EXERCICE 2 — Analyse STRIDE des menaces

Contexte professionnel

Vous poursuivez votre mission de cybersécurité pour **ShopNow**, la plateforme e-commerce en refonte. Après avoir réalisé la **cartographie complète des actifs**, vous devez maintenant identifier les **menaces** qui pèsent sur le système.

Le CTO exige une analyse **STRIDE** complète pour :

- anticiper les attaques possibles,
- prioriser les exigences de sécurité,
- préparer les tests de sécurité,
- orienter l'architecture Zero Trust.

Objectifs pédagogiques

À l'issue de cet exercice, l'étudiant doit être capable de :

- appliquer **STRIDE** à un système réel,
- identifier les menaces pertinentes pour chaque actif,
- comprendre les impacts potentiels,
- préparer la dérivation d'exigences de sécurité (Exercice 3),
- raisonner comme un architecte sécurité.

Nous reprenons l'architecture de l'exercice 1

Rappel des actifs analysés

Répondez à ces questions sous la forme d'un rapport en anglais (le rapport devra prendre en compte une page de garde, un sommaire, une numérotation de page et une conclusion et bien sûr la réponse aux questions.

ID	Actif
A1	Client

A2	Administrateur
C1	Front-end
C2	Backend
C3	Base de données
C5	API Auth
C6	API paiement
D1	Données clients
D2	Données commandes
D4	Tokens d’authentification
F1	Flux d’authentification
F2	Flux paiement
F4	Flux commandes

