SPARX SYSTEMS

EA Global Summit 2020

June 1st to 5th | Connect with World's Prolific Sparx EA Practitioners

Cyber Security Modelling

Bob

Sparx Systems Central Europe

4th June

PDT 03.00
CET 12.00
AEST 20.00

30 Min

Register

eaglobalsummit.com

ENTERPRISE ARCHITECT

Pro Cloud Server

Prolaborate

DDos ATTACK

SPARX SYSTEMS CENTRAL EUROPE

Learning Objectives

- Develop broader cybersecurity awareness
- Get familiar with the concept of threat modeling
- Modeling threats using the Cyber Security Profile (based on STRIDE) introduced in Enterprise Architect 15.1
- Analyzing, visualizing and communicating the threat model to all stakeholders

Sparx Systems HQ

Sisters Companies

ENTERPRISE ARCHITECT

SPARX SYSTEMS CENTRAL EUROPE

threat

/θrɛt/

noun

noun: **threat**; plural noun: **threats**

1. a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done.
   "members of her family have received **death threats**"

   Similar: threatening remark | warning | ultimatum | intimidating remark

   - LAW
     a menace of bodily harm, such as may restrain a person's freedom of action.

2. a person or thing likely to cause damage or danger.
   "hurricane damage poses a major **threat to** many coastal communities"
   - the possibility of trouble, danger, or ruin.
     "the company faces the threat of liquidation proceedings"

     Similar: danger | peril | hazard | menace | risk | possibility

Origin

GERMANIC → thrēat

OLD ENGLISH → thrēat

DUTCH: verdrieten (grieve) → threat

GERMAN: verdriessen (irritate) → threat

Old English *thrēat* 'oppression', of Germanic origin; related to Dutch *verdrieten* 'grieve', German *verdriessen* 'irritate'.

