BUREAU VERITAS

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

Control of threat landscape

The NIS2 directive requires you to gain control of your threat landscape. Threat Modeling helps you do this.

Why choose Threat Modeling?

When securing an application, system or the complete chain, it is important to know from which perspective threats arise and how your company can be attacked. The goal of **Threat Modeling** is to gain insight into the systems or applications in your network and to determine the relevant threats to these. You can use the results of the Threat Modeling session to to set priorities within your security strategy or to devise research questions for your pentesting assignments. Our Threat Modeling experts use a number of recognized methodologies and frameworks to perform Threat Modeling. The ones we use most often are STRIDE, MITRE's ATT&CK™ framework and Unified Kill Chain. We might use another methodology that is more relevant to your specific sector. Let us help you gain insight into threats so that you can take action.

How Threat Modeling works:

Preparing the session

During this phase, our experts discuss the scope of the Threat Modeling with you, to determine which staff should be present at the interactive session. We will also ask you for design documentation, if you have this, or other input.

Threat Modeling Session

This creative session is the heart of Threat Modeling. Using one of several recognized methodologies, our experts and yours will actively brainstorm on relevant threats. This gives a picture of threats and possible attack vectors.

Advising on threats and priorities

You receive a Threat Modeling report. This details the scope and documents relevant threats. Our experts also actively weigh priorities and give you concrete recommendations on the next steps to take.

Secura
A BUREAU VERITAS COMPANY

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. We help clients all over Europe to raise their cyber resilience. Our clients range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also provide audits, forensic services and awareness training.

Secura 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

What problem did the client 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.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

info@secura.com

+31 (0) 88 888 3100

secura.com