Cyber Security Modeling in EA

Peter Lieber

SPARX SERVICES CENTRAL EUROPE

Peter Lieber

Modeling assists in all challenges of daily business

Innovation needs models

SPARX SERVICES CENTRAL EUROPE

SPARX SERVICES CENTRAL EUROPE

COMPACT: Cost-Efficient Smart System Software Synthesis

- Create important technological innovations to automate the software development and configuration flow for ultra-constrained IoT nodes.
- The automation methodology follows the OMG notion of model-driven architecture (MDA) and applies it to the development of IoT node software.
- The approach proposed by the COMPACT project will make the development of IoT software, and thus of IoT devices, much shorter and more efficient.

https://www.edacentrum.de/compact/

SPARX SERVICES CENTRAL EUROPE

COMPACT

Why Threat modeling?

- Brings solid foundation for building secure and safety solutions addressing confidentiality, integrity and availability
- Avoid introducing vulnerabilities
  - Proactively identify potential security threats and address them prior to production
- Identify vulnerabilities in an existing solution

SPARX SERVICES CENTRAL EUROPE

OMG Hot Topic!

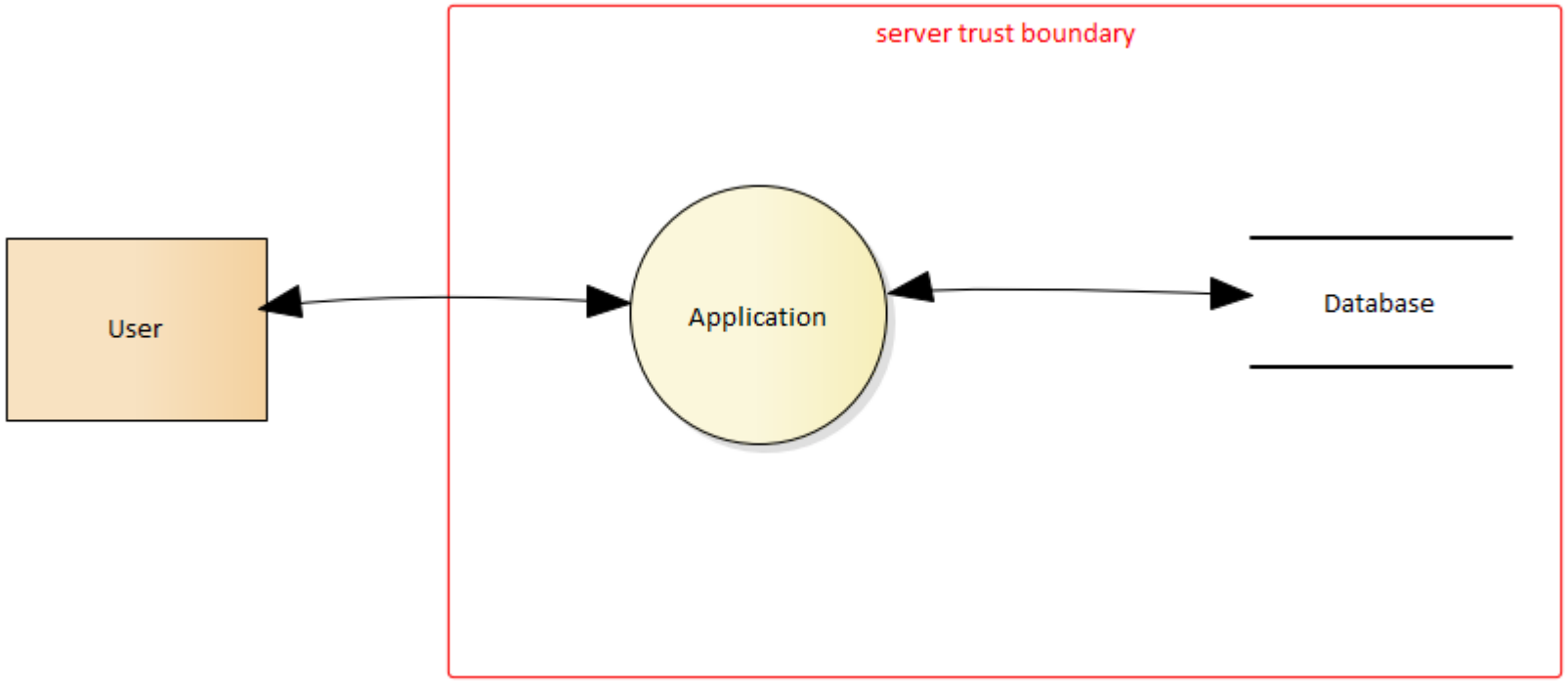
- The Object Management Group® (OMG®) System Assurance Task Force in collaboration with the Government Domain Task Force has issued a Request for Proposal (RFP) for a Unified Modeling Language (UML®) Threat & Risk Model.

