



POLITECNICO
MILANO 1863

Hitchhiker's guide to threat modeling

Simone Curzi

Principal Consultant, Cyber
Microsoft Security CyberOps Resilience
Security Service Line | Industry Solutions - Microsoft Security

OWASP Italy Day 2023

Politecnico of Milan - 11th September 2023



OWASP FOUNDATION

Agenda



Let me present myself
What is Threat Modeling?
What should I threat model?
Is Threat Modeling a tool?
Demo

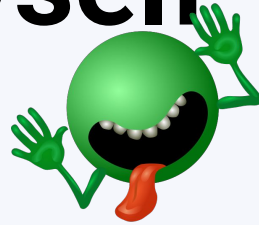
Open: Everything at OWASP is radically transparent from our finances to our code.

Innovative: We encourage and support innovation and experiments for solutions to software security challenges.

Global: Anyone around the world is encouraged to participate in the OWASP community.

Integrity: Our community is respectful, supportive, truthful, and vendor neutral

Let me present myself



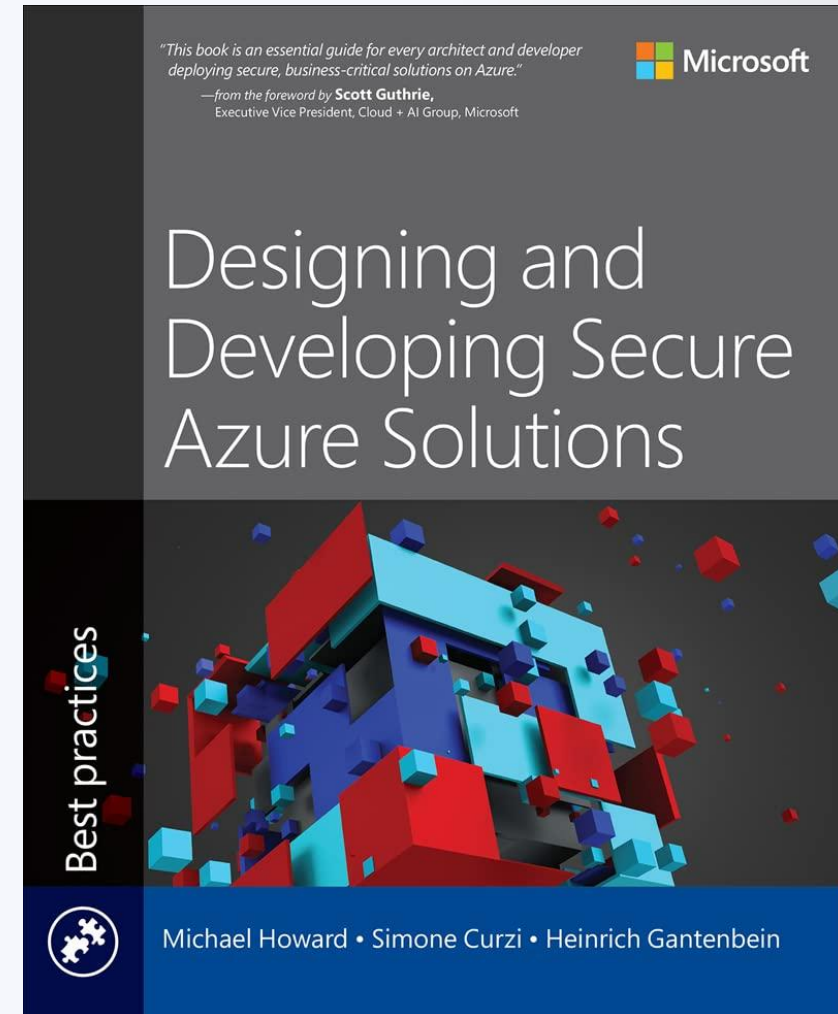
23 years in Microsoft

Current role: Principal Consultant, Cyber

