Detect and Respond to Cyber Threats across OT and IT

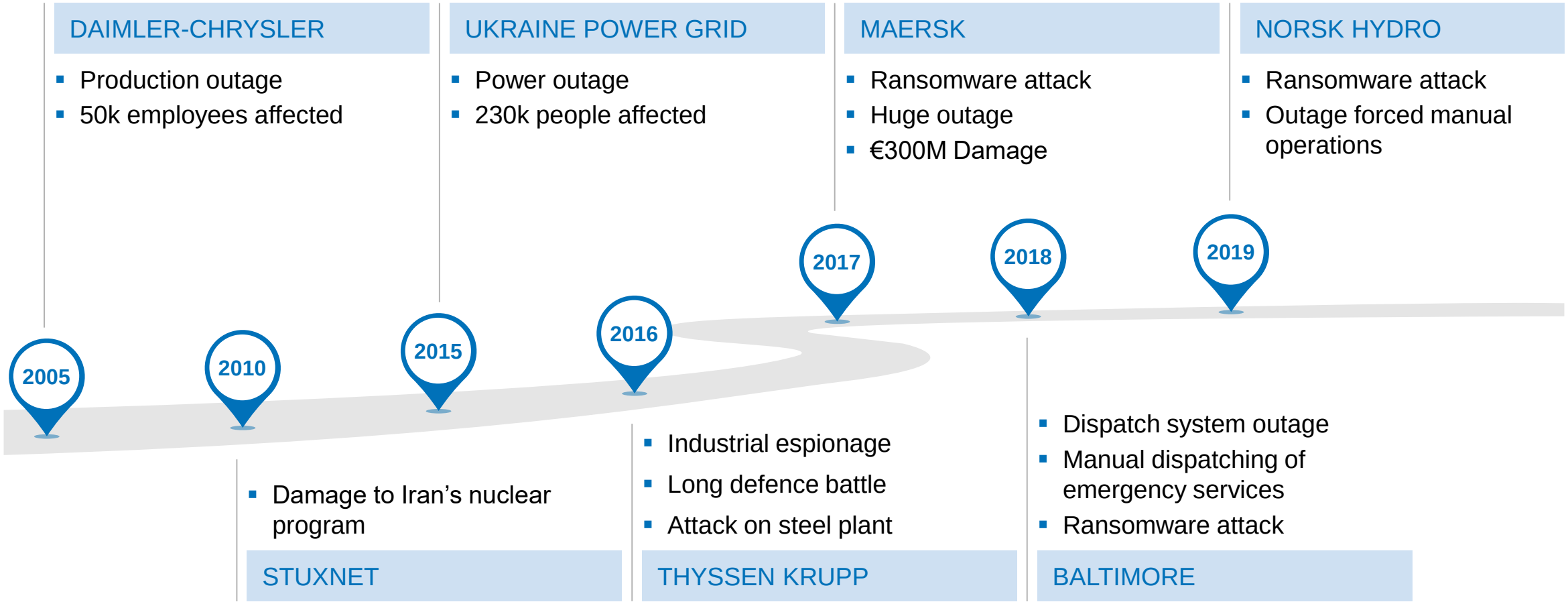
Wolfgang Kiener

Global Head, Advanced Threat Center of Excellence

TÜVRheinland®
Precisely Right.

