RAISING YOUR CYBER RESILIENCE

BUREAU VERITAS

SECURITY INNOVATION
A BUREAU VERITAS COMPANY

Threat Modeling

Digital security risks are growing explosively. But how do you know which risks pose the biggest threat to your organization? Threat Modeling helps you to identify potential threats before they materialize, so you can develop strategies to prevent or mitigate them.

Threat Modeling gives you:

Insight into threats

Which threats are relevant to your organization? Our experts can help you determine these.

Clarity on priorities

Now that you have sight of threats, we can help you determine priorities for prevention and mitigation.

Control of threat landscape

The NIST SP 800-171 requires you to identify and document the specific threats to organizations operations and assets. Threat Modeling helps you do this.

Why Choose Threat Modeling?

Our threat modeling process yields a complete system security model that can be used to create an actionable test plan for security auditing, to form the core of design review efforts, and to provide an understanding of the risk profile of a system. Effective threat modeling requires security expertise as well as intimate knowledge of the application and implementation. We work closely with your team to drive and explain the process, providing perspective to ensure that we identify the full range of threats your software faces.

How Threat Modeling works:

1 **Understand architecture and security requirements.**
A basic understanding of system functionality and design is achieved via documentation, walkthroughs, and interviews.

2 **Identify assets and roles.**
The system is divided into a series of assets. These assets represent items of value to the users of the system or to the business that deploys it. The users who interact with the system are then categorized based on what actions they can take against these assets.

3 **Build an activity matrix.**
An activity matrix is defined, which is a set of explicit mappings specifying what assets each role in the system can interact with, and under what conditions. Evaluation of this matrix yields the threats against the system, from a requirements perspective.

4 **Identify threats that put assets at risk.**
From the threats the activity matrix yields, a prioritized set of potential threats is determined.

5 **Identify attacks that could be used to realize threats.**
For each threat, attacks are defined based on the most likely methods by which the threat could be realized.

6 **Identify testable conditions that each attack requires to be successful.**
For each attack defined, a set of conditions required for it to be successful is determined. This set of attacks and conditions can form the basis of further test planning work. From these conditions, mitigations can be created that represent key actions that can be taken to reduce the risk of attack.

SECURITY INNOVATION
A BUREAU VERITAS COMPANY

About Security Innovation/ Bureau Veritas

Security Innovation is a leader in software security, providing comprehensive assessment solutions to secure software from design to deployment, across all environments, including web, cloud, IoT, and mobile. Leveraging decades of expertise and as part of Bureau Veritas, a global leader in Testing, Inspection, and Certification, we seamlessly integrate world-class security into development processes, safeguarding the way companies build and deliver products.

Security Innovation is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80,000 employees and is active in 140 countries.

Example case | Threat Modeling

Which problem did the customer have?

A client within the public domain wanted to create a pentesting calendar. However, they did not really know how their applications - a few dozen - were related or connected to each other.

Result

We used a preliminary Threat Modeling session to map this client's network. This session revealed which applications were the most important. We then conducted Threat Modeling for their most critical applications. At the end of the project the client had insight into the application landscape and was able to prioritize which applications needed further testing.

Interested?

Contact us today to start raising your cyber resilience.

✉ sisales@securityinnovation.com

☎ +1 877 839 7598

securityinnovation.com