EXERCICE 1 — Identifier les actifs critiques

Contexte complet : Plateforme e-commerce "ShopNow"

Tu es consultant cybersécurité pour **ShopNow**, une entreprise qui exploite une plateforme de e-commerce. L'entreprise prépare une refonte de son architecture pour :

- améliorer la performance,
- renforcer la sécurité,
- intégrer un nouveau prestataire de paiement,
- se mettre en conformité RGPD.

ShopNow a déjà subi :

- des attaques de bots saturant l'API catalogue,
- des tentatives de credential stuffing,
- des erreurs de configuration exposant des logs sensibles.

Le CTO te demande de réaliser un **Threat Modeling complet**, en commençant par **la cartographie des actifs**.

Objectif de l'exercice

Identifier **tous les actifs** du système, les organiser, les décrire, et évaluer leur **criticité** pour préparer :

- STRIDE
- les exigences de sécurité
- l'architecture Zero Trust
- les tests de sécurité

A. Données

ID	Actif
D1	Données clients (PII)
D2	Données de commandes
D3	Données produits
D4	Tokens d'authentification (JWT, refresh)
D5	Logs applicatifs
D6	Données de paiement (références transactionnelles)
D7	Secrets / clés API / variables d'environnement

B. Composants techniques

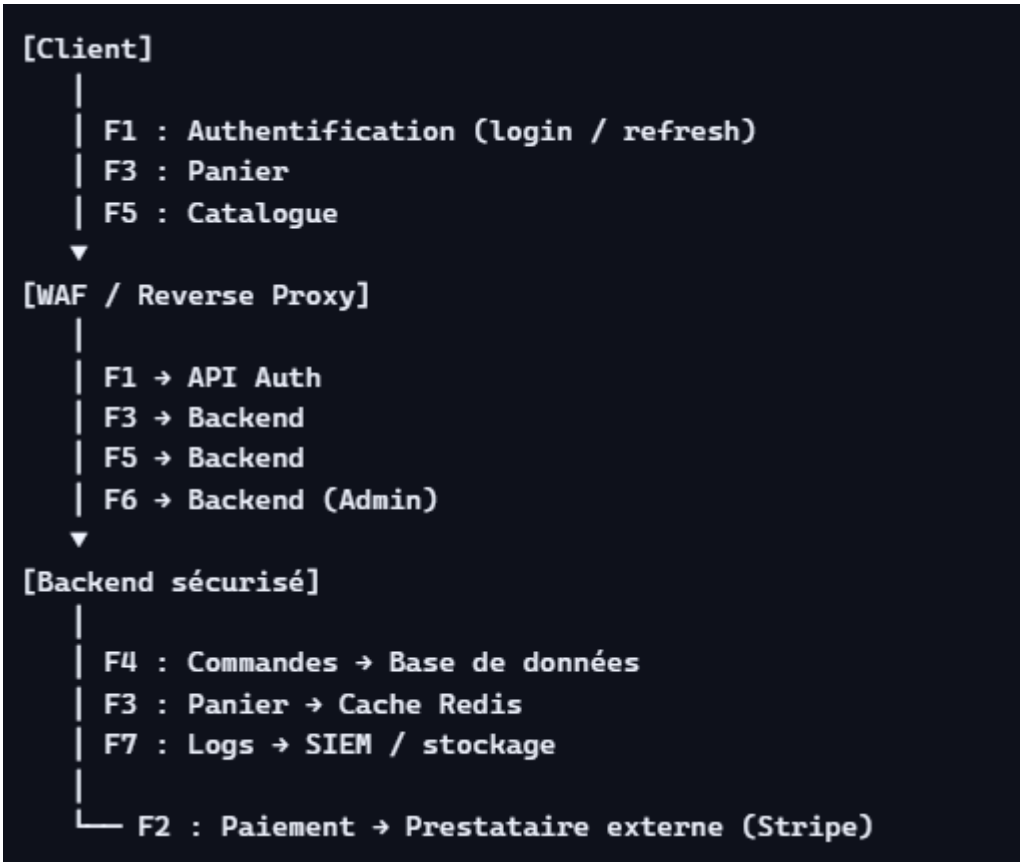
ID Actif

C1 Front-end Web (React)
C2 Backend / API Node.js
C3 Base de données PostgreSQL
C4 Cache Redis
C5 API d'authentification
C6 API de paiement externe (Stripe)
C7 CDN / serveur de fichiers
C8 Reverse proxy / WAF