Leader of the WW SDL Community for 5 years

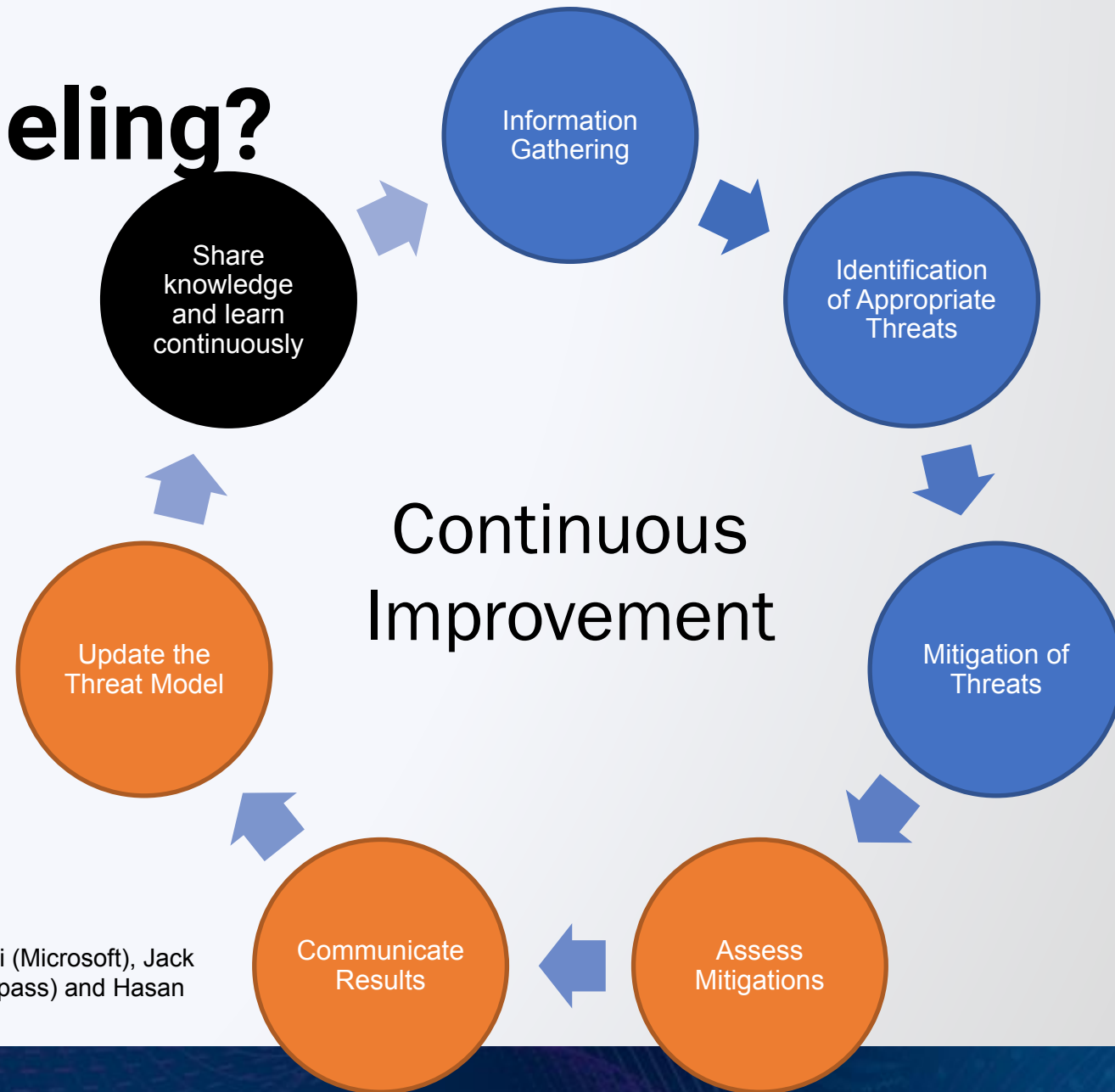
SME for the WW Security and SDL Communities

- 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
- Blog & papers author (Evolving Threat Modeling, Integrating threat modeling with DevOps - Security documentation | Microsoft Learn)
- Active participant of the Open Group project for adopting Open FAIR as part of Threat Modeling processes
- Author of a Threat Modeling tool, Threats Manager Studio



What is Threat Modeling?

Threat Modeling is a process to understand **security threats** to a system, determine **risks** from those threats, and establish appropriate **mitigations**.

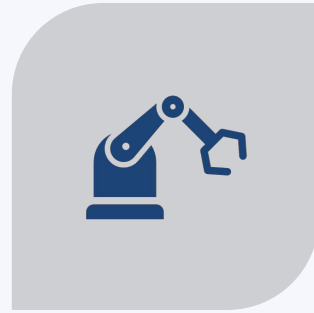


From study "Evolving Threat Modeling for Agility and Business Value" by Simone Curzi (Microsoft), Jack Freund (VisibleRisk), Arun Prabhakar (Security Compass), Altaz Valani (Security Compass) and Hasan Yasar (SEI, Carnegie Mellon University), <https://bit.ly/evolvetm>.

