

THREATNEXIS · THREAT MODELING & ATTACK

Free Toolkit · v1.0 · June 2025 · threatnexus.co

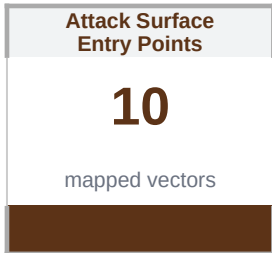
Total Assets Inventoried	Total Threats Identified	Critical / High Risks	Avg Maturity Score
11	10	5	1
assets tracked	threats logged	need immediate action	out of 5.0

HOW TO USE THIS WORKBOOK

1.  **Asset Inventory** List all digital, human, and physical assets. A
2.  **Threat Register** Log threats using STRIDE. Enter Likelihood (
3.  **Attack Surface** Map every entry point for each asset. Note at
4.  **Maturity Scorecard** Rate your current maturity level (0-5) across :
5.  **Risk Heat Map** Auto-generated from your Threat Register. R
6.  **90-Day Roadmap** Prioritized action plan based on your findings

 **PREMIUM TOOLKIT:** Executive dashboard · Board-ready reports · Auto-scoring · I

ATTACK SURFACE ANALYSIS



Assign sensitivity and criticality.
[1-5] and Impact (1-5) — scores auto-calculate
Authentication, encryption, and monitoring status
six key domains. Gaps auto-highlight.
Review and present to leadership.
Assign owners and due dates.

Industry variants · threatnexus.com

ASSET INVENTORY & CLASSIFICATION

Asset ID	Asset Name	Category	Owner	Data Sensitivity
A-001	Customer Portal (Web App)	Application	IT / Dev Team	PII / Financial
A-002	Internal HR System	Application	HR / IT	PII / HR Data
A-003	AWS S3 Buckets	Cloud Storage	DevOps	Internal Docs
A-004	Active Directory / Azure AD	Identity	IT Admin	All Credentials
A-005	Payment Processing API	API	Dev Team	PCI Data
A-006	Employee Laptops (Fleet)	Endpoint	IT	Mixed
A-007	Corporate Email (M365)	SaaS	IT	Confidential
A-008				
A-009				
A-010				

↑ Add more assets above. Asset IDs are referenced in the Threat Register and Attack Surface tabs.

[Phase 01]

Internet Exposed?	Criticality	Notes
Yes	Critical	Public-facing login portal
No	High	Contains employee PII
Yes (partial)	High	Review bucket policies
No	Critical	Core identity infrastructure
Yes	Critical	PCI DSS in scope
Indirect	Medium	Remote workforce
Yes	High	Phishing target

THREAT REGISTER [Phase 04 · STRIDE · NIST SP 800-30]

Threat ID	Threat Description	Asset	STRIDE Category	Likelihood (1-5)	Impact (1-5)	Gross Score (Auto)
T-001	Credential stuffing attack against customer login	A-001	Spoofing	5	4	20
T-002	Privilege escalation via misconfigured IAM role in AWS	A-003	Elevation of Privilege	3	5	15
T-003	Ransomware via phishing email to employee	A-006	Denial of Service	4	5	20
T-004	Exposed S3 bucket leaking customer records	A-003	Info Disclosure	3	5	15
T-005	Supply chain attack via third-party payroll vendor	A-002	Tampering	2	5	10
T-006	Insider threat: privileged admin abuses PII access	A-001	Info Disclosure	2	4	8
T-007	DDoS against public-facing customer portal	A-001	Denial of Service	3	3	9
T-008						
T-009						
T-010						

SP 800-30]

Controls in Place	Residual Risk Rating	Priority (Auto)
limiting (partial), Basic IAM policies	High	1-Critical
filtering	Critical	2-High
None identified	High	1-Critical
Contractual obligations	Critical	2-High
role separation	High	3-Medium
CDN, basic rate limiting	Medium	3-Medium
	Low	3-Medium

ATTACK SURFACE INVENTORY [P

Entry Point ID	Entry Point Name	Asset	Vector Type	Authentication?
EP-001	Login page (HTTPS)	A-001	Web UI	Yes (MFA partial)
EP-002	REST API /v2/auth	A-001	API	JWT Token
EP-003	S3 Bucket (logs)	A-003	Cloud Storage	IAM Role
EP-004	Employee email inbox	A-007	Email / Phishing	Yes (MFA)
EP-005	Admin RDP / VPN	A-004	Remote Access	Yes (VPN + AD)
EP-006	Third-party payroll vendor	A-002	Vendor Access	Federated SSO
EP-007	USB ports (laptops)	A-006	Physical	No
EP-008	Webhook endpoints	A-005	API	HMAC Signature
EP-009				
EP-010				

hase 03]

