USING IEC 62443-4 FOR THE CYBER RESILIENCE ACT

Christoph Schmittner, Sebastian Chlup, Korbinian Christl

PRESENTER

- **Safety and security engineering** and management in industrial and research projects in automotive, railways and manufacturing

- **Involved in IEC and ISO** Standards regarding safety and security

EUROPEAN REGULATORY FRAMEWORK

Cyber Resilience Act – evolving topic

EUROPEAN APPROACH TO REGULATION

	Self-Assessment	Third-Party-Assessment
Product • **Risk-based approach** • **EU regulation** with **essential requirements** • For selected domains, **technical** specifications are addressed in **harmonized standards** • Based on this **Product conformity assessment**	CE	0123
Process • **Product conformity assessment** requires **quality management system** • ISO 9001 is a harmonized standard, but management system and requirements on certification differ depending on domain		CERTIFIED ISO 9001:2015 COMPANY

EUR-Lex - 52016XC0726(02) - EN - EUR-Lex (europa.eu)

FRAMEWORK

Proposal 2022/0272(COD) "Cyber Resilience Act"

Regulation 2019/881 "Cybersecurity Act"

Proposal 2020/0359/(COD) "NIS2"

Regulation 765/2008 "CE marking"

Regulation 768/2008/EC "conformity assessment procedures"

AUSTRIAN INSTITUTE OF TECHNOLOGY

Market surveillance authorities

Notified bodies / TÜV, DEKRA, …

Manufactures, importers, distributors

Standards developing organisation

Conformity Assessment

Declaration of Conformity

Technical Documentation
Risk analysis, SBOM, Architectures

Essential Requirements
Security properties (by design / in entire lifecycle)
Vulnerability handling
Reporting of incidents and exploited vulnerabilities

Harmonized standards

Common specifications

Cybersecurity Certification Scheme

CYBER RESILIENCE ACT

- **Cyber Resilience Act** defines the overall Framework
- Related to all **products with digital elements**
- **Cybersecurity** requirements for **European market access**

Might get removed

Default category

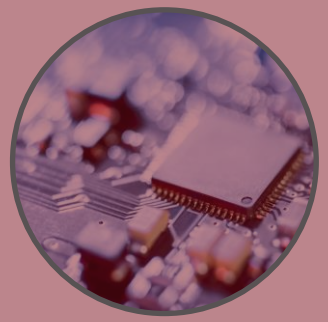
- **Self assessment**

Anti-virus software, boot managers, digital certificate issuance software, operating systems, network interfaces, internet routers, microprocessors, and microcontrollers

Class I – critical products

External Audit

Routers, Password manager, Firewalls, Virtual Private Networks (VPNs), runtime systems supporting virtualized execution



Class II – highly critical products

- **Third-party assessment (based on harmonized standard)**
- CPUs, Smartcards, Operating system, HSMs, Industrial firewalls, Smartcards, Smartcard readers, Secure elements

Risk Assessment: Functionality, Intended use, Impact

European Cyber Resilience Act (CRA) (european-cyber-resilience-act.com)

APPLICABILITY OF THE CYBER RESILIENCE ACT

Cyber Resilience Act applies to all products with digital elements

Excluded: Sectors with pre-existing cybersecurity requirements

- Energy
- Medical
- Railways
- Automotive

Requirements depend on criticality

RATING OF CRITICALITY

Cybersecurity-Related Functionality

Authentication
Access Control
Intrusion Prevention
Endpoint Security
Network Protection

Core System Functions

Network Management
Configuration Control
Virtualization
Personal Data Processing
Disruption Potential

TIMELINE

15.09.2022 proposed by the European Commission

19.7.2023 Council decision to start trilouge

+20 months after regulation passed: Vulnerability and Incident report is required

