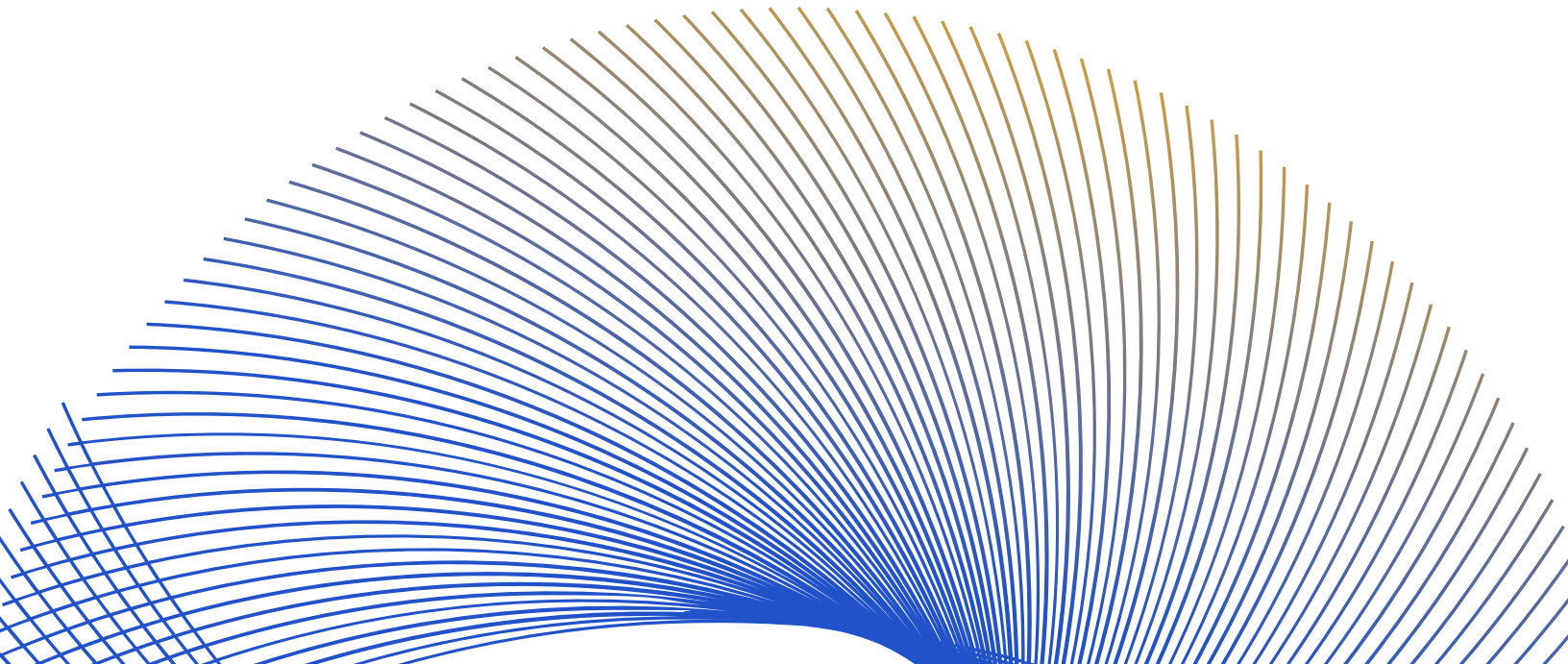
ThreatModeler®

7 EASY STEPS for Building a Scalable Threat Modeling Process

By Archie Agarwal

Founder & Chief Innovation Officer of ThreatModeler

Contents



Introduction

With the rapid expansion of data-driven technologies, cybersecurity has become a major concern in recent years. Looking at the current state of cybersecurity, leading industry analysts are forecasting this trend will continue for the foreseeable future. Depending on the sensitivity of the assets being compromised, the number of records exfiltrated, or the type of data that is breached, cyberattacks can easily cost enterprise-level organizations hundreds of millions of dollars in mitigation, legal costs, and business loss.

Current State of Cybersecurity

Until recently, cybersecurity was a second thought. Despite the growing threat environment, many organizations continue to utilize vulnerability scanners as their primary means of identifying potential exploits. The rationale behind this approach is understandable but ultimately flawed. While security programs across enterprises have matured, effective risk-mitigation techniques – in the form of secure architecture and software development – have not been given appropriate attention. Efforts to put a process of secure development in place have been largely theoretical.

Security awareness has increased throughout the years, but so has the prevalence of powerful hacking tools available to both amateur and professional attackers. The need to secure an organization is crucial in today's world. Potential threats are gradually becoming actual exploits – with very costly repercussions. Many techniques have been developed to solve an extensive range of cybersecurity problems. One of the most effective methods of ensuring application security in the design process is threat modeling.

- Security programs have improved, but security as a whole remains on the back-burner.
- Threat modeling revolutionizes cybersecurity by providing proactive mitigation throughout the design and production phases.

Responding to an attack post-production costs at least 80% more than the cost of proactive mitigation integrated throughout the design and production phases.