What should you threat model?



The solution



CI/CD



Administration

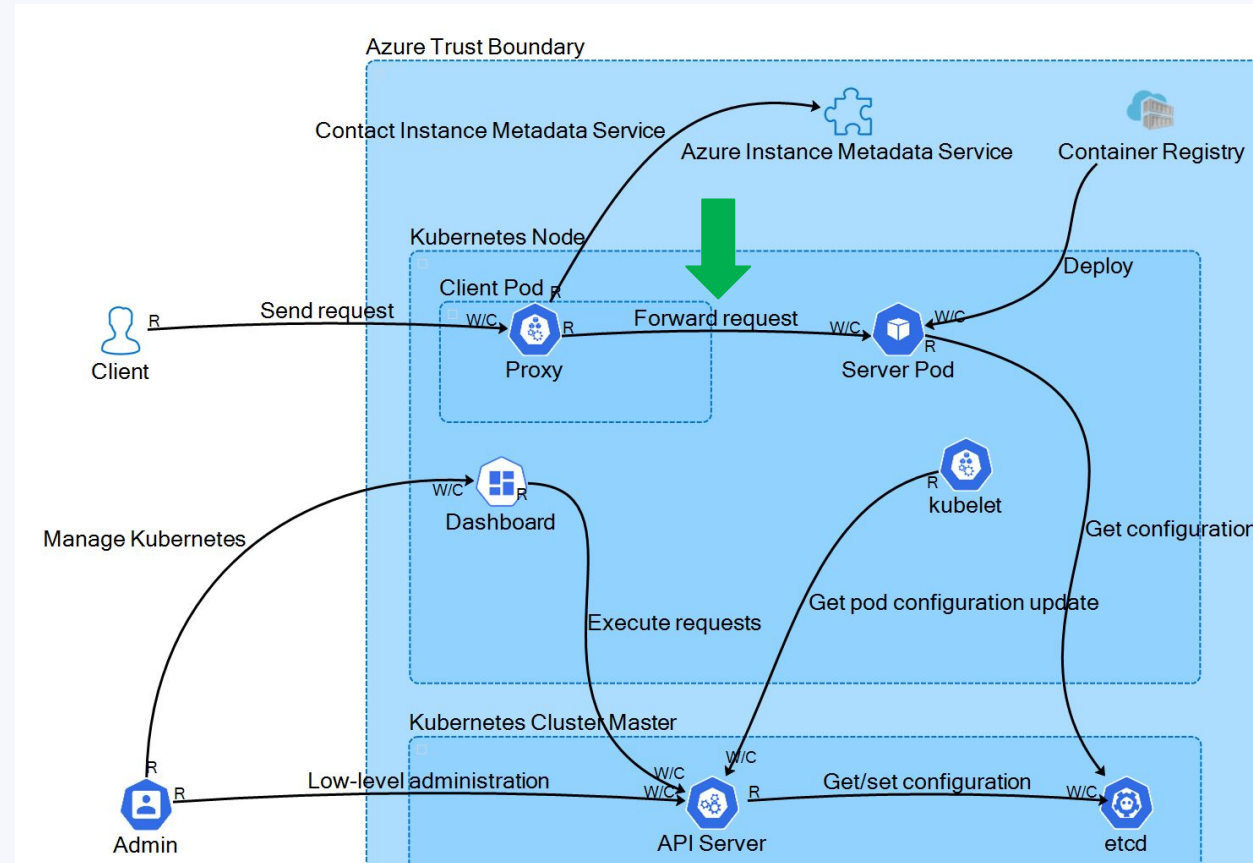


Specific Scenarios
(ex.: Data Scientist)

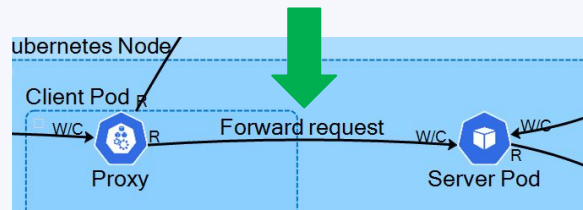


DevSecOps
environment

“I do Threat Modeling! I use tool XYZ!”



