

0111101010101  
1010101001001  
1011010010010  
0110SECURITY0  
010101THREAT0  
0110100100110  
0101001001001

# THREAT MODELING

24-7-2023

## TABLE OF CONTENT

Introduction .....	3
Objective .....	3
Threat modeling manifesto .....	3
Threat modeling in SDLC .....	3
Four Key Questions.....	4
Structured Process.....	4
Benefits .....	5
Threat Modeling Tools.....	5
<b>Configuration of Iriusrisk</b> .....	5
References.....	6

# INTRODUCTION

A threat is something that impacts the negatively of an organization and A threat model is a structured representation of a threat. It considers an application and its environment in the context of security.

Threat modeling is the concept of gathering, organizing, and analyzing all the information. It enables us to apply threat modeling software and makes decisions about applications' security risks. A threat model also prioritizes the list of security risks in each software development life cycle phase, such as requirement, design, or implementation in applications.

Threat model researcher and practitioner author introduce a model to inform, educate, and inspire other practitioners to adopt the model and improve their security and privacy.

## Objective

Threat Modeling provides a set of activities that improve security by identifying threats and defining countermeasures to prevent or mitigate their effects on systems. A threat is an undesirable event that impacts negatively it may be malicious such as DDOS or Incidental (Deleting a file). A threat Model is a planned activity to detect and access the threat or vulnerability of an application.

## Threat modeling manifesto

Threat modeling manifesto follows two guidelines:

1. Values: A value is something that has worth for organizations.
2. Principles: It describes the Basic truths of threat modeling. Three types of fundamental principles.
  - a. Primary or general truths
  - b. Patterns (Highly recommended)
  - c. Anti-Pattern (Should be avoided)

## Threat modeling in SDLC

It is best practice to apply threat modeling continuously through software development. It highly recommends that Threat Modeling defines in early Stages such as the planning Phase and refined throughout the Life Cycle.

Recommended to update the threat model after such Events:

- A new feature is Released.
- Security incidents occur.
- Architectural or infrastructure changes

## Four Key Questions

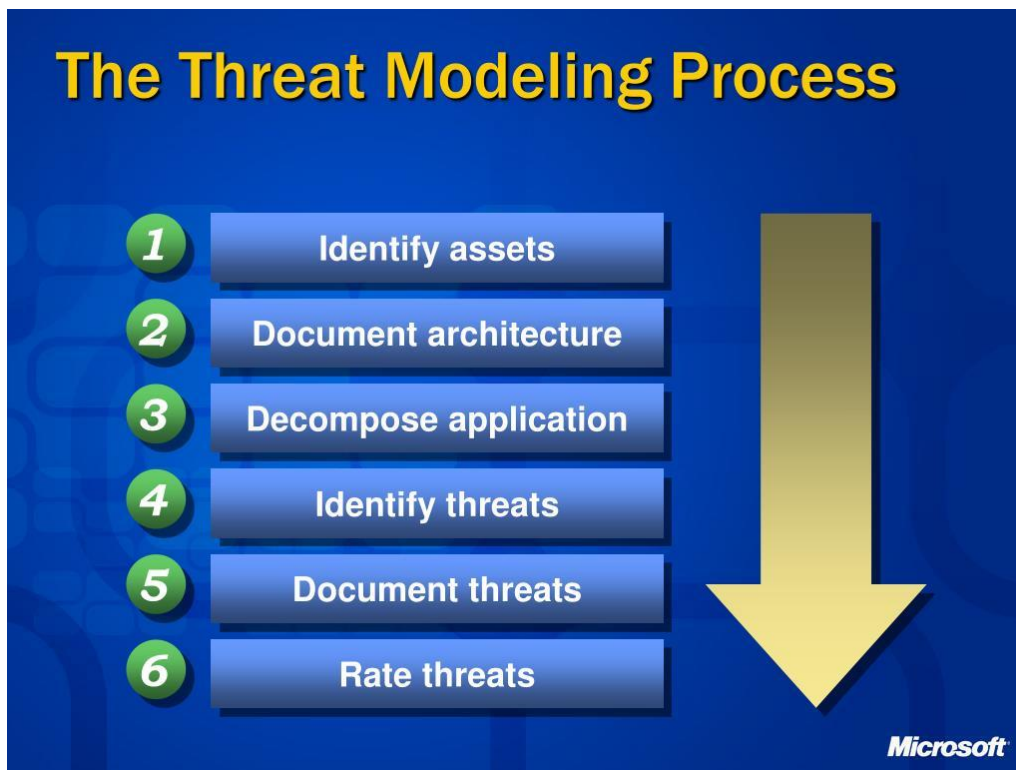
There are the following four questions framework helps to organize threat modeling.