C. Flux

ID	Flux
F1	Flux d'authentification
F2	Flux de paiement
F3	Flux panier
F4	Flux commandes
F5	Flux catalogue
F6	Flux administrateur
F7	Flux logs

Schéma des flux



Légende des flux

Flux	Description
F1	Authentification (login, refresh, logout)
F2	Paiement (création transaction, validation)
F3	Panier (ajout, suppression, mise à jour)
F4	Commandes (création, mise à jour, consultation)
F5	Catalogue (liste produits, détails)
F6	Administration (gestion produits, stocks)
F7	Logs (envoi vers SIEM ou stockage interne)

D. Acteurs

ID	Acteur
A1	Client
A2	Administrateur
A3	Prestataire de paiement
A4	Services internes (cron, batch)

2. Cartographie par zones (Security Zones)

Zone 1 — Client / Navigateur

- A1 Client
- C1 Front-end
- D4 Tokens

Risques : XSS, vol de tokens, manipulation du DOM.

Zone 2 — DMZ / Edge

- C8 Reverse proxy / WAF
- C7 CDN

Rôle :

- Terminaison TLS
- Filtrage
- Rate limiting

Zone 3 — Backend sécurisé

- C2 Backend
- C5 API Auth

- C4 Cache
- D5 Logs
- D7 Secrets

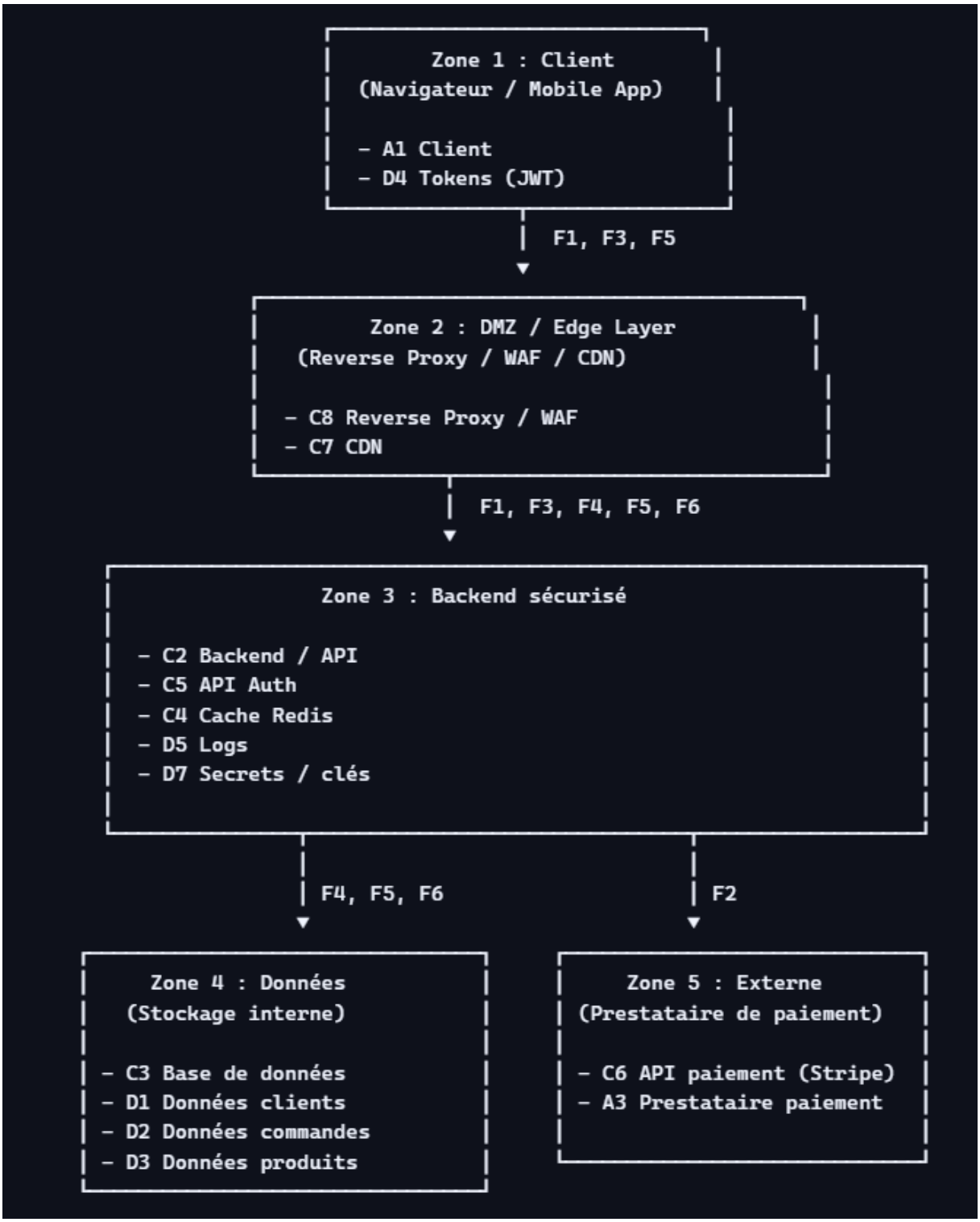
Zone 4 — Données

- C3 Base de données
- D1 Données clients
- D2 Données commandes
- D3 Données produits

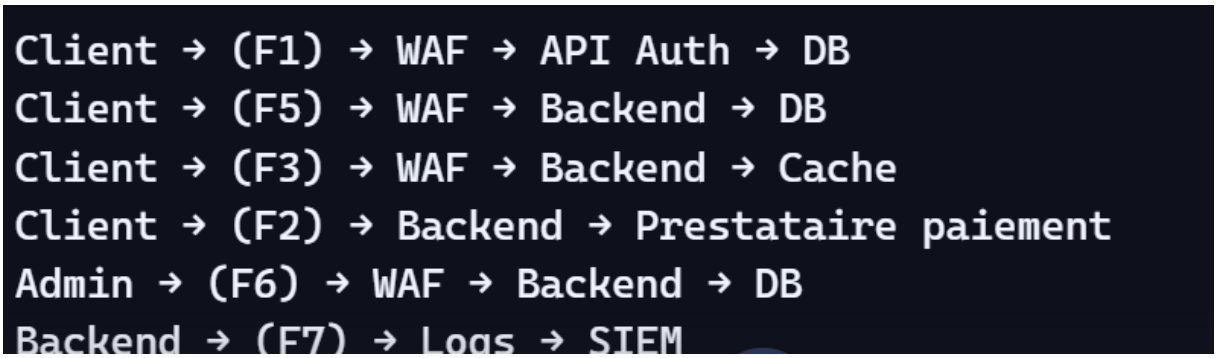
Zone 5 — Externe

- C6 API de paiement
- A3 Prestataire paiement

Schéma des zones


Zone 1 : Client
(Navigateur / Mobile App)
- A1 Client
- D4 Tokens (JWT)
F1, F3, F5
Zone 2 : DMZ / Edge Layer
(Reverse Proxy / WAF / CDN)
- C8 Reverse Proxy / WAF
- C7 CDN
F1, F3, F4, F5, F6
Zone 3 : Backend sécurisé
- C2 Backend / API
- C5 API Auth
- C4 Cache Redis
- D5 Logs
- D7 Secrets / clés
F4, F5, F6
F2
Zone 4 : Données
(Stockage interne)
- C3 Base de données
- D1 Données clients
- D2 Données commandes
- D3 Données produits
Zone 5 : Externe
(Prestataire de paiement)
- C6 API paiement (Stripe)
- A3 Prestataire paiement

