ThreatModeler
Identify • Classify • Prioritize • Mitigate

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2017

THREATMODELER™ DATASHEET

Key Features

Centralized Threat Library

Threat Analytics

Abuse Cases

Intelligent Threat Engine

Role-Based Access Control

Real-Time Collaboration

Threat Tracer

Threat Tree / Threat Profiler

Web-Based, Platform-Independent

Comprehensive Bi-directional Web Services API

Key Benefits

Automated Threat Modeling

Scalability

Predictive, Actionable Output

Real-Time Threat Intelligence

Cascading Synchronization of New Threats With Existing Threat Models

Consolidation of Threat Data From Independent Industry Sources and Libraries

Mitigation Recommendations

Perpetual License; No Per-User Limit

ThreatModeler™

ThreatModeler™ is the world's most powerful threat modeling software product. Web-based and platform-independent, it has been designed to fill a critical and growing need among today's information security professionals: to build threat models of their organizations' data, software, hardware, or infrastructure. ThreatModeler™ automates the process of threat modeling, allowing organizations to scale their threat modeling initiatives across hundreds – or even thousands – of threat models.

ThreatModeler's™ interface is easy to master, for security experts and non-experts alike. Users need simply to provide functional information about their applications or systems. ThreatModeler's™ innovative Intelligent Threat Engine (ITE) then automatically analyzes this information and identifies a list of potential threats, ranked by risk; a list of security requirements; and test cases. This information is necessary to the solid foundation of any secure SDLC initiative.

As applications, systems, and infrastructure change – and as new threats are identified – ThreatModeler™ automatically updates its threat models enterprise-wide. The product's scalable design is intended to allow users to build, update, and reuse threat models in a collaborative manner. This forward-looking architecture affords organizations the leverage to scale their initiatives across hundreds – or even thousands – of threat models.

ThreatModeler™ can display threat analytics in multiple ways. It provides a view of threats in a high-level, top-down, enterprise-wide dashboard. ThreatModeler's™ output data can be analyzed all the way down to the individual threat and its source. CISOs and their teams can use this level of detail to identify, classify, prioritize, and mitigate the risks inherent in today's ever-expanding threat landscape.

These and other features make ThreatModeler™ far and away the premier product in the rapidly-maturing field of threat modeling. Representing significant technological advances beyond any other threat modeling product, ThreatModeler™ is the only product of its kind available today.

Centralized Threat Library

ThreatModeler™ compiles and consolidates threat data from well-known industry sources – like CAPEC, WASC-TC, the OWASP Top 10, and others – into a comprehensive centralized threat library. These threats are categorized as to risk under the industry standard risk rating. ThreatModeler™ frequently updates this centralized library, as new threats are identified and published.

ThreatModeler
Identify • Classify • Prioritize • Mitigate

About the Company

ThreatModeler was founded in 2010 to address a critical and growing demand among information security professionals: how to achieve a more proactive approach to building security into applications and systems.

ThreatModeler's flagship product, ThreatModeler™, is the industry's first automated, consistent, collaborative, and scalable threat modeling software. Nearly four years in intensive development, it has been built and refined in conjunction with the specific needs and requests of industry specialists.

ThreatModeler's founder is Anurag Agarwal, who has more than two decades' experience in the IT world. For fifteen of those years, he worked in the web application security field at a number of companies, among them Citigroup, Cisco, HSBC, GE Medical Systems, and many others. Well-known in the field, he is a published author of articles on secure design and coding.

Mr. Agarwal is a former Director of Education Services at WhiteHat Security, and is actively involved in the Web Application Security Consortium (WASC) and the Open Web Application Security Project (OWASP).

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

Automated Threat Modeling

The manual approach to threat modeling is labor-intensive and cumbersome; output is static, hard to update, and inconsistent. ThreatModeler™ revolutionizes this approach, automatically building threat models from the functional information users provide about their applications and systems. ThreatModeler's™ output is consistent, concrete, and actionable. And it confers significant cost savings, better structure, and higher-quality threat analysis, over the old manual approach.

Intelligent Threat Engine (ITE)

At the core of ThreatModeler™ is the unique Intelligent Threat Engine (ITE). This innovation represents the culmination of years of information security and threat modeling experience and expertise, and is the processing power behind ThreatModeler.™. Once the threat model has been built, the ITE automatically predicts where potential threats exist to that application or system; ranks them by risk; and generates abuse cases**.**

Threat Analytics Dashboards and Reporting

ThreatModeler™ provides reports and a Threat Analytics dashboard to display concise and up-to-date metrics at a glance. The Threat Analytics dashboard presents a cumulative view of threats across the entire application portfolio, and can trace an individual threat back to its origin. Additionally, the Enterprise Top 10 Threats list view is constantly updated and made current – whenever a change is made to any threat model – to help executives and their teams prioritize their mitigation strategies. And with the help of reports like Data Exposure, Threat Portfolio, and others, they can stay ahead of the information security risks to their organizations.

Deployment Models

The Ownership Site License (OSL) is a perpetual-license software model: the customer owns the licensed software. The OSL is best suited for organizations, which have the time and resources to manage and administer the entire threat modeling process in-house.

The SaaS Private Cloud Offering (PCO) is an annual subscription-based model. MyAppSecurity, Inc. builds, maintains, and updates threat models for the PCO customer. PCO is ideal where an organization may not wish to manage and hire resources to build the threat modeling process in-house.

Arrange a Product Demonstration

Experience the power of ThreatModeler™ for yourself. Contact ThreatModeler today to schedule a free online demo. Watch as we build a threat model in real time, specific to your industry or organization. Go to **www.threatmodeler.com**; call us at **201-632-3634**; or write us at **sales@threatmodeler.com**.