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

There is more than one approach to solving these questions. There is no right way to solve it. It helps to refine search space to determine threats to focus on.

- **Assess Scope** - What are we working on? This might be as small as a sprint, or as large as a whole system.
- **Identify what can go wrong** - This can be as simple as a brainstorm, or as structured as using STRIDE, Kill Chains, or Attack Trees.
- **Identify countermeasures or manage risk** - Decide what you are going to do about each threat. That might be to implement mitigation or apply the accept/transfer/eliminate risk management approaches.
- **Assess your work** - Did you do a good enough job for the system at hand?

## Structured Process



## Benefits

Threat modeling provides the following benefits:

- Provide a Clear Line of sight to justify security efforts.
- Security decisions are made rationally.
- Assurance Agreement to defend and explain application security.

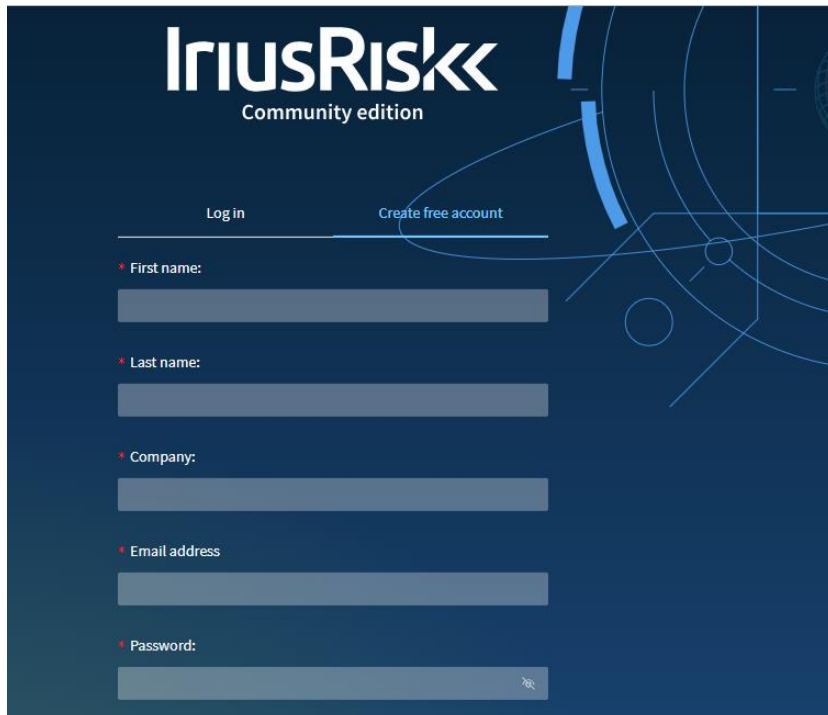
## Threat Modeling Tools

There is a wide selection of commercial as well as open-source threat modeling software to choose from. The following is a list of the top threat modeling tools that you should keep on hand for threat modeling.

- IriusRisk
- Threagile
- Tutamen
- Cairis (Computer-Aided Integration of Requirements and Information Security)
- Kenna VM
- OWAPS Threat Dragon
- SecuriCAD by Foreseeti
- ThreatModeler
- Microsoft Threat Modeling Tool
- SD Elements by Security Compass

### CONFIGURATION OF IRIUSRISK

IriusRisk is a threat modeling and SDL risk management platform that turns DevSecOps into reality. The Community Edition is a free version that helps you to mitigate cyber threats rapidly and manage risks across SDLC.

The image shows the IriusRisk Community edition login and registration interface. The background is dark blue with a subtle geometric pattern. The IriusRisk logo is at the top left, with 'Community edition' written below it. There are two links: 'Log in' and 'Create free account'. Below these are five input fields, each with a red asterisk and a label: 'First name:', 'Last name:', 'Company:', 'Email address', and 'Password:'. The 'Password:' field has a small icon of a key and a lock on the right side.

## REFERENCES

1. [Threat Modeling | OWASP Foundation](#)
2. [Threat Modeling Manifesto](#)
3. [Top 10 Threat Modeling Tools - zenarmor.com](#)