Public whitepaper · Editorial perspective

Frameworks in context

A practical guide to complementary threat modeling

> A practical perspective on choosing complementary threat-modeling methods, adversary knowledge and security requirements - with context, evidence and human judgment at the center.

Start with the decision

A framework becomes useful when it helps a team make a better decision about a real system. Before selecting one, establish what the system is intended to do, whose interests it affects, which information it handles and what decision the analysis must support. A design review, a privacy assessment and a mitigation discussion may need different perspectives.

There is no requirement to treat a single method as the entire security process. Carnegie Mellon University's Software Engineering Institute describes methods with different emphases and explains that complementary approaches can be combined. The practical challenge is to choose a useful combination without losing a clear account of the system, the assumptions and the decisions. [1]

02

Understand what each resource contributes

STRIDE is a structured way to consider categories of security threats, including identity spoofing, data tampering and information disclosure. It helps teams ask security questions about a system model. It does not, by itself, establish the likelihood or business consequence of a particular threat. [2]

PASTA is a risk-centered threat-modeling methodology that connects business objectives, technical scope and analysis of plausible attacks. Its value is the connection between technical concerns and the consequences an organization is trying to manage. [3]

LINDDUN concentrates on privacy threats. This perspective can reveal concerns about how people are identified, how information is linked or disclosed, and whether data practices align with expectations. Security and privacy analyses can share system context while investigating different harms. [4]

Attack trees describe ways an adversary could reach a goal. Breaking a goal into alternative or dependent steps helps a team examine its assumptions and discuss where a defensive measure might interrupt a scenario. [5]

MITRE ATT&CK is an adversary-behavior knowledge base. It offers a shared reference for discussing observed techniques and defensive coverage; it is not a substitute for modeling the organization's own system. [6]

OWASP ASVS supplies application-security requirements that support design, development and verification. Requirements help turn a security intention into something a team can inspect or test. They play a different role from a method used to discover threats. [7]

Choose complementary questions

Begin with the question that matters most: what could undermine this design, what privacy harm could occur, or which business outcome is at risk? Then select a second perspective that addresses a meaningful gap. A collection of framework names is less useful than a clear explanation of what each contributes.

Keep a short record of the scope, chosen approaches, assumptions and evidence still needed. Agree on who will review the findings and what would justify revisiting them. This makes the analysis easier to maintain when architecture, data use or business priorities change.

A hypothetical customer-records example

Consider an application that calls an API to retrieve customer records. The first task is to describe the intended access: which person or service should obtain which records, for what purpose? The team then identifies the relevant identities, data flows and authorization boundaries.

A STRIDE discussion could examine unauthorized disclosure or identity misuse. A privacy review could ask whether the returned information exceeds the stated purpose. An attack tree could explore alternative routes to an unauthorized-access goal. Relevant adversary knowledge can inform the discussion, while application-security requirements help frame what must be verified.

The output should be a reviewable decision, not simply a longer list. For example, the team might propose narrower permissions and targeted authorization checks, identify an accountable owner, and state what evidence would demonstrate that the response is effective. This is an illustrative reasoning exercise, not a claim about a tested product or customer deployment.

Keep human judgment visible

People remain responsible for interpreting evidence, resolving conflicting objectives and accepting residual risk. A useful review makes uncertainty visible and allows a recommendation to be challenged. Record the reason for the decision, its owner and the conditions that should trigger another review. That record connects analysis to responsibility without pretending that a framework can eliminate uncertainty.

The Modelo perspective

Modelo Security's direction brings proprietary research and established industry perspectives into the same security conversation. The emphasis is on understanding systems, examining threats and supporting accountable decisions. This public paper explains that perspective at a conceptual level. It is an editorial guide, not a peer-reviewed study, implementation specification, endorsement by the referenced organizations or claim that every framework is available as a production integration.

References

[1] CMU SEI - Threat Modeling: A Summary of Available Methods (2018) · sei.cmu.edu

[2] Microsoft - Threats: Microsoft Threat Modeling Tool · learn.microsoft.com

[3] VerSprite - PASTA Threat Modeling · versprite.com

[4] KU Leuven - LINDDUN Privacy Threat Modeling · linddun.org

[5] Bruce Schneier - Attack Trees (1999) · schneier.com

[6] MITRE - ATT&CK: Design and Philosophy (2020) · mitre.org

[7] OWASP - Application Security Verification Standard · asvs.owasp.org