ThreatModeler®

THREAT MODELING METHODOLOGIES: WHAT IS VAST?

Oct 9, 2018 | Methodology, Threat Modeling

Vast Threat Modeling is a unique and advanced approach to cybersecurity, specifically designed to address the complexities of large-scale enterprise systems. It stands for Visual, Agile, Simple Threat modeling, and is the only methodology that offers scalability across an entire organization. Vast Threat Modeling encapsulates the entire Software Development Life Cycle (SDLC), leveraging three key pillars: automation, integration, and collaboration. This makes it an effective tool for identifying, evaluating, and prioritizing potential threats, thus enhancing overall enterprise security.

There are a variety of threat modeling methodologies that provide a framework for the complex process of protecting enterprise systems from external threats.

Some, like OCTAVE, focus on the practice of reviewing systems for potential threats. Others, like STRIDE or PASTA, focus on the point of view of a developer or an attacker.

While each of these threat modeling methodologies has strengths and can be used to identify, evaluate, and prioritize remediation of potential threats to a network, they lack

ThreatModeler®

manual tools or systems, which must be developed and maintained by employees of varying skill and expertise throughout an organization, are time-consuming and inefficient.

Why Threat Modeling Matters: Threat Modeling Benefits for the CISO and Key Stakeholders

Of all threat modeling methodologies, the only one to supports enterprise-wide scalability is VAST: Visual, Agile, Simple Threat modeling. The VAST methodology is unique because it is founded on the idea that threat modeling is only useful if it encircles the entire software development life cycle (SDLC), throughout the whole enterprise.

ThreatModeler, the first commercially available automated threat modeling tool for enterprises, provides significant, quantifiable, valuable, and actionable output to stakeholders across the organization. ThreatModeler utilizes the VAST methodology to identify threats based on a customizable, comprehensive threat library.

The VAST methodology incorporates three necessary pillars to support a scalable solution: automation, integration, and collaboration.

3 Pillars For Scalable Threat Modeling Methodologies

1. Automation

Threat models are limited by the number of resource hours an application evaluation consumes. Conducting a thorough threat evaluation of a single application using manual processes could take several hours. Then multiply that by every application in an enterprise, and by several re-evaluations and updates required for ongoing post-deployment threat modeling.

Automated threat modeling eliminates the repetitive portion of threat modeling, taking the time needed to update a model from hours to minutes. This allows a threat modeling process to be ongoing – threats can be evaluated during design, implementation, and post-deployment on a regular basis. It also allows threat modeling to be scaled to encompass the entire enterprise, ensuring that threats are identified, evaluated, and prioritized throughout.

Often times, key stakeholders worry that threat modeling is too challenging to produce actionable results. Read our blog post where we debunk 5 Common Myths About Threat Modeling.

2. Integration

A threat modeling process must integrate with the tools used throughout the SDLC to provide consistent results for evaluation. These tools may include those targeted to support the Agile framework for software development, which emphasizes adaptive planning and continuous

week sprints. For threat modeling methodologies to support Agile DevOps, the threat model itself must be Agile, supporting the short-term sprint structure and employing threat modeling in an environment of continuous improvement and updates.

VAST is the only threat modeling methodology that was created with the principles of Agile DevOps to support scalability and sustainability.

3. Collaboration

An enterprise-wide threat modeling system requires buy-in from key stakeholders, including software developers, systems architects, security managers, and senior executives throughout the organization.

Scalable threat modeling requires these stakeholders to collaborate – using a combined view of different skill sets and functional knowledge to evaluate threats and prioritize mitigation. Without collaboration, an enterprise-wide view is impossible to achieve. On the other hand, collaboration helps a company scale threat modeling activities to cover all stages of the SDLC and respond to new threats with a deeper understanding of the risks posed to the organization as a whole.

VAST threat modeling works best for enterprises that need to automate and scale threat modeling across the entire DevOps portfolio, and are looking for the process that will complement an Agile framework of continuous delivery. Integration with Agile, as well as other production tools in use by the team forms the foundation for a collaborative, comprehensive threat modeling process that leverages the strengths and skills of key stakeholders throughout the organization.

Developing A VAST Threat Modeling Program

ThreatModeler is an automated threat modeling software that strengthens an enterprise's SDLC by identifying, predicting and defining threats, empowering security and DevOps teams to make proactive security decisions.

Using VAST, ThreatModeler provides a holistic view of the entire attack surface, enabling enterprises to minimize their overall risk. ThreatModeler's easy one-step process flow diagrams, visual interface, and up-to-date threat databases empower organizations to enable non-security professionals to strategically prioritize and address threats.

To see how ThreatModeler can drive and scale security throughout your enterprise, schedule a demo with one of our security experts today.

ThreatModeler®

What is the main limitation of traditional threat modeling methodologies when it comes to scalability in large enterprises?

Traditional threat modeling methodologies lack scalability as they often rely on manual tools or systems, which are time-consuming and inefficient. This makes it difficult to implement effective threat modeling throughout an enterprise as it grows in complexity.

How does the VAST methodology differ from other threat modeling methodologies?

What are the three pillars for scalable threat modeling methodologies?

How does VAST support Agile DevOps in threat modeling?

How does ThreatModeler utilize the VAST methodology to benefit enterprises?

What is the role of automation in the VAST methodology?