Encrypted?	Monitored?	Exposure Level
Yes (TLS 1.3)	Partial	Medium
Yes	No	High
Yes (SSE)	No	High
Yes	Partial	High
Yes	No	Critical
Unknown	No	Critical
No	No	Medium
Yes	No	High

THREAT MODELING MATURITY SCORECARD [NIST]

Scale: 0 = Nonexistent | 1 = Initial | 2 = Developing | 3 = Defined | 4 = Managed

Domain	Current Level (0-5)	Target Level (0-5)	Gap (Auto)
Asset Inventory & Classification	2	4	2
Threat Identification (STRIDE / PA	1	3	2
Attack Surface Management	2	4	2
Risk Scoring & Prioritization	1	3	2
Threat Register Maintenance	0	3	3
Executive / Board Reporting	0	3	3

OVERALL AVERAGE MATURITY	1		
--------------------------	---	--	--

CSF / CIS]

| 5 = Optimized

Maturity Label
(Auto)

2 — Developing

1 — Initial

2 — Developing

1 — Initial

0 — Nonexistent

0 — Nonexistent



RISK HEAT MAP (Auto-populated from Threat Register)

↑ Likelihood					
	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
L5	0 threat(s) Score: 5	0 threat(s) Score: 10	0 threat(s) Score: 15	1 threat(s) Score: 20	0 threat(s) Score: 25
L4	0 threat(s) Score: 4	0 threat(s) Score: 8	0 threat(s) Score: 12	0 threat(s) Score: 16	1 threat(s) Score: 20
L3	0 threat(s) Score: 3	0 threat(s) Score: 6	1 threat(s) Score: 9	0 threat(s) Score: 12	2 threat(s) Score: 15
L2	0 threat(s) Score: 2	0 threat(s) Score: 4	0 threat(s) Score: 6	1 threat(s) Score: 8	1 threat(s) Score: 10
L1	0 threat(s) Score: 1	0 threat(s) Score: 2	0 threat(s) Score: 3	0 threat(s) Score: 4	0 threat(s) Score: 5

Legend: Green = Low (1-7) | Yellow = Medium (8-14) | Orange = High (15-19) | Red = Critical

90-DAY REMEDIATION ROADMAP

Task ID	Action Item	Phase	Threat Reference	Owner
R-001	Enable MFA on all critical systems	Days 1-30 · Quick Wins	T-001, T-002	
R-002	Audit and remediate S3 bucket permissions	Days 1-30 · Quick Wins	T-004	
R-003	Deploy email security (DMARC, DKIM, SPF)	Days 1-30 · Quick Wins	T-003	
R-004	Conduct phishing simulation #1	Days 1-30 · Quick Wins	T-003	
R-005	Create initial asset inventory	Days 1-30 · Quick Wins	All	
R-006	Review and audit all admin accounts	Days 1-30 · Quick Wins	T-002	
R-007	Formalize threat register in shared platform	Days 31-60 · Foundation	All	
R-008	Conduct STRIDE analysis on top 10 assets	Days 31-60 · Foundation	All	
R-009	Implement basic SIEM alerting	Days 31-60 · Foundation	T-001, T-004	
R-010	Issue third-party vendor security questionnaires	Days 31-60 · Foundation	T-005	
R-011	Patch management policy rollout	Days 31-60 · Foundation	T-003	
R-012	EDR deployment across endpoints	Days 31-60 · Foundation	T-003	
R-013	First board security briefing	Days 61-90 · Maturity	All	
R-014	Complete attack surface mapping exercise	Days 61-90 · Maturity	All	
R-015	Tabletop ransomware exercise	Days 61-90 · Maturity	T-003	
R-016	Establish quarterly threat modeling cadence	Days 61-90 · Maturity	All	
R-017	IAM policy review and cleanup	Days 61-90 · Maturity	T-002	
R-018	Incident response plan draft	Days 61-90 · Maturity	T-003, T-004	

□ □ □ □ □

[illegible]