Threatnexis · Cybersecurity Consulting

🔴 Free Resource

Threat Modeling & Attack Surface Analysis

A practitioner's guide to identifying, mapping, and prioritizing threats across your organization's attack surface — before adversaries do.

Framework

STRIDE · PASTA · NIST SP 800-30

Type

Reference Guide + Worksheets

Level

Intermediate

Version

1.0 · June 2025

Navigation

Table of Contents

- Phase 4 — Risk Rating & Register

- Risk Heat Map

- Maturity Assessment

- 90-Day Roadmap

- SEO & Resource Metadata

- References & Version History

- Premium Toolkit & Consulting

01 · Overview

Purpose

This document provides a structured methodology for conducting Threat Modeling and Attack Surface Analysis — two of the most high-value, underutilized security practices available to organizations of all sizes.

Whether you are a solo practitioner, an internal security team, or a consultant working with clients, this guide gives you the **why**, the **what**, and enough of the **how** to get started today.

Golden Rule Teach the methodology. Sell the implementation. Consult on the customization. This document earns your trust — the Premium Toolkit saves your time.

02 · Scope

Scope & Definitions

This guide applies to any organization seeking to identify and reduce risk exposure across its digital and physical attack surface.

In Scope

- Web applications, APIs, and mobile apps
- Cloud infrastructure (AWS, Azure, GCP)
- On-premises systems and network perimeter
- Third-party integrations and vendor access points
- Identities, credentials, and privileged access
- Data flows, storage, and transmission paths

Key Definitions

Term	Definition
Threat	Any potential event or action that could cause harm to an asset.
Threat Actor	The individual, group, or automated system capable of executing a threat.
Attack Surface	The total set of entry points through which an attacker could attempt to access or affect a system.
Vulnerability	A weakness in a control, process, or configuration that a threat can exploit.
Risk	The potential for loss expressed as Likelihood × Impact.
Residual Risk	The risk remaining after controls have been applied.
STRIDE	Threat categorization: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
PASTA	Process for Attack Simulation and Threat Analysis — a risk-centric threat modeling methodology.

What is Threat Modeling?

Threat modeling is a structured, proactive approach to identifying security risks *before*

they become incidents. Think of it as a fire drill — but instead of practicing the exit route, you are walking the building looking for where fires are most likely to start and patching those problems in advance.

Why most organizations skip this Threat modeling feels theoretical until something breaks. Then it becomes obvious that five hours of structured analysis upfront would have prevented weeks of incident response. Start before you have to.

The Business Case in Three Sentences

Every hour you spend identifying threats before they are exploited saves you an estimated 30–100× in breach response costs. Clients who see a structured threat model trust you more. Regulators who see a threat model fine you less.

🎯

Proactive vs Reactive

Identify vulnerabilities in design, not after deployment — when they are

exponentially cheaper to fix.

📐

Structured Thinking

Forces teams to think like attackers, systematically and completely, not just based

on intuition.

🗂️

Compliance Evidence

Satisfies requirements in NIST CSF, ISO 27001, SOC 2, HIPAA, and PCI DSS.

💬

Board Communication

Translates technical risk into business language that executives and directors can act on.

04 · Attack Surface

Understanding the Attack Surface

Your attack surface is everything an attacker can touch, probe, send data to, receive data

from, or otherwise interact with. It expands every time you add a new integration, hire a new employee with system access, or deploy a new cloud resource.

Category	Examples	Typical Entry Points	Risk Level
Digital Surface	Web apps, APIs, cloud storage, SaaS tools, databases	Login pages, API endpoints, misconfigured S3 buckets, exposed admin panels	High
Human Surface	Employees, contractors, executives, IT admins	Phishing, vishing, social engineering, credential theft, insider threat	Critical
Physical Surface	Offices, server rooms, workstations, USB ports	Tailgating, removable media, unattended terminals, unsecured hardware	Medium

The Invisible Attack Surface Shadow IT, forgotten cloud accounts, deprecated APIs, and legacy systems that "nobody uses anymore" are consistently among the top breach entry points. You cannot protect what you cannot see.

The Threatnexis Methodology

Threatnexis uses a four-phase approach that blends the best of STRIDE, PASTA, and NIST SP 800-30 into a practical, consultant-ready workflow.

01

Scope & Discover

Define boundaries and inventory all assets

02

Identify Threats

Apply STRIDE to each asset and data flow

03

Map Attack Surface

Document entry points and exposure levels

04

Rate & Prioritize

Score risks and build treatment roadmap

Phase 01 · Scope

Asset Discovery Worksheet FREE

Before you can model threats, you need to know what you are protecting. Use this worksheet to inventory your key assets and assign preliminary classifications.

