THREAT MODELING 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.

https://www.linkedin.com/in/altazvalani/

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
- 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

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

Agenda

The Evolving Threat Modeling paper

The Maturity Model

Next Steps

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

Altaz Valani

Arun Prabhakar

Hasan Yasar

Jack Freund

Simone Curzi

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

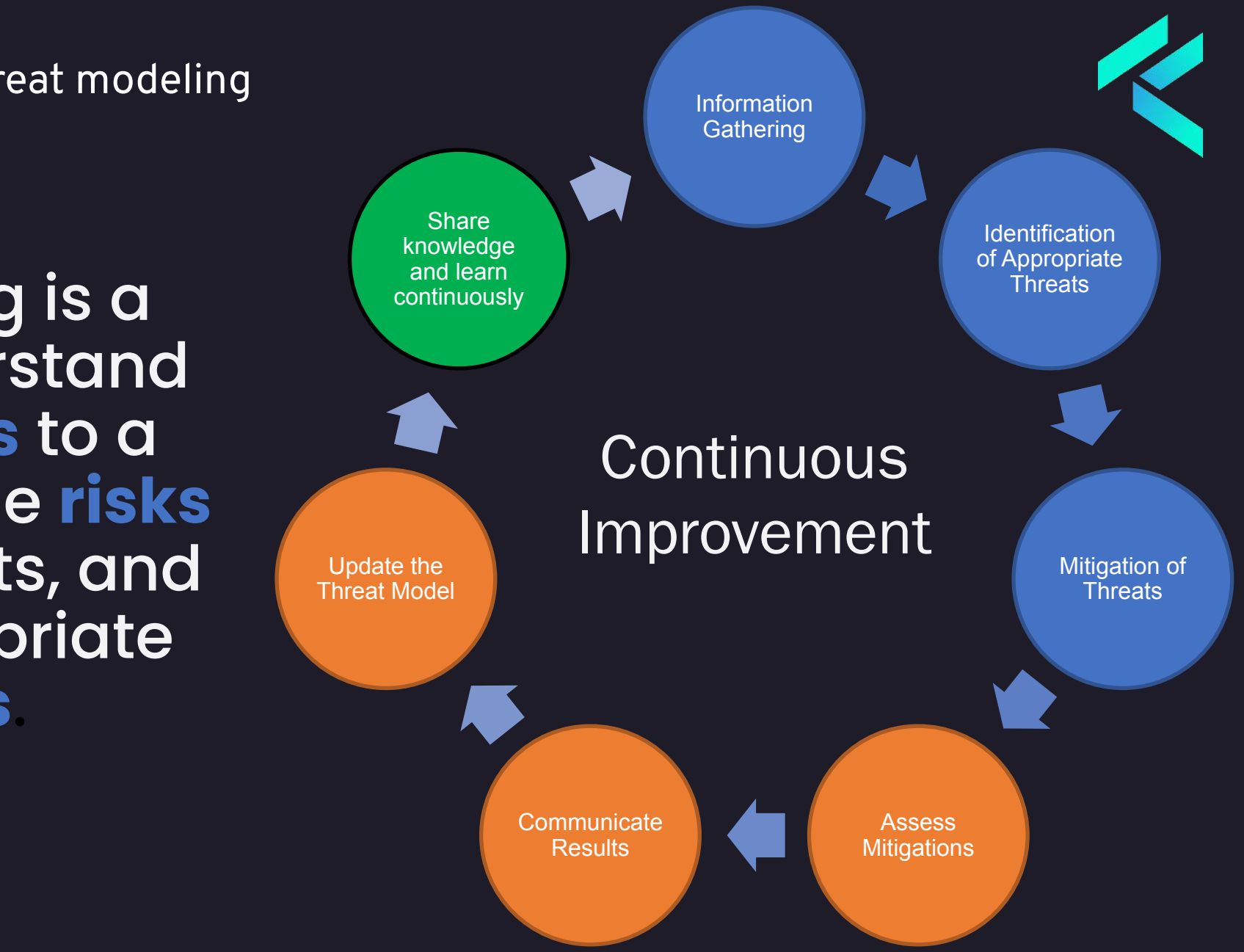
Threat Modeling Manifesto/Capabilities

Source: https://www.threatmodelingmanifesto.org/.

