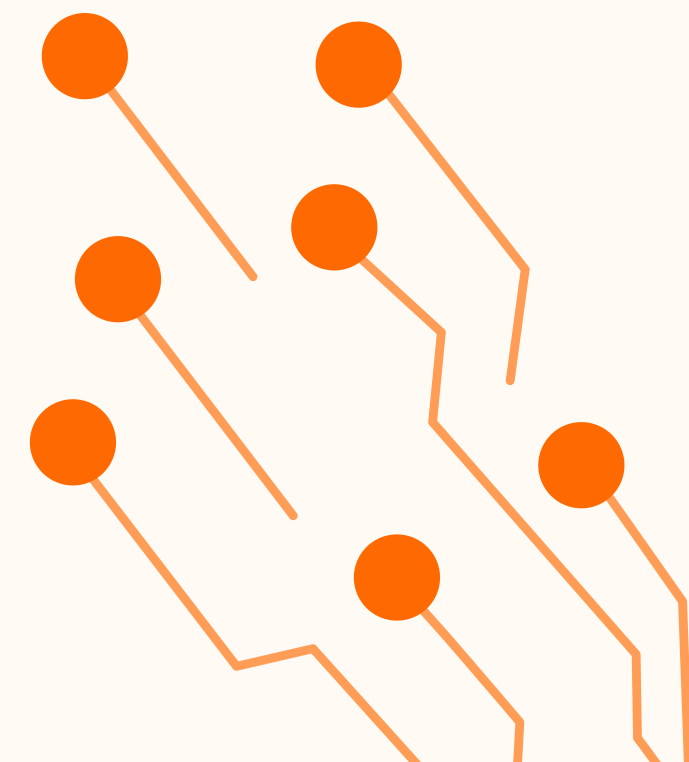
API exposées sans authentification

Fuite de secrets dans le code source (GitHub, Docker, .env)

Permissions IAM trop larges (principe du moindre privilège non respecté)

Services mal configurés (buckets publics, ports ouverts)

Manque de surveillance ou d'alertes (logs non activés)



AUTHENTIFICATION ET AUTORISATION

PROTOCOLES COURANTS	PROTOCOLE	FONCTION	UTILISATION TYPIQUE
	OAuth 2.0	Délégation d'accès sans partager le mot de passe	Connexion via Google / Facebook
	OpenID Connect (OIDC)	Authentification moderne basée sur OAuth 2.0	Applications web modernes
	SAML 2.0	Authentification dans les environnements d'entreprise	Connexion à Office 365, Salesforce
	Kerberos	Authentification réseau interne (Active Directory)	Environnements hybrides

BONNES PRATIQUES

- MFA obligatoire pour tout accès administrateur.
- Ne jamais stocker les mots de passe en clair.
- Utiliser des gestionnaires d'identité centralisés (Azure AD, AWS IAM Identity Center).
- Journaliser toutes les tentatives de connexion.

AUTHENTIFICATION ET AUTORISATION

➤ AUTHENTIFICATION : VÉRIFIER L'IDENTITÉ

L'authentification consiste à **valider** que l'utilisateur ou service est bien celui qu'il prétend être.

➤ NIVEAUX D'AUTHENTIFICATION

- **Simple (Single Factor)** : mot de passe uniquement.
Risqué : vulnérable au phishing et aux fuites.
- **Multifactorielle (MFA)** : ajout d'un facteur de possession (téléphone, clé physique).
Renforce la sécurité, même en cas de vol d'identifiants.
- **Fédérée / SSO (Single Sign-On)** : l'utilisateur s'authentifie via un fournisseur de confiance (Azure AD, Google, Keycloak).
Simplifie la gestion des comptes et des mots de passe.

✚ AUTORISATION : CONTRÔLER LES ACTIONS

Principes

- RBAC (Role-Based Access Control) : gestion par rôle (lecteur, contributeur, admin).
- PBAC (Policy-Based Access Control) : gestion par politiques Cloud (IAM Policy, Azure Policy).
- ABAC (Attribute-Based Access Control) : gestion par attributs (heure, IP, équipe).

POURQUOI FAUT-IL GARDER LE RÔLE “ADMIN” PAR DÉFAUT
DANS UN PROJET CLOUD ?