+40 month safter regulation passed: SW&HW has to comply with new regulations

CRA: ESSENTIAL REQUIREMENT

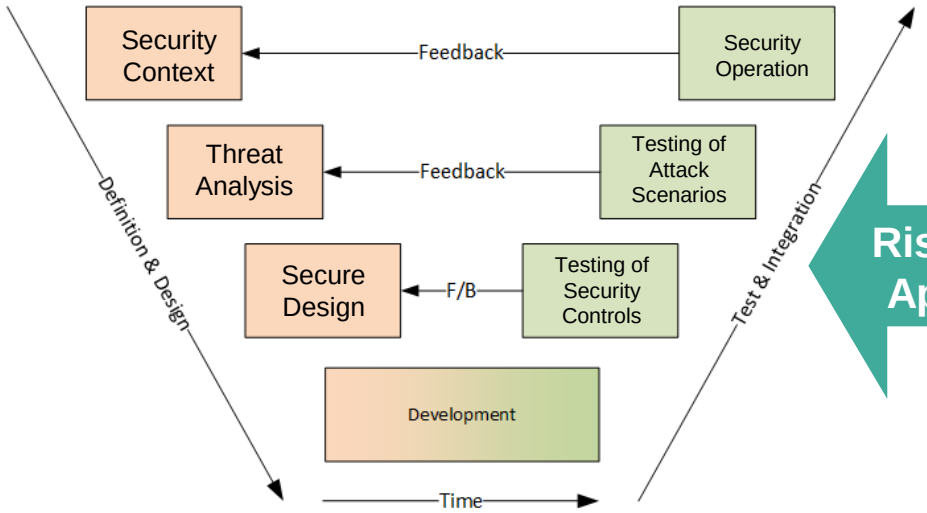
Products designed, developed and produced in such a way that an **appropriate level of cybersecurity based on the risks is ensured**

- Conduct risk assessment throughout product lifecycle.
- Risk Evaluation based on intended use, foreseeable application, operational environment and assets.
