Increasing importance of cybersecurity for Railways

Martin Kunz- SIEMENS Mobility Germany

17.01.2023 | RATA Finland

SIEMENS

#WHOAMI

Martin Kunz -Senior Technical Sales Consultant for **Rail Cyber Security** at SIEMENS Mobility Customer Services in Germany

SIEMENS

- **Senior Technical Sales Consultant for Rail Cyber Security**
  Apr 2020 - Present · 2 yrs 9 mos
  Erlangen, Bavaria, Germany
- **Senior Business Development consultant for SIEMENS MindSphere Cloud**
  Oct 2017 - Apr 2020 · 2 yrs 7 mos
  Alpharetta, Georgia, United States and Erlangen, Bavaria, Germany
- **Senior Product & Business Developer for Industrial Security Services**
  Jan 2015 - Sep 2017 · 2 yrs 9 mos
  Alpharetta, Georgia, United States

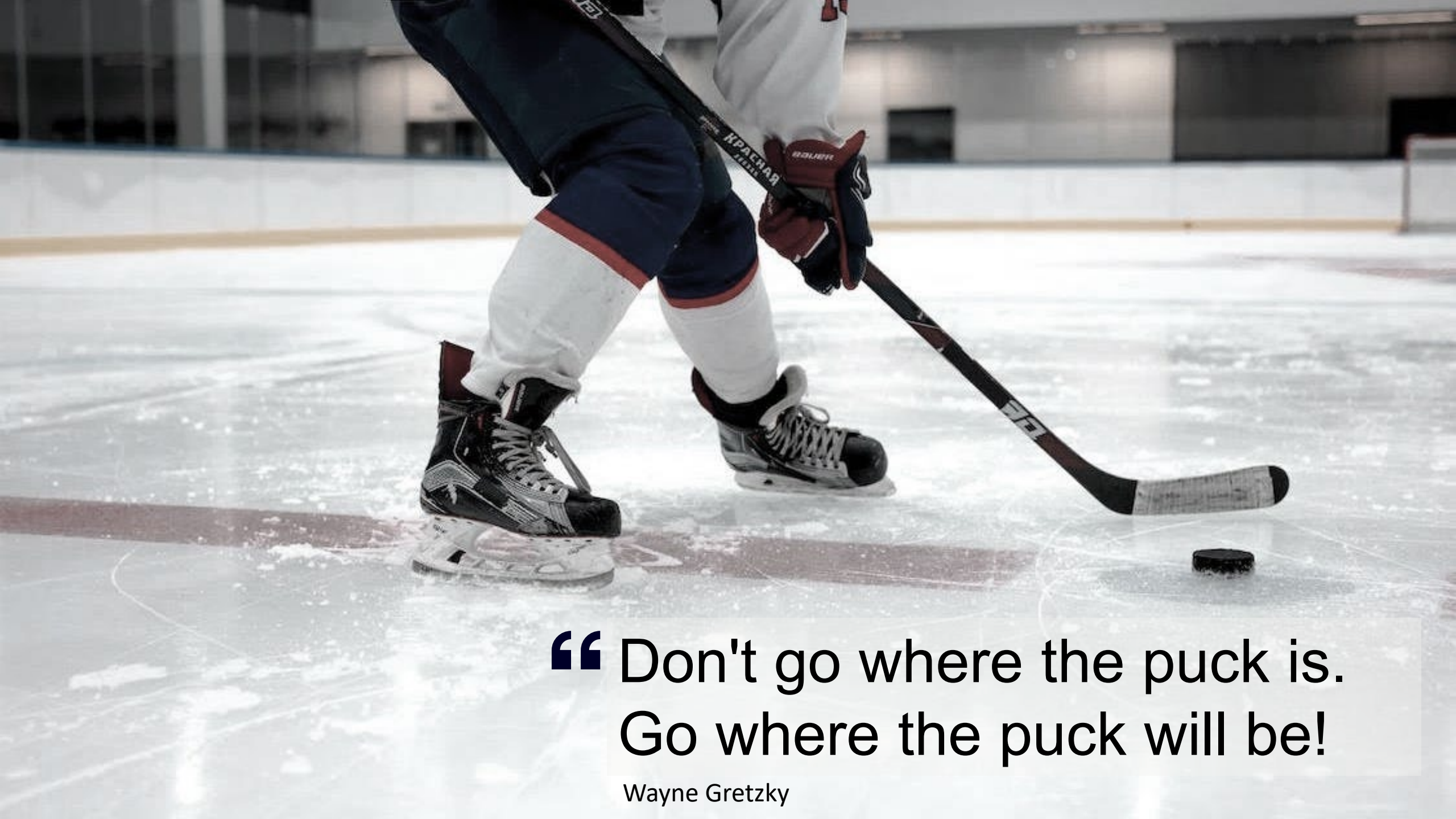
Licenses & certifications

GIAC Security Leadership (GSLC)
GIAC Certifications
Issued Sep 2021 · Expires Sep 2025

Cybersecurity Fundamentals Specialist ISA/IEC 62443
International Society of Automation (ISA)

Industrial Control Systems Cybersecurity 301 with Red Team/Blue Team exercise
Idaho National Laboratory

SIEMENS



> “Don't go where the puck is.
> Go where the puck will be!
>
> Wayne Gretzky

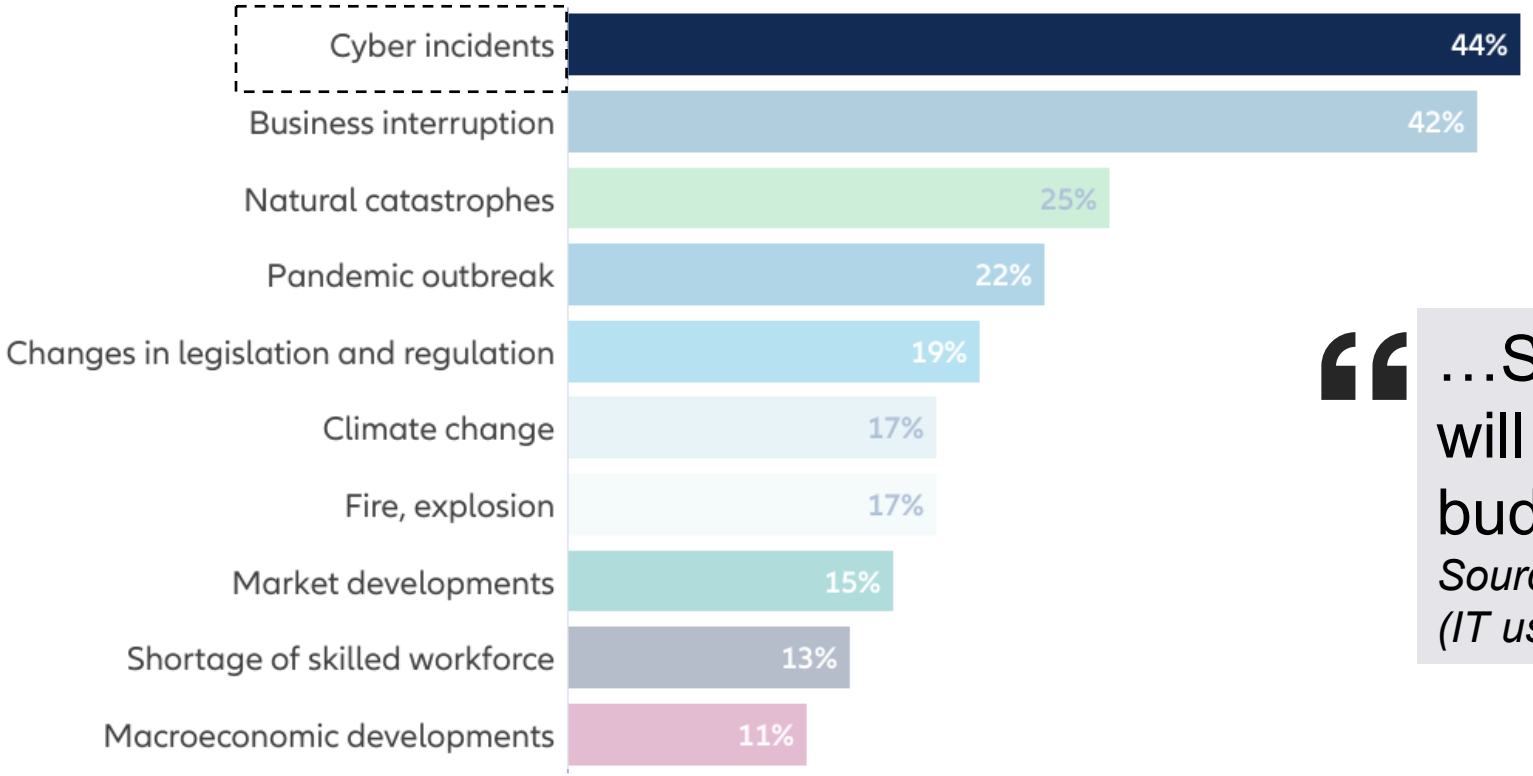
The most important Business Risks and Threat Landscape 2022
CYBERSECURITY SPENDING higher than ever

