GROWNET — Security Threat Model

(Asset Protection & Business Continuity Focused)

---

1. Purpose & Security Objectives

هدف این سند:

حفاظت از **داده، درآمد، اعتبار برند، و تداوم کسب‌وکار**

امنیت ضعیف=

- ریسک حقوقی / GDPR) قراردادها(
- ریسک برند (از دست رفتن اعتماد)
- ریسک توقف کسب‌وکار(downtime / ransomware)

---

2. Assets & Data Classification

2.1 Critical Assets

Asset	Sensitivity
User data	High
Campaign & ranking logic	High
Payment data	Very High
API keys & secrets	Critical
ML / algorithm logic	High

2.2 Data Classification

Class	Examples
Public	Landing pages
Internal	Metrics, configs
Confidential	User profiles
Restricted	Auth tokens, keys

اصل Least Privilege + Need-to-Know :

---

3. Threat Actors (Who Attacks Us?)

Actor	Motivation
Opportunistic attacker	Easy money
Competitor	IP theft
Malicious insider	Privilege abuse
Script kiddie	Misconfiguration
Automated bots	Credential stuffing

---

4. Attack Surface Overview

Entry Points

- Web frontend
- Public APIs
- Admin panel
- CI/CD pipelines
- Cloud infrastructure
- Third-party integrations

هر feature جدید = افزایش سطح حمله

---

5. Threat Modeling Methodology

We use a **STRIDE-inspired approach**:

Threat	Meaning
S	Spoofing
T	Tampering
R	Repudiation
I	Information Disclosure
D	Denial of Service
E	Elevation of Privilege

---

6. Key Threat Scenarios

6.1 Authentication Attacks

- Credential stuffing
- Token reuse
- Session hijacking

Controls

- MFA (admin)
- Rate limiting
- Secure cookie flags
- Token rotation

6.2 Authorization Failures

- Horizontal privilege escalation
- Admin access misuse

Controls

- RBAC
- Policy-based authorization
- Authorization tests

6.3 Data Leakage

- Misconfigured storage
- Over-permissive APIs

Controls

- Encryption at rest
- Field-level access control
- Data minimization

6.4 Payment & Billing Abuse

- Fake transactions
- Refund manipulation

Controls

- External PSP isolation
- Idempotent payment APIs

- Audit logs

6.5 Infrastructure Attacks

- DDoS
- Cloud misconfiguration

Controls

- Network segmentation
- Managed firewall
- Rate limiting

---

7. Cryptography & Key Management

Encryption

Layer	Method
Data at rest	AES-256
Data in transit	TLS 1.2+

Key Management

- Centralized KMS
- No hardcoded secrets
- Rotation policy every 90 days

Keys are **assets**, not config.

---

8. Identity & Access Management (IAM)

Principles

- Least privilege
- Zero-trust mindset
- Explicit access grants

Controls

- Role-based access
- Separate prod/non-prod access
- Time-limited elevated access

---

9. Secure Development Practices

- Static code analysis
- Dependency vulnerability scans
- Secret detection in CI
- Security review for risky features

Security debt = compound interest

---

10. Logging, Monitoring & Alerting

What We Log

- Auth events
- Privilege changes
- Data exports
- Payment actions

Monitoring

- Anomaly detection
- Failed login spikes
- Access pattern deviations

---

11. Incident Response Plan

Incident Types

- Data breach
- Account compromise
- Service outage
- Insider misuse

Response Phases

1. Detect
2. Contain
3. Eradicate
4. Recover
5. Post-mortem

MTTR < 24h for critical incidents

---

12. Legal & Compliance Considerations

- GDPR readiness
- Data retention policy
- Breach notification procedures
- Vendor security requirements

---

13. Third-Party & Vendor Risk

Vendor Controls

- Minimal scopes
- Contractual security clauses
- Periodic review

Vendor breach = your breach

---

14. Security Metrics (Board-Level)

Metric	Target
Security incidents	0 critical
Mean detection time	<1h
Mean recovery time	<24h
Open critical vulns	0

---

15. Security Roadmap

Phase	Focus
Now	Baseline controls
6 months	Pen-test
12 months	SOC2 prep
Scale	Continuous threat modeling

---

16. Why This Protects Capital

این تیم امنیت را هزینه نمی‌بیند؛
آن را بیمه سرمایه و رشد می‌داند.

ضعف امنیت=
burn rate پنهان
ریسک حقوقی
مرگ اعتماد بازار