Threat Modeling

Identify & Mitigate Threats,
While Maximizing Security Investments.

What is Threat Modeling?

Threat modeling is a service in which we identify and specify potential threats, such as vulnerabilities or lack of defense mechanisms in an organization, followed by prioritizing risk mitigations to close security gaps. The service equips the security team with an analysis of what security controls are required based on the current information systems and the threat landscape, the most likely attacks to anticipate, the attackers' expected methodology, motive, and target systems.

Threat Modeling is one of the most expedient and efficient tools organizations can employ to create clear resource priorities, enhance their security posture and maximize their security investments.

How does Threat Modeling work for me?

HolistiCyber experts proactively identify attackers, their motivations, attack vectors, and targets within an organization, deliver clear and straightforward analysis, and provide the mitigation tactics to counter these threats.
Our domain experts have years of experience in threat modeling and securing for large enterprises in major industries such as utilities, software companies, banking, financial services, media, and entertainment.

The service typically includes these general steps.
1) Creating a model representing the systems and environments to be analyzed and identifying what each application does and its security properties.
2) Identifying critical business processes, assets, and company risk tolerance.
3) Identifying relevant threat actors (internal and external).
4) Analyzing environments from the attackers' vantage point.
5) Prioritizing threats based on analysis.
6) Based on all the above, outlining and prioritizing measures to mitigate the risks and improve security posture.

WHAT SHOULD YOU EXPECT?

- **Prioritize security resources to where they create the best value**
- **Answer questions relating to where the organization is most vulnerable to attacks, what are the top risks, and what should be done to reduce these risks.**
- **Report and recommendations adapted to unique company business needs, priorities, and risk appetite.**
- **Implementing effective risk controls.**
- **Clear prioritization of security threats that need to be handled immediately vs. items that do not pose an immediate risk.**
- **Non-intrusive service - analyses conducted on a model representation of the business environment.**
- **Countermeasure identification and residual risk analysis.**

What would an attacker do?

When analyzing the attack surface, these are some of the angels our experts will look at:

- How can attackers reach and compromise high-value assets? (What potential attack paths exist to get and compromise the organization's high-value assets?
- Which of these paths is easier for attackers?
- How hard is it for attackers to reach and compromise these high-value assets?
- Which countermeasures will discourage attackers and get them to look for easier targets in other enterprises?

Value for business

One of the critical challenges in managing cybersecurity is determining how to prioritize and allocate resources to manage risks with the best effect per dollar spent. Our experts have designed a process for threat modeling to optimize investments in cyber security while considering all essential parts guiding decision-making.

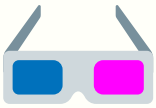
This service allows organizations to make informed decisions when managing and improving their cybersecurity defense plan. It effectively elevates the organization's cyber risk posture, as it identifies and quantifies risks proactively and holistically, steering security measures to where they create the best value.

Identifying and managing vulnerabilities and risks before they are exploited enables companies to proactively make risk-based decisions on what measures to implement.

Analyses are conducted on a model representation of the business environment, which means they are non-intrusive.

Threat modeling improves incident response by helping identify incidents faster, understanding their severity, and assisting incident responders in acting faster and more effectively. Incident responders should provide a feedback loop to continually update threat models.

Why HolistiCyber?



1. **Nation-state-grade expertise** - our staff of white-hat security experts is composed of former military and government offensive practitioners who can examine the attack surface from the vantage point of the attacker and not only from the company's vantage point. We have a solid grasp of the sophisticated tooling available to today's attackers and access to those attack tools.
2. **Holistic approach** - we tie compliance, remediation, and mitigation solutions to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.

"HolistiCyber's advanced cyber attacker approach and deep cyber security knowledge exposed critical vulnerabilities that were not visible with previous services. The results of the HolistiCyber recommendations were so thorough and enlightening that we are now compelled to perform annual cyber security reviews."

CISO, Financial Institution, USA