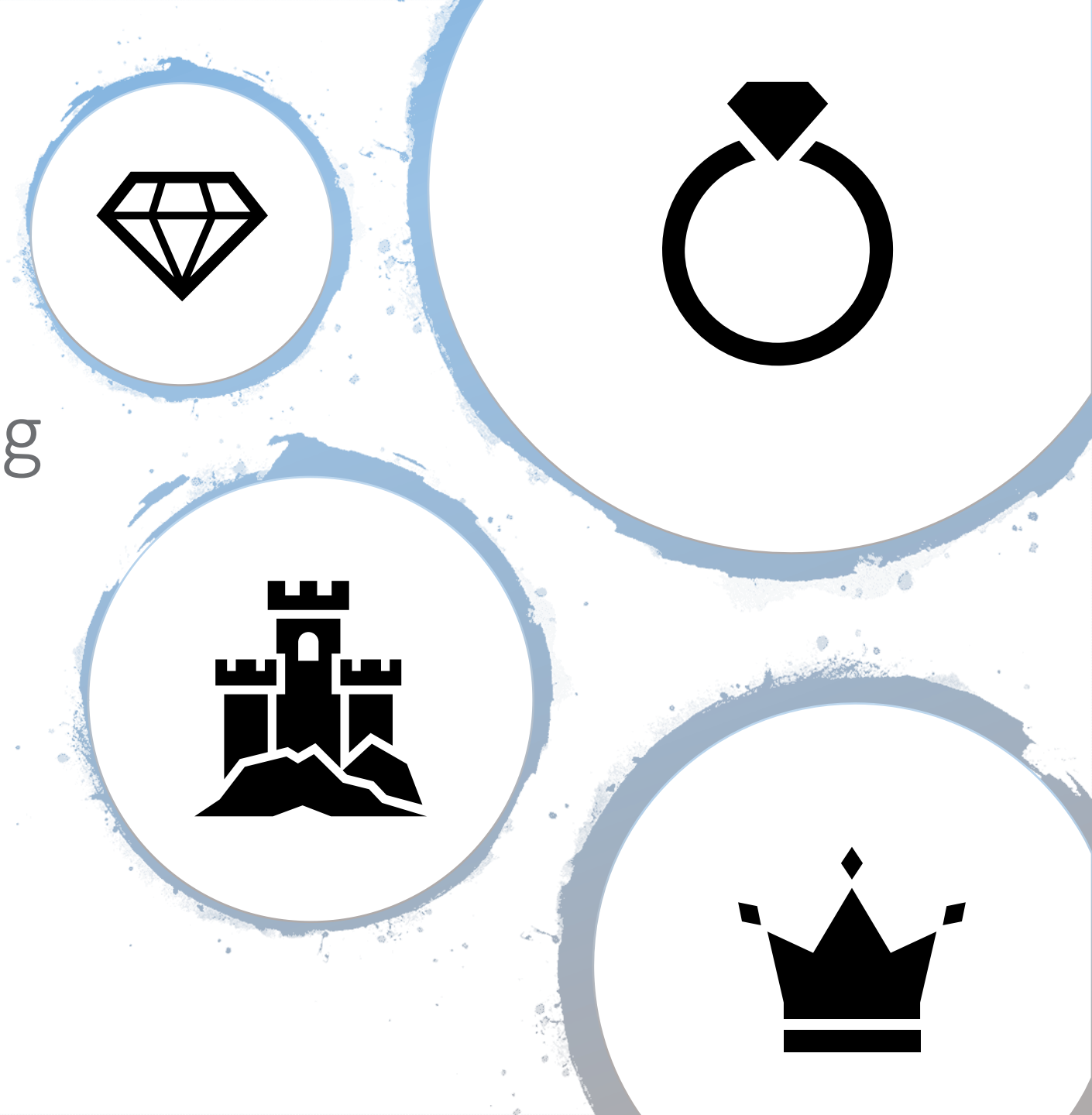
ENTERPRISE ARCHITECT

SPARX SYSTEMS CENTRAL EUROPE

https://www.lexico.com/en/definition/threat

What is Threat Modeling

- **Structured Process**
  - Examination of a system for potential weaknesses



What is Threat Modeling

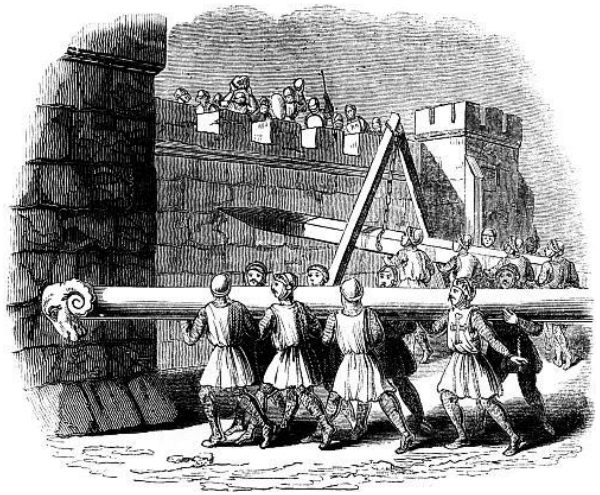
Structured Process

- Examination of a system for potential weaknesses

Systematic approach

- Based on a conceptual model of weaknesses and threats

https://www.castlesworld.com/tools/motte-and-bailey-castles.php



https://en.wikibooks.org/wiki/Castles_of_England/Methods_of_Attack

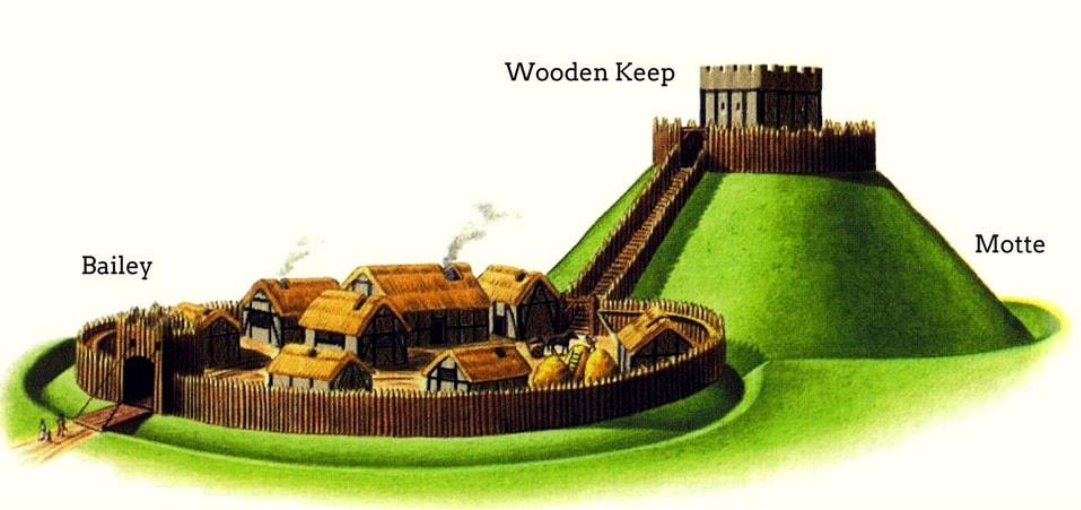
What is Threat Modeling

Structured Process

- Examination of a system for potential weaknesses
- Resolving identified weaknesses

Systematic approach

- Based on a conceptual model of weaknesses and threats



https://www.castlesworld.com/tools/concentric-castles.php

https://deadliestwarrior.fandom.com/wiki/Huo_Chien

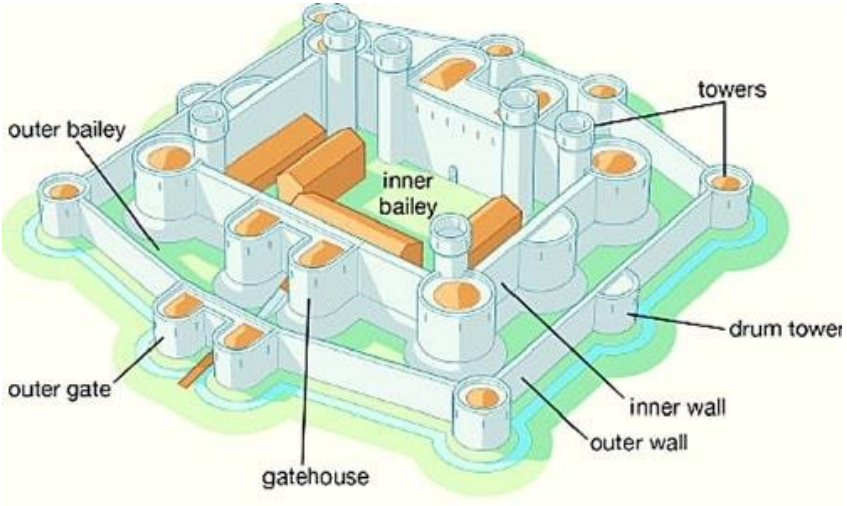
What is Threat Modeling

Structured Process

- Examination of a system for potential weaknesses
- Resolving identified weaknesses

Systematic approach

- Based on a conceptual model of weaknesses and threats
- Keeping the model of weaknesses and threats up to date