www.threatrisk.org

SPARX SERVICES CENTRAL EUROPE

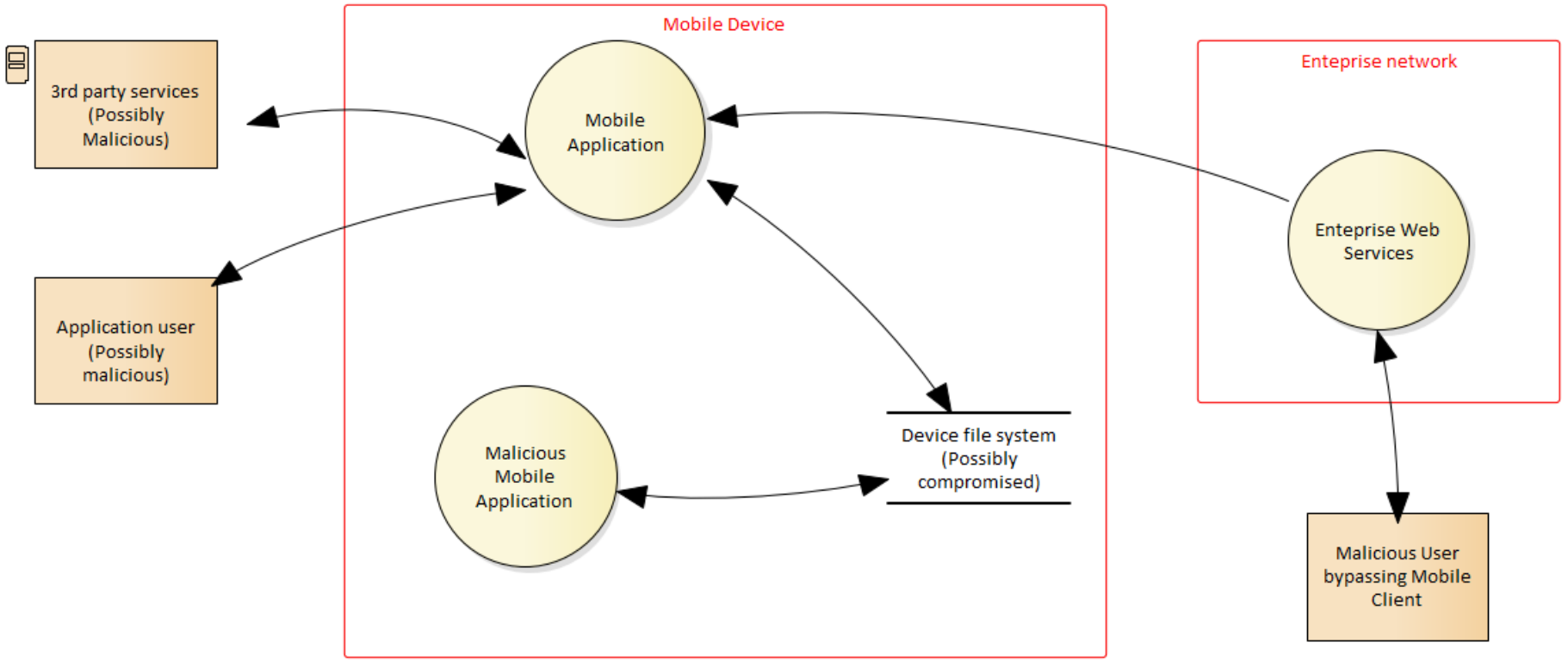
OMG OBJECT MANAGEMENT GROUP®

The evolution of systems 1/3



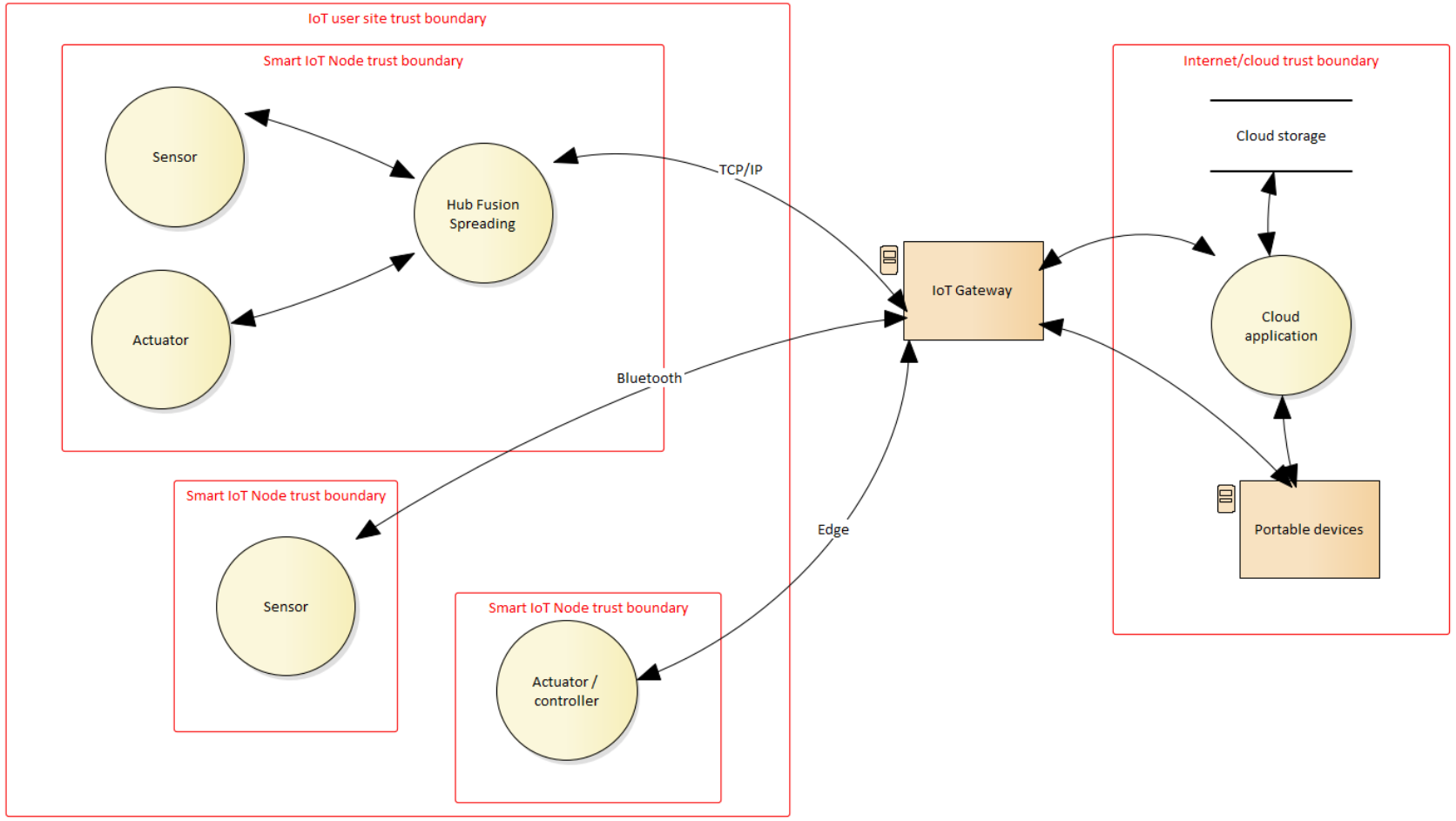
SPARX SERVICES CENTRAL EUROPE