- Align security requirements with risks during risk treament
- Regularly update documented risk assessment.

CRA AND IEC 62443-4

- IEC 62443-4 focuses on **secure development of products** (used in industrial automation and control systems)

- 4-1 Secure product development lifecycle



Risk-based Approach

- 4-2 Technical Security requirements

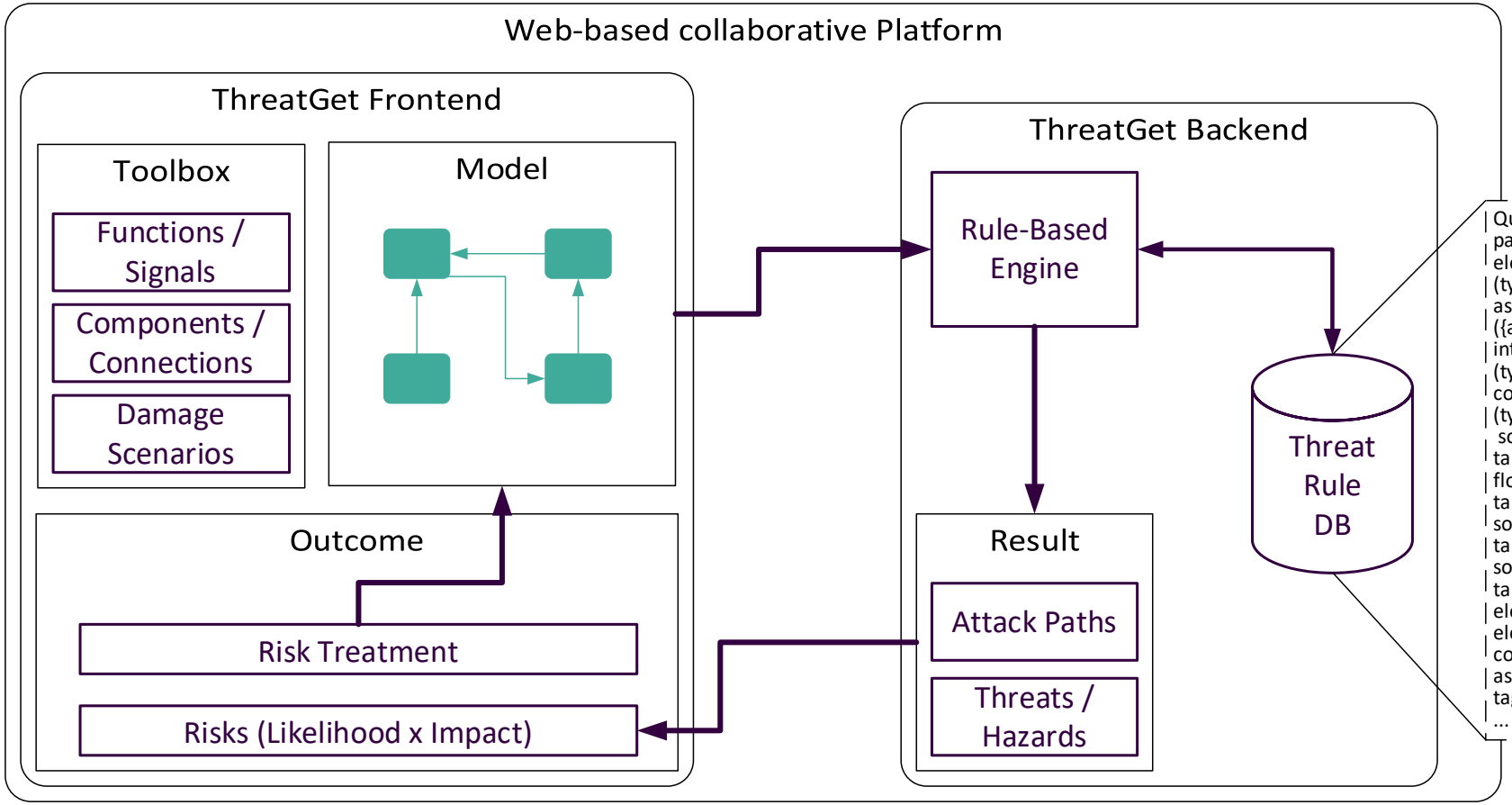
4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CYBERSECURITY BY DESIGN