#	Asset Name	Category	Owner	Data Sensitivity	Internet Exposed	Business Criticality
A-001	Customer Portal (Web App)	Application	IT / Dev Team	PII / Financial	Yes	Critical
A-002	Internal HR System	Application	HR / IT	PII / HR Data	No	High
A-003	AWS S3 Buckets	Cloud Storage	DevOps	Internal Docs	Yes (partial)	High
A-004	Active Directory / Azure AD	Identity	IT Admin	All Credentials	No	Critical
A-005	Payment Processing API	API	Dev	PCI Data	Yes	Critical

#	Asset Name	Category	Owner Team	Data Sensitivity	Internet Exposed	Business Criticality
A-006	Employee Laptops (Fleet)	Endpoint	IT	Mixed	Indirect	Medium
A-007	Corporate Email (M365)	SaaS	IT	Confidential	Yes	High
A-008	[Add your asset]					

Consulting Tip Run this exercise in a 2-hour workshop with IT, operations, and business leaders in the room. You will consistently find 30–50% more assets than IT alone can identify.

Phase 02 · Threat Identification

STRIDE Threat Categories FREE

STRIDE is a threat classification model developed by Microsoft. It gives analysts a

---

consistent lens to apply to every asset, data flow, and trust boundary — ensuring nothing

---

gets overlooked.

STRIDE	Threat Type	Description	Common Example	NIST Mapping
S	Spoofing	Impersonating a user, system, or process to gain unauthorized access	Credential theft, phishing, session hijacking	IA-4, IA-5
T	Tampering	Unauthorized modification of data in transit or at rest	Man-in-the-middle, SQL injection, config change	SI-3, SI-7
R	Repudiation	Denying performance of an action without the ability to prove otherwise	Missing audit logs, unsigned transactions	AU-2, AU-9
I	Info Disclosure	Exposing information to unauthorized parties	Data breach, exposed API keys, unencrypted backups	SC-8, SC-28
D	Denial of Service	Disrupting legitimate access to systems or data	DDoS, ransomware, resource exhaustion	SC-5, CP-10
E	Elevation of Privilege	Gaining capabilities beyond authorized levels	Privilege escalation, misconfigured IAM, sudo abuse	AC-6, CM-6

STRIDE Application Worksheet

Asset	S — Spoofing	T — Tampering	R — Repudiation	I — Info Disc.	D — DoS	E — PrivEsc
Customer Portal	✓ High	✓ Med	✓ Low	✓ Critical	✓ High	✓ High
Azure AD / IAM	✓ Critical	✓ High	✓ Med	✓ High	✓ Low	✓ Critical
Payment API	✓ Critical	✓ Critical	✓ Med	✓ Critical	✓ High	✓ High
Corporate Email	✓ Critical	✓ Low	✓ Med	✓ High	✓ Med	✓ Med
[Your Asset]						

Phase 03 · Attack Surface

Attack Surface Inventory FREE

Entry Point	Asset	Vector Type	Authentication ?	Encrypted ?	Monitored ?	Exposure
Login page (HTTPS)	Customer Portal	Web UI	Yes (MFA partial)	Yes (TLS 1.3)	Partial	Medium
REST API /v2/auth	Customer Portal	API	JWT Token	Yes	No	High
S3 Bucket (logs)	Cloud Storage	Cloud Storage	IAM Role	Yes (SSE)	No	High
Employee	M365 /	Email /	Yes (MFA)	Yes	Partial	High

Entry Point	Asset	Vector Type	Authenticated?	Encrypted?	Monitored?	Exposure
email	Exchange	Phishing				
Admin RDP / VPN	Internal Servers	Remote Access	Yes (VPN + AD)	Yes	No	Critical
Third-party payroll vendor	HR System	Vendor Access	Federated SSO	Unknown	No	Critical
USB ports (laptops)	Endpoints	Physical	No	No	No	Medium
Webhook endpoints	Payment API	API	HMAC Signature	Yes	No	High

Red Flag Pattern Any entry point marked "No" under both Authenticated and Monitored should be treated as an immediate finding — regardless of perceived business impact.

Phase 04 · Risk Rating

Threat Register FREE

Risk Score = Likelihood (1–5) × Impact (1–5) = 1–25. Critical: 20–25 · High: 15–19 · Medium: 8–14 · Low: 1–7.

