How ThreatModeler™ Benefits Key Stakeholders

Executives / CISOs

With ThreatModeler™, they're able to**:**

- Meet application security policy objectives by adopting a scalable, repeatable, collaborative, and automated process organization-wide to promote consistency, enforce security requirements, and reduce overall risk exposure.
- Map application security policies to security requirements to drive, track, and measure security initiatives using dashboards, reports, trends, and checklists.
- Integrate with real-world threat intelligence to clarify application risk and communicate the potential business impact to executive management should a security breach occur.
- Calculate costs and prioritize mitigation efforts based upon risk rankings, threat intelligence, reports, dashboards, and metrics to align mitigation strategy with budget allocation.

Directors / Managers

With ThreatModeler™, they're able to**:**

- 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 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™, they're able to**:**

- 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.
- 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.

ThreatModeler | 101 Hudson Street | Jersey City, NJ 07302
Ph: 201-632-3634 |sales@threatmodeler.com | www.threatmodeler.com

Project Managers

With ThreatModeler™, they're able to:

- Identify security defects in the architecture to help ensure threats are mitigated up front.
- 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

Developers

With ThreatModeler™, developers are able to**:**

- 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 the attack surface to meet organizational quality standards, 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.

ThreatModeler | 101 Hudson Street | Jersey City, NJ 07302
Ph: 201-632-3634 |sales@threatmodeler.com | www.threatmodeler.com