

APPLICATION THREAT MODELING

# Discover threats and vulnerabilities in the architecture of your application to create applications that are “Secure by Design”

Threat modeling is a key **shift-left** activity that shifts application security earlier in the development lifecycle.

Identify threats to your applications prior to application or feature development. Enable your developers to better understand the attack surface and where security controls are needed to counter threats.

A natural evolution of every application security program is to seek ways to shift-left to identify security defects earlier in the software development lifecycle (SDLC). Application threat modeling is a cost-effective way to:

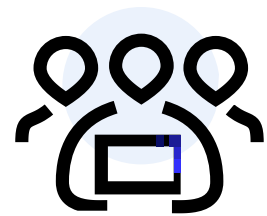
- ✓ Discover and identify design-related flaws and potential threats to your application
- ✓ Design effective compensating security controls to mitigate those threats
- ✓ Provide peace of mind that you have performed your due-diligence to mitigate security risks in your environment

Threat modeling can help your organization to create applications that are secure-by-design, helping you to avoid costly design flaws that are difficult to fix after the application has already been developed.



Our strategic application threat modeling will help you to understand the design of your system, identify possible attack paths, and determine where additional security controls need to be considered to strengthen the design of your application. Our experts will help you answer the four critical questions of threat modeling so that you have confidence in your team’s proactive approach:

1. What are we building?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?



## Put a Highly-Trained, **ELITE** Team on Your Side

More than 70% of our workforce consists of tenured cybersecurity engineers, architects and consultants.

Our highly-certified Application Security consultants have a wealth of experience gained from threat modeling applications across all industries.

## Hundreds of Industry and Product Certifications



# Application Threat Modeling Benefits:



## What's Included in Our Threat Modeling

As part of GuidePoint's threat modeling services, we evaluate applications against industry-leading practices from OWASP, NIST and SANS, and align security threats to the six categories found in Microsoft's STRIDE approach. With our application threat modeling service, you gain a comprehensive assessment that includes:

- ✓ Review of application architecture diagrams and design documents
- ✓ Expert-led whiteboarding sessions with your key stakeholders to identify key data flows and application entry points
- ✓ Review of attack surface and sensitive data flows to identify possible attack paths and threats
- ✓ Validation that your current security controls are appropriate enough to mitigate risk and where it is necessary to build in additional security controls
- ✓ Custom data flow diagrams, attack trees, asset summaries, listing of threat actors, security control summaries, and a prioritized list of possible threats

## Additional Strategic AppSec Services:



### Application Security Program Assessment

- ✓ Holistic review of the AppSec program and strategy
- ✓ Interview and documentation-based review to tailor a strategy to your organization
- ✓ Includes detailed current state, future state, and roadmap of initiatives



### Application Architecture Reviews

- ✓ Uncover design flaws and vulnerabilities prior to writing any code
- ✓ Understand the system architecture and visualize data flows and attack trees
- ✓ Identify security controls that need to be strengthened



### AppSec Training and Learning

- ✓ Hands-on training across any AppSec capability, including penetration testing, threat modeling, and secure coding
- ✓ Instructor led, by industry leaders

## About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.