CRA – and IEC 62443 with ThreatGet

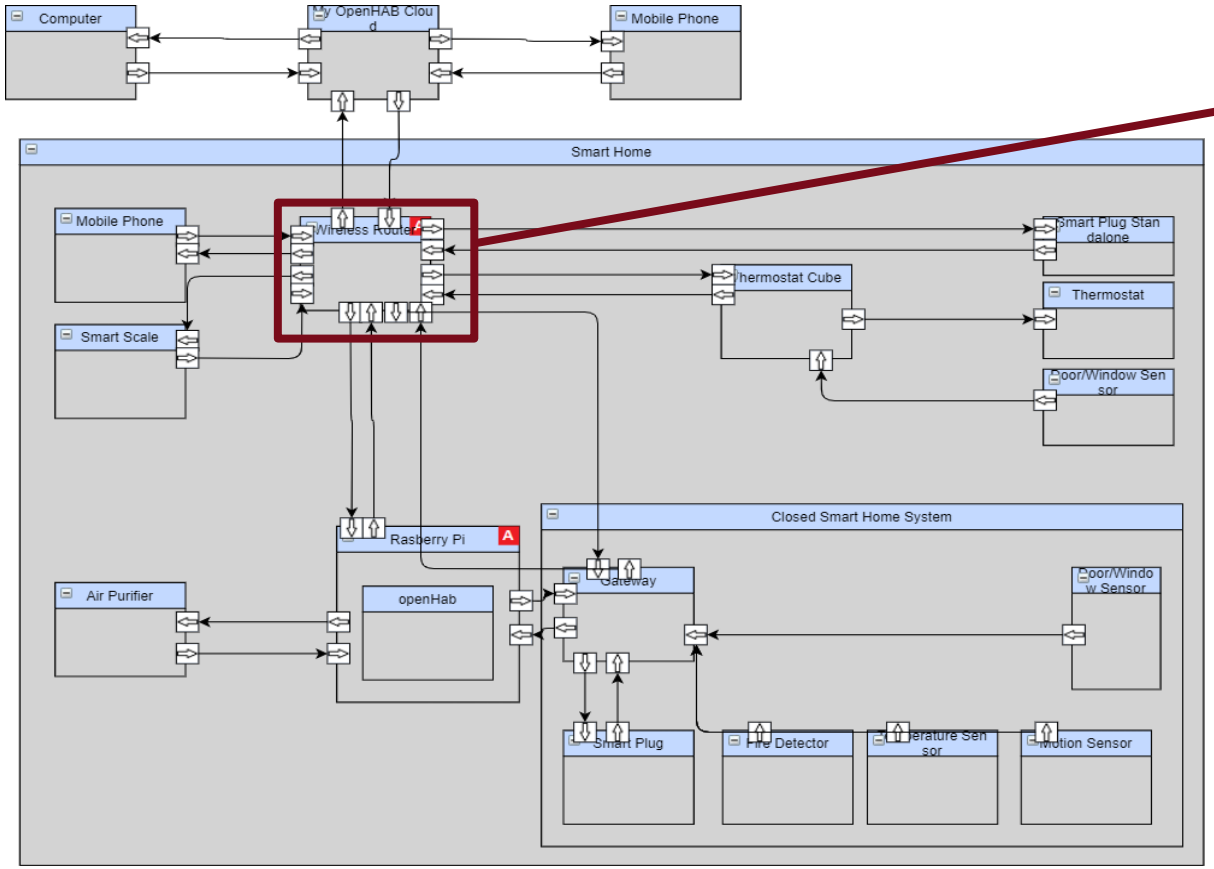
SAFETY & SECURITY BY DESIGN




```
Query -> query (& query) + query (| query) + pattern
pattern -> element_pattern  connector_pattern  flow_pattern
element_pattern -> (element_pattern (| element_pattern)+) ELEMENT
(type_filter)? ({element_filters})?
asset_pattern -> (asset_pattern (| asset_pattern)+)  ASSET (type_filter)?
({asset_filters})?
interface_pattern -> (interface_pattern (| interface_pattern)+)  INTERFACE
(type_filter)? ({interface_filters})?
connector_pattern -> (connector_pattern (| connector_pattern)+) CONNECTOR
(type_filter)? {
 source_element_filter  (& source_interface_filter)?  & target_element_filter  (&
target_interface_filter)? (& connector_filters)}
flow_pattern -> (flow_pattern (| flow_pattern)+) FLOW {source_filter &
target_filter (& flow_filters)}
source_element_filter -> SOURCE element_pattern
target_element_filter -> TARGET element_pattern
source_interface_filter -> SOURCE interface_pattern
target_interface_filter -> TARGET interface_pattern
element_filters -> element_filters (& element_filters) + ( element_filters (|
element_filters)+ ) tagged_value_filter  asset_filter  relation_filter
connector_filter  flow_filter  capability_filter
asset_filters -> asset_filters (& asset_filters)+ ( asset_filters (| asset_filters)+ )
tagged_value_filter capability_filter
...
```

