

5 THREAT MODELING FRAMEWORKS

EVERY SECURITY ENGINEER
SHOULD KNOW IN **2026-27**



WHY THREAT MODELING?

Fix it in design, not after the breach.



Threat modeling helps you:

-  Find security flaws before code is written
-  Prioritize risks that actually matter
-  Reduce costly late-stage remediation
-  Speak the same language as devs, architects, and the business

The right framework helps you ask the right security questions early.

1. STRIDE

Think Like an Attacker. Threat by Threat.

Focus: Categorizing threats

S | S — Spoofing

T | T — Tampering

R | R — Repudiation

I | I — Information Disclosure

D | D — Denial of Service

E | E — Elevation of Privilege



Best for:

Applications, APIs, and system architectures.



Key Takeaway:

Use STRIDE when you need a structured way to identify common threat types.

2. PASTA

Connect Technical Threats to Business Risk



Focus: Risk-centric, attacker-minded

A seven-stage process that links business objectives to technical threats and real attack simulations.

Best for:

Complex applications, high-risk environments, and business-driven threat analysis.

Key Takeaway:

Use PASTA when you need to connect technical threats to business risk and real attack.

3. LINDDUN

Threat Modelling for Privacy

Focus: Privacy threats

- L** — Linking
- I** — Identifying
- N** — Non-repudiation
- D** — Detecting
- D** — Data Disclosure
- U** — Unawareness / Unintervenability
- N** — Non-compliance



Best for:

Privacy-heavy systems, personal data, and compliance use cases.



Key Takeaway:

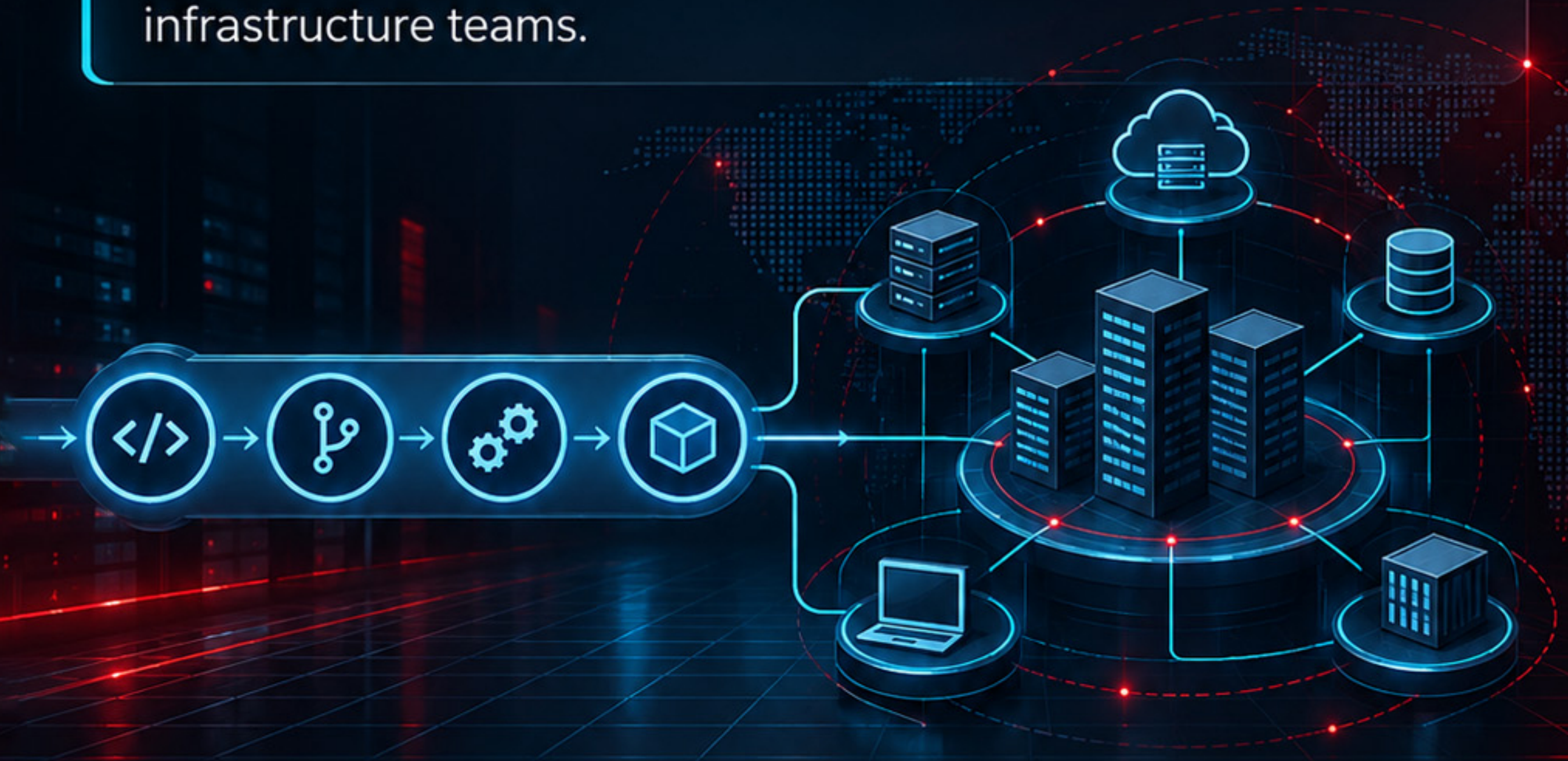
Use LINDDUN when your system handles personal data and privacy is a priority.

4. VAST

Threat Modelling at Enterprise Scale

Focus: Agile, DevOps, and scalable threat modeling

Designed for large organizations, using application and operational threat models to support development and infrastructure teams.



Best for:

Large organizations and scalable security programs.



Key Takeaway:

Use VAST when you need threat modeling that scales across many teams and fast release cycles.

5. TRIKE

Start With Risk. Map the Permissions.

Focus: Risk-based, permission-driven modeling.

Analyzes actors, assets, actions, and permissions to identify where system behavior creates unacceptable risk.



Best for:

Risk-focused security teams, permission-heavy systems, and structured security assessments.

Key Takeaway: Use Trike when you need to evaluate who can do what to which asset, especially in permission-heavy systems.

THREAT MODELING WITH STRIDE

Fast-Track Hands-On Bootcamp

Move from identifying threats to engineering mitigations.



INFOSECTRAIN

Educate. Excel. Empower.



Real Architectures



4 Hands-On Workshops



STRIDE Methodology



17-18 October 2026 | 10 CPEs

~~₹9,999~~

₹4,999 + GST

APPLY STRIDE TO REAL-WORLD ARCHITECTURES >>