Allianz

The most important global business risks for 2022

Allianz Risk Barometer 2022

Based on the insight of 2,650 risk management experts from 89 countries and territories (% of responses). Figures do not add up to 100% as up to three risks could be selected

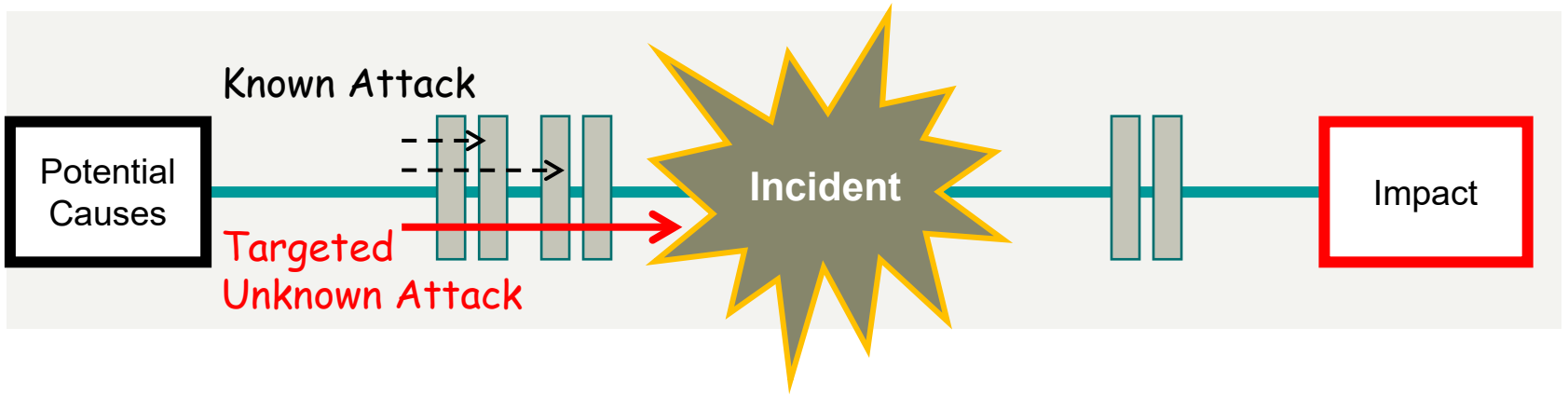


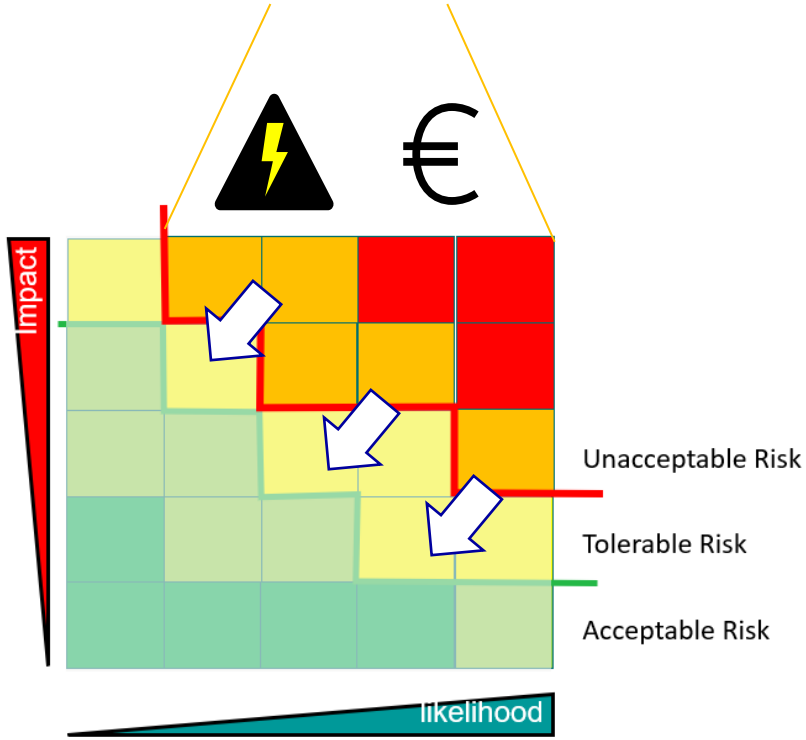
Source: Allianz Global Corporate & Specialty

> …Six out of ten European CIOs will spend almost 10% of their budget on IT-security.
> *Source www.cio.de*
> *(IT user association VOICE 2022)*