Source: https://www.threatmodelingmanifesto.org/capabilities/.

We started defining threat modeling

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



The different perspectives on threat modeling

Many Methodologies

- STRIDE
- PASTA
- Attack Trees

Different Tools

- Automated tools
- Visual modeling

Different Approaches

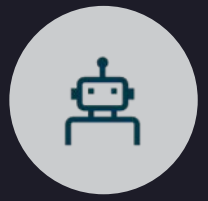
- Attacker centric
- Asset centric
- Developer centric

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

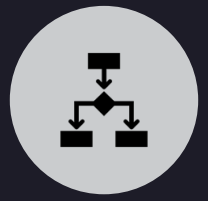
Desired Outcome

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

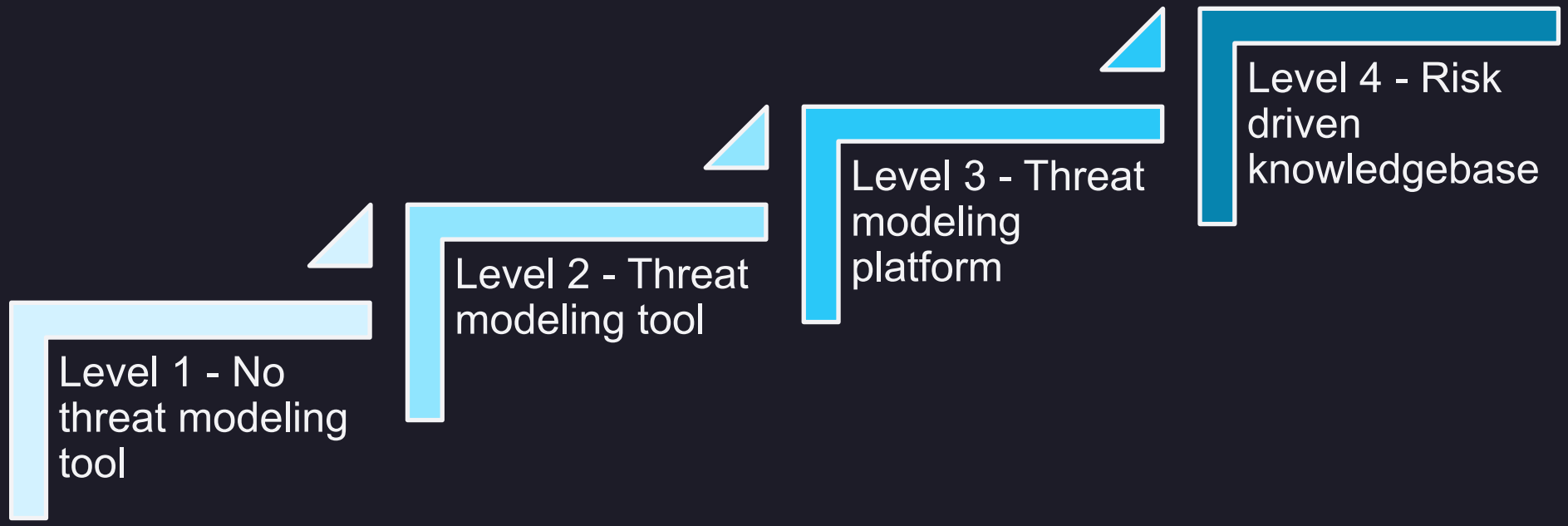
Provide value to stakeholders

Integrated threat modeling

The Threat Modeling Maturity Model

Finally...

