12/02/2026

Exercice 6

Rapport

COUPEAU Laurent
XXXXXXXXXXXX

Table des matières

Aucune entrée de table des matières n'a été trouvée.

1. Introduction

This report presents a complete **incident detection and response strategy** for the ShopNow ecommerce platform. It builds directly on:

- **Exercise 1:** Asset inventory
- **Exercise 2:** STRIDE threat analysis
- **Exercise 3:** Security requirements
- **Exercise 4:** Zero Trust architecture

ShopNow wants to evolve from a purely preventive posture to a **defendable and observable** security model. This requires:

- logging the right events,
- detecting anomalies quickly,
- responding with structured playbooks,
- and aligning detection with Zero Trust principles.

This report includes:

1. A mapping of **critical assets → security events to log**
2. A set of **SIEM correlation rules**
3. **Three complete incident response playbooks**
4. An explanation of how detection reinforces Zero Trust
5. KPIs and strategies to avoid alert fatigue

2. Security Event Mapping (Logging Strategy)

The table below identifies **what must be logged**, **why**, and **how it relates to STRIDE**.

Logging must be:

- **centralized**,
- **timestamped**,
- **signed**,
- **immutable**,
- and **sent to the SIEM**.

2.1 Event Mapping Table

Asset	**Event to Log**	**Concrete Example**	**STRIDE Threat**	**Log Criticality**
D1 – Customer Data	Read/write operations, exports	Admin exports customer list	Information Disclosure	**High**
D2 – Orders Data	Order creation/update/delete	Order amount modified	Tampering / Repudiation	**High**
D4 – Tokens	Token creation, refresh, invalidation	Same token used twice	Spoofing	**High**
D6 – Payment Data	Payment attempts, failures, anomalies	Payment > 3× average	Tampering / Fraud	**High**
C2 – Backend	4xx/5xx spikes, admin endpoint access	Sudden 500 errors	DoS / Tampering	**High**
C3 – Database	Privileged queries, schema changes	Superuser login	Elevation / Info Disclosure	**High**
C5 – Auth API	Login, logout, MFA, failures	20 failed logins/min	Spoofing	**High**
F1 – Auth Flow	Login attempts, token refresh	Token refresh from new IP	Spoofing	**High**
F2 – Payment Flow	Payment anomalies	Repeated failed payments	Tampering / DoS	**High**
F4 – Orders Flow	Order creation/update	Order modified after payment	Tampering	**High**
A2 – Admin	Admin login, role changes, sensitive actions	Admin login from new country	Elevation / Spoofing	**High**

Justification: All these assets are **critical** (Exercises 1–3). Their compromise leads to **fraud, GDPR violations, revenue loss, or full system compromise**.

3. SIEM Alerting Rules

Below are **8+ SIEM rules**, each with:

- trigger condition,
- STRIDE threat,
- business impact,
- alert priority.

These rules must be implemented in the SIEM to detect attacks early.

3.1 SIEM Rules Table

Rule	Trigger Condition	STRIDE Threat	Business Impact	Priority
R1 – Credential Stuffing	>10 failed logins/min on C5	Spoofing	Account takeover	**High**
R2 – Token Anomaly	Same token used from 2 countries in <1h	Spoofing	Session hijacking	**High**
R3 – Payment Fraud Pattern	Payment amount >3× user average	Tampering	Financial loss	**High**
R4 – API Error Spike	500 errors > threshold on C2	DoS	Service outage	**High**
R5 – Admin Login Anomaly	Admin login from unusual IP/country	Spoofing / Elevation	Full system compromise	**High**
R6 – DB Superuser Access	Superuser login outside maintenance window	Elevation	DB compromise	**High**

R7 – Mass Data Export	Large export of D1 or D2	Information Disclosure	GDPR breach	**High**
R8 – Repeated Payment Failures	>5 failed payments/min	DoS / Fraud	Revenue loss	**Medium**
R9 – Suspicious Order Activity	Order modified after payment	Tampering	Fraud	**High**
R10 – WAF Blocking Spike	Sudden increase in blocked requests	DoS / Recon	Attack in progress	**Medium**

4. Incident Response Playbooks

Each playbook follows the required structure:

