ThreatModeler®

Threat Modeling Benefits for the CISO and KEY STAKEHOLDERS

IMPACT EVERY ASPECT OF YOUR ORGANIZATION WITH ACTIONABLE SECURITY BENEFITS

Threat Modeling for Cybersecurity ROI

Every member of your team has a stake in making your company successful. CISO and other C-Suite executives set the strategic direction. Security practitioners protect the organization's valuable assets. The DevOps team creates needed functional and secure products. Project managers, architects, and others each have a critical role to play in building a secure organization.

Foster sustainable cybersecurity ROI by developing the three pillars of a **scalable threat modeling practice**. First, security investments must provide a high degree of automation, allowing the tool's outputs to scale across the full IT stack. Second, security tools need to fully integrate with existing toolsets and workflows to enhance productivity without disruption. Finally, the security tool needs to enable cross-functional collaboration to eliminate siloed security efforts.

ThreatModeler is the #1 automated **threat modeling** platform offering sustainable cybersecurity ROI through each of the three key pillars, with proven results across diverse enterprise environments.

Enterprise threat modeling with ThreatModeler will positively impact every aspect of your business while helping the organization reduce risk, improve compliance, and accelerate secure development. Get started by scheduling a **live demo** of our software today.

CISO and other Security Executives

With ThreatModeler, you can:

- Meet application security policy objectives across the organization. Through ThreatModeler's scalable, collaborative, and automated process, the CISO is equipped to lead the organization's adoption and enforcement of consistent security policies, thereby reducing overall risk exposure.
- Map application security policies to security requirements. ThreatModeler's Executive Dashboard and reporting capabilities enable the CISO to drive, track, and measure security initiatives enterprise-wide.
- Integrate with real-world, real-time threat intelligence. Clarify application risk and communicate the potential business impact to executive management should a security breach occur.
- Determine and sustain cyber security ROI. In existing and proposed initiatives, align mitigation strategy with budget allocations and overall business strategy using specific tools and outputs for the CISO.

Directors / Managers

With ThreatModeler, you can:

- Adopt a scalable, repeatable, threat modeling process that integrates with existing workflows and enables collaboration between all stakeholders.
- Leverage dashboards, reports, trends, and checklists to view threats and validate proper security controls are in place.
- Produce a measurable cyber security ROI by employing a framework to develop secure applications from the ground up, reducing the cost of fixing production vulnerabilities.
- Enforce consistency by linking pre-defined security requirements to all re-usable application and system components across the enterprise.

Security Architects / Security Analysts

With ThreatModeler, you can:

- Leverage an automated, scalable, and repeatable threat modeling framework that integrates with existing workflows and processes.
- Assess the effectiveness of security controls and hardening guidelines to meet application security policy requirements and mitigate risk.
- Make security testing more effective by targeting the most critical entry points in applications.
- Measure and communicate penetration test results to executive management and development teams through automatically generated reports.

Project Managers

With ThreatModeler, you can:

- Identify security defects in the architecture to ensure threats are identified up front and help mitigate risks.
- Enforce consistency by linking pre-defined security requirements to all application components.
- Include re-usable code for all components to meet both security requirements and quality standards.
- Keep up-to-date with risk exposure by viewing real-time dashboards that display the current status of security posture across their application portfolio.

Application Architects and Developers

With ThreatModeler, you can:

- Develop applications securely by implementing pre-defined security requirements such as passwords, encryption, session management, cookie handling, input validation, etc.
- Achieve code consistency and reduce attack surface entry points to meet organizational quality standards. Mitigate risk by applying recommended security controls and coding guidelines.
- Use automatically generated abuse cases to increase security awareness and learn how attackers exploit code components to carry out threats.

The ThreatModeler Platform Enables You To:

Establish true cross-functional collaboration
Collaborate between all stakeholders establishing a framework to build secure applications from the ground up.

Understand the relevant threats before deployment
Automated your threat modeling process to keep up with the evolving threat landscape and changing IT environment.

Integrate with existing technologies
Integrate with your existing DevOps, CI/CD pipeline, and IT stack toolsets to make existing security investments more effective.

Enterprise Support
Analyze easy-to-understand dashboards and reporting via a web browser to prioritize and manage risk across all threat-modeled applications.

For more information, support, or inquiries, please contact us at:

support@threatmodeler.com **+1 201 266-0510** **threatmodeler.com**