3. Cartographie des flux



4. Tableau complet d'analyse de criticité

Actif	Description	C	I	D	Impact métier	Criticité finale
Données clients	PII : nom, email, adresse	Élevée	Élevée	Moyenne	Très fort (RGPD, réputation)	Très élevée
Données commandes	Historique, montants	Moyenne	Élevée	Moyenne	Fort	Élevée
Données produits	Catalogue, prix	Faible	Moyenne	Moyenne	Moyen	Moyenne
Tokens auth	JWT, refresh	Élevée	Élevée	Faible	Très fort (usurpation)	Très élevée
Logs applicatifs	Traces techniques	Moyenne	Moyenne	Moyenne	Moyen	Moyenne
Données paiement	Références transactionnelles	Élevée	Élevée	Élevée	Très fort	Très élevée
Secrets / clés	Clés API, secrets	Élevée	Élevée	Moyenne	Très fort	Très élevée
Front-end	Interface utilisateur	Faible	Moyenne	Élevée	Moyen	Moyenne
Backend	Logique métier	Moyenne	Élevée	Élevée	Fort	Élevée
Base de données	Stockage central	Élevée	Élevée	Élevée	Très fort	Très élevée
Cache Redis	Sessions, paniers	Moyenne	Moyenne	Élevée	Moyen	Moyenne
API Auth	Login, tokens	Élevée	Élevée	Moyenne	Très fort	Très élevée
API paiement	Stripe	Élevée	Élevée	Élevée	Très fort	Très élevée

Flux paiement	Transactions	Élevée	Élevée	Élevée	Très fort	Très élevée
Flux auth	Login / refresh	Élevée	Élevée	Moyenne	Très fort	Très élevée
Administrateurs	Accès privilégiés	Élevée	Élevée	Élevée	Très fort	Très élevée

Légende du tableau d'analyse de criticité

Le tableau utilise plusieurs colonnes pour évaluer la sensibilité et l'importance de chaque actif. Voici la signification précise de chaque élément.

1. C — Confidentialité

Niveau de sensibilité des données si elles sont divulguées.

- **Faible** : données publiques ou non sensibles
- **Moyenne** : données internes, non critiques
- **Élevée** : données personnelles, financières, secrets, tokens

2. I — Intégrité

Importance de garantir que l'actif ne soit pas altéré.

- **Faible** : modification sans impact majeur
- **Moyenne** : modification gênante mais non critique
- **Élevée** : modification pouvant causer fraude, pertes financières, litiges

3. D — Disponibilité

Importance que l'actif soit accessible et opérationnel.

- **Faible** : interruption tolérable
- **Moyenne** : interruption gênante mais non bloquante
- **Élevée** : interruption critique (perte de revenus, arrêt du service)

4. Impact métier

Conséquence directe pour l'entreprise en cas de compromission.

- **Faible** : impact limité, facilement récupérable
- **Moyen** : perturbation notable, coûts modérés
- **Fort** : impact opérationnel important, pertes financières
- **Très fort** : atteinte à la réputation, sanctions légales, perte de clients

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.

- ✓ **Quels sont les actifs informationnels réellement sensibles ?** (PII, secrets, tokens, données financières…)
- ✓ **Quels composants techniques sont critiques pour la sécurité ?** (auth, DB, cache, WAF…)
- ✓ **Quels flux transportent des données sensibles ?** (auth, paiement, commandes…)
- ✓ **Quelles zones de sécurité doivent être isolées ?** (DMZ, backend, data…)
- ✓ **Quels acteurs ont des privilèges élevés ?** (admin, prestataire…)
- ✓ **Quels actifs, s'ils sont compromis, provoquent un impact métier majeur ?**
- ✓ **Quels actifs doivent être protégés en priorité dans une stratégie Zero Trust**
- ✓ **Comment la criticité d'un actif évolue-t-elle lorsqu'il est combiné à d'autres actifs dans un flux métier ?**
- ✓ **Quels actifs pourraient devenir critiques dans le futur en fonction de l'évolution du système (scalabilité, nouvelles fonctionnalités, nouvelles menaces) ?**

Glossaire complet — Exercice 1 (Security by Design / Threat Modeling)

A — Concepts de sécurité

Confidentialité (C)

Propriété garantissant que seules les personnes autorisées peuvent accéder à une information. Exemple : données clients, tokens, secrets.