The evolution of systems 2/3

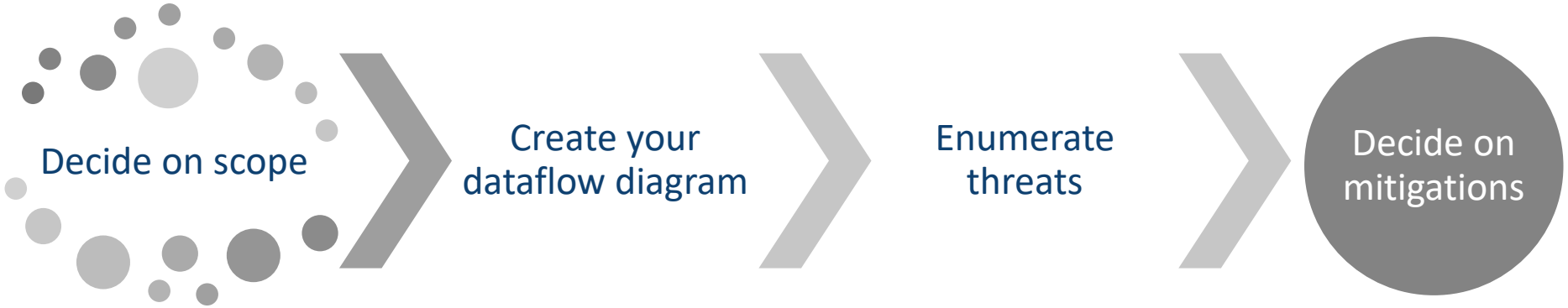


SPARX SERVICES CENTRAL EUROPE

The evolution of systems 3/3



Threat modeling concepts



SPARX SERVICES CENTRAL EUROPE

Threat modeling with STRIDE

