Threat modeling .

**Threat modeling provides a structured for informed decision making about risk management.**

1. Assessment scope(software/hardware/process
2. Identify threat agents(adversaries ,contractors , employee, trusted partners
3. Identify possible attacks (data exfiltration, social engineering, spoofing
4. Understanding existing countermeasures
5. Identify exploitable vulnerabilities
6. Prioritize identified risks-Likelihood & Impact
7. Identify countermeasure to reduce threats

Threat modeling is a process by which potential threats, such as [structural vulnerabilities](https://en.wikipedia.org/wiki/Structural_vulnerability_(computing)) can be identified, enumerated, and prioritized

Microsoft provide STRIDE Threat modeling technique

**P.A.S.T.A.**

**The Process for Attack Simulation and Threat Analysis (PASTA) is a seven-step, risk-centric** methodology.[[10]](https://en.wikipedia.org/wiki/Threat_model#cite_note-10) It provides a seven-step process for aligning business objectives and technical requirements, taking into account compliance issues and business analysis. **The intent of the method is to provide a dynamic threat identification, enumeration, and scoring process**. Once the threat model is completed security subject matter experts develop a detailed analysis of the identified threats. Finally, appropriate security controls can be enumerated. **This methodology is intended to provide an attacker-centric view of the application and infrastructure from which defenders can develop an asset-centric mitigation strategy.**

### Trike

**The focus of the Trike methodology is using threat models as a risk-management too**l. Within this framework, threat models are used **to satisfy the security auditing process**. **Threat models are based on a “requirements model**.” The requirements model establishes the stakeholder-defined “acceptable” level of risk assigned to each asset class. Analysis of the requirements model yields a threat model form which threats are enumerated and assigned risk values. The completed threat model is used to construct a risk model based on asset, roles, actions, and calculated risk exposure

### VAST

**VAST is an acronym for Visual, Agile, and Simple Threat modeling. The underlying principle of this methodology is the necessity of scaling the threat modeling process across the infrastructure and entire SDLC, and integrating it seamlessly into an Agile software development methodolog**y. The methodology seeks to provide actionable outputs for the unique needs of various stakeholders: application architects and developers, cybersecurity personnel, and senior executives. The methodology provides a unique application and infrastructure visualization scheme such that the creation and use of threat models do not require specific security subject matter expertise.

## **Generally Accepted IT Threat Modeling Processes**

### Visual Representations based on Data Flow Diagrams -The Microsoft methodology, PASTA, and Trike each develop a visual representation of the application-infrastructure utilizing data flow diagrams

### Visual Representations based on Process Flow Diagrams -The VAST methodology distinguished between application threat models (ATM) and operational or infrastructure threat models

## **Threat Modeling Tools**

### Microsoft’s free threat modeling tool

### MyAppSecurity offers the first commercially available threat modeling tool

### IriusRisk offers both a community and a commercial version of the tool.

### securiCAD is a threat modelling and risk management tool by the Scandinavian company foreseeti

### SD Elements by Security Compass

.