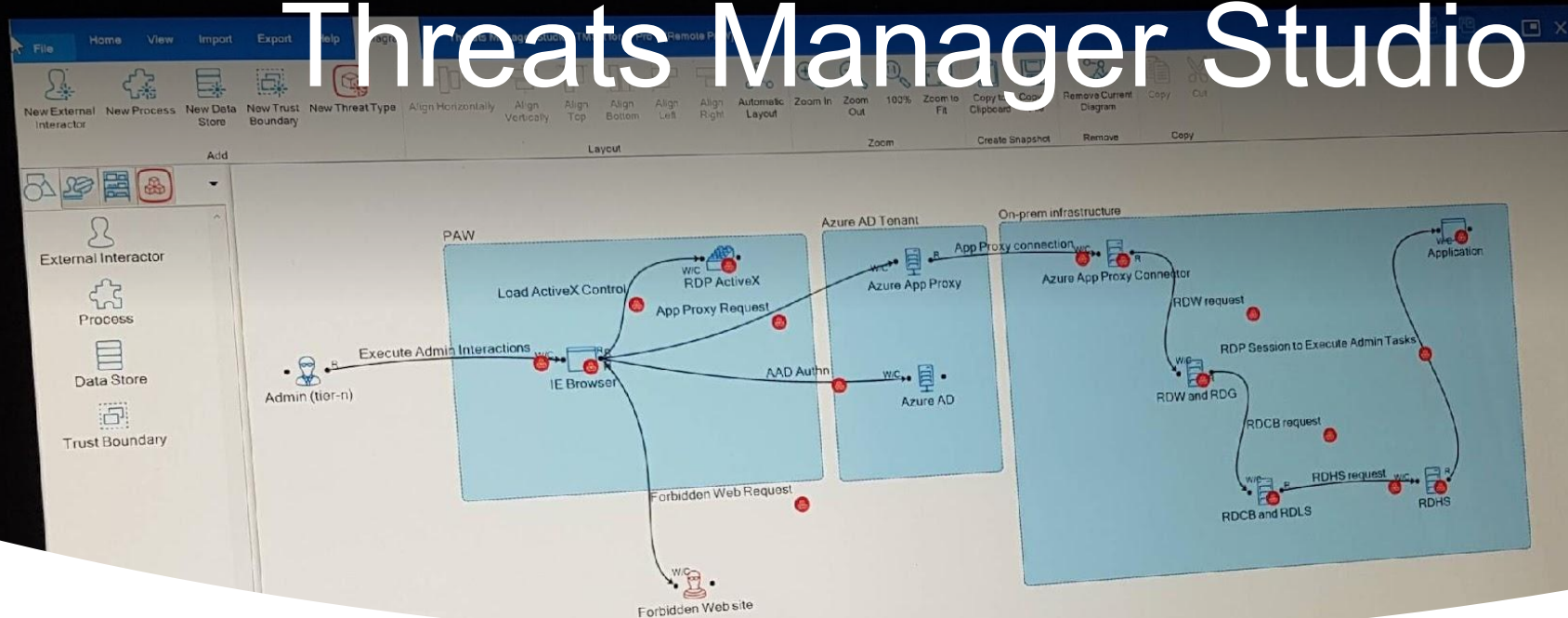
How many Threat Modeling products identify Threats



Would you be able to understand anything from that???