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

4.1 Playbook 1 — Token Compromise (D4 / F1)

Detection

- SIEM triggers R2 (token used from two countries)
- Unusual login patterns detected
- User reports suspicious activity

Containment

- Immediately revoke affected tokens
- Force logout of the user
- Block suspicious IP addresses
- Require MFA re-authentication

Eradication

- Identify root cause:
    - XSS?
    - Phishing?
    - Malware?
- Patch vulnerabilities
- Reset user password

Recovery

- Issue new tokens
- Restore normal access
- Monitor account for 48 hours

Lessons Learned

- Improve token protection (HttpOnly, Secure, SameSite)
- Strengthen anomaly detection
- Update WAF rules

4.2 Playbook 2 — Suspected Customer Data Leak (D1)

Detection

- SIEM triggers R7 (mass export)
- Unusual DB queries detected
- External report of leaked data

Containment

- Isolate affected systems
- Disable compromised accounts
- Block suspicious IPs
- Freeze DB access except for security team

Eradication

- Identify breach vector
- Patch vulnerabilities
- Remove malicious access

- Rotate secrets and DB credentials

Recovery

- Restore DB integrity
- Notify DPO (GDPR requirement)
- Notify affected users if required
- Resume normal operations

Lessons Learned

- Improve DB access controls
- Enhance log monitoring
- Review data minimization practices

4.3 Playbook 3 — DoS Attack on C2/C5

Detection

- SIEM triggers R4 (API error spike)
- WAF detects abnormal traffic
- Increased latency and timeouts

Containment

- Activate stricter rate limiting
- Enable WAF emergency rules
- Block malicious IP ranges
- Scale infrastructure if possible

Eradication

- Identify attack source
- Apply long-term IP blocking
- Patch vulnerabilities exploited

Recovery

- Gradually relax rate limits
- Monitor traffic stability
- Restore normal service levels

Lessons Learned

- Improve DoS resilience
- Add caching layers
- Enhance monitoring thresholds

5. Alignment with Zero Trust

Detection and response reinforce Zero Trust in several ways:

5.1 Continuous Verification

- SIEM alerts validate identity continuously
- Token anomalies trigger re-authentication
- Admin anomalies trigger MFA challenges

5.2 Least Privilege Enforcement

- Alerts detect privilege misuse
- Playbooks restrict access during incidents

5.3 Microsegmentation

- Containment isolates compromised zones
- Prevents lateral movement

5.4 Dynamic Policies

- Block IPs dynamically
- Increase rate limiting during attacks
- Require MFA after suspicious events

5.5 Full Visibility

- Immutable logs
- Real-time monitoring
- Correlation across all zones

Zero Trust is not only preventive—it is **reactive and adaptive**.

6. KPIs for Detection & Response

To measure effectiveness:

Detection KPIs

- **MTTD (Mean Time To Detect)**
- % of incidents detected automatically
- Number of false positives
- Number of false negatives

Response KPIs

- **MTTR (Mean Time To Respond)**
- Time to contain incident
- Time to revoke compromised tokens
- Time to block malicious IPs

Operational KPIs

- % of logs ingested into SIEM
- % of critical assets monitored
- Alert fatigue index (alerts per analyst per hour)

7. Avoiding Alert Fatigue

Alert fatigue is a major risk. To avoid it:

7.1 Prioritize Alerts

- High-impact alerts must be few and actionable
- Medium/low alerts must be aggregated

7.2 Tune Rules

- Reduce noise
- Adjust thresholds
- Use behavioral baselines

7.3 Group Alerts into Incidents

- Multiple failed logins → one "credential stuffing" incident

- Multiple payment failures → one “payment anomaly” incident

7.4 Automate Responses

- Auto-block IPs
- Auto-revoke tokens
- Auto-trigger MFA

8. Conclusion

This incident detection and response plan ensures that:

- ShopNow can detect attacks early
- Incidents are handled consistently and efficiently
- Zero Trust principles are enforced dynamically
- Sensitive assets (D1, D2, D4, D6) are protected
- Critical components (C2, C3, C5) are monitored
- Sensitive flows (F1, F2, F4) are supervised

This plan transforms ShopNow into a **defendable, observable, and resilient** platform.