ThreatModeler

Identify • Classify • Prioritize • Mitigate

Building an Effective, Enterprise-wide Threat Modeling Practice with ThreatModeler™

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

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2017

Introduction

In 2015, practical threat modeling – after years of conceptual discussion, theorizing, and debate – is rapidly becoming recognized as a necessary and vital part of an organization's information security process.

As new threats are emerging – and as more and more companies are getting hacked – the most challenging questions facing CISOs today are these:

- *What threats are present in our application portfolio?*
- *How might a threat against one application make its way into another application?*
- *What could be the impact on our organization if a particular threat were to be carried out?*
- *How can we obtain a more realistic view of application risk across our entire application portfolio?*
- *How can we effectively prioritize threat mitigation efforts?*
- *How can we reduce the high cost of fixing production vulnerabilities?*
- *How can we keep current with the ever-changing threat landscape and automatically discover new threats that may be present in our applications?*

All of these questions have a single solution: build an enterprise-wide threat modeling practice. Such a practice allows CISOs to be effective not only in identifying, but also in mitigating those threats. And it helps them to be proactive in building more secure systems and applications from the ground up.

Regardless of the threat-modeling methodology used, a successful threat-modeling practice should follow these principles:

- ***Practicality:*** *users should be able to create a threat model with minimal effort and time;*
- ***Understandability:*** *a threat model should be straightforward and clear to everyone, including non-security professionals;*
- ***Comprehensiveness:*** *a threat model should categorize all known threats; and new threats, as they are recognized, should be added to libraries;*
- ***Reusability and repeatability:*** *the ability to reuse a threat model, in whole or in part, avoids replication of work and saves a lot of time and effort;*

- ***Consistent and actionable output:*** *the threat model must generate reliable, consistent and useful information as to threats, their impact on the organization, and related mitigation steps;*
- ***Scalability:*** *a large enterprise might need to build hundreds or even thousands of threat models. A threat modeling practice should allow an organization to scale the initiative across all of its applications and systems.*

This real-world, current, actionable output is exactly what ThreatModeler™ provides. ThreatModeler™ enables CISOs and their teams to create a consistent, collaborative and scalable enterprise-wide threat modeling practice. The CISO and the organization can then use this actionable output to (i) reduce the high cost of fixing production vulnerabilities; (ii) minimize risk exposure; (iii) identify and address risk organization-wide; and (iv) achieve a measurable ROI. ThreatModeler™ is a feature-rich, fully-supported threat modeling product which enables organizations large and small to build and maintain threat models with ease and at a reasonable cost.

Key ThreatModeler™ Features:

Today's constantly changing threat landscape requires an aggressive approach to threat modeling. ThreatModeler™ is a robust, powerful and unique product designed to accomplish the threat modeling tasks which the modern enterprise requires. ThreatModeler™ makes it possible to construct up-to-date threat models not in months or weeks, but in days, or even hours. Here are highlights of just some of ThreatModeler's™ key features, and how they can help information security professionals to build a successful threat modeling practice.

1. **Centralized Threat Library.** Every organization should know the potential threats against it, and the impact those threats could have on its data and systems. ThreatModeler™ compiles, consolidates, utilizes, and updates threat data obtained from well-known industry sources – like CAPEC; WASC-TC; the OWASP Top 10, and others – into a comprehensive and centralized threat library, and categorizes the threats by risk.
2. **Intelligent Threat Engine.** At the core of ThreatModeler™ is the remarkable Intelligent Threat Engine (ITE). This innovation represents years of information security and threat modeling experience and expertise. The user needs only to provide the functional information of an application or system, the ITE automatically predicts where potential threats exist to

that application or system, ranks them by risk, and specifies relevant security controls and test cases.

3. **Actionable Output.** The key to any successful threat modeling practice is the output of a threat model. Traditionally, that output has taken the form of a lengthy report, which was often quickly shelved unread. Today, industry demands, from a threat model, much more useful and meaningful information. ThreatModeler™ provides valuable and actionable output, which various stakeholders can utilize for their specialized purposes.

   For example, Threat Dashboard is intended for IT Risk and Security staff to review the list of threats categorized by risk, whereas Abuse Cases are intended to help developers build secure code. Threat Tracer can be used to trace a threat back to its origin, while Threat Profiler will provide more details about the threat and the attacker. And Real-time Threat Intelligence helps keep threat libraries and threat models current and up-to-date, to ensure that the latest threats are promptly identified and addressed.

4. **Dashboards and Reporting.** For any process to be successful, there must be measurement criteria, and some form of dashboards and reports, to present concise and up-to-date information. ThreatModeler™ provides an Enterprise Risk Dashboard, which provides a cumulative view of threats across the entire application portfolio. The Enterprise Top 10 Threats list is updated with every change made to any threat model. And it ranks the current top 10 threats – across the entire organization – to help CISOs prioritize their mitigation strategy. With reports like Data Exposure report and Threat Portfolio report, organizations can stay on top of the risks to their organization.

5. **Integration.** ThreatModeler™ includes an open, comprehensive, bi-directional RESTful web services API that allows organizations to integrate ThreatModeler™ with their existing tools and technologies, like GRC applications, bug tracking systems, network and application scanners, etc.

6. **Collaboration.** ThreatModeler™ is designed to be collaborative software. Threat models can be built, updated, and reused in a collaborative manner by different team members. Various stakeholders can log in to ThreatModeler™ to review the output of a threat model. Relevant information is displayed to them based on their role.

7. **Scalability/Reusability.** ThreatModeler's™ architecture enables the organization to build, maintain, and continually update – across an entire

enterprise – hundreds, or even thousands of threat models. The advantage to the organization is the ability to scale its threat modeling initiative to include its entire application and system portfolio.

Summary

As highlighted in this brief overview, ThreatModeler™ introduces many innovative features, which are firsts in the security industry. And it does so in a powerful, easy-to-use, consistent, and collaborative package. ThreatModeler™ brings the science and art of threat modeling to an entirely new professional level. And it does so at a cost within reach of organizations large and small.

ThreatModeler™ is a major achievement in this highly specialized area of the information security world. It represents a significant step – beyond any system or tool available today – for the purpose of assessing an organization's comprehensive information security threats.

As explained throughout this white paper, ThreatModeler™ combines ease of use, and collaborative features, to generate comprehensive, reusable, scalable, and enterprise-wide actionable output. For the corporate information security professional, this actionable output represents a new level of proactive power never before available in the industry.

ThreatModeler™ Deployment Models

ThreatModeler™ is offered in two distinct license-and-deployment models. In both models, the ThreatModeler™ software is installed at the customer's secure, hardened network: no threat modeling data ever leaves the customer premises. Fees are based upon the number of threat models built, not on "users" or "seats." Each deployment model allows for unlimited users.

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

About ThreatModeler

ThreatModeler was founded in 2010 to address a critical and growing demand among information security professionals: how to achieve a more comprehensive 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.

Anurag Agarwal is the founder of ThreatModeler. Mr. Agarwal 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).

Schedule a ThreatModeler™ Product Demo

Contact ThreatModeler today to experience a free online product demo. Watch as we build a real-world, meaningful threat model, in real time, before your eyes. Go to **www.threatmodeler.com**; call us at **201-632-3634**; or write us at **sales@threatmodeler.com**.

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