EXERCICE 6 — Détection d'incidents & réponse (SIEM, alerting, playbooks)

Contexte professionnel

ShopNow veut passer d'une posture purement préventive à une posture **défendable et observable**. Après avoir mis en place des logs, un SIEM et des contrôles Zero Trust, l'entreprise souhaite :

- détecter rapidement les incidents,
- réagir de manière structurée,
- limiter l'impact métier.

Objectifs pédagogiques

L'étudiant doit être capable de :

- Identifier les **événements de sécurité** critiques à journaliser.
- Définir des **règles de corrélation** et d'alerte.
- Concevoir des **playbooks de réponse** à incident.
- Relier les incidents aux menaces STRIDE et aux actifs critiques.

Consigne générale

Rapport en anglais (page de garde, sommaire, numérotation, conclusion).

Travail demandé

1. **Cartographie des événements de sécurité**

Pour les actifs critiques (D1, D2, D4, D6, C2, C3, C5, F1, F2, F4, A2), complétez :

| Actif | Type d'événement à logguer | Exemple concret | Menace STRIDE associée | Criticité log (Haute/Moyenne/Faible) |

2. **Règles d'alerte SIEM**

Proposez au moins 8 règles d'alerte, par exemple :

   - **Tentatives de login échouées** sur C5 > seuil → suspicion credential stuffing.
   - **Création de commandes anormales** (montant, fréquence) → suspicion fraude.
   - **Accès admin A2 depuis IP inhabituelle** → suspicion usurpation.

Pour chaque règle :

   - Condition de déclenchement,

- Menace STRIDE,
- Impact métier,
- Priorité d'alerte.

3. **Playbooks de réponse à incident**

Définissez au moins 3 playbooks :

- Compromission de token (D4 / F1),
- Suspicion de fuite de données clients (D1),
- Attaque DoS sur C2/C5.

Pour chaque playbook :

- Détection,
- Containment,
- Eradication,
- Rétablissement,
- Leçons apprises.

4. **Alignement avec Zero Trust**

Expliquez comment la détection et la réponse :

- renforcent le principe "Never Trust, Always Verify",
- permettent d'ajuster dynamiquement les politiques (blocage IP, durcissement MFA, etc.).

5. Quels sont les **indicateurs clés** d'une bonne capacité de détection ?

6. Comment éviter la **fatigue d'alertes** ?

ANNEXE A — Événements de sécurité à journaliser

Actif	Événements critiques
C5 API Auth	login, logout, MFA, échecs
D4 Tokens	création, refresh, invalidation
C2 Backend	erreurs 4xx/5xx, accès admin
C3 DB	requêtes anormales, accès superuser
F2 Paiement	montants, anomalies, refus

ANNEXE B — Règles SIEM types

Règle	Condition	Menace
R1	>10 échecs login/min	Spoofing
R2	Token utilisé depuis 2 pays	Spoofing
R3	Montant commande > 3× moyenne	Tampering
R4	500 API > seuil	DoS

ANNEXE C — Playbook modèle

1. Detection
2. Containment
3. Eradication
4. Recovery
5. Lessons Learned