# Threat Modeling with OWASP, MITRE, and STRIDE

Threat modeling can apply to a wide range of things, including software, applications, systems, networks, distributed systems, Internet of Things (IoT) devices, and business processes.

In 2020, a group of threat modeling practitioners, researchers and authors got together to write the *Threat Modeling Manifesto*. The Manifesto contains values and principles connected to the practice and adoption of Threat Modeling:

- **Values**: A value in threat modeling is something that has relative worth, merit, or importance.
- **Principles**: There are three types of principles: (i) fundamental, primary, or general truths that enable successful threat modeling, (ii) patterns that are highly recommended, and (iii) anti-patterns that should be avoided.

OWASP Threat modeling is a process for capturing, organizing, and analyzing all of this information. This applied to software and risk identification. Typical threat modeling efforts also produce a prioritized list of security improvements to the concept, requirements, design, or implementation of an application

Threat modeling is a structured method of assessing risks associated with a system or application. Developers must take time to understand what threats exist to their system. Once they know what threats exist, they must assess the impact of each threat and decide if any of them pose a high enough risk to warrant mitigation.

## How does the threat modeling process work?

There are several threat modeling frameworks and methodologies, including STRIDE, PASTA, CVSS, MITRE, OWASP, attack trees, Security Cards, and HTML.

The key steps are similar in most of these processes.

They include:

1. **Form a team.** This team should include all stakeholders, including business owners, developers, network architects, security experts and C-level execs.
2. **Establish the scope.** Define and describe what the model covers. Create an inventory of all components and data included and map them to architecture.
3. **Determine likely threats.** Create what-if exercise builds and threat scenarios, including threat or attack trees, to identify possible vulnerabilities or weaknesses.
4. **Rank each threat.** Determine the level of risk each threat poses and rank them to prioritize risk mitigation.
5. **Implement mitigations.** Decide how to mitigate each threat or reduce the risk.

6. **Document results.** Document all findings and actions, so future changes to the application, threat landscape and operating environment are assessed and the threat model updated.

## Threat Modeling Scope

Why do Threat Modeling?

Threat agents include individuals or groups that can carry out a specific threat. An individual or group that wants to harm a company by stealing information or using it to make money is a threat agent. Organizations that will spend large amounts of money to hire people to steal information or use it to make money are also threat agents. Individuals or groups that will develop malware or hacking into systems are also threat agents.

Executing preventive controls after the modeling may completely block a particular attack from happening. For example, if we identify a threat that our users' personal information may get identified by some application logging, and we decide to obliterate that application logging, we have blocked that threat. Mitigation means reducing the likelihood or impact of a threat without totally blocking it.

### MITRE ATT&CK Framework

MITRE is a federally funded research and development center (FFRDC) of the US government. One of its areas of research is cybersecurity, and the MITRE ATT&CK framework.

MITRE ATT&CK supports cybersecurity by providing a framework for threat modeling, penetration testing, defense development, and similar cybersecurity exercises.

*The combination of Tactics and techniques provides concrete guidance for a threat modeling exercise.*

Under each Technique or Sub-Technique, MITRE provides additional data, including:

- Technique description
- Affected platforms
- Required permissions
- Data sources for detection
- "Procedures" (known malware, tools or threat actors using the technique)
- Mitigations
- Detection methods
- References

### STRIDE threat modeling

STRIDE is a threat modeling framework developed by Microsoft employees and published in 1999. It focused the STRIDE threat model on the potential effects of distinct threats to a system:

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Escalation of privileges

Based on this information, it is possible to assess the risk and impact of each potential threat and develop countermeasures to mitigate it.

## Collaboration between Pen testing and Threat Modeling.

Threat modeling teams that test applications and platforms use similar techniques as pen testers. Threat modeling is normally carried out by internal AppDev, DevOps, and SecOps teams. Pen testers, however, are typically a 3rd party external with the expertise for ethical hacking engagement.

*A 1st level of engagement* could include a collaboration across the threat modeling team and the pen testers achieved in the same agile sprints. While selecting the team for the threat modeling along with defining the scope and documenting the expected threats, a 3rd party white-hat pen tester could be a member of this team. White-hat pen engagements often involve both the AppDev and pen tester working together to determine a full scope engagement. The white-pen tester normally granted access to usernames and passwords, IP addresses of the targeting hosts, along with the expectation of testing criteria. Forming a collaboration between a white-hat 3rd pen tester and the internal threat modeling team would produce a more complete 360 degree view. Without a collaboration, threat modeling results would be based on solely internal resource knowledge. Having an independent 3rd party pen tester, the threat modeling results will be considerably more valuable with both parties' input and expertise.

*A 2nd level of engagement* would be a collaboration between a black-hat pen tester and threat modeling team. Within this collaboration engagement, the black-hat tester would have no prior knowledge of the application or platform. SecOps would be the internal sponsor of this engagement, not AppDev, DevOps, and NetOps.

If the black-hat pen team discovers vulnerabilities, the threat modeling, white-hat and black-hat pen testers will compare notes to see if either party discovered the same security issue or different ones. The entire sprint engagement, including threat modeling, white-hat, and black-hat team results, should merge into the MITRE attack portal. This portal serves as a merged threat modeling platform along with actual attack analysis from both pen testing engagements. This consolidation can help to ensure that a potential and actual threat is properly identified during threat modeling and provides guidance on how to mitigate the potential risk using a combination of detection and mitigation strategies.

### Threat Collaboration Modeling Across the Lifecycle

Threat modeling is best applied continuously throughout a software development project. The process is essentially the same at different levels of abstraction, although the information gets more and more granular throughout the lifecycle. Ideally, a high-level threat model should be defined early in the concept or planning phase, and then refined throughout the lifecycle.

Updating threat collaboration models is advisable after events, such as:

- They released a new feature
- Security incident occurs
- Architectural or infrastructure changes

This threat modeling pen testing collaboration workstream should be added as a business operational function with every application or variance of a platform.

## Summary

The point at which you should carry out a penetration test requires an organization first to identify the assets that are to be included in the project's scope. The identified threats and vulnerabilities will then form a concrete input to your risk assessment, while the identified remediation sprints to reduce the risk.

Please let us know here at CYBRI if you have questions regarding your ISO 27000 VAPT testing, or if you'd like to learn more about how we can help.

# What makes CYBRI one of the Premier penetration testing companies?

Our outstanding penetration testing company services have attracted several clients that range from small startups to huge multinational companies. We are dedicated to improving cybersecurity across the board, which means that our services to your organization continue even after the pen test report has been delivered.

No matter the size of your organization, we will assess all of your cybersecurity needs from scratch to provide security measures tailored to your business needs. Our experts are always available to all of our clients in an advisory capacity should you wish to contact us.

# Discuss your project with us!

Click here to go to our site, fill out the form and the engagement team will contact you shortly!
**https://cybri.com/red-team/**