https://www.castlesworld.com/tools/concentric-castles.php

https://www.pbs.org/video/1812-niagara-frontier-fort-george-cannon-firing/

ENTERPRISE ARCHITECT

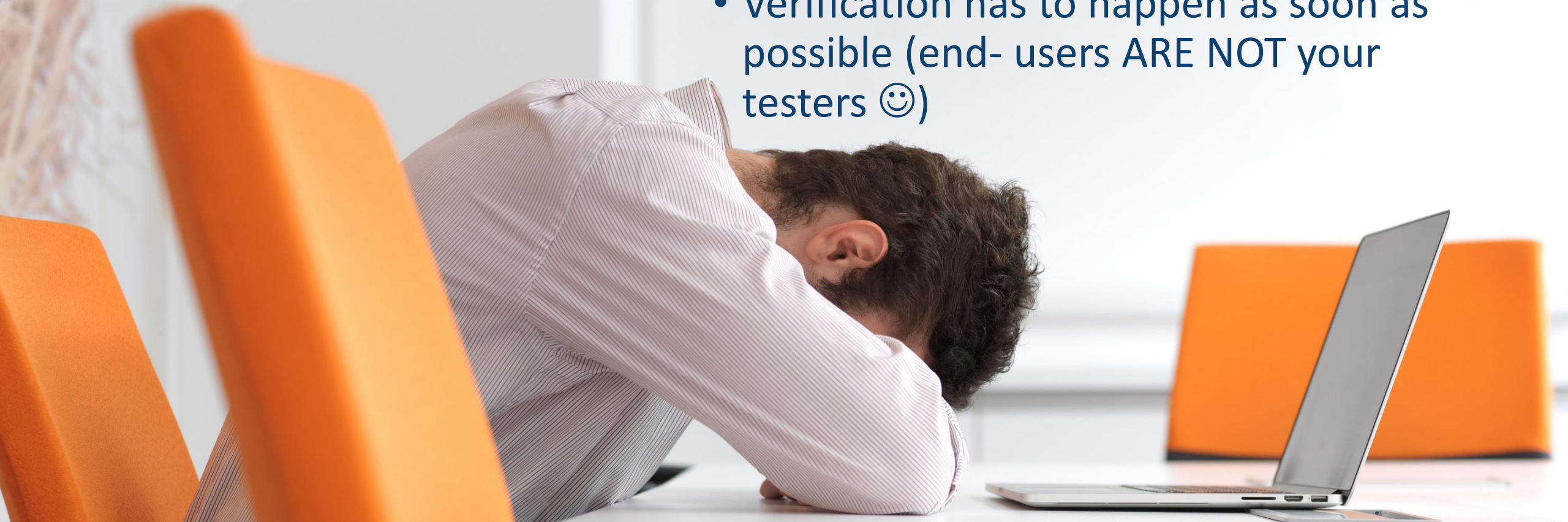
SPARX SYSTEMS CENTRAL EUROPE

Nowadays challenges…

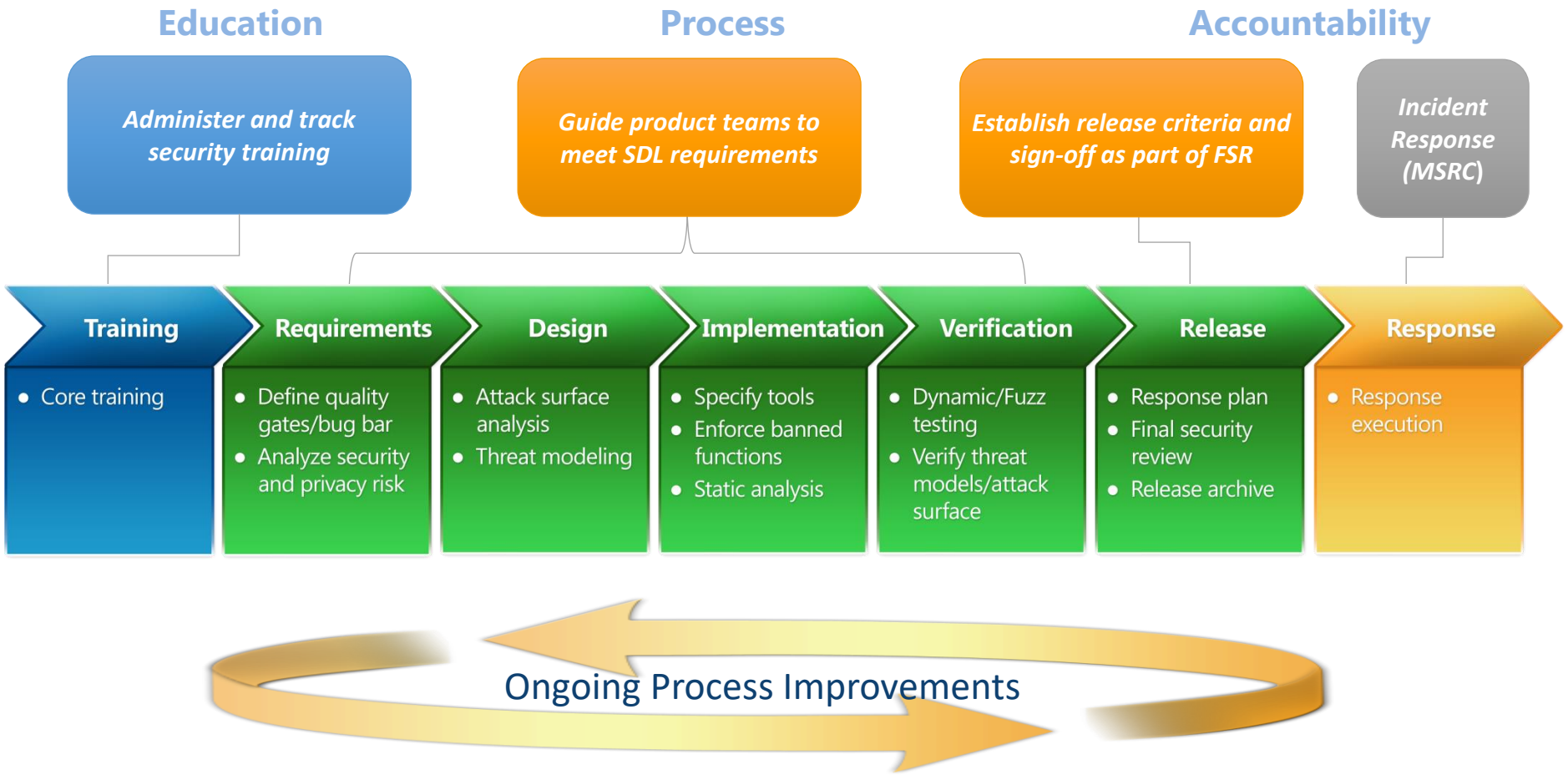
- Servers are wide open to the internet with no authentication.
- Backdoor “service” passwords on systems are published in easily obtained service manuals.
- Some devices have nothing even resembling security.
- Increased Usage of Third-Party Products (Commercial and Open Source)
- Standalone Device Vulnerabilities – Firmware can be maliciously altered and uploaded, replacing authentic file
- … you name it

Cybersecurity is not in a development DNA!