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

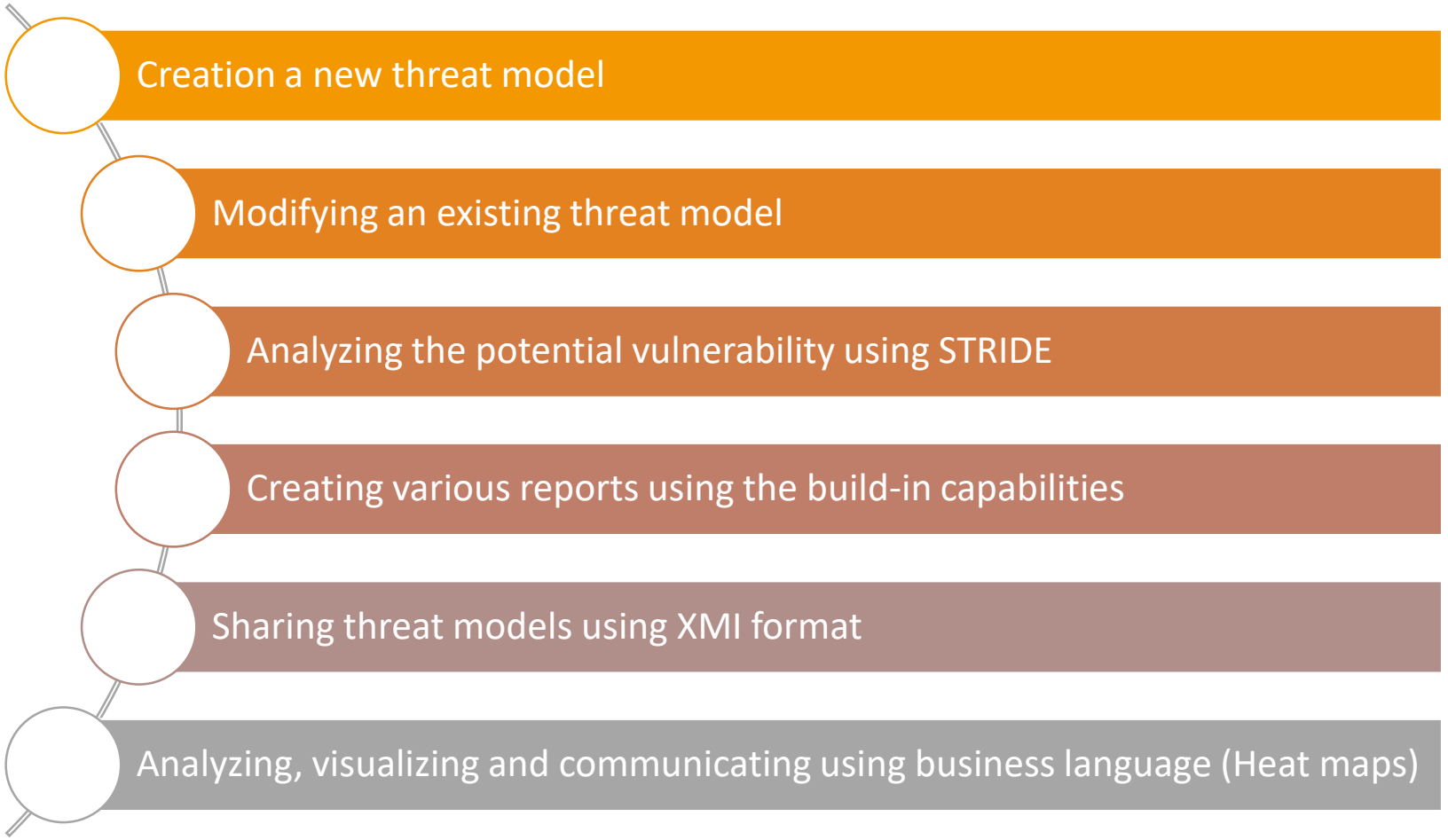
- More important than fitting a threat to a category is using the model to help you describe the threat and design an effective mitigation