Attack prevention alone is not sufficient. The “bad guys” will eventually get in
INVEST ALSO IN EARLY DETECTION AND IMPACT REDUCTION to limit risks

LIKELIHOOD x IMPACT = RISK





Risk Analysis → Anticipate (1) → Withstand → Recover → *Lessons Learned*

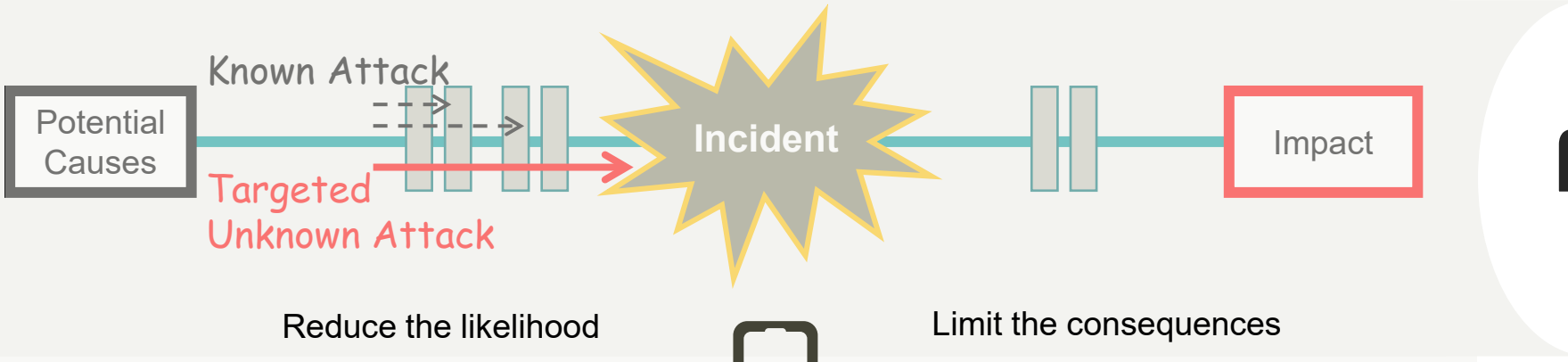
Reduce the likelihood

Limit the consequences

Adapt

(1) Cyber resilience principles by NIST SP800-160

The biggest impact is on the RAIL-OT-systems
CYBERSECURITY FOR RAIL needs specific expertise and solutions