Threat Modeling Revolutionizes Cybersecurity

Threat modeling is a process by which organizations can shift their security approach from reactively plugging exploits to proactively and systematically understanding and addressing potential threats in the design stage. This process identifies potential threats to the system, data/asset exposure, logical/architectural vulnerabilities, and relevant security controls to help evaluate security decisions, serve as a guide for security testing, and minimize risk exposure.

Threat modeling enables organizations to understand their attack surface and various paths to exploit a system. Organizations are able to prioritize their mitigation strategy and identify the right controls that can be implemented to prevent a data breach.

Threat modeling enables organizations to:

1. Allow security and development teams to pinpoint high-value targets (assets) and data exposure early in the design phase – before applications are moved to production.
2. Promote the use of secure code, enforcing standards organization-wide.
3. Enable pen testers to focus on the most critical entry points in applications.
4. Generate reports and checklists to validate that proper security controls are in place to meet compliance objectives.

Although threat modeling has been around for years, it has not reached its climax despite the many benefits it provides. This is due to the old approach it has communicated. Traditionally, threat modeling has been a labor-intensive and manual process that requires lots of resources and produces outdated outputs within days of delivery. As enterprises become aware of the need for threat modeling, they are uncertain of how to implement the process throughout their organization and scale it across an entire cyber ecosystem consisting of thousands of applications, networks, or cloud infrastructure.

The threat modeling process discussed in this paper provides a holistic view of the entire attack surface, enabling enterprises to minimize their overall risk. When fully incorporated, the outlined approach to threat modeling provides organizations with an effective way to prioritize and mitigate vulnerabilities before exploitation, producing a significant and achievable return on the organization's development and security investment.

This guide introduces a simple seven-step process to building a repeatable, scalable, and actionable threat modeling process that can be easily implemented across your organization at any scale. The process developed is based on ThreatModeler's automated threat modeling solution, which upholds an enterprise's SDLC by identifying, predicting and defining threats, empowering security and DevOps teams to make proactive security decisions.

ThreatModeler's process allows organizations to ensure software security across a limitless number of programs or IT operations – without the need to invest capital in the security of each individual application or subsystem.

7 Easy Steps

FOR BUILDING A SCALABLE THREAT MODELING PROCESS

1 Build a Threat Library

Identifying threats help organizations generate relevant mitigating controls. To reach an appropriate level of security at a reasonable cost, organizations need to know which threats are applicable to them and the potential impact if a given threat is exploited. Thus, the first step is to build a threat library that is unique to your organization.

New threats are created for mobile devices, web services or different types of applications continuously.

Even though there are public threat libraries such as MITRE's CAPEC, WASC-TC and OWASP, some threats are unique to your organization. For example, if you're building a medical device or an ATM machine, there will be threats unique to your business that do not concern others.

To support reliable and systematic security standards throughout the organization, the threat library should be built from a template to define threat properties.

These will include:

Details on how the threat can be executed

Security controls which can effectively mitigate the threat

Profiles of hypothetical attackers including their motivation and skill set

Technical and business impacts of the threat on the organization, based on real-time breach data

It is important to consider the risk a threat represents to the organization. This will prioritize and focus mitigation resources on high-risk threats, vulnerabilities, and software components.

Identify Mitigation Strategy

There are two ways to mitigate a threat. The first one is by implementing relevant security requirements in the code, thereby addressing the issue at its source. The second way is adding a security control (i.e., compensating control) to mitigate the threat before it reaches the source (e.g., WAF, firewall, SSO, etc.). Enterprises have made investments in an overflow of compensating controls either as a detective or preventive measure. Security requirements are the basis for building security in the system. These requirements indicate the system's course of action and what must not be allowed to happen. Compensating controls, on the other hand, are the foundation for the first line of defense (and, in some cases, the only line of defense).

When all potential threats have been evaluated, along with a resolution of the threats that must be mitigated, the next step is to identify security requirements. Organizations need to know how to mitigate each identified threat. From a security perspective, it is important to know the threats and risks to the organization, but from a developer's perspective, the main concern is the security requirements necessary to mitigate a given threat. The list of threats also helps Security Architects identify the compensating controls that can be implemented to prevent these threats from reaching the vulnerable source.

After customizing a threat library, it is important to include the costs to implement each security control along with the risk levels to help in the decision-making process of prioritizing mitigation efforts. Security controls and security requirements should be applied in situations where the cost to implement them is not higher than the anticipated risk.

Reuse Threat Patterns

When an organization identifies a threat and its associated risks and mitigations, this same “threat pattern” will remain across various applications. Building a threat pattern library allows organizations to reuse the work that has been completed, enabling them to scale quickly across hundreds of thousands of applications.

Applications are built from individual features, and each feature can be attacked. Consider your threat model from an applications perspective, and assume you have a feature like LOGIN. Whenever you wish to build a threat model for the LOGIN feature, you think in terms of potential attack vectors. If you have a weak password policy, for example, potential exploits could include a brute-force or dictionary-based password attack, a denial-of-service attack using an account lockout or session fixation, or any other path common to authenticating to an application.