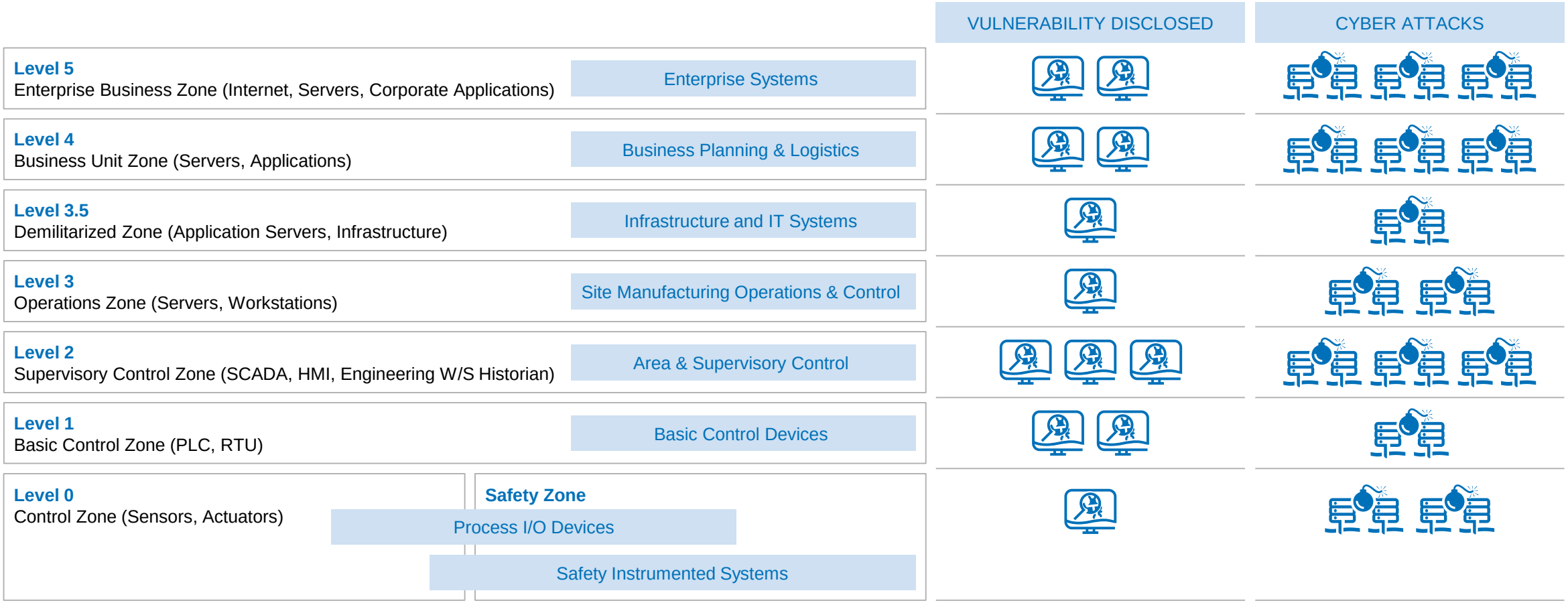
Attack frequency and impact is increasing

Attacks impact the business, but more important: attackers target business and safety



Vulnerability and Attack Trends Analysis

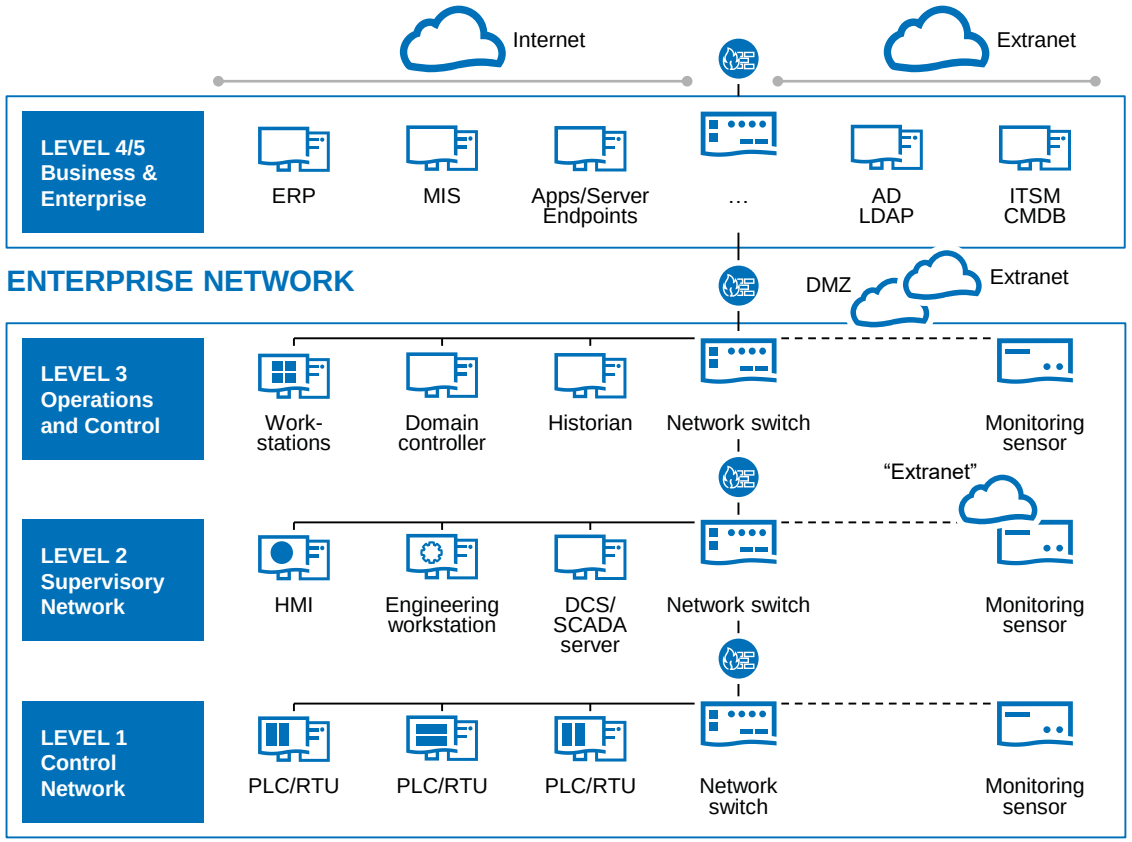
Comparing vulnerability and attack trends indicate corporate systems see most attacks; providing access for threat actors to exfiltrate data and infiltrate industrial networks



TÜVRheinland®
Precisely Right.