- Insert security practices as a part of your software development lifecycle
- Verification has to happen as soon as possible (end- users ARE NOT your testers ☺)

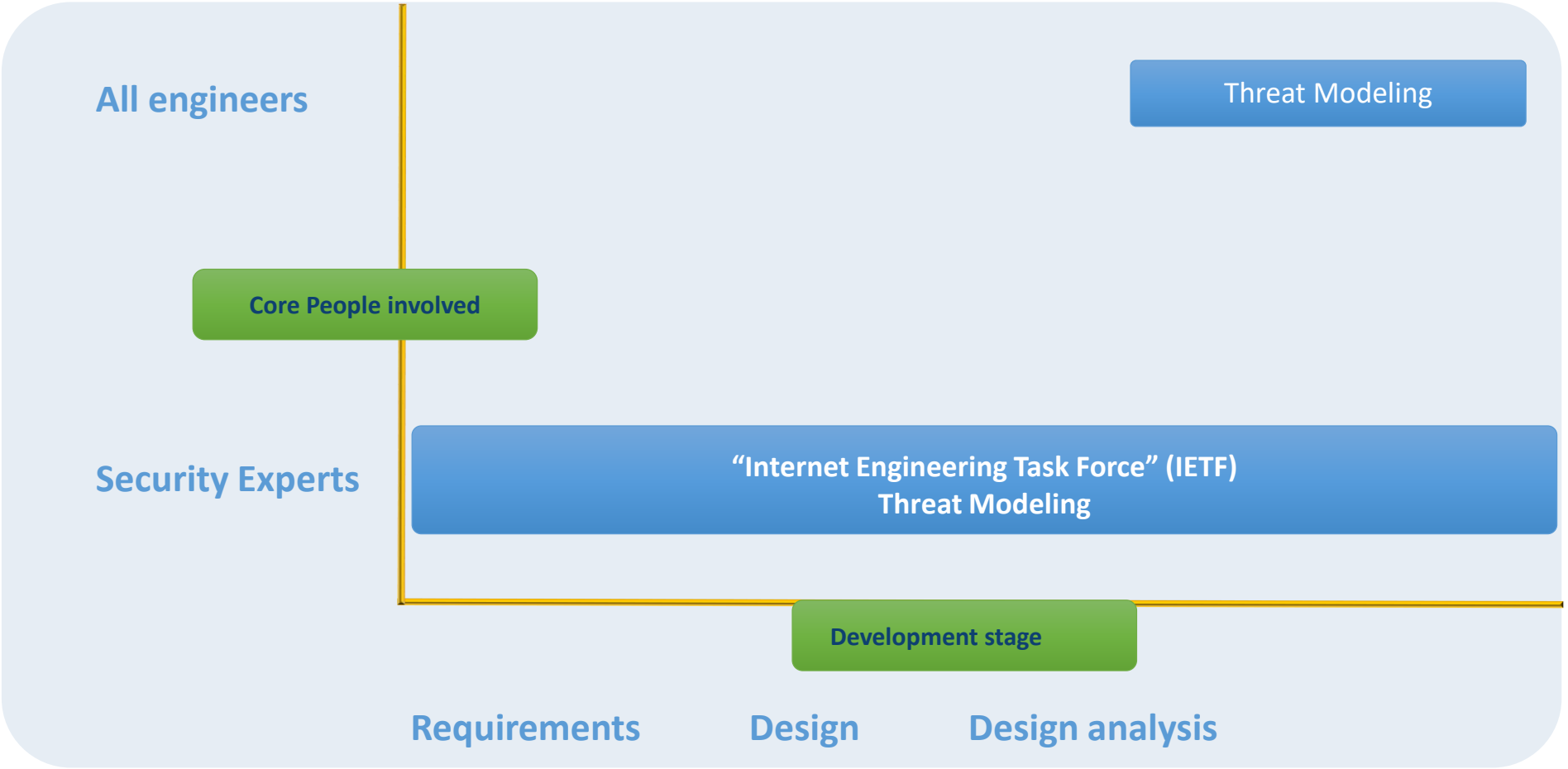


Microsoft | Security Development Lifecycle



https://www.microsoft.com/en-us/securityengineering/sdl/

Terminology and Context

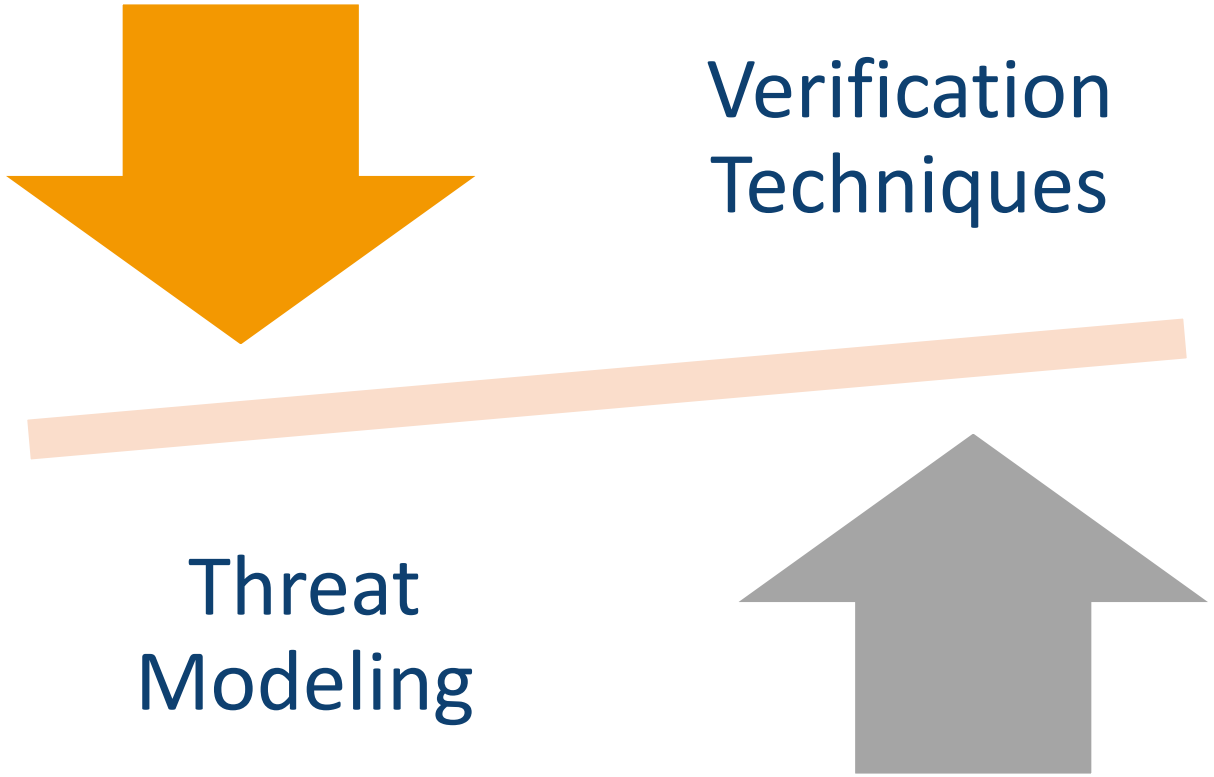


Threat Modeling in Software Development