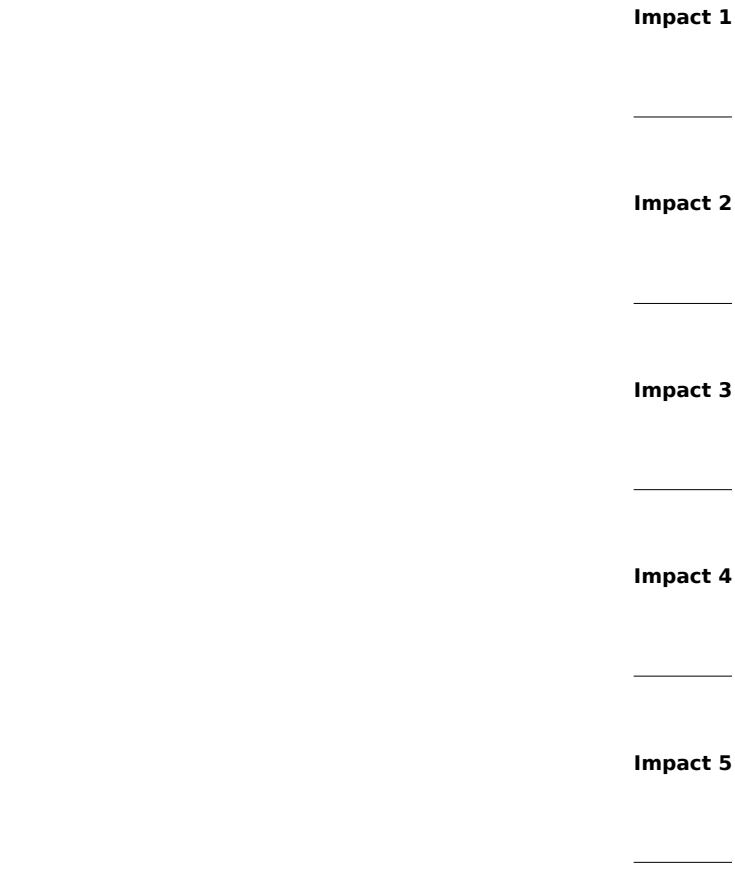
ID	Threat Description	Asset	STRIDE	L	I	Score	Controls in Place	Residual Risk	Priority
T-001	Credential stuffing attack against customer login	Customer Portal	Spoofing	5	4	**20**	Rate limiting (partial), CAPTCHA	High (14)	1
T-002	Privilege escalation via	AWS Cloud	Elevation	3	5	**15**	Basic IAM	Critical	2

ID	Threat Description	Asset	STRIDE	L	I	Score	Controls in Place	Residual Risk	Priority
	misconfigured IAM role in AWS						policies	(18)	
T-003	Ransomware via phishing email to employee	All Endpoints	DoS / Tamper	4	5	**20**	AV, email filtering (partial)	High (16)	1
T-004	Exposed S3 bucket leaking customer records	AWS S3	Info Disclosure	3	5	**15**	None identified	Critical (15)	1
T-005	Supply chain attack via third-party payroll vendor	HR System	Tampering	2	5	**10**	Contractual obligations only	High (10)	3
T-006	Insider threat: privileged admin abuses access to PII	Customer DB	Info Disclosure	2	4	**8**	Role separation (partial)	Medium (6)	4
T-007	DDoS against public-facing customer portal	Customer Portal	DoS	3	3	**9**	CDN, basic rate limiting	Low (4)	5
T-008	[Add your threat]								

Visual Tool

Risk Heat Map FREE

The 5×5 heat map plots threats by Likelihood (Y axis) and Impact (X axis). Threats in the upper-right are highest priority.



10

15

T-001

25

L4

4

8

12

16

T-003

L3

3

T-007

9

T-002

T-004

L2

—

2

—

4

—

6

—

T-006

———

T-005

———

L1

—

1

—

2

_

3

_

4

_

5

_

Low (1–4) Low-Med (5–9) Medium (10–14) High (15–19) Critical (20–25)

Maturity Assessment

_____

Threat Modeling Maturity Scorecard FREE

Scale: 0 = Nonexistent · 1 = Initial · 2 = Developing · 3 = Defined · 4 = Managed · 5 =

Optimized

Asset Inventory & ClassificationLevel 2 — Developing

Threat Identification (STRIDE / PASTA)Level 1 — Initial

Attack Surface ManagementLevel 2 — Developing

Risk Scoring & PrioritizationLevel 1 — Initial

Threat Register MaintenanceLevel 0 — Nonexistent

Executive / Board ReportingLevel 0 — Nonexistent

Roadmap

90-Day Remediation Roadmap

Days 1–30 · Quick Wins

- Enable MFA on all critical systems
- Audit and remediate S3 bucket permissions

- Deploy email security (DMARC, DKIM, SPF)
- Conduct phishing simulation #1
- Create initial asset inventory
- Review all admin accounts