Threats Manager Studio



Implements a
modern Threat
Modeling vision



Designed and
implemented by
Threat Modeling
experts



Composed of a
growing set of
functionalities



Free, public, and
open source
<https://threatsmanager.com>



It allows you to
create your own
experience

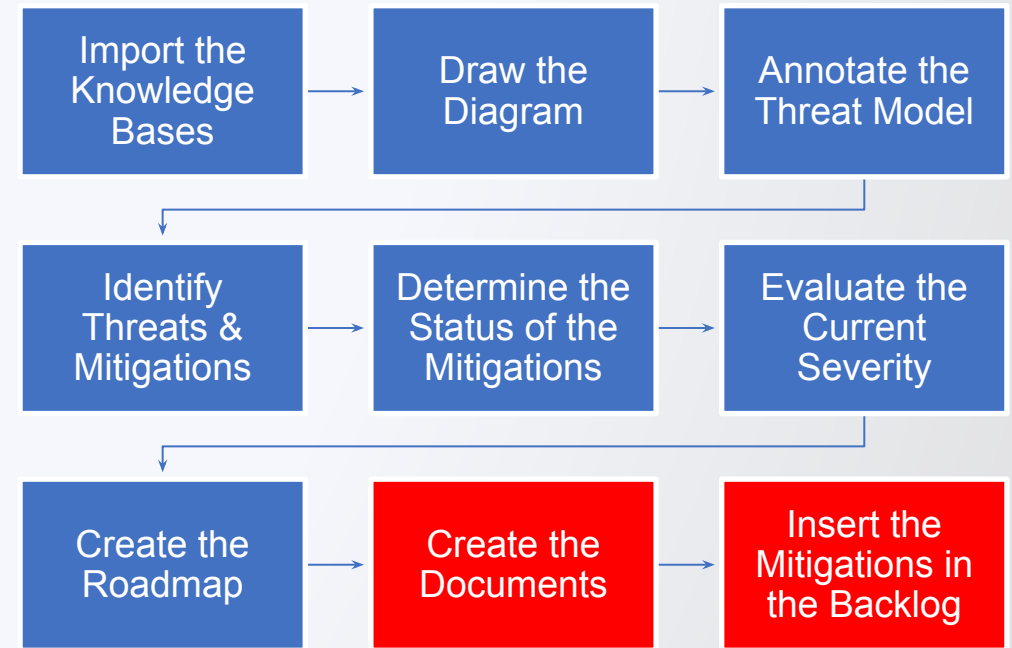
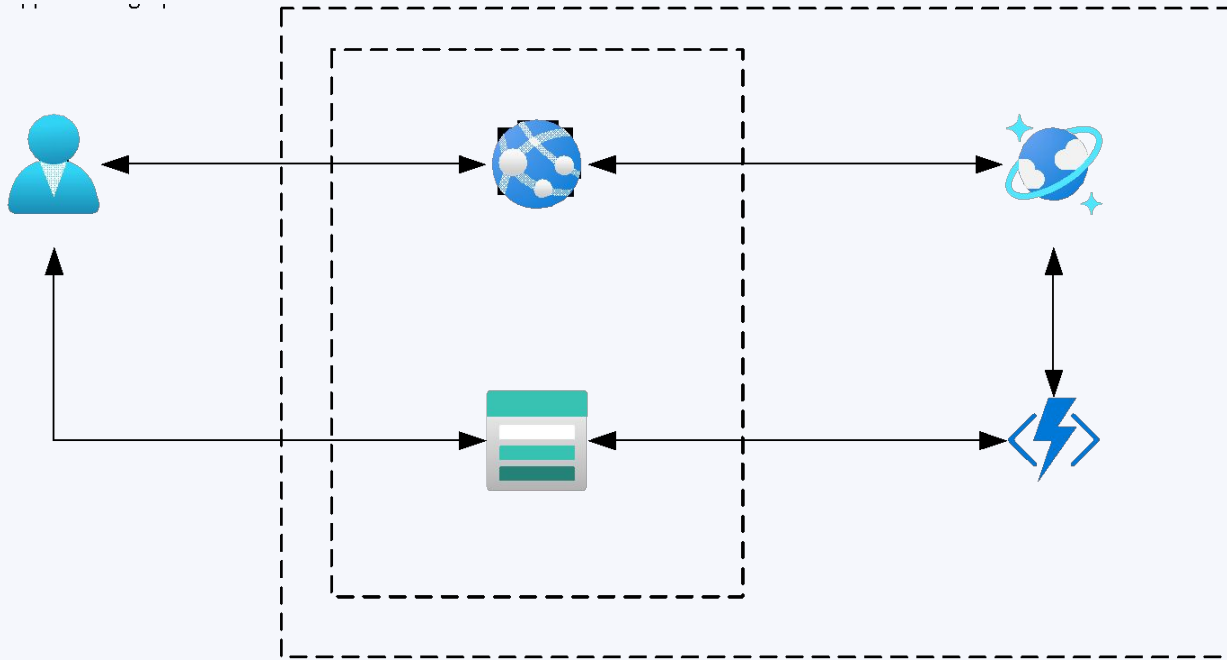
Important



Threats Manager Studio is **NOT** a Microsoft Product and is **NOT** supported by Microsoft.

It is not a commercial product either but can be freely used for business purposes (see <https://threatsmanager.com/license>)

Threat Modeling demo with TMS



Thank you to our sponsors





OWASP 2023
ITALY DAY