SECURITY CONTEXT

- Intended use, foreseeable application, operational environment and assets



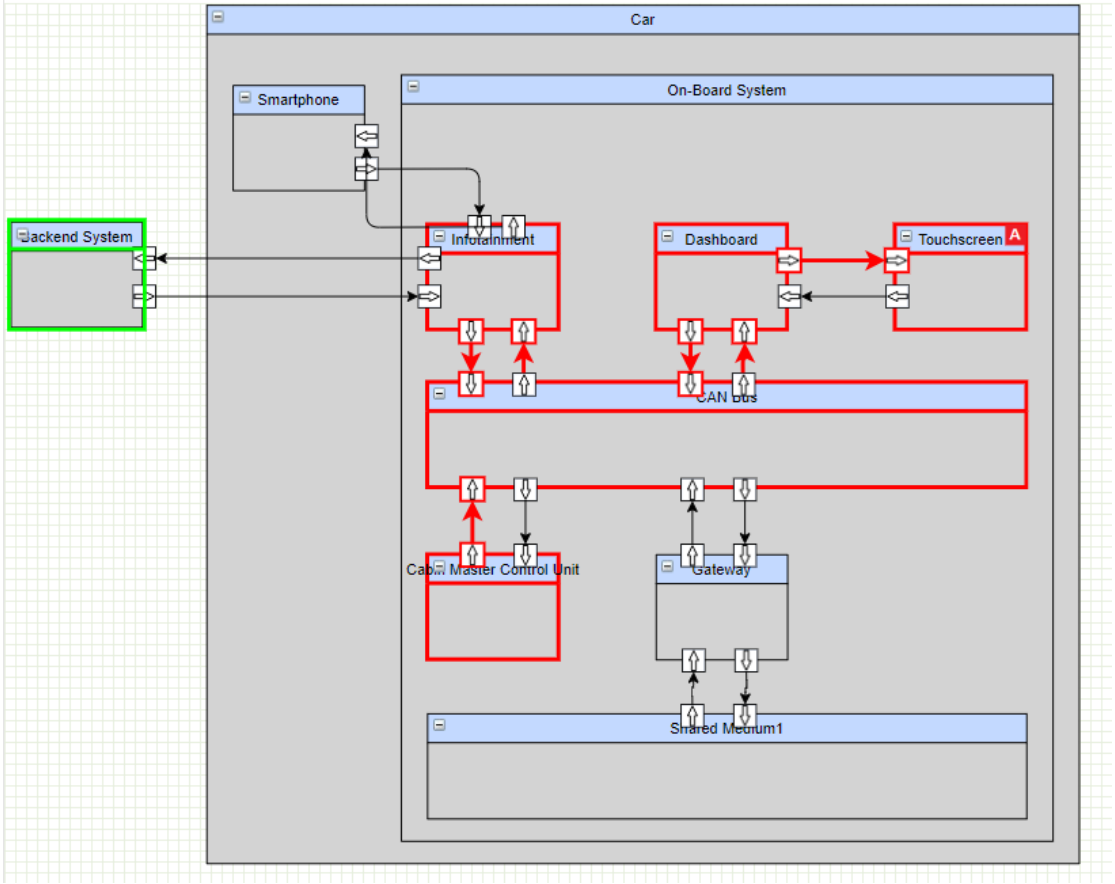
Wireless Router for IoT / Smart Home

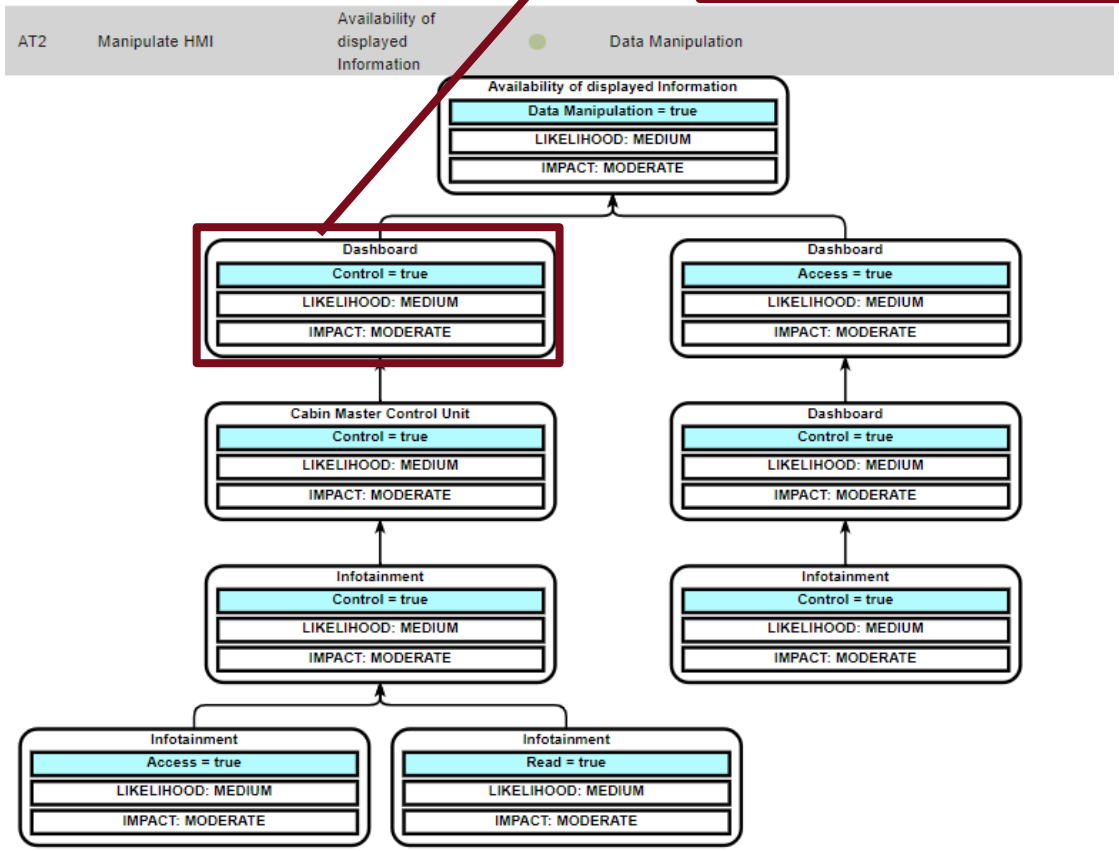
TAGGED VALUES

Property	Value
Anomaly Detection	undefined
Hardware Based Security	undefined
Malware Protection	undefined
Physical Protection	undefined
Sandboxing	undefined
Secure Boot	undefined
Trusted	undefined
Updatable	undefined

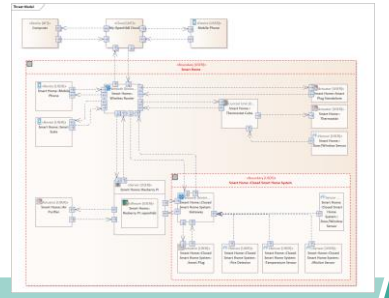
AUTOMATED ASSESSMENT OF THREATS AND RISKS

Risk Treatment can be defined on each Threat



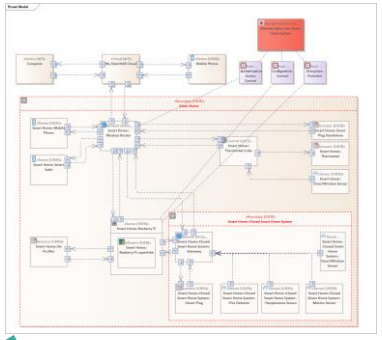


EXAMPLE



Model system architecture

Add known assets



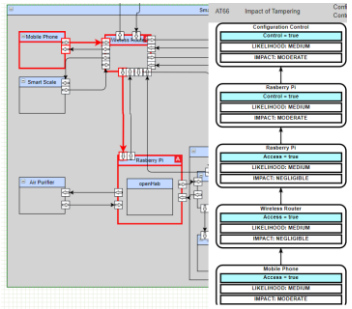
System Lifecycle

Identify direct risks

Analysis Results

ID	TITLE	SOURCE	TARGET	RISK	THREAT TYPE
T1	Install manipulated Software	openHab	openHab		TAMPERING
T2	Physical Tampering	Computer	Computer		TAMPERING
T3	Physical Tampering	Mobile Phone	Mobile Phone		TAMPERING
T4	Compromise by software	openHab	openHab		ELEVATION OF PRIVILEGE
T5	Man in the middle attack on a wireless connection	My OpenHAB Cloud	Mobile Phone		TAMPERING

Consider operational environment



Define security requirements

Title:
Attacker gains access to next element

Aquired Capability:
Access -> true on Wireless Router

Risk Level: 5

Description:
Control of an element gives allows an attacker to access connected elements

Likelihood: HIGH
Impact: SEVERE
Category: ELEVATION OF PRIVILEGE

Security Properties

Port52
Authentication = undefined
Input Control = undefined

Risk Treatment

Risk Treatment: MITIGATE

Rationale
Require authentication on incoming smart home connections

THREATGET®

- CRA requires risk-based security on product level
- IEC 62443-4 gives guidance on product and process level for security
- ThreatGet automates security-by-design, enabling IEC 62443-4 and CRA

THANK YOU!

Christoph Schmittner, Sebastian Chlup, Korbinian Christl