When you consider the potential for exploits across other applications that utilize the same or a similar LOGIN feature, each application is subject to the same vulnerabilities. This only changes with applications built upon alternative platforms, infrastructures, or technologies requiring a completely different approach to the LOGIN.

Threat pattern libraries help organizations improve reusability across multiple applications by allowing them to build attack trees of each component in a centralized library, with updates reflected automatically and the opportunity to use threat patterns everywhere once written.

Develop Actionable Output

The next step is to develop an effective threat model and convert it into actionable output. A structural representation of a threat modeling process – attack surface identification – can recognize risks in a cyber ecosystem to prioritize mitigation of potential threats. Threat modeling can be a valuable source to understand components and how to mitigate threats.

The threat modeling process helps a good security system find a balance between what is likely to happen and what is relevant. From a security executive point of view, the model needs to clearly identify the organization's high-value targets that attackers will likely prioritize. Developers must think like the attacker. This can be accomplished once the system is finally understood. Organizations also need to know their data exposure and the feasible cost of a breach. This will help them focus on the security requirements that need to be generated based on the threat model.

A good way to comprehend the mind of attackers is building abuse cases. These cases create mitigating controls and provide developers with precise knowledge about the system's behavior. By analyzing unanticipated events, organizations can proficiently enforce the security and validity of the system they develop.

Automation, Integration, Collaboration

With actionable output identified, organizations can automate the process, integrate it with their existing workflow, and get various stakeholders to collaborate together. From an automation and scalability perspective, stakeholders will want to automate as much of the work of building a threat model and defining the threats as possible.

The next step is to integrate the threat modeling process into their existing workflow and DevOps toolchain, such as JIRA, ServiceNow, or Jenkins. Threat modeling is about threat enumeration, not risk modeling.

Many enterprises are already using GRC (governance, risk management, and compliance) tools like ARCHER, so there is no reason to duplicate these tools with a threat model or to develop a completely different risk methodology. In these cases, the best approach is to integrate their risk engine with the threat model being developed.

Architects

Provide Functional Information about the Application Architectural Risk Analysis

Security Team

Identify Threats & Mitigations

Targeted Threat Testing

Vulnerability Management

Senior Executives

Assess Threat Profile

Risk Management

Developers

Implement Correct Mitigation Steps & Security

Standards Using Abuse Cases

Peer Code Review

Reporting

Reporting and measuring the effectiveness of the threat model is the next step of the process. During this stage, stakeholders and decision-makers will want to review the organization's threat portfolio and identify the top ten threats, either from an application or an enterprise perspective.

Effective threat modeling is not a security-team driven process. To achieve the scalability required for a successful threat modeling process, developers and architects should play an active role in every step of the process. Threat management focuses on protecting the organization by preventing attacks that might mitigate the system while updating it with the latest data about threats for a fast response.

Collaboration and efficiency throughout the SDLC are key points in this stage of the process. An online dashboard connecting stakeholders will help each one access essential reports based on their individual roles.

Reporting provides a measurable and accountable state of application security monitoring, allowing observation of trends in the application security profile.

Operationalizing

From an operationalizing point of view, the threat modeling process should be built to handle tens, hundreds, or even thousands of applications – and keep them up to date in a reasonable amount of time. It will scale across thousands of developers or stakeholders simultaneously, bringing them all together to work collaboratively and continuously minimize the organization's risk exposure.

Organizations are now realizing the cost benefits of incorporating threat modeling earlier in the SDLC. Traditionally, companies run vulnerability scans only after the application is developed and ready to go to production. Yet the scan comes back with a list of critical vulnerabilities that must be fixed before production, demanding a significant amount of time, money, and resources. The threat modeling process reduces cost and time expenditure by allowing organizations to understand the attack surface and introduce relevant controls to diminish the overall exposure to cyber threats.

A scalable threat modeling process builds a threat model in hours or days – depending on the size of the application – updating it with every release and making use of reusable templates. Although it is impossible to guarantee 100% **security**, effective risk management can assure 100% **risk acceptance and mitigation**, ensuring the protection needed to minimize damage for any given threat.

The goal of threat modeling is to identify threats ahead of time and classify those threats based on risk, so that the mitigation efforts can be prioritized to reduce the risk to the web application.

ThreatModeler

#1 Automated Platform

ThreatModeler™, the first automated enterprise threat modeling solution, strengthens an enterprise's SDLC by identifying, predicting and defining threats across all applications and devices in the operational IT stack. CISOs and other InfoSec executives will gain a comprehensive understanding of their entire attack surface, defense-in-depth strategy, and compensating controls, so they can strategically allocate resources and scale their output.

Organizations recognize significant resources and cost reduction by identifying and mitigating threats during the design stage of the SDLC. 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.

Since its inception in 2011, ThreatModeler's robust interface and consistent forward-thinking has been fueled by a team of threat modeling experts that specialize in cybersecurity, pioneering a completely new way for threat models to be built. ThreatModeler is currently partnered with leading Fortune 1000 companies in the financial, medical, and IoT industries. For more information on ThreatModeler, visit threatmodeler.com and schedule a demo or request a free initial evaluation.

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

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