Intégrité (I)

Propriété garantissant que les données ne peuvent pas être modifiées de manière non autorisée. Exemple : modification frauduleuse d'un prix.

Disponibilité (D)

Propriété garantissant que les services et données sont accessibles lorsqu'ils sont nécessaires. Exemple : API indisponible → perte de ventes.

Impact métier

Conséquence directe pour l'entreprise en cas de compromission d'un actif (financier, légal, réputationnel).

Criticité

Niveau global de risque associé à un actif, basé sur C/I/D + impact métier.

B — Architecture & zones

Zone de sécurité

Segment logique ou physique du système isolé pour limiter les risques. Exemples : DMZ, backend sécurisé, zone données.

DMZ (Demilitarized Zone)

Zone intermédiaire entre Internet et le réseau interne, contenant les composants exposés (WAF, reverse proxy).

Backend sécurisé

Zone interne contenant la logique métier, les API, les services sensibles.

Base de données

Zone contenant les données persistantes (clients, commandes, produits).

Zone externe

Services tiers critiques (ex : prestataire de paiement).

C — Composants techniques

Front-end

Interface utilisateur (navigateur, application mobile). Exemple : React, Angular.

Backend / API

Serveur exécutant la logique métier et exposant des endpoints REST/GraphQL.

API d'authentification

Service gérant l'identification, les tokens, les permissions.

Base de données (DB)

Système de stockage structuré (PostgreSQL, MySQL).

Cache (Redis)

Stockage rapide pour sessions, paniers, tokens temporaires.

CDN (Content Delivery Network)

Réseau distribué servant les fichiers statiques (images, JS, CSS).

Reverse Proxy

Serveur intermédiaire filtrant et redirigeant les requêtes vers le backend.

WAF (Web Application Firewall)

Pare-feu applicatif filtrant les attaques web (SQLi, XSS, bots).

API de paiement

Service externe gérant les transactions (Stripe, PayPal).

D — Flux

Flux d'authentification

Échanges liés au login, refresh token, logout.

Flux de paiement

Échanges entre le backend et le prestataire de paiement.

Flux panier

Ajout, suppression, modification d'articles.

Flux catalogue

Consultation des produits.

Flux administrateur

Gestion interne (stocks, promotions, produits).

Flux logs

Transmission des journaux vers un SIEM ou stockage interne.

E — Acteurs

Client

Utilisateur final de la plateforme e-commerce.

Administrateur

Utilisateur interne avec privilèges élevés (gestion du catalogue, commandes).

Prestataire de paiement

Service tiers traitant les transactions financières.

Services internes

Tâches automatisées (cron, batchs, workers).

F — Données sensibles

PII (Personally Identifiable Information)

Données permettant d'identifier une personne (nom, email, adresse).

Tokens d'authentification (JWT)

Jetons permettant d'authentifier un utilisateur sans stocker de session côté serveur.

Secrets / clés API

Informations sensibles permettant d'accéder à des services internes ou externes.

Logs applicatifs

Traces techniques pouvant contenir des informations sensibles.

G — Concepts cybersécurité avancés

Security by Design

Approche consistant à intégrer la sécurité dès la conception du système.

Threat Modeling

Méthode d'analyse permettant d'identifier les menaces, vulnérabilités et risques.

Zero Trust

Modèle de sécurité basé sur le principe : *ne jamais faire confiance, toujours vérifier*.

Credential Stuffing

Attaque consistant à tester automatiquement des couples email/mot de passe volés.

Botnet

Réseau de machines automatisées pouvant saturer un service.