Achieving a complete picture across OT and the entire enterprise

Attackers do not distinguish between OT and IT



OT Production Plant

DETECTION AND RESPONSE IN OT/IT ENVIRONMENTS

Data from
- Security Infrastructure
- Endpoints, Servers, ….
- Application/Transaction
- Vulnerabilities

Data from
- Passive OT Monitoring
- Security Infrastructure
- Application/Transaction
- Vulnerabilities

Data from
- Passive OT Monitoring
- Security Infrastructure
- Vulnerabilities

Asset Discovery

Communication Profile

Vulnerability Assessment

Threat Detection

Threat Modelling

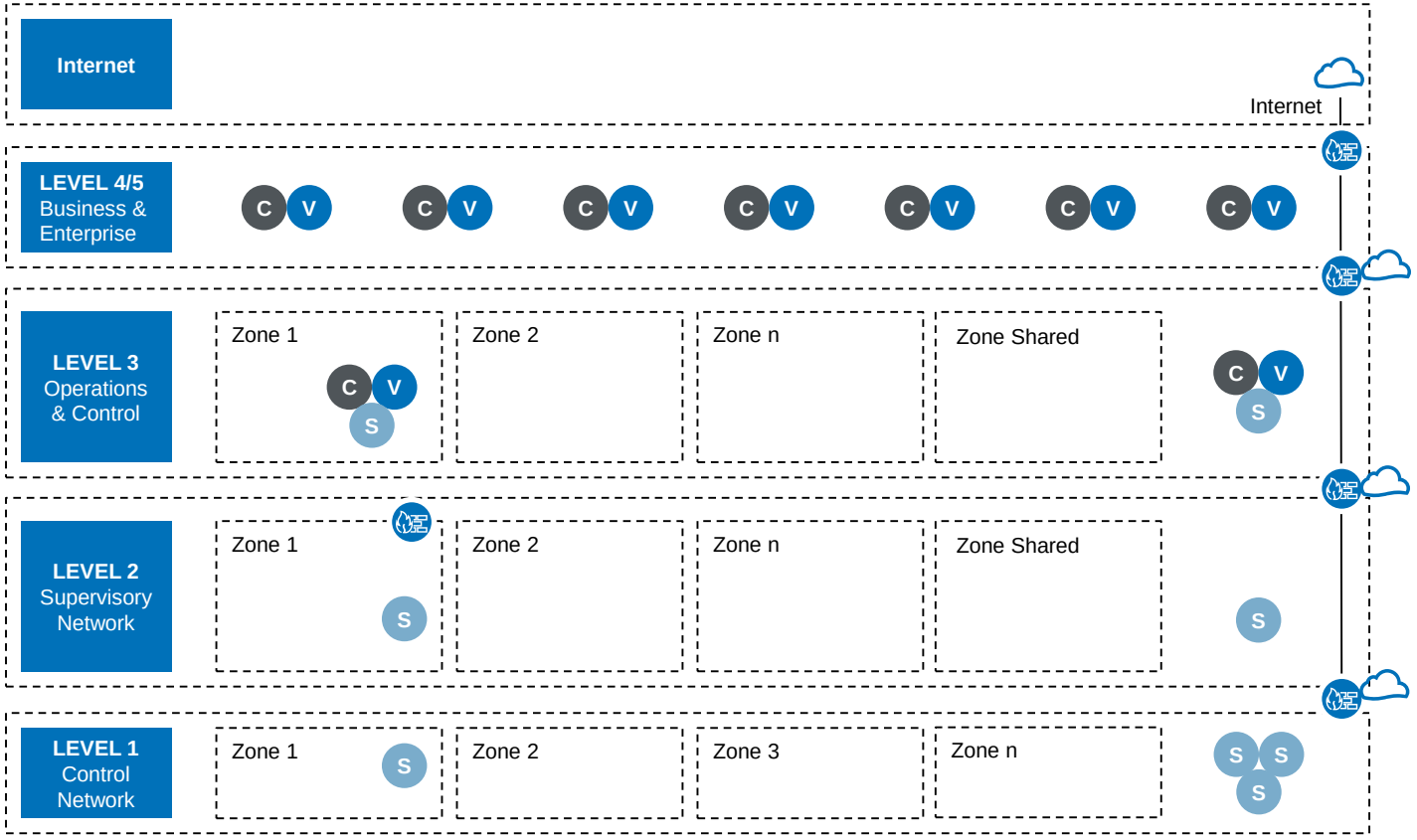
Efficient Compliance