SPARX SERVICES CENTRAL EUROPE

STRIDE definitions

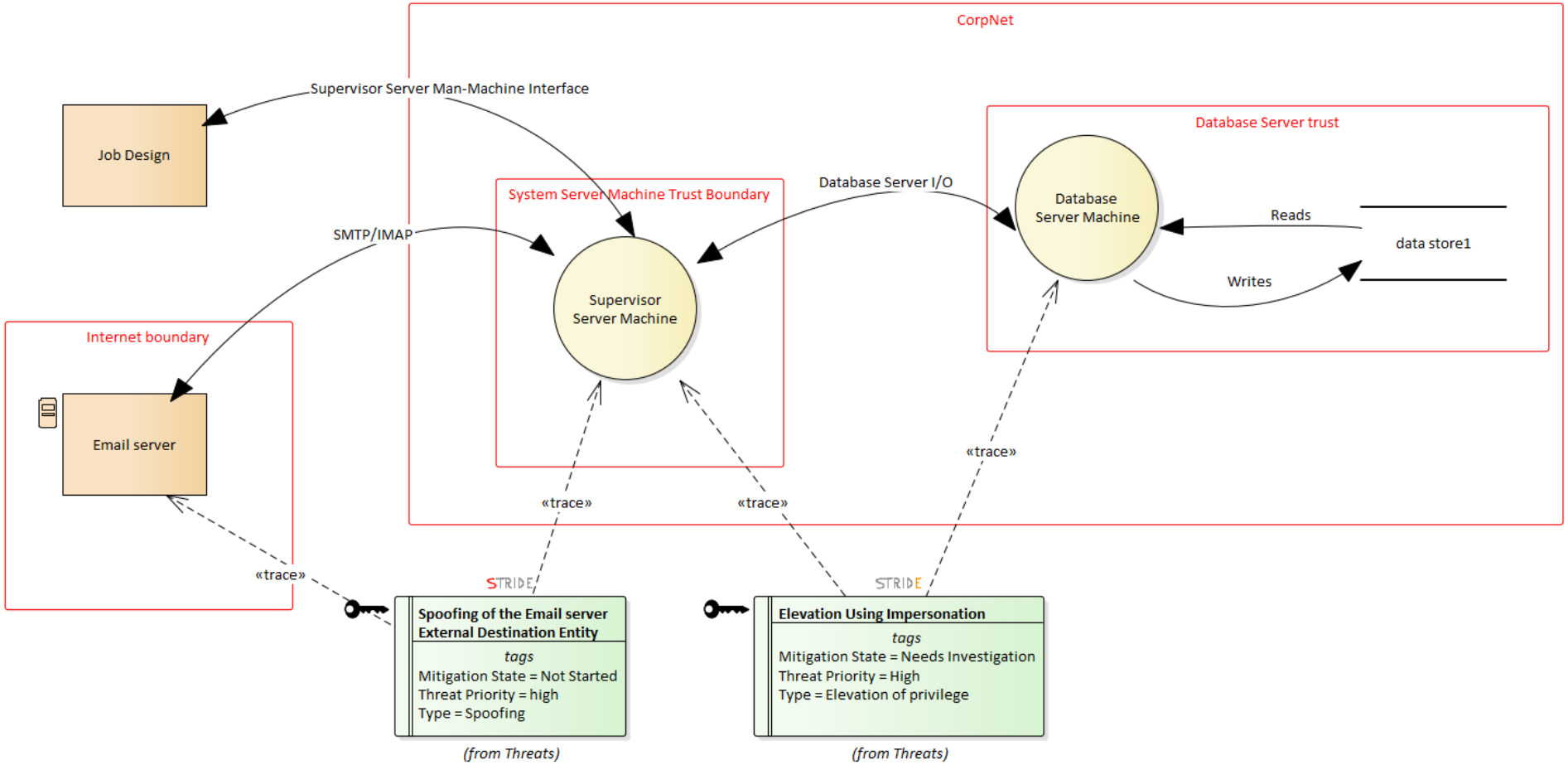
Threat	Property	Threat Definition
Spoofing	Authentication	Spoofing threats involve an adversary creating and exploiting confusion about who is talking to whom. Spoofing threats apply to the entity being fooled, not the entity being impersonated. Thus, external elements are subject to a spoofing threat when they are confused about what or whom they are talking to.
Tampering	Integrity	Tampering threats involve an adversary modifying data, usually as it flows across a network, resides in memory, on disk, or in databases.
Repudiation	Non-repudiation	Repudiation threats involve an adversary denying that something happened.
Information disclosure	Confidentiality	Exposing information to someone not authorized to see it.
Denial of service	Availability	Deny or degrade service to users.
Elevation of privilege	Authorization	Gain capabilities without proper authorization.

