BLACKDUCK®

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 otherwise have been considered.

Four security sink holes to avoid

Threat modeling defines your entire attack surface by identifying

- **Threats that exist beyond canned attacks**
  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.
- **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.
- **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.
- **Components that need additional protection**
  Highlight assets, threat agents, and controls to determine which components attackers are most likely to target.

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.

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

Six benefits of threat modeling

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

- Detect problems early in the SDLC—even before a single line of code is written
- Spot design flaws that traditional testing methods and code reviews might overlook
- Evaluate new forms of attack that might not otherwise be considered
- Maximize your testing budget by helping you target your testing and code review
- Identify holes in your requirements process
- 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

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.