Exercice 5 — SECURITY BY DESIGN & RISK ENGINEERING

CONTEXTE

La société **MedData+** développe une plateforme numérique nationale destinée à :

Fonctionnalités principales

- centraliser les dossiers médicaux
- permettre la télémédecine
- stocker imageries médicales
- permettre la prescription électronique
- intégrer les données d'objets connectés (montres santé…)
- accès patient via application mobile
- accès médecins via portail web
- API ouverte aux hôpitaux partenaires

Utilisateurs

- patients
- médecins
- hôpitaux
- laboratoires
- administrateurs techniques
- partenaires externes

Données traitées

- données médicales
- données biométriques
- historique traitements
- prescriptions
- données d'assurance
- informations personnelles
- identifiants nationaux de santé
- logs d'accès
- données IoT santé temps réel

Architecture actuelle

- cloud public multi-régions
- API REST accessible internet
- stockage cloud objet
- authentification email/mot de passe
- sessions valides 30 jours
- accès API via token statique
- chiffrement au repos uniquement
- sauvegardes hebdomadaires
- logs conservés 14 jours
- monitoring partiel
- aucun MFA
- partage dossiers via lien sécurisé

TRAVAIL DEMANDÉ

PARTIE 1 — Analyse des Actifs & CIA

1) Identifier au moins 8 actifs critiques du système.

2) Évaluer pour chacun :

- Confidentialité
- Intégrité
- Disponibilité
- Impact en cas de compromission

Une présentation sous forme de tableau est fortement recommandée.

PARTIE 2 — Analyse des Menaces & Risques

Identifier **10 risques majeurs** incluant :

- cyberattaques
- erreurs humaines
- défaillances techniques
- abus internes

Pour chaque risque :

- décrire la cause probable
- décrire l'impact
- évaluer la probabilité (Faible / Moyenne / Élevée)
- évaluer l'impact (Faible / Moyen / Élevé)

- déterminer la criticité en justifiant brièvement

Utiliser une matrice simple Probabilité × Impact.

PARTIE 3 — Threat Modeling STRIDE

Appliquer la méthodologie STRIDE aux éléments suivants :

- authentification patient
- API partenaires
- objets connectés santé
- partage dossiers médicaux

Pour chaque élément :

- identifier au moins une menace STRIDE
- préciser la catégorie (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
- proposer une mesure de mitigation adaptée

PARTIE 4 — Vulnérabilités & OWASP

Identifier au minimum 8 vulnérabilités concrètes présentes ou probables dans l'architecture actuelle.

Pour chacune :

- décrire la vulnérabilité dans le contexte MedData+
- l'associer à une catégorie OWASP Top 10 (2021)
- justifier brièvement le lien

Les réponses purement théoriques sans lien avec le contexte ne seront pas validées.

PARTIE 5 — Security by Design

Identifier au minimum 6 principes du Security by Design non respectés dans l'architecture actuelle.

Pour chacun :

- nom du principe
- élément d'architecture concerné
- conséquence potentielle
- correction nécessaire

Les réponses doivent être directement liées au contexte fourni.

PARTIE 6 — Architecture Sécurisée

Proposer une architecture intégrant :

- défense en profondeur
- gestion des identités et des accès
- sécurisation des API
- protection des données sensibles
- surveillance et audit
- continuité de service

Un schéma d'architecture logique est fortement recommandée.

Le schéma doit montrer :

- principaux composants
- zones de sécurité (ex : public / services / données)
- flux principaux
- mécanismes de protection

PARTIE 7 — RGPD & Conformité

Identifier :

- les données sensibles et catégories particulières
- les obligations légales majeures
- les risques de non-conformité
- les mesures nécessaires pour assurer la conformité

Les réponses doivent être argumentées et liées au contexte médical.

PARTIE 8 — Gestion d'un Incident Majeur

Scénario

Une attaque par ransomware bloque l'accès aux dossiers médicaux.
Des données semblent avoir été exfiltrées.

Décrire :

1. actions immédiates (0–24h)
2. obligations légales
3. communication interne/externe
4. reprise d'activité
5. mesures post-incident

PARTIE 9 — Plan Stratégique d'Amélioration

Proposer :

Court terme (urgent)

Moyen terme

Long terme

Justifier les priorités selon les risques.

Livrable attendu

Vous devrez produire un **rapport d'analyse formel**, au format **PDF**.

Identification obligatoire

Le document devra impérativement comporter, en première page (page de titre) ou en tout début de document, les informations suivantes :

- **Nom**
- **Prénom**
- **Adresse e-mail**

Tout document ne comportant pas clairement ces éléments d'identification ne pourra pas être traité.

Ce document devra :

- reprendre l'ensemble des questions ou parties demandées dans le sujet ;
- présenter vos réponses de manière structurée, argumentée et professionnelle ;
- inclure les éléments demandés dans l'exercice (tableaux, analyses, classifications, justifications, schémas, etc.) lorsque cela est explicitement requis ;
- expliciter vos hypothèses lorsque certaines informations ne sont pas précisées dans le sujet ;
- justifier vos choix et votre raisonnement de manière claire et cohérente.

Le rapport devra être rédigé dans un format professionnel (page de titre, sections numérotées, tableaux ou éléments visuels lisibles si nécessaires).
Il devra refléter une démarche d'analyse rigoureuse conforme aux principes du *Security by Design*.