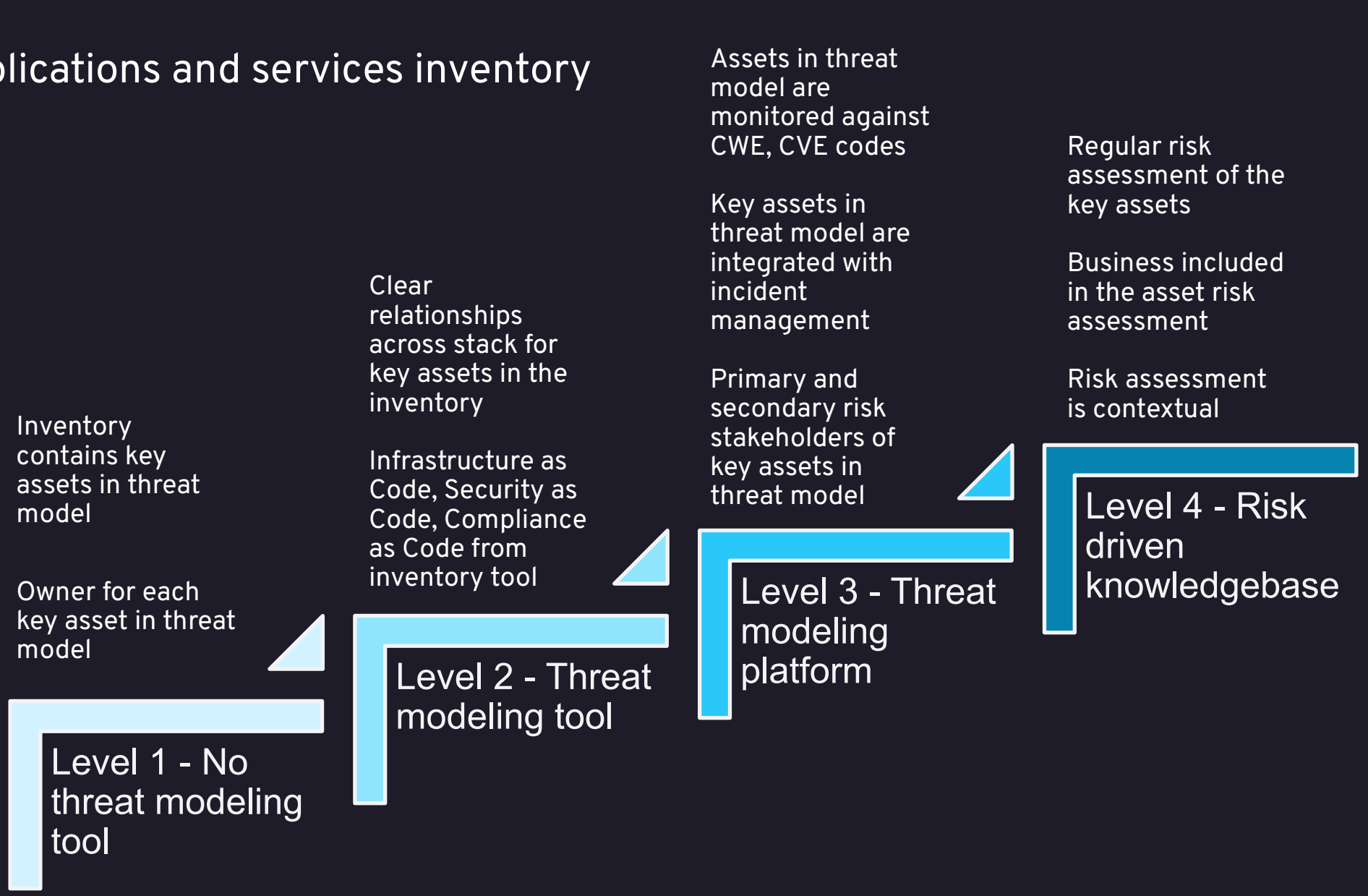
Maturity levels of threat modeling



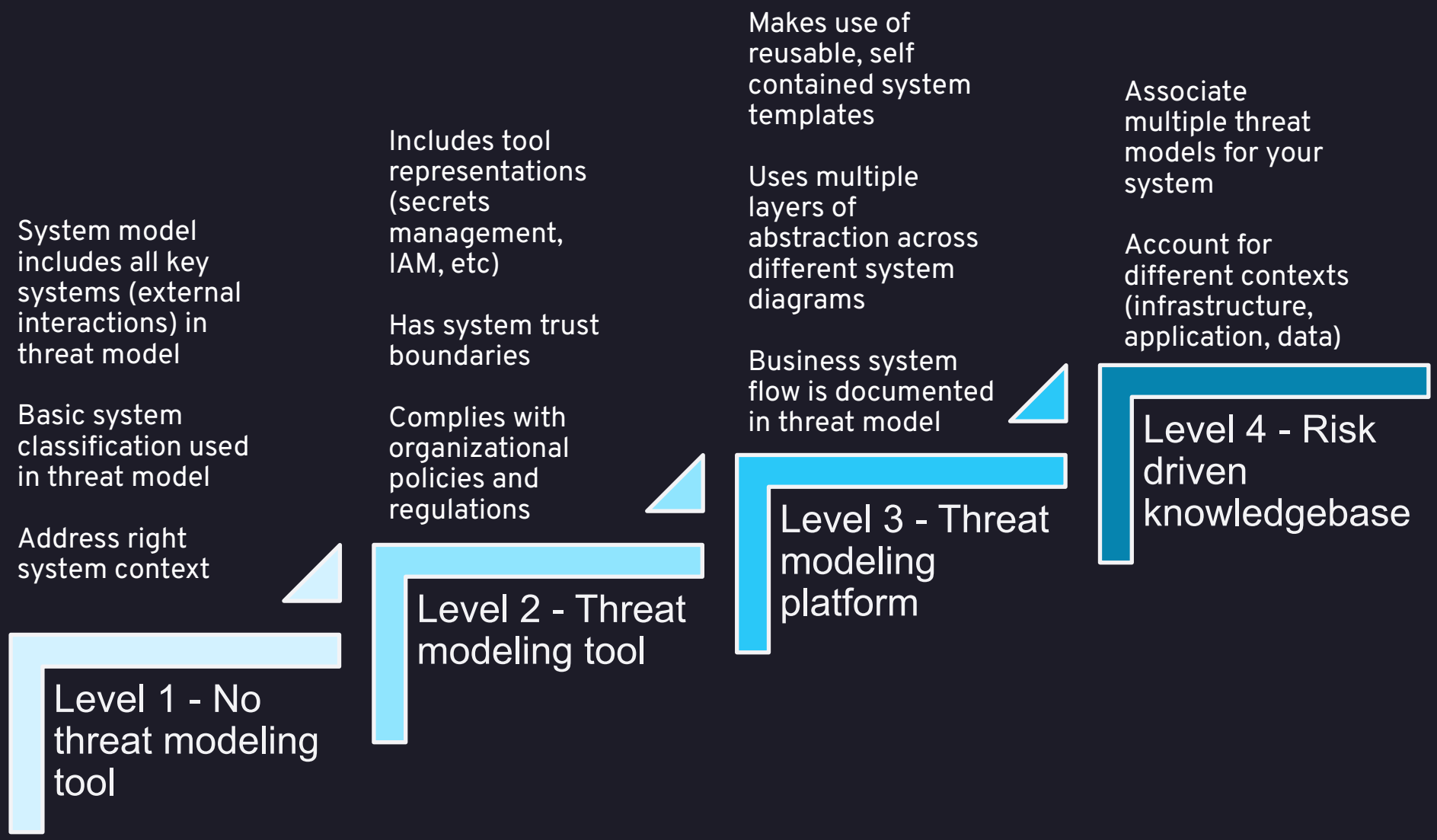
Tool categories throughout threat modeling maturity

- Threat Modeling Value Stream Alignment
- Application & infrastructure architecture system modeling
- Threat categorization such as CWE codes
- Mitigation categorization tool
- Applications and Services Inventory
- Static Threat Model Analysis Tool
- Dynamic Threat Model Analysis Tool (Simulated data flow)
- OSINT tools (Shodan, Searchcode)
- Dashboard/reporting system
- Root Cause Analysis Tool
- Event and Monitoring Management and Incident Response
- Intelligence Knowledge base that contain information about threats and mitigations
- Issue Tracker
- Threat severity calculator
- Risk management system (risk identification, mitigation approval, threshold, ..)

