SYNOPSYS®

www.synopsys.com |

Threat Modeling

We bring to light potential weaknesses in the design of your application

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 have otherwise been considered.

Avoid four security sink holes

Threat modeling defines your entire attack surface by identifying:

1. Threats that exist beyond canned attacks

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

2. Where threat agents exist relative to the architecture

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

3. Top-N lists, attackers, and doomsday scenarios

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

4. Components that need additional protection

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

The best way to stop a hacker is to think like one

We adjust to fit your needs

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.

6 benefits of threat modeling

When you're serious about security, threat modeling is the most effective way to:

1. Detect problems early in the SDLC—even before a single line of code is written.
2. Spot design flaws that traditional testing methods and code reviews might overlook.
3. Evaluate new forms of attack that might not otherwise be considered.
4. Maximize your testing budget by helping you target your testing and code review.
5. Identify holes in your requirements process.
6. Save money by remediating problems before releasing software and performing costly code rewrites.

Threat models include:

- Assets prioritized by risk
- Threats prioritized by likelihood
- Attacks most likely to occur
- Current countermeasures likely to succeed or fail
- Remediation measures to reduce the threats

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com