- Software development is about creating applications that enable users to perform some tasks.
- Secure development requires determining what a user shouldn't do and ensuring that the code properly restricts users to authorized actions.
- Threat modeling is a design activity to do just that.

Threats are not vulnerabilities!

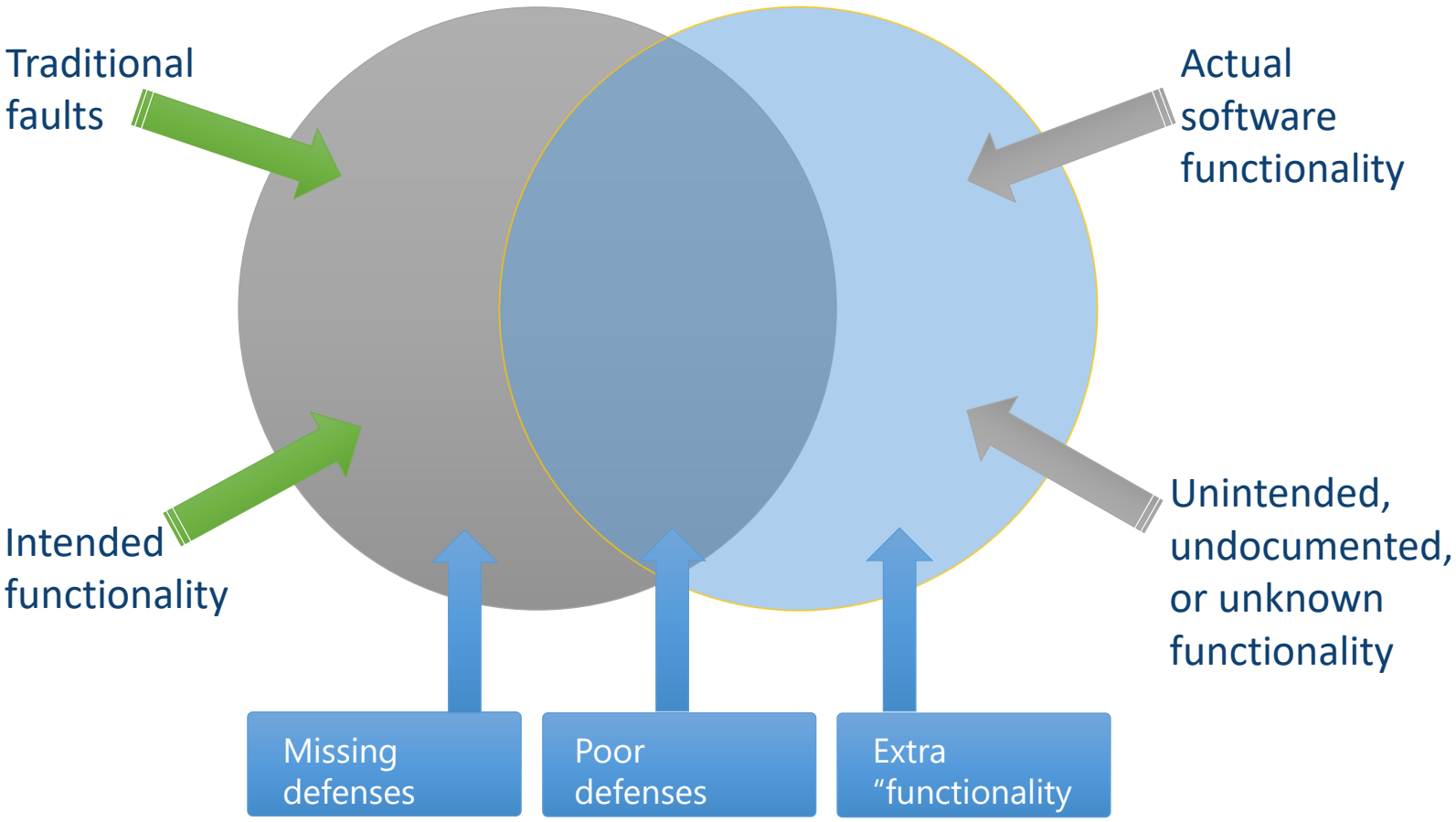
Threat modeling can be performed before a product or service has been implemented.