EA scenarios coverage

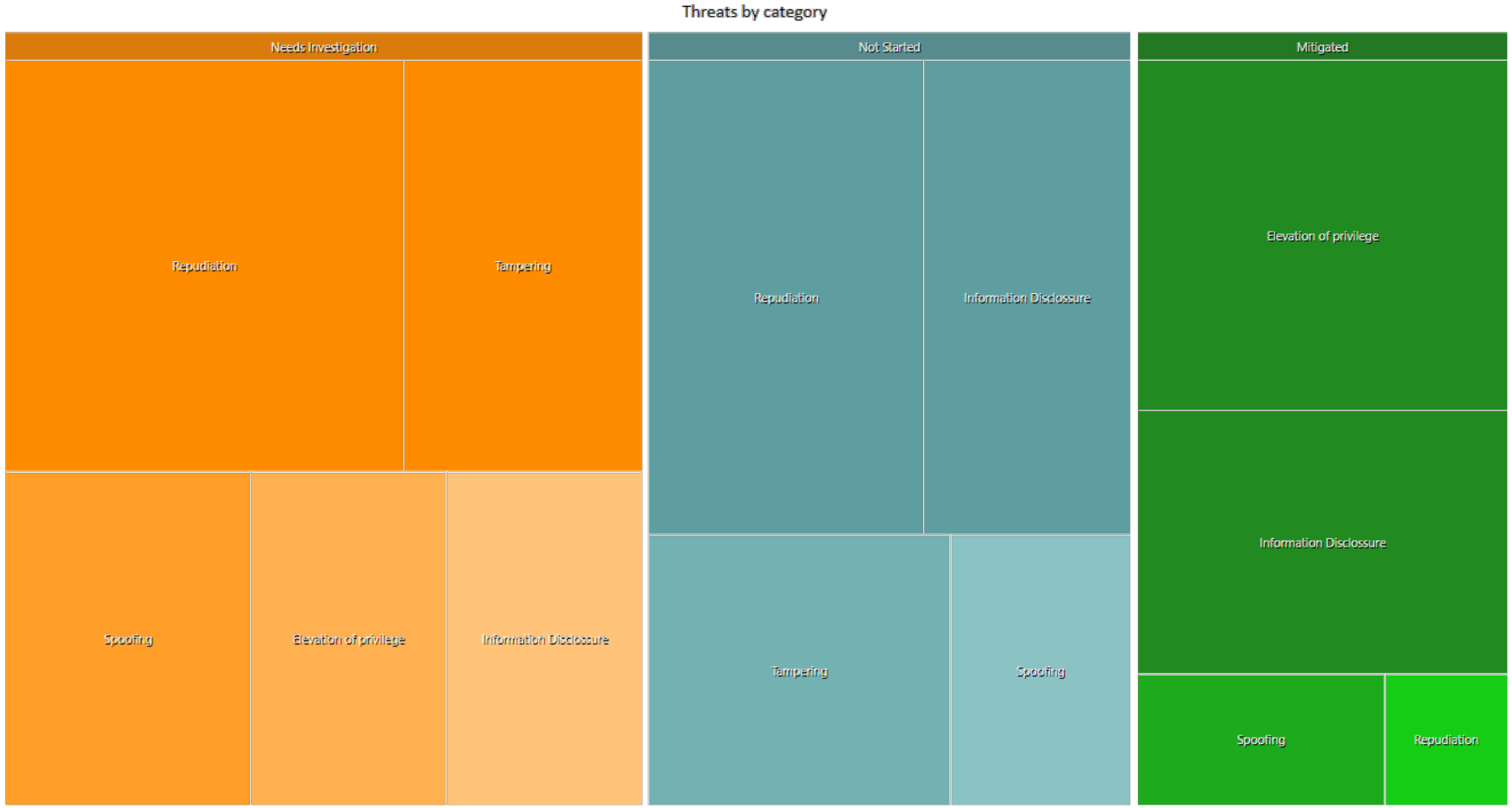


SPARX SERVICES CENTRAL EUROPE

Screenshots



Threat Modeling Analysis



SPARX SERVICES CENTRAL EUROPE

Validation Rules Implemented

	Category	Short threat title	Rule	Description	Linked to
1.	Spoofing	Spoofing the {source.Name} Process	source is 'ThreatModelElements::external system' and (target is 'ThreatModelElements::Process' or target is 'ThreatModelElements::data store') and 'DataFlow' crosses 'ThreatModelElements::Trust boundary'	{source.Name} may be spoofed by an attacker and this may lead to unauthorized access to {target.Name}. Consider using a standard authentication mechanism to identify the source process.	'source' and 'target'
2.	Spoofing	Spoofing the {source.Name} External Entity	source is 'ThreatModelElements::external system' and target is 'ThreatModelElements::Process'	{source.Name} may be spoofed by an attacker and this may lead to unauthorized access to {target.Name}. Consider using a standard authentication mechanism to identify the external entity.	'source' and 'target'
3.	Elevation Of Privilege	Elevation Using Impersonation	(source is 'ThreatModelElements::external system' or source is 'ThreatModelElements::Process') and target is 'ThreatModelElements::Process'	{target.Name} may be able to impersonate the context of {source.Name} in order to gain additional privilege.	'source' and 'target'
