## CONNECT MASTERCLASS

# Threat Modeling Maturity Model

March 14, 11:00am-noon ET

Simone Curzi, Principal Consultant, Cyber @Microsoft

Altaz Valani, Principal Advisory Director @Info-Tech Research Group



## About me



Altaz Valani Principal Advisory Director Info-Tech Research Group



- Active collaborator across many open communities in Security, AI, and DevSecOps.
- Board Member at OASIS Open.
  - In the past, Vice-Chair of Security Forum at The Open Group and collaborator on Zero Trust, IT4IT, Digital Operating Model.
  - Conference speaker, podcast host, mentor, researcher.



## About me



Simone Curzi Principal Consultant, Cyber Microsoft

#### 24 years in Microsoft

#### Current role: Principal Consultant, Cyber

- Regular speaker to conferences like MS [Tech]Ready, MS Spark, DevSecOps Days, (ISC)2 Security Congress
- Co-author of a book on Azure Security for developers, with Michael Howard and Heinrich Gantenbein
- <u>Blog</u> & papers author (<u>Evolving Threat Modeling</u>, <u>Integrating threat modeling with DevOps – Security</u> <u>documentation | Microsoft Learn</u>)
- Active participant of the Open Group project for adopting Open FAIR as part of Threat Modeling processes
- Author of a Threat Modeling tool, <u>Threats Manager</u> <u>Studio</u>

s://www.linkedin.com/in/simone-curzi-a357b334/

#### Agenda











#### The Evolving Threat Modeling paper

#### What is it?

- The context in which it has been developed
- The problems we wanted to address

Why a Maturity Model for threat modeling?

And why "Evolving Threat Modeling" and not simply "Threat Modeling Maturity Model"?

#### WHITEPAPER

## **Evolving Threat Modeling for Agility** and Business Value



Source: https://bit.ly/evolvetm. Published March 2021.







Altaz Valani

Arun Prabhakar





Hasan Yasar

Jack Freund



Simone Curzi

#### Threat Modeling Manifesto/Capabilities



## THREAT MODELING MANIFESTO



## Source: <a href="https://www.threatmodelingmanifesto.org/">https://www.threatmodelingmanifesto.org/</a>.



Threat Modeling is critical to achieving design goals for system security and data privacy.

This document provides a catalog of capabilities to help you cultivate value from your Threat Modeling practice.

We are the <u>team</u> behind the <u>Threat Modeling Manifesto</u>. We have combined our collective experience in a conscious effort toward group consensus to create this document.

We have identified the following threat modeling capabilities to help you create or refine a roadmap for your threat modeling program and understand where your program is.

We feel that organizations that implement these capabilities will meet their secure design objectives and avoid many pitfalls and challenges when performing threat modeling.

### Source: <a href="https://www.threatmodelingmanifesto.org/capabilities/">https://www.threatmodelingmanifesto.org/capabilities/</a>.



The different perspectives on threat modeling



#### Many Methodologies



- STRIDEPASTA
- Attack Trees

#### **Different Tools**

- Automated tools
- Visual modeling

#### Different Approaches

- Attacker centric
- Asset centric
- Developer centric

#### Different Objectives

- Adhere to regulations
- Managing risk
- Assess threat landscape



Question: What is the best approach?

#### Biggest pain points with the traditional approaches





Totally reliant on automated tools



A silo approach to threat modeling



Diagrams as the only way to enumerate threats



Processes are more static than dynamic



Overthinking at the initial stages than doing it incrementally



Using checklist to discover only known threats

#### The increasing demand for evolving threat modeling



Current Scenario

- 1. Project development methodologies are following Agile and DevOps
- 2. Advanced solutions with the use of emerging technologies and platforms
- 3. MVPs and periodic releases demand speed in building products
- 4. DevSecOps principles recommend codifying security controls in software
- 5. Several stakeholders showing great interest in threat models, especially leadership

#### Desired Outcome

- 1. This means threat modelers work in **close collaboration** with teams
- 2. This leads to new **threat patterns** and attack methods
- 3. This requires the threat modeling process to be **flexible** and **scalable**
- 4. This means **mitigations** will be the core activity in threat models and not threats
- 5. Hence the focus is on **risk**, ROI and establishing value to the business

#### Effective threat modeling





Layered threat modeling



Integrate threat models



Actionable outcome



Continuous activity



Provide value to stakeholders







### The Threat Modeling Maturity Model

Finally...

