TOREON

# Threat Modeling

◆ PRODUCT SHEET ◆

YOUR COACH IN DIGITAL SECURITY

## Toreon Solution: Threat Modeling

# What is Threat Modeling?

Threat Modeling is a structured approach to identify and evaluate system threats, potential vulnerabilities and mitigating controls. It allows us to consider, document, and assess the security implications of conceptual designs on all layers of the solution.

Threat Modeling is a team exercise, involving system owners, program/project managers, architects, and developers. It is used to implement security by design, review the security of an existing system or to augment security tests.

# Benefits of Threat Modeling

Threat Modeling is often called 'Whiteboard hacking'. It is a way of bringing business owners and IT around the table to analyze the security of an application, information (IT) or operational technology (OT) system.

Threat Modeling allows to talk about risk in a structured and guided way, using 'risk patterns' that are relevant to the system (such as Privacy, industrial security, safety).

In some industries such as Medical Device Manufacturing and Automotive, it has become the de facto standard for proving security compliance on a technical level.

Some of the benefits of Threat Modeling are:

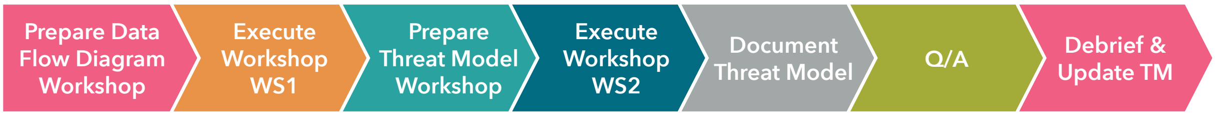
- TM brings business and IT to the table in a focused discussion.
- It allows for a high level security risk assessment methodology and risk matrix to be directly applied to a design, bridging the gap between Corporate Security Governance and design.
- It creates a living piece of security documentation that can evolve with the system. When the system is changed, the Threat Model is updated to reflect a new reality.
- It clearly shows how complex systems are linked and dependent on external systems, which may be a weakness.
- A Threat Model enhances the value of penetration testing, by highlighting areas of interest, where penetration tests should be focused.

# Methodology of Threat Modeling

Toreon uses the STRIDE methodology for its Threat Modeling practice. STRIDE stands for 'Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege'.

These are the categories of threats that are investigated.

A typical Threat Modeling assignment involves the following steps:



Prepare Data Flow Diagram Workshop

Execute Workshop WS1

Prepare Threat Model Workshop

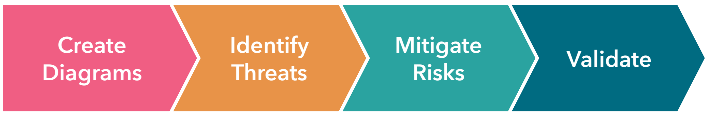
Execute Workshop WS2

Document Threat Model

Q/A

Debrief & Update TM

During the workshops we use the following approach to gain insights on the threats and vulnerabilities inherent to the design in question, and how to mitigate the risks that result from it:



Create Diagrams

Identify Threats

Mitigate Risks

Validate

- Create diagrams. An understanding of the environment and the included systems and applications enables us to build relevant and accurate Threat Models. Important during this step is the identification of your security objectives and potential business impacts. These objectives help to focus the Threat Modeling activity and determine the required staff and effort for the following steps. The main output of this step is a logical diagram or reference architecture of the environment. This diagram focuses on Data Stores, Data Flows and Trust Boundaries.
- Identify threats. The diagrams created during the previous step combined with threat scenarios give an indication of which scenarios are most relevant to the environment. Other threats are evaluated from industry accepted sources.
- Mitigate risks. As part of this step we review the relevant scenarios to identify the possible controls that mitigate the risk levels that are defined. We define control categories in order to focus on areas with the most threats and their related risk impact.
- Validate. Validate the Threat Model. Is each relevant threat mitigated? If any, what is the residual risk? What does this residual risk mean as business risk?

# Prerequisites

For Threat Modeling, we require:

- Available information on the (new) system;
- Access to lead system, network and application architects and developers of the systems in scope during the workshops and review meetings.

# What we deliver

The end result of a Threat Modeling project is a much improved understanding of the system and its security profile.

We deliver a Threat Model report, which is a clear and understandable report on the system, with the diagrams, risk evaluation and conclusions.

Diagrams are delivered in changeable format for later adaptation. A management summary provides insights for non-technical readers.

We present our findings as needed to IT and business.

# Our credentials

Toreon is a leader in Threat Modeling. Our experts have used their experience in the field to create one of the world's most sought after Threat Modeling Training.

See https://www.toreon.com/threatmodeling/

Having taught this training at the prestigious cybersecurity conference 'Black Hat Las Vegas' for the last 3 years and at many multi-national companies as an in-house training, we are committed to bringing knowledge about Threat Modeling to the foreground in every cybersecurity practice.

Our commitment is to create a more secure digital society, by sharing our knowledge, teaching and coaching our clients to increase their security maturity.

**Toreon BV**
**Grotehondstraat 44**
**B-2018 Antwerpen,**
**Belgium**

**T +32 33 69 33 96**
**toreon@toreon.com**
**www.toreon.com**