4.	Elevation Of Privilege	{target.Name} May be Subject to Elevation of Privilege Using Remote Code Execution	target is 'ThreatModelElements::Process' and 'DataFlow'crosses 'ThreatModelElements::Trust boundary'	{source.Name} may be able to remotely execute code for {target.Name}.	'source' and 'target'

SPARX SERVICES CENTRAL EUROPE

Threat Modeling for specific industries

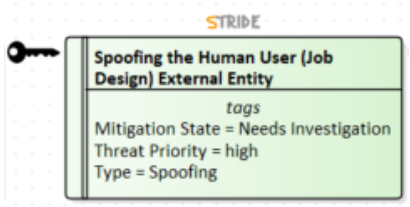
- Available
  - General – https://cybersecurity.sparxservices.eu
- Coming Soon (In collaboration with Austrian Institute of Technology – Cyber Security Modeling with AI)
  - Automotive
  - Critical Infrastructure (e.g. energy sector)
  - Transportation
  - Aviation

SPARX SERVICES CENTRAL EUROPE

SPARX SERVICES CENTRAL EUROPE

Business decisions

- Visualization of STRIDE category and mitigation status will be displayed as a decoration to a "threat" element.
  - Rationale: One trust diagram elements can have n-threats identified



- Threat(s) will be connected to the Trust diagrams' source and target elements involved in the threat (no longer to a connector).
  - Rationale: Creating relationships between elements can be later better utilized by EA regular features like traceability window, insert related elements, document generation, heat maps …)

SPARX SERVICES CENTRAL EUROPE