#### Maturity levels of threat modeling





#### Tool categories throughout threat modeling maturity



Threat Modeling Value Stream Alignment



Static Threat Model Analysis Tool



Event and Monitoring Management and Incident Response

Knowledge base that

contain information

about threats and



Application & infrastructure architecture system modeling

such as CWE codes

categorization tool

Applications and

Services Inventory

Threat

categorization

Mitigation



flow)

OSINT tools (Shodan, Searchcode)

Dashboard/reporting

system

Root Cause

Analysis

Tool



mitigations Issue Tracker

Intelligence



Threat severity calculator



Risk management system (risk identification, mitigation approval, threshold, ..)



#### Applications and services inventory

Inventory contains key assets in threat model

Owner for each key asset in threat model

> Level 1 - No threat modeling tool

Clear relationships across stack for key assets in the inventory

Infrastructure as Code, Security as Code, Compliance as Code from inventory tool

Level 2 - Threat modeling tool

Level 3 - Threat modeling platform

Assets in threat

monitored against CWE, CVE codes

model are

Key assets in

threat model are

integrated with

management

Primary and

key assets in

threat model

secondary risk

stakeholders of

incident

Regular risk assessment of the key assets

Business included in the asset risk assessment

Risk assessment is contextual

Level 4 - Risk driven knowledgebase





#### Application & Infrastructure architecture system modeling

System model includes all key systems (external interactions) in threat model

Basic system classification used in threat model

Address right system context

> Level 1 - No threat modeling tool

Includes tool representations (secrets management, IAM, etc)

Has system trust boundaries

Complies with organizational policies and regulations

> Level 2 - Threat modeling tool

Makes use of reusable. self contained system templates

Uses multiple lavers of abstraction across different system diagrams

Business system flow is documented in threat model

Level 3 - Threat modeling platform

Associate multiple threat models for your system

Account for different contexts (infrastructure. application, data)

Level 4 - Risk driven knowledgebase

#### Threat categorization such as CWE codes

Using industry knowledge bases (CAPEC, CWE, ATT&CK)

Internal knowledge bases

Threats across different systems are associated to create new or different insights

modeling

Structured approach to maintain and apply your internal threat model knowledge base across its lifecycle

Constructing threats in your threat model that are relevant to the business

Level 4 - Risk driven knowledgebase

Level 1 - No threat modeling tool



Using threat categories to identify threats

Using threat categories to identify mitigations

> Level 2 - Threat modeling tool

Level 3 - Threat platform

#### Mitigation categorization tool

Defined standard mitigations (maybe using a defensive framework like STRIDE, OCTAVE, etc. as guidance) against threat categories

Extend the categories beyond preventative to include, for example, corrective and detective mitigations

> modeling platform

Structured approach to maintain and apply your internal knowledge base (knowledge lifecycle)

Knowledge is accessible to others for determining additional mitigations

Level 4 - Risk driven knowledgebase

Identified one or more mitigations for each threat

Level 1 - No threat modeling tool

Level 2 - Threat modeling tool

Level 3 - Threat



#### Static threat model analysis tool

Integrated process to automatically validate the threat model and identify problems in the tool

Using best practice guidelines (ex. OWASP Top 10) as part of the threat modeling process

Level 1 - No threat modeling tool Updating the threat model as soon as errors are discovered

Level 2 - Threat modeling tool

Integrated into your automated DevOps pipeline

Feedback loop that automatically creates threat modeling update tasks and activities

Level 3 - Threat modeling platform Create your own policies or rules

Automated feedback loop to business and technical teams so that it creates rules for your threat model

Centralized view around quality of all your threat models (dashboards)

Level 4 - Risk driven knowledgebase



#### Dynamic threat model analysis tool (simulated data flow)

Identified key users (including malicious insiders, attacks to privileged roles) and tested whether mitigations prevent breach

Considered and contextualized known past attack scenarios

Tested all documented assumptions about external systems/services that interact with the system

Level 2 - Threat modeling tool

Simulated most relevant environment and scenarios aligned to organizational risk (from knowledge base or public repository)

Simulation rules easily understandable and manageable

Considered most important attacker profiles as aligned with organizational risk

> Level 3 - Threat modeling platform

Simulations rules map to business priorities and specific scenarios (regulatory compliance, architecture, functional cases, etc)

Expand simulation rules and scenarios based on the attacks you are seeing

Continuously improve based on known KPIs ( accuracy of % of false positives, calculated vs real severity, coverage of threats)

Level 4 - Risk driven knowledgebase

Someone playing the threat agent and another playing the defender

> Level 1 - No threat modeling tool





### Next Steps

What you should get out of it

#### Next steps



Walk before you run

Definition & Terminologies

TM Process & workflows

Stakeholder requirements



Involve multiple SME

•Discover the unknowns

•Learn the art



Learn & Grow

Top 10 Security threats

•Documents & Templates



First, Do It Yourself

• Applying the concepts

•Using a tool

5

Mature your Threat Models

Do it continuously

Collaborate with teams

•Contribute to the Industry





