ÉTUDE DE CAS 1

Migration hybride et sécurisation d'un ERP médical

Scénario :

L'entreprise MedicaPlus, 350 employés, spécialisée dans la gestion de données médicales sensibles (patients, ordonnances, comptes-rendus), souhaite moderniser son système d'information vieillissant.

Actuellement, 80 % du SI est encore on-premise :

Infrastructure actuelle

- Active Directory local (AD DS)
- ERP interne sous Windows Server + SQL Server
- Serveur de fichiers contenant 120 To de documents médicaux
- Sauvegardes locales uniquement
- VPN IPSec ancien, instable
- Pas de chiffrement systématique
- Aucune supervision Cloud

Objectifs de l'entreprise

- Déployer l'ERP dans Azure App Service
- Migrer la base SQL vers Azure SQL Database
- Stocker les documents sensibles dans Azure Storage
- Garantir la conformité RGPD
- Mettre en place une architecture hybride fiable
- Assurer un PRA Cloud (RTO/RPO à définir)
- Implémenter une authentification moderne (Azure AD)

Architecture cible (proposée par la direction technique)

- Azure AD + Azure AD Connect
- Azure App Service (ERP web)
- Azure SQL Database (Business Critical)
- Azure Storage (fichiers patients)
- Azure Key Vault (secrets + certificats)
- Azure VPN Gateway (hybride)
- Azure Application Gateway + WAF
- Azure Monitor + Log Analytics
- Azure Backup / Recovery Vault

Contraintes de sécurité

- Données médicales → très sensibles
- Accès externes limités aux médecins et administratifs
- Haute disponibilité obligatoire
- Authentification forte MFA attendue
- Audit et traçabilité exigés
- Données localisées en UE

Travail demandé

1. Analyser le scénario et identifier les risques principaux, dans les catégories :
    - Confidentialité
    - Intégrité
    - Disponibilité
    - Authentification & IAM
    - Réseau hybride
    - Conformité RGPD
2. Créer une matrice de risques (probabilité × impact).
3. Proposer une architecture Azure corrigée et sécurisée, en détaillant :
    - IAM / RBAC
    - WAF
    - VPN / VNet / segmentation
    - Logging / monitoring
    - Sécurisation des données (SQL + Storage + clés)
4. Établir un plan de migration complet (ERP + SQL + fichiers).
5. Proposer un PRA Cloud (RTO, RPO, services utilisés).
6. Rédiger une recommandation finale (2–4 pages) destinée à la direction.

ÉTUDE DE CAS 2

Refonte sécurité et scalabilité d'un site e-commerce mondial

Scénario

L'entreprise GlobalShop, site e-commerce international, subit :

- des pannes fréquentes,
- un manque de scalabilité,
- une fuite S3 médiatisée l'année dernière,
- une explosion des coûts AWS.

Elle réalise 200 000 visites / jour, avec des pics à 2 millions durant les ventes flash.

L'infrastructure actuelle AWS est mal architecturée.

Infrastructure existante

- EC2 pour le front-end, sans Auto Scaling
- RDS MySQL en instance unique
- S3 avec un bucket devenu public par erreur
- CloudFront configuré partiellement
- Aucun WAF
- IAM : comptes admin partagés
- Secrets stockés dans les fichiers .env
- CloudTrail et GuardDuty désactivés
- VPC plate, peu segmentée

Objectifs de GlobalShop

- Construire une architecture hautement disponible
- Gérer automatiquement les pics de charge
- Renforcer la sécurité afin d'éviter une nouvelle fuite
- Améliorer les performances internationales
- Implémenter une logique DevSecOps
- Optimiser les coûts (FinOps)

Architecture cible envisagée par l'équipe technique

- CloudFront (CDN mondial)
- Application Load Balancer
- Auto Scaling Group EC2 ou ECS Fargate
- RDS Aurora MySQL (multi-AZ)
- ElastiCache Redis
- S3 privé + URL signées
- Secrets Manager
- VPC 3-tiers (public / private / database)
- GuardDuty + Security Hub
- CI/CD GitHub → CodeBuild → CodeDeploy

Contraintes de sécurité / performance

- Site monétisé → indisponibilité = pertes financières majeures
- Données personnelles (RGPD)
- Historique de fuite → risque réputationnel
- Traçabilité obligatoire
- Attaques DDoS fréquentes
- Délai maximum d'interruption très faible

Travail demandé

1. Analyser les risques majeurs du SI AWS, dans les domaines :
    - Confidentialité
    - Disponibilité
    - Intégrité
    - Performance
    - IAM
    - Coûts (FinOps)
2. Proposer un schéma d'architecture AWS complet, incluant :
    - CDN / WAF / ALB
    - Compute (EC2 ASG ou ECS Fargate)
    - Base de données + réplication
    - VPC segmenté
    - Gestion des secrets
    - Logging / détection d'incidents
3. Définir une stratégie IAM Zero Trust pour toutes les équipes.
4. Écrire un plan DevSecOps, incluant scans, alertes et automatisation.
5. Déterminer un RTO et un RPO adaptés à un site e-commerce international.
6. Rédiger une réponse à incident en cas de nouvelle fuite S3 (procédure attendue).