Schéma des zones de sécurité

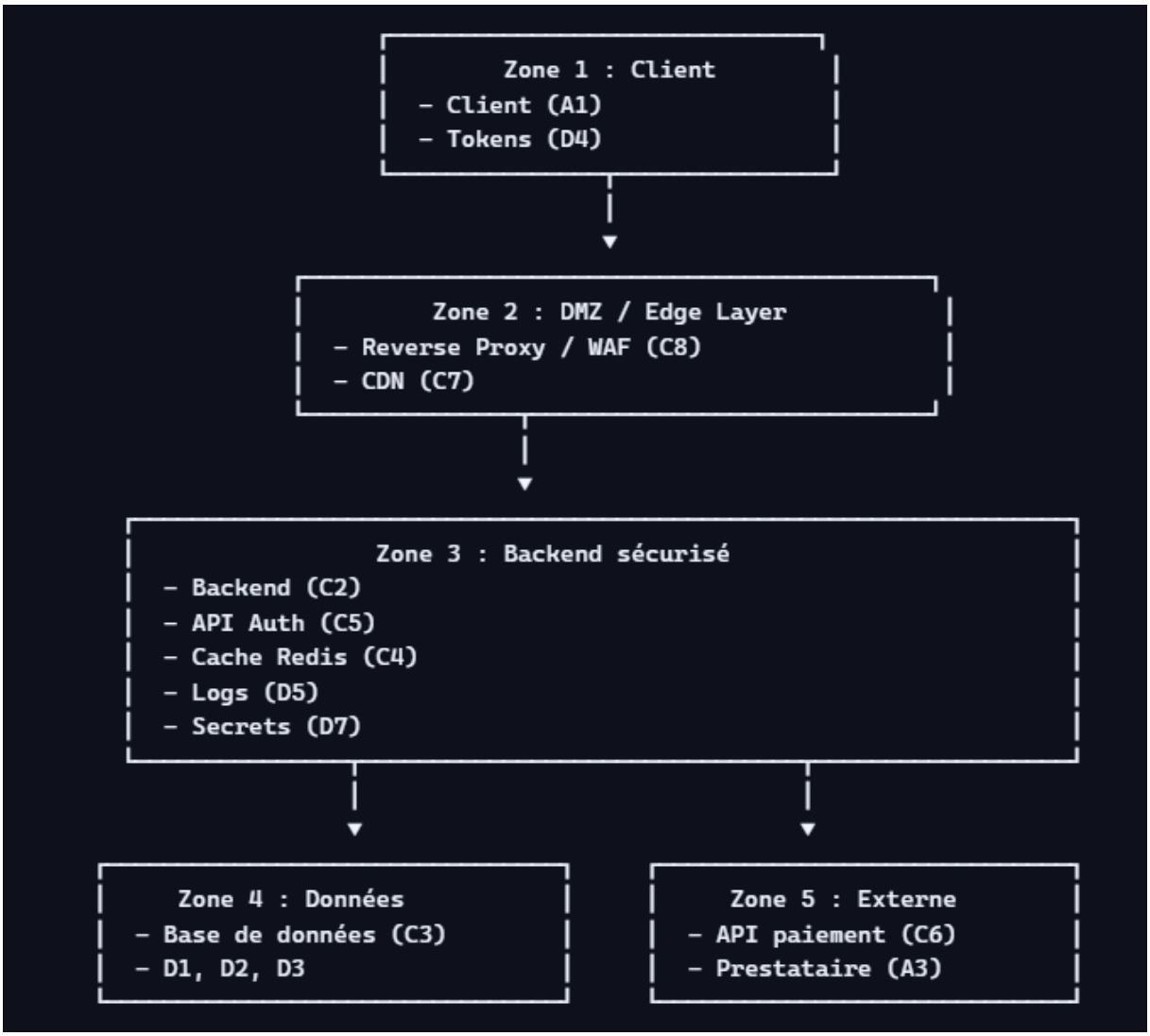

Schéma des flux

```
Client → (F1 Auth) → WAF → API Auth → DB
Client → (F5 Catalogue) → WAF → Backend → DB
Client → (F3 Panier) → WAF → Backend → Redis
Client → (F2 Paiement) → Backend → Prestataire paiement
Admin → (F6 Admin) → WAF → Backend → DB
Backend → (F7 Logs) → SIEM
```

Analyse STRIDE complète

Rappel STRIDE :

Lettre	Menace
S	Spoofing (usurpation d’identité)
T	Tampering (altération de données)
R	Repudiation (déni d’action)
I	Information Disclosure (divulgation)
D	Denial of Service (indisponibilité)
E	Elevation of Privilege (élévation de privilèges)

Tableau STRIDE A compléter

Actif / Flux	S	T	R	I	D	E

Légende du tableau STRIDE

S — Spoofing

Usurpation d'identité (vol de token, credential stuffing, session hijacking).

T — Tampering

Modification non autorisée de données ou de requêtes (ex : altération d'un montant).

R — Repudiation

Capacité d'un attaquant à nier une action (ex : absence de logs fiables).

I — Information Disclosure

Divulgation d'informations sensibles (PII, tokens, logs).

D — Denial of Service

Indisponibilité du service (saturation API, blocage DB).

E — Elevation of Privilege

Obtention de privilèges supérieurs (ex : accès admin).

1. Appliquer STRIDE à un système réel

Identifier et classifier les menaces selon les six catégories STRIDE, en tenant compte du contexte technique et métier de ShopNow. Faites moi en plus un schéma pour montrer plus explicitement quelle catégorie touche quels actifs.

2. Identifier les menaces pertinentes pour chaque actif

Analyser les actifs critiques (données, flux, composants, acteurs) et déterminer les menaces spécifiques qui les concernent.

3. Comprendre et qualifier les impacts potentiels

Évaluer les conséquences **techniques** (exploitation, propagation, compromission) et **métier** (fraude, RGPD, perte de revenus) de chaque menace.

4. Prioriser les menaces selon leur gravité

Hiérarchiser les menaces en fonction :

- de leur impact métier,
- de leur exploitabilité,

- de leur exposition,
- des dépendances externes,
- et du contexte opérationnel.

5. Préparer la dérivation d'exigences de sécurité (Exercice 3)

Transformer les menaces identifiées en exigences de sécurité concrètes, mesurables et intégrables dans un backlog Agile.

6. Raisonner comme un architecte sécurité

Adopter une vision systémique : interdépendances, propagation des risques, zones de confiance, flux sensibles, points d'entrée critiques.

7. Discuter les limites de STRIDE et ses compléments

Comprendre que STRIDE :

- ne couvre pas la probabilité,
- ne remplace pas une analyse de risques,
- doit être complété par des **abuse cases**, **MITRE ATT&CK**, ou une **analyse métier**.