Days 31–60 · Foundation

- Formalize threat register in shared platform
- Conduct STRIDE analysis on top 10 assets
- Implement basic SIEM alerting
- Third-party vendor security questionnaires
- Patch management policy rollout
- EDR deployment across endpoints

Days 61–90 · Maturity

- First board security briefing
- Complete attack surface mapping exercise
- Tabletop ransomware exercise
- Establish quarterly threat modeling cadence
- IAM policy review and cleanup

- Incident response plan draft

SEO & Distribution

Resource Metadata

Primary SEO Details
Primary Keywordthreat modeling framework
SEO TitleThreat Modeling & Attack Surface Analysis: Free Template & Guide (2025)
Meta DescriptionDownload our free threat modeling worksheet and attack surface analysis
template. Includes STRIDE, risk heat map, maturity scoring, and 90-day roadmap.
SEO Slug/threat-modeling-attack-surface-analysis-template
Search IntentInformational → Commercial Investigation
Commercial IntentHigh — readers are actively building or buying threat modeling programs

Secondary Keywords

attack surface analysisSTRIDE threat modelthreat register template

cybersecurity risk assessmentNIST SP 800-30risk heat map template

vCISO threat modelingPASTA methodologyattack surface management

security risk register

People Also Ask / FAQ Seeds

?

What is threat modeling and why does my company need it?

Structured identification of security risks before they become incidents —

answers the "what could go wrong" question proactively.

?

What is the difference between STRIDE and PASTA?

STRIDE categorizes threat types per component; PASTA is an end-to-end risk simulation process. STRIDE is easier to start with; PASTA is more comprehensive.

?

How often should you conduct a threat modeling exercise?

At minimum annually, and every time a major system change, new integration, or significant business change occurs.

?

What does attack surface management involve?

Continuously discovering, classifying, and reducing the set of entry points an attacker could use — digital, human, and physical.

?

How do you present threat modeling results to a board?

Lead with business risk in dollars, not technical findings. Use a heat map, top-5

threats in plain English, and a prioritized action list with budget estimates.

Related Blog Topics (10 Posts)

1. How to Run a Threat Modeling Workshop in 4 Hours
2. STRIDE vs PASTA: Which Threat Model is Right for You?
3. The 10 Most Common Attack Vectors in SMBs (2025)
4. How to Build a Risk Register Your Board Actually Reads
5. Attack Surface Analysis for AWS: A Practitioner's Checklist
6. What is a vCISO and Do You Need One?
7. Ransomware Threat Modeling: A Step-by-Step Guide
8. How to Map Your Organization's Human Attack Surface
9. Third-Party Risk: Your Biggest Attack Surface You're Ignoring
10. From Threat Model to Board Presentation in 5 Steps

Standards & References

Standard	Relevance	Publisher
NIST SP 800-30 Rev.1	Risk assessment methodology and terminology	NIST
NIST CSF 2.0	Identify function — asset management and risk assessment	NIST
STRIDE	Threat categorization model	Microsoft
PASTA	Attack simulation and threat analysis process	VerSprite
ISO/IEC 27005:2022	Information security risk management	ISO
OWASP Threat Modeling	Application-level threat modeling guidance	OWASP Foundation
MITRE ATT&CK	Threat actor tactics, techniques, and procedures	MITRE
CIS Controls v8	Specific security controls mapped to threat categories	CIS

Version History

Version	Date	Author	Changes
1.0	June 2025	Threatnexis	Initial release — methodology, STRIDE, threat

Version	Date	Author	Changes
			register, heat map, maturity scorecard, 90-day roadmap
1.1	Q3 2025 (planned)	—	Add PASTA supplement, cloud-specific attack surface tables, healthcare variant

Need More Than a Template?

The free version teaches the methodology. The Premium Toolkit delivers the implementation — ready for clients, boards, and regulators.

Premium Toolkit

- Executive dashboard with automated scoring
- Full STRIDE + PASTA workbook (Excel)
- Color-coded heat maps (auto-calculated)
- Board-ready PowerPoint template
- Sample findings & recommendations
- Industry-specific versions
- 90-day roadmap with budget estimates

Consulting Services

- Full threat modeling engagement
- Attack surface discovery & mapping
- Gap assessment against NIST / ISO
- Board & executive risk briefings

- Fractional CISO retainer
- Vendor risk management program
- Tabletop exercise facilitation

Insider Community

- Monthly templates & checklists
- Breach analysis breakdowns
- Live Q&A with consultants
- Early access to new resources
- Community risk register library
- Peer consultant network

Unlock the Premium Toolkit → Book a Free Consultation Subscribe Free