Global Solution : Migration vers le Cloud.

1. Risques Clés

1. Exposition des données sensibles
    - Sans chiffrement solide, les informations peuvent être récupérées en transit ou stockées dans des fichiers mal configurés.
    - OWASP appelle ça “Sensitive Data Exposure”.
2. Perte de contrôle sur les ressources
    - Une fois sur le Cloud, on dépend du fournisseur : hyperviseurs, patchs, localisation des serveurs…
    - L’ANSSI rappelle l’importance de vérifier les preuves d’audit.
    - Du côté OWASP (ASVS), il faut documenter l’architecture et séparer clairement les environnements (dev, prod).
3. Attaques sur l’environnement Cloud
    - Les interfaces API, SSH ou RDP ouvertes au public deviennent la cible de brute-force ou d’injection de malwares (cryptominers, ransomwares).
4. Non-conformité réglementaire
    - Si le prestataire n’est pas compatible RGPD ou RGS, on risque des amendes.
    - Vérifier les clauses contractuelles, la localisation des données, et l’homologation PASSI ou RGS (ANSSI).

2. Recommandations Simples

2.1 Avant la Migration : Audit & Choix du Fournisseur

- Inventaire des Actifs : lister toutes les applications, bases, flux. Classer les données par niveau de sensibilité (public, interne, confidentiel).
- Évaluer le fournisseur Cloud :
    - Vérifier les Certifications ANSSI.
    - Région géographique (France-centre, UE-Ouest, etc.) pour respecter le RGPD et le RGS.
    - SLA clairs sur la sécurité, les mises à jour et la localisation des données.

2.2 Chiffrement & Protection des Données

- Au repos :
    - Activer le chiffrement natif sur les disques, buckets, bases managées.
    - Idéalement, utiliser des clés gérées par l’entreprise (CMK).
- En transit :

    - TLS 1.2+ pour tous les échanges (API, consoles, applications).
    - VPN IPsec ou OpenVPN entre votre réseau et le Cloud.
- OWASP : Appliquer le guide sur “Cryptography at Rest & in Transit”.
- ANSSI : privilégier les algorithmes recommandés et assurer la rotation régulière des clés.

2.3 Contrôle d’Accès

- Principes de base :
    - Moindre privilège : chaque utilisateur ou service ne dispose que des droits strictement nécessaires.
    - Séparer administrateur et utilisateur courant.
- MFA obligatoire :
    - Choisir des tokens physiques (FIDO2, YubiKey) pour les comptes à privilèges.
- Gestion des rôles :
    - Créer des rôles granulaires (ex. « Backup-Operator », « Security-Auditor »).
    - Rotation automatique des clés d’accès tous les 60-90 jours.
- OWASP : vérifier régulièrement les permissions, désactiver les comptes inactifs.
- ANSSI : implémenter une fédération d’identité pour éviter la création de comptes locaux inutiles.

2.4 Surveillance & Détection

- Centraliser les logs :
    - API logs, CloudTrail/CloudWatch (AWS), Azure Monitor, GCP Audit Logs.
    - Alimenter un SIEM (Wazuh, ELK + Wazuh) pour corréler les événements.
- IDS/IPS & WAF :
    - Déployer un IDS/IPS (Snort/Suricata, ou service managé AWS GuardDuty, Azure Defender).
    - Ajouter un WAF compatible règles OWASP ModSecurity pour vos applications Web.
- ANSSI : suivre le guide SIEM et règles de détection PASSI.
- OWASP : respectez le “Logging Cheat Sheet” (horodatage UTC, logs immuables, anonymisation PII).

2.5 Plan de Réponse aux Incidents

- Scénarios types :
    - Bucket mal configuré — exfiltration de données.
    - VM compromise — cryptominage ou mouvement latéral.

    - Clé API volée — création de ressources factices.
- Playbook Cloud :
    - Contenir (isoler la ressource, révoquer les clés),
    - Analyser (audit des logs, sauvegardes),
    - Notifier (RGPD, équipe interne, clients si nécessaire),
    - Remédier (patch, reconfiguration),
    - Documenter (retour d'expérience).
- ANSSI : suivre le guide "Gestion de crise SSI".
- OWASP : intégrer le "Incident Response Guide" pour gérer rapidement les failles OWASP Top Ten.

2.6 Sensibilisation & Formation

- Ateliers réguliers :
    - OWASP Top 10 pour les développeurs (injection SQL, XSS, etc.).
    - ANSSI – hygiène informatique : mots de passe, phishing, mises à jour.
- Guides pratiques :
    - Fiches réflexes "Activer la MFA", "Vérifier une ACL S3, un NSG Azure".
    - Référentiels ANSSI + OWASP Quick Reference pour le codage sécurisé.
- Simulations :
    - Phishing interne pour sensibiliser le personnel.
    - CTF Cloud orienté découverte de failles OWASP dans un environnement test.

3. Stratégie de Sécurité Cloud Résumée

1. Choix d'un fournisseur certifié
    - AWS (région Paris), Azure (France-Centre/Sud), GCP (europe-west).
    - Certifications ANSSI.
2. Architecture Zero Trust
    - Ne jamais faire confiance par défaut : MFA, IAP (Identity-Aware Proxy), micro-segmentation (VPC/VNet).
    - Endpoint Protection (antimalware, EDR) conforme ANSSI.
3. Gestion de la Gouvernance des Données
    - Taggage des ressources (sensibilité, criticité).
    - Politiques de cycle de vie (RGPD, RGS) : archivage, suppression automatique.
4. Contrôles Dynamiques et IaC
    - Déploiement sécurisé via Terraform/Ansible validé ANSSI.
    - Scanning IaC (Checkov, KICS) pour détecter les mauvaises configurations (S3 publics, RDP ouvert).
5. CASB & DLP

    - Solution CASB (Microsoft Defender for Cloud Apps, Palo Alto Prisma) pour surveiller Shadow IT et bloquer la fuite de données.
    - Politiques DLP en ligne avec les recommandations ANSSI.
6. Formation Continue
    - Modules OWASP Top 10 et ANSSI “Hygiène informatique”.
    - Exercices de simulation (phishing, red team vs blue team).

4. Conclusion

En conclusion si global solution veut faire une migration vers le cloud il faut :

- Faire un audit sérieux (ANSSI, OWASP ASVS).
- Chiffrer à fond (au repos + en transit).
- Gérer les accès avec rigueur (IAM, MFA, rôles granulaires).
- Surveiller en permanence (SIEM, IDS/IPS, WAF).
- Prévoir un incident response plan dédié Cloud (ANSSI & OWASP).
- Former et sensibiliser tout le monde (développeurs, administrateurs, utilisateurs).