

# Exercice 4 — AUDIT COMPLET & SÉCURISATION D'UNE PLATEFORME NUMÉRIQUE

---

## CONTEXTE

---

Une entreprise lance **WorkShare**, une plateforme collaborative permettant :

### Fonctionnalités

- partage de documents
  - messagerie interne
  - gestion de projets
  - signature électronique
  - connexion via Google/Microsoft
  - accès invité via lien public
  - API publique pour intégration partenaires
- 

### Données stockées

- documents professionnels
  - contrats signés
  - données personnelles des employés
  - messages internes
  - logs d'activité
  - adresses IP
  - signatures électroniques
- 

### Architecture actuelle

- application web cloud
  - stockage fichiers sur serveur distant
  - API accessible via internet
  - authentification par mot de passe simple
  - comptes administrateurs partagés
  - sauvegardes hebdomadaires
  - logs conservés 7 jours
  - liens publics permanents
  - accès API via clé unique
- 

## TRAVAIL DEMANDÉ

---

---

## PARTIE 1 — Analyse des Actifs & CIA

---

1) Identifier les actifs critiques

2) Pour chaque actif, analyser :

- Confidentialité
- Intégrité
- Disponibilité
- Impact métier si compromis

---

## PARTIE 2 — Analyse des Risques

---

Identifier **8 risques majeurs**.

Pour chacun :

- cause
- impact
- gravité (faible / moyen / critique)

---

## PARTIE 3 — Threat Modeling (STRIDE)

---

Identifier au moins **1 menace STRIDE** pour :

- authentification
- API publique
- partage de documents
- signature électronique

---

## PARTIE 4 — Vulnérabilités & OWASP Top 10

---

Identifier les vulnérabilités présentes et les associer à l'OWASP.

---

## PARTIE 5 — Security by Design

---

Identifier **5 principes Security by Design non respectés** et expliquer pourquoi.

---

## PARTIE 6 — Défense en profondeur

---

Proposer une architecture de sécurité en couches :

- périmètre
  - réseau
  - application
  - authentification
  - données
- 

## PARTIE 7 — Conformité RGPD

---

Identifier :

- données personnelles traitées
  - risques RGPD
  - obligations légales
  - mesures nécessaires
- 

## PARTIE 8 — Plan d'amélioration priorisé

---

Proposer :

- 5 actions urgentes
- 5 améliorations moyen terme
- 3 mesures long terme

Justifier les priorités.

---

### 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*.