THREAT MODELING MANIFESTO

What is threat modeling?

Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

At the highest levels, when we threat model, we ask four key questions:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

Why threat model?

When you perform threat modeling, you begin to recognize what can go wrong in a system. It also allows you to pinpoint design and implementation issues that require mitigation, whether it is early in or throughout the lifetime of the system. The output of the threat model, which are known as threats, informs decisions that you might make in subsequent design, development, testing, and post-deployment phases.

Who should threat model?

You. Everyone. Anyone who is concerned about the privacy, safety, and security of their system.

How should I use the Threat Modeling Manifesto?

Use the Manifesto as a guide to develop or refine a methodology that best fits your needs. We believe that following the guidance in the Manifesto will result in more effective and more productive threat modeling. In turn, this will help you to successfully develop more secure applications, systems, and organizations and protect them from threats to your data and services. The Manifesto contains ideas, but is not a how-to, and is methodology-agnostic.

The Threat Modeling Manifesto follows a similar format to that of the Agile Manifesto by identifying the two following guidelines:

- **Values**: A value in threat modeling is something that has relative worth, merit, or importance. That is, while there is value in the items on the right, we value the items on the left more.
- **Principles**: A principle describes the fundamental truths of threat modeling. 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.

Values

We have come to value:

- A culture of finding and fixing design issues over checkbox compliance.
- People and collaboration over processes, methodologies, and tools.
- A journey of understanding over a security or privacy snapshot.
- Doing threat modeling over talking about it.
- Continuous refinement over a single delivery.

Principles

We follow these principles:

- The best use of threat modeling is to improve the security and privacy of a system through early and frequent analysis.
- Threat modeling must align with an organization's development practices and follow design changes in iterations that are each scoped to manageable portions of the system.
- The outcomes of threat modeling are meaningful when they are of value to stakeholders.
- Dialog is key to establishing the common understandings that lead to value, while documents record those understandings, and enable measurement.

These patterns benefit threat modeling:

Systematic Approach

Achieve thoroughness and reproducibility by applying security and privacy knowledge in a structured manner.

Informed Creativity

Allow for creativity by including both craft and science.

Varied Viewpoints

Assemble a diverse team with appropriate subject matter experts and cross-functional collaboration.

Useful Toolkit

Support your approach with tools that allow you to increase your productivity, enhance your workflows, enable repeatability and provide measurability.

Theory into Practice

Use successfully field-tested techniques aligned to local needs, and that are informed by the latest thinking on the benefits and limits of those techniques.

These anti-patterns inhibit threat modeling:

Hero Threat Modeler

Threat modeling does not depend on one's innate ability or unique mindset; everyone can and should do it.

Admiration for the Problem

Go beyond just analyzing the problem; reach for practical and relevant solutions.

Tendency to Overfocus

Do not lose sight of the big picture, as parts of a model may be interdependent. Avoid exaggerating attention on adversaries, assets, or techniques.

Perfect Representation

It is better to create multiple threat modeling representations because there is no single ideal view, and additional representations may illuminate different problems.

About

Our intention for the Threat Modeling Manifesto is to share a distilled version of our collective threat modeling knowledge in a way that should inform, educate, and inspire other practitioners to adopt threat modeling as well as improve security and privacy during development.

We developed this Manifesto after years of experience thinking about, performing, teaching, and developing the practice of, Threat Modeling. We have diverse backgrounds as industry professionals, academics, authors, hands-on experts, and presenters. We bring together varied perspectives on threat modeling. Our ongoing conversations, which focus on the conditions and approaches that lead to the best results in threat modeling, as well as how to correct when we fail, continue to shape our ideas.

You can always find the current version of this manifesto at https://www.threatmodelingmanifesto.org/.

Authors

The working group of the Threat Modeling Manifesto consists of individuals with years of experience threat modeling for security or privacy.

- Zoe Braiterman
- Adam Shostack
- Jonathan Marcil
- Stephen de Vries
- Irene Michlin
- Kim Wuyts
- Robert Hurlbut
- Brook S.E. Schoenfield
- Fraser Scott
- Matthew Coles
- Chris Romeo
- Alyssa Miller
- Izar Tarandach
- Avi Douglen
- Marc French

The working group would like to thank Loren Kohnfelder and Sheila Kamath for their technical edit review and expert feedback on the document content and structure.