SYNOPSYS®

Threat modeling identifies the types of threat agents that cause harm and adopts the perspective of malicious hackers to see how much damage they can do. We look beyond the typical canned list of attacks to think about new attacks or attacks that may not otherwise have been considered.

Threat modeling defines your entire attack surface by identifying

Standard attacks don't always pose a risk to your system. A threat model identifies the attacks that are unique to how your system is built.

Model the location of threat agents, motivations, skills, and capabilities to identify where potential attackers are positioned in relation to your system's architecture.

Create and update your threat models to keep frameworks ahead of internal or external attackers relevant to your applications.

Highlight assets, threat agents, and controls to determine which components attackers are most likely to target.

We recognize that every organization has a different risk profile and tolerance, so we tailor our approach to your needs and budget. Our holistic threat modeling approach consists of two essential steps

1. We review the system's major software components, security controls, assets, and trust boundaries.
2. We then model those threats against your existing countermeasures and evaluate the potential outcomes.