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": ["s3:GetObject", "s3:PutObject"],  
    "Resource": "arn:aws:s3:::logs-app/*"  
  }]  
}
```

◀ INTÉGRER LA SÉCURITÉ DANS LE CYCLE DE VIE APPLICATIF (DEVSECOPS)

➤ QU'EST-CE QUE LE DEVSECOPS ?

ÉTAPE	OBJECTIF	OUTILS RECOMMANDÉS
Planification	Identifier les menaces et exigences de sécurité	Threat Modeling, STRIDE
Développement	Respecter les bonnes pratiques de code sécurisé	SonarQube, OWASP Dependency Check
Intégration	Scanner le code et les dépendances	GitLab CI, Snyk, Trivy
Déploiement	Vérifier la conformité des ressources Cloud	Terraform validate, tfsec, Checkov
Exploitation	Surveiller et corriger les vulnérabilités	CloudWatch, Azure Monitor, Sentinel

◀ INTÉGRER LA SÉCURITÉ DANS LE CYCLE DE VIE APPLICATIF (DEVSECOPS)

Exemple : pipeline CI/CD sécurisé

```
stages:  
  - test  
  - security  
  - deploy  
  
test:  
  script: pytest tests/  
  
security:  
  script: trivy fs .  
  
deploy:  
  script: terraform apply -auto-approve
```

- Bénéfices
 - Réduction du coût de correction des failles.
 - Automatisation et standardisation de la sécurité.
 - Confiance accrue dans les livraisons.

➤ Discussion de groupe

QUELS SONT LES AVANTAGES POUR UNE ENTREPRISE D'INTÉGRER LA SÉCURITÉ DANS LES PIPELINES CI/CD ?

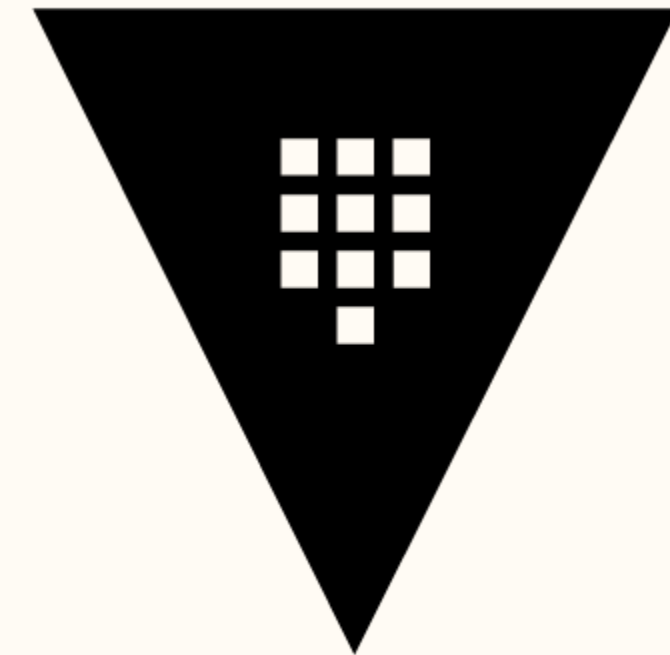


Gestion sécurisée des secrets



Ne pas stocker :

- Clés API, tokens, mots de passe dans le code
- .env dans GitHub
- Confiance accrue dans les livraisons.



HashiCorp

Vault

DÉTECTION ET RÉPONSE AUX INCIDENTS

La détection vise à repérer rapidement une anomalie ou une attaque. Elle repose sur la collecte et l'analyse des logs.

➤ OUTILS DE SURVEILLANCE

PLATEFORME	OUTIL	FONCTION
AWS	CloudTrail / GuardDuty	Traçabilité + détection comportementale
Azure	Sentinel / Defender for Cloud	SIEM + corrélation d'événements
GCP	Security Command Center	Vue centralisée de la posture sécurité

➤ EXEMPLES D'ÉVÉNEMENTS À SURVEILLER

- Connexion d'un utilisateur depuis un pays inhabituel.
- Création d'un utilisateur admin non autorisé.
- Modification suspecte de configurations réseau.

◀ DÉTECTION ET RÉPONSE AUX INCIDENTS

La détection vise à repérer rapidement une anomalie ou une attaque. Elle repose sur la collecte et l'analyse des logs.

Réponse aux incidents

➤ Étapes d'un plan de réponse

1. **Identification** → reconnaître l'incident.
2. **Confinement** → isoler les systèmes compromis.
3. **Éradication** → supprimer les causes (comptes, malware, configurations).
4. **Rétablissement** → restaurer les services depuis sauvegardes fiables.
5. **Retour d'expérience** → documenter et prévenir la récurrence.

➤ Exemple concret

Une API sur Azure subit un grand nombre de requêtes depuis l'étranger.

- Blocage IP via WAF (Azure Front Door ou AWS WAF).
- Notification via Sentinel / CloudWatch.
- Changement immédiat des tokens API.
- Audit des logs pour identifier l'origine.



POURQUOI FAUT-IL TOUJOURS CONSERVER
LES JOURNAUX MÊME APRÈS L'INCIDENT ?



ÉVALUER ET AMÉLIORER EN CONTINU

La sécurité n'est jamais acquise. Elle doit être **mesurée, testée et améliorée régulièrement**.

➤ BONNES PRATIQUES

- Réaliser des revues mensuelles IAM (suppression des comptes inactifs).
- Effectuer des tests de pénétration réguliers.
- Automatiser les audits avec : AWS Security Hub Azure Policy GCP Forseti / Security Command Center
- Mettre en place un tableau de bord de conformité (ISO 27001, RGPD, SOC 2).