Rail & Cybersecurity experts

Certified processes (ISO 27001/IEC 62443)

Anticipate & Adapt

- Control- / Risk-**Assessments**
- **Penetration Tests**
- Software Vulnerability **Scanning & Management**
- **“Security-for-Safety”**

Specific Cybersecurity Solutions for railways

Withstand & Recover

- Rail specific **IDS-solutions** (1)
- Connecting logs from rail & safety systems to **SIEM** (2) **/SOC** (3)
- Develop Rail OT **IR-Playbooks** (4,5) and use cases
- **Incident Response support with** Rail-System- & Cybersecurity-Experts

(1) IDS = Intrusion Detection Systems
(2) SIEM= Security Incident Event Management
(3) SOC= Security Operation Center
(4) OT = Operations Technology
(5) IR = Incident Response

Cyber Defense Center (CDC) project in Europe:
LESSON'S LEARNED: Journey from reactive to proactive & resilient Rail-Operator

Need for change

- Attack prevention alone is not enough
- Public "known" incidents
- Complex, diverse number of IT/OT assets
- "Firefighting" reactive mode
- Gaps in people, processes and technology

Business Case

- Rough roadmap & tender
- Budget and approval to hire experts
- External know-how transfer needed
- Goal: Cyber Resilience
  - Build CDC for IT and rail-OT

Project Start

- Agile Frame contract
- Pre-selected Partners incl. **SIEMENS Mobility & CYS**
- Different Job profiles via "Mini tenders" timeboxed -> Low risk for all parties

Today (after ~3 years)

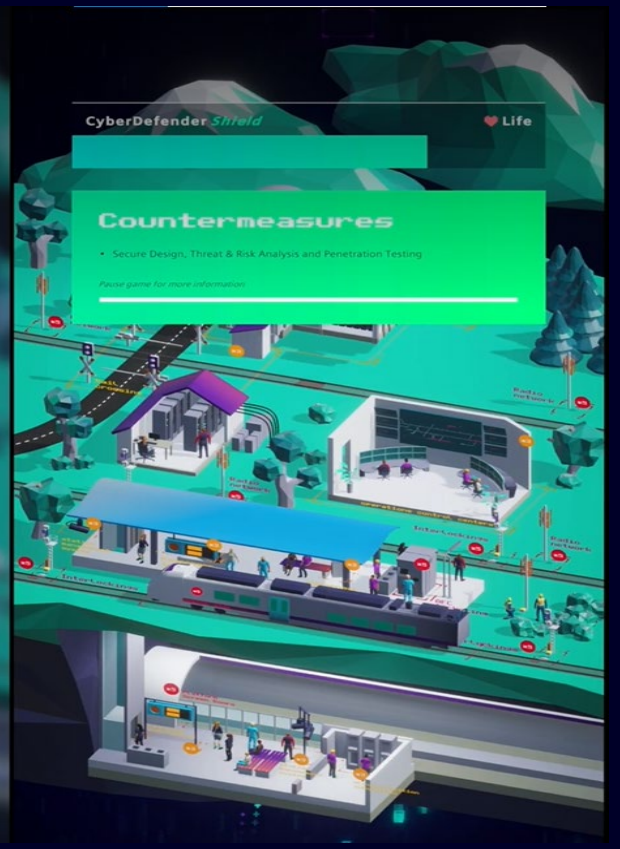
- Centralized in-house team with on-demand external support
- SOC, SIEM and IDS for IT. OT (in progress)
- Ability to detect and defend cyber attacks

Cyber Defense Center (CDC) project in Europe:

LESSON'S LEARNED: Journey from reactive to proactive & resilient Rail-Operator

Efficient **OT-Cyber Risk** reduction requires both internal and **external rail- & security expertise !**

Visit our booth



Q&A

SIEMENS