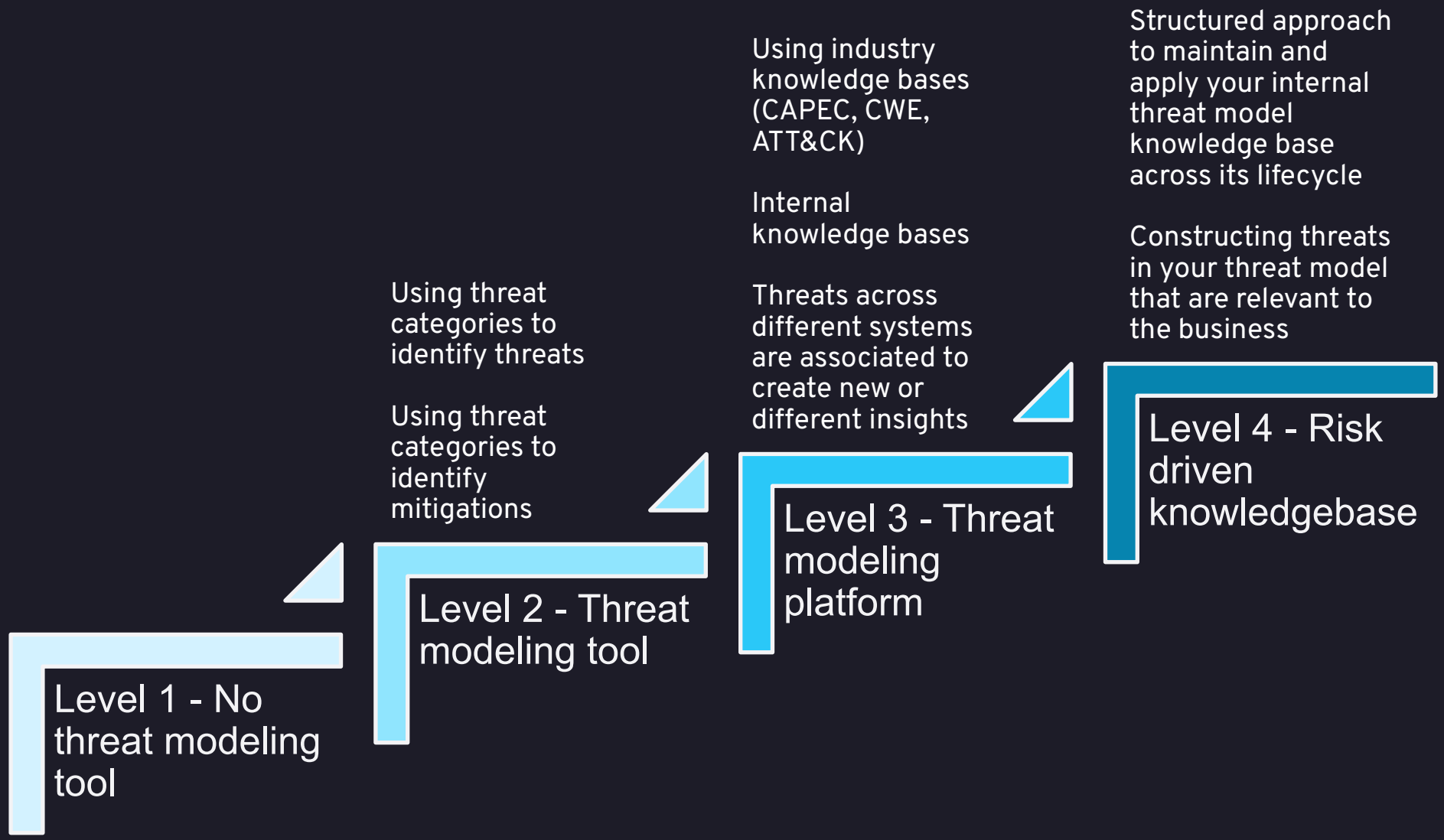
Applications and services inventory



Application & Infrastructure architecture system modeling

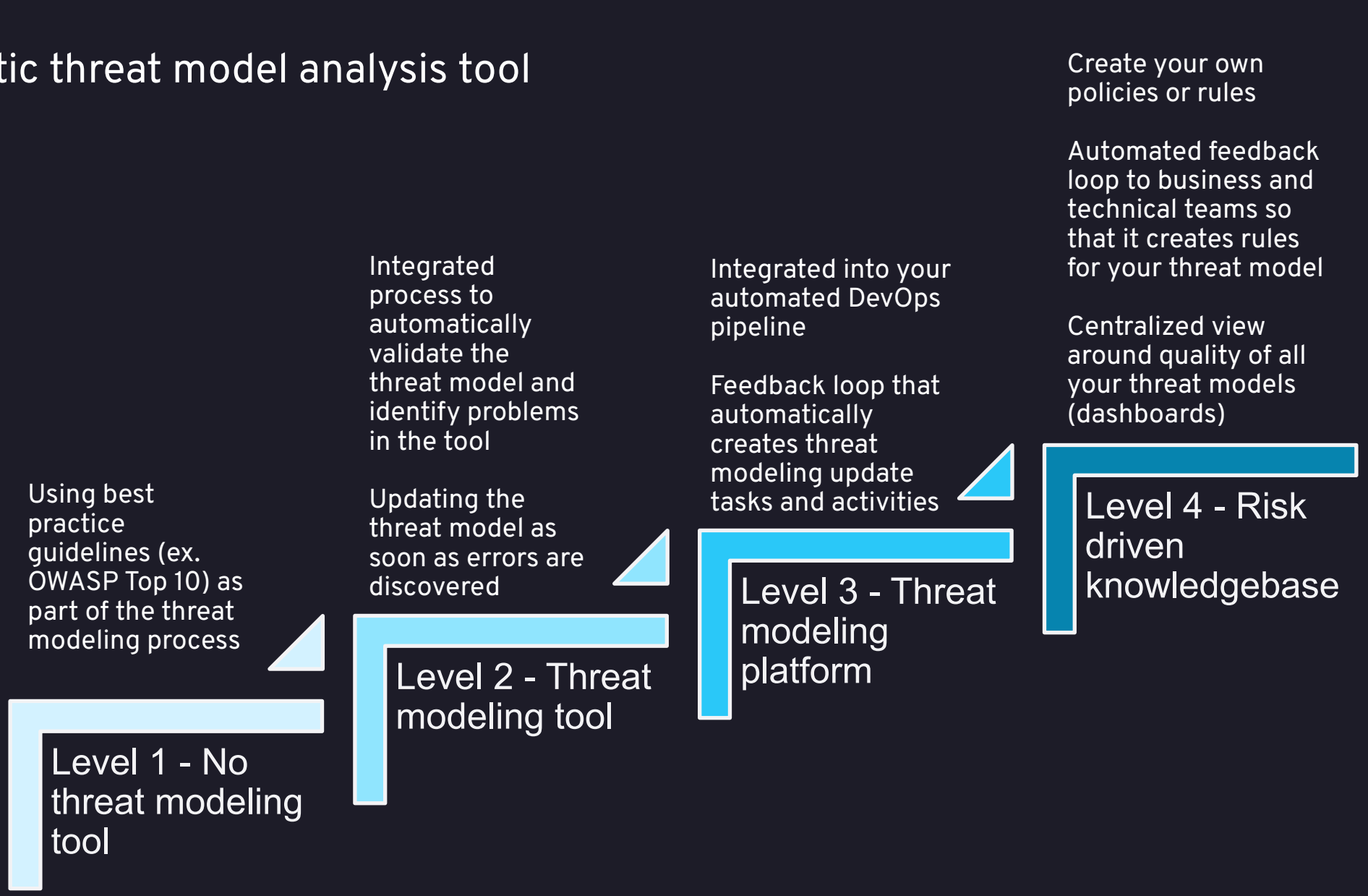


Threat categorization such as CWE codes



Mitigation categorization tool

Static threat model analysis tool



Dynamic threat model analysis tool (simulated data flow)

Level 1 - No threat modeling tool

Someone playing the threat agent and another playing the defender

Level 2 - Threat modeling tool

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 3 - Threat modeling platform

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 4 - Risk driven knowledgebase

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)

Next Steps

What you should get out of it

Next steps

1. Walk before you run
   - Definition & Terminologies
   - TM Process & workflows
   - Stakeholder requirements
2. Learn & Grow
   - Top 10 Security threats
   - Documents & Templates
3. First, Do It Yourself
   - Applying the concepts
   - Using a tool
4. Involve multiple SME
   - Discover the unknowns
   - Learn the art
5. Mature your Threat Models
   - Do it continuously
   - Collaborate with teams
   - Contribute to the Industry

Q&A