➤ INDICATEURS DE SÉCURITÉ (KPI)

INDICATEUR

Nombre d'incidents détectés / mois
Délai moyen de correction d'une faille
Taux de comptes MFA activés
% de ressources auditées

OBJECTIF

Suivre la réactivité
Évaluer la maturité DevSecOps
Suivi de la conformité
Mesure du périmètre couvert



ACTIVITÉ PRATIQUE



SCÉNARIO

VOUS ÊTES CONSULTANT SÉCURITÉ POUR UNE PME QUI MIGRE SON SI VERS AWS.

- ELLE STOCKE DES DONNÉES CLIENTS SENSIBLES SUR S3 BUCKET et BDD S3
- ELLE VEUT ASSURER DISPONIBILITÉ + CONFIDENTIALITÉ + CONFORMITÉ.

TRAVAIL DEMANDÉ (EN SOUS-GROUPES)

- DÉCRIRE LES MÉCANISMES DE CHIFFREMENT RECOMMANDÉS.
- PROPOSER UNE POLITIQUE DE GESTION DES CLÉS (ROTATION, STOCKAGE, DROITS).
- DÉFINIR UNE STRATÉGIE DE SAUVEGARDE ET RESTAURATION (RTO/RPO ADAPTÉS) SELON L'USAGE.
- DONNER DES RECOMMANDATIONS POUR LA CONFORMITÉ RGPD.
- PROPOSER UNE POLITIQUE DE GESTION DE DROIT DES RESSOURCES PAR EQUIPE (ADMINISYS, CHEF DE PROJET, DEV)

Divers

TOP 10 des services AWS les plus vendus / les plus utilisés

➤ Instance (les plus vendus de toute l'offre AWS)

EC2

Fonctions serverless ultra vendues (coût faible, très scalable).



Amazon
EC2



AWS Lambda

Fonctions serverless ultra vendues (coût faible, très scalable).

ECS / EKS

ECS : Orchestration Docker simple et internalisée AWS

EKS : Kubernetes managé → énorme adoption entreprise



AWS ECS



Divers

➤ Stockage – services très consommés

S3 – Simple Storage Service

Object storage, réplication, versionning, etc.



EBS – Elastic Block Store

Volumes attachés aux EC2.

EFS – Elastic File System

Partage de fichiers réseau, vendu régulièrement pour clusters, containers, etc.



Divers

Bases de données

RDS

Base SQL managée (MySQL, PostgreSQL, MariaDB, Oracle, SQL Server).

DynamoDB

Base NoSQL gérée → utilisée par énormes workloads.

ElastiCache (Redis/Memcache)

Cache distribué très utilisé pour les apps web.

Divers

Web

CloudFront

CDN mondial → beaucoup utilisé pour S3, sites web statiques, APIs.

Route 53

DNS, très peu cher → massivement utilisé..

WAF – AWS Web Application Firewall

Protection des API/applications → un best seller.



Etude de cas



ETAPE 1 : COMPRENDRE LE CONTEXT

- Modèle de déploiement : Cloud public / privé / hybride / multcloud
- Services concernés : S3, Azure Storage, EC2, RDS, API Gateway, VPN, etc.
- Données manipulées : sensibles ? personnelles ? production ?
- Contraintes : RGPD, conformité interne, disponibilité, SLA.



Etude de cas



ÉTAPE 2 : IDENTIFIER LES RISQUES

s'appuyer sur les catégories vues au Chapitre 2 :

- Confidentialité (IAM, clés, exposition publique, API...)
- Intégrité (modification non voulue, suppression, ransomware Cloud)
- Disponibilité (panne région, DDoS, dépendance VPN)
- Conformité (RGPD, stockage hors UE)
- Réseau (tunnel hybride, firewall, segmentation)
- IAM / Authentification
- Sauvegardes & récupération



Etude de cas



ÉTAPE 3 : ÉVALUER LA CRITICITÉ

- Probabilité (faible/moyenne/forte)
- Impact (faible/moyen/fort)
- Placer dans une matrice 2×2 ou 3×3 (voir Chapitre 2).

ÉTAPE 4 : PROPOSER DES MESURES

- Prévention (IAM, encryption, WAF, segmentation réseau...)
- Détection (logs, SIEM, alertes Cloud...)
- Réponse (procédure d'incident, restauration, rotation de clés...)



Etude de cas



ÉTAPE 5 : DOCUMENTER ET PRÉSENTER

Un livrable doit inclure :

- Contexte
- Risques + niveau de criticité
- Mesures proposées
- Schéma (réseau / IAM / flux)
- Conclusion avec recommandations prioritaires