ENTERPRISE ARCHITECT

SPARX SYSTEMS CENTRAL EUROPE

Security Testing



ENTERPRISE ARCHITECT

SPARX SYSTEMS CENTRAL EUROPE

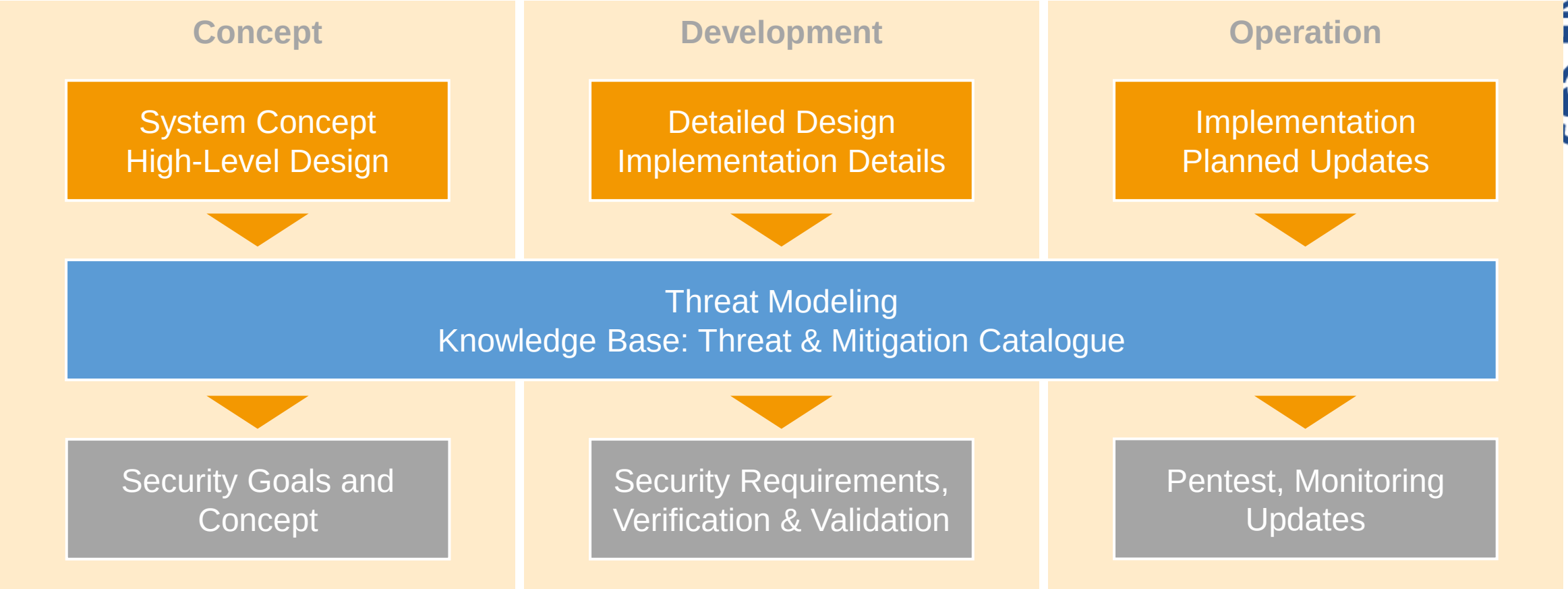
How Threat Modeling Helps?

Threat Modeling enables you to:

- Identify threats
- Identify vulnerabilities
- Identify mitigating factors
- Perform risk analysis
- Prioritize security fixes
- Derive security test cases



When do we Threat Model



ENTERPRISE ARCHITECT

SPARX SYSTEMS CENTRAL EUROPE

Threat modeling in Enterprise Architect

- Create DFDs (Data Flow Diagrams)
  - Include processes, data stores, data flows
  - Include trust boundaries
  - Diagrams per scenario may be helpful
- Identify Threats
  - Get specific about threat manifestation
- Mitigate
  - To address or alleviate a problem
- Validate the whole threat model
  - Validate Quality of Threats and Mitigations
  - Validate Information Captured

Classifying Threats

STRIDE is an acronym for the threat types of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege

More important than fitting a threat to a category is using the model to help you describe the threat and design an effective mitigation

Understanding the STRIDE Threats

Threat	Property	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	Pretending to be any of billg, microsoft.com or ntdll.dll
Tampering	Integrity	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN.
Repudiation	Non-repudiation	Claiming to have not performed an action.	“I didn’t send that email,” “I didn’t modify that file,” “I certainly didn’t visit that web site, dear!”
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site.
Denial of Service	Availability	Deny or degrade service to users	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Elevation of Privilege	Authorization	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example but going from a limited user to admin is also EoP.

https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

Cyber Security in Enterprise Architect enables

- Create Trust Diagrams per scenarios
- Analyzing the potential vulnerability using STRIDE and form a mitigation
- Tracing threats and vulnerabilities to your Software/Systems models
- Creating various reports using the build-in capabilities
- Sharing threat models using standards (XMI, OSLC)
- Analyzing, visualizing and communicating using business language

ENTERPRISE ARCHITECT

ENTERPRISE ARCHITECT

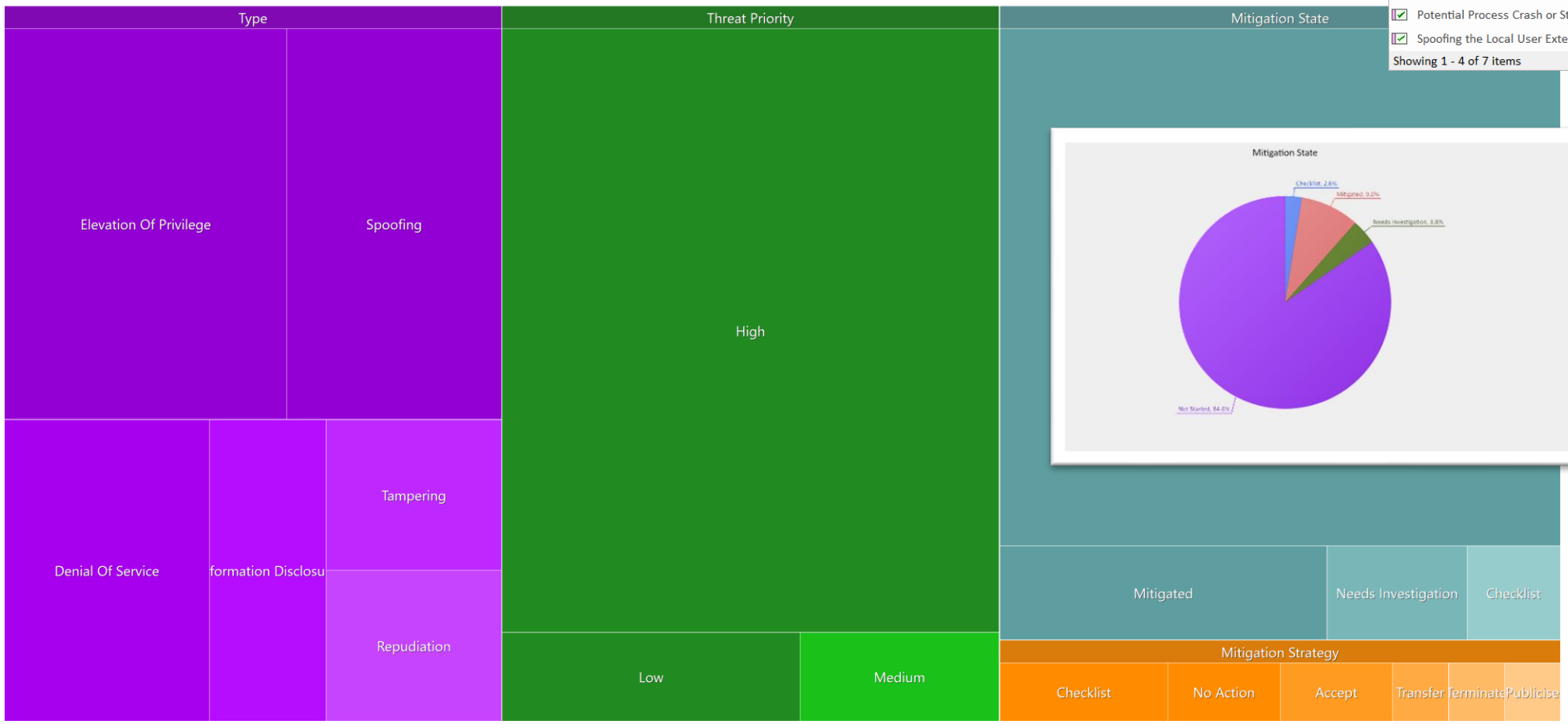
SPARX SYSTEMS CENTRAL EUROPE

Have you ever wanted to:

- Analyze your threat models by visual aggregation or relevance?
- Absorb information in new ways?
- Identify emerging trends with ease and respond quickly?
- Interact directly with your data?
- Communicate with a new business language?

You can do this in EA …

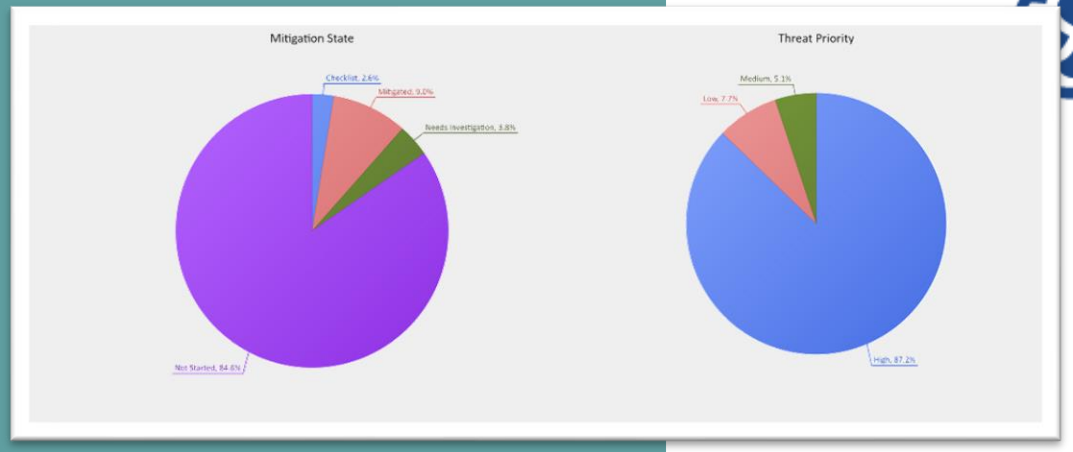
Threats overview



Mitigated Threats

Name	value
Potential Excessive Resource Consumption for Castle service or LSA	Mitigated
Elevation Using Impersonation	Mitigated
Potential Process Crash or Stop for Remote Castle service	Mitigated
Spoofing the Local User External Entity	Mitigated

Showing 1 - 4 of 7 items



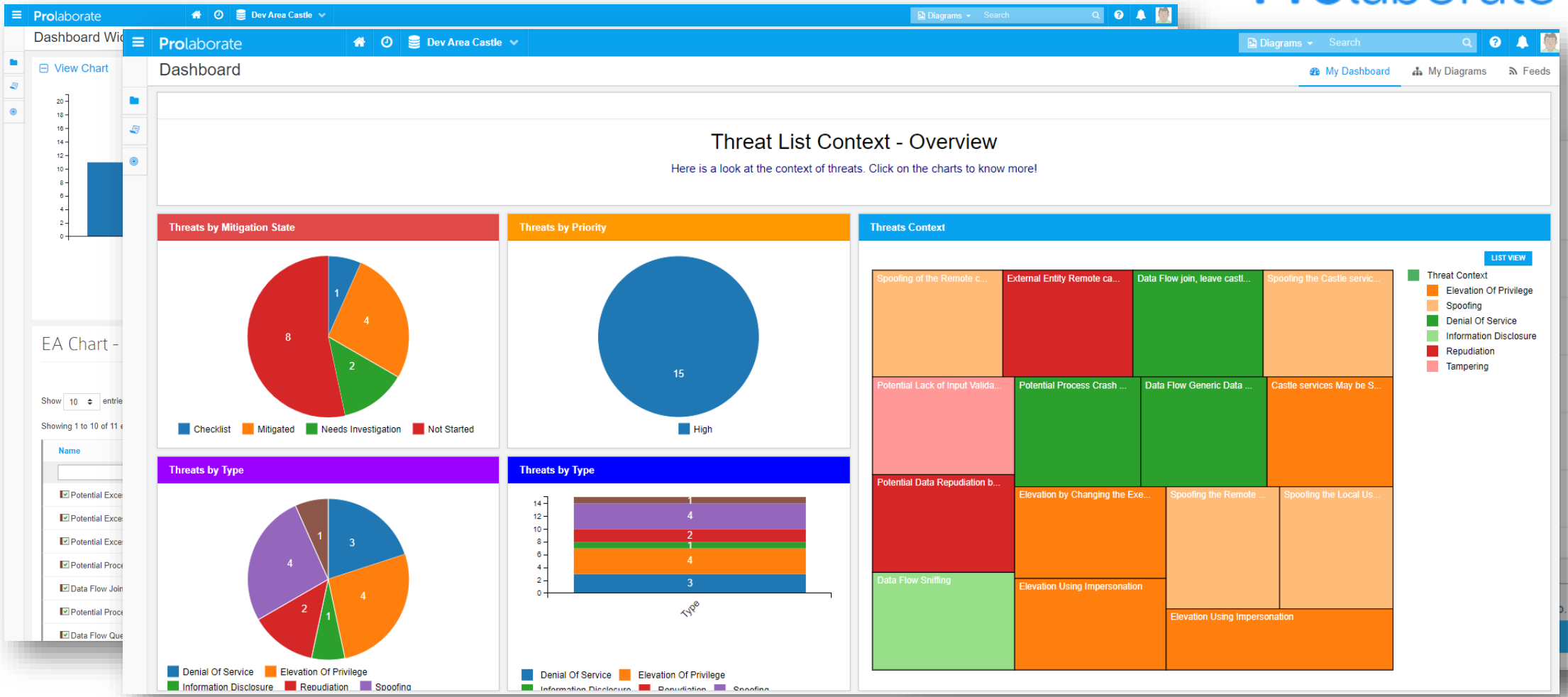
SPARX SYSTEMS CENTRAL EUROPE

ENTERPRISE ARCHITECT

...or this in Prolaborate

ENTERPRISE ARCHITECT

Prolaborate



SPARX SYSTEMS CENTRAL EUROPE

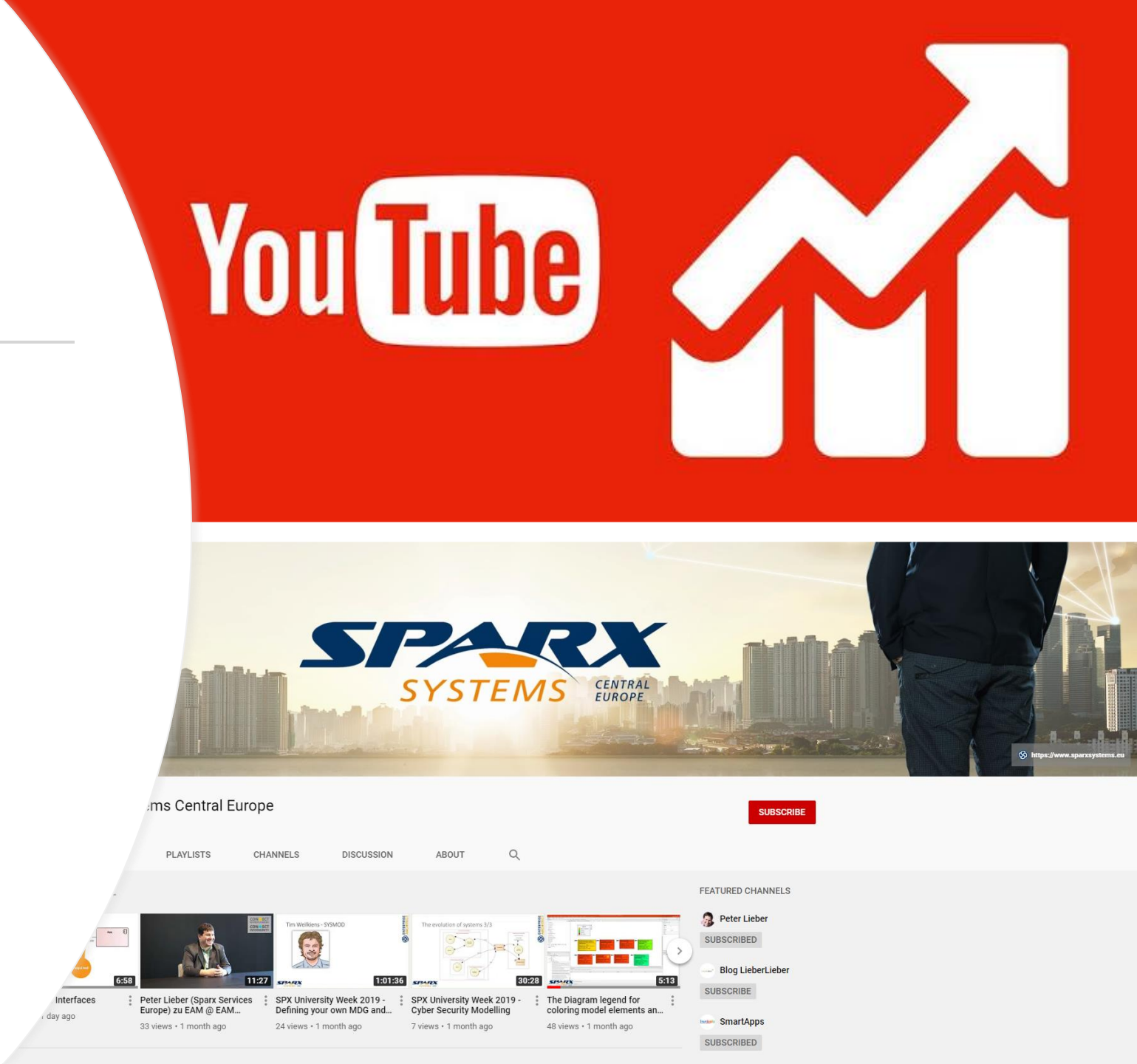
sales@sparxsystems.eu

ENTERPRISE ARCHITECT

SPARX SYSTEMS CENTRAL EUROPE

Training – Consulting
sales@sparxsystems.eu

YouTube channel
https://www.youtube.com/user/sparxce



Bob Hruska
LinkedIn

Build a security culture

Save money and reputation

Questions?

ENTERPRISE ARCHITECT

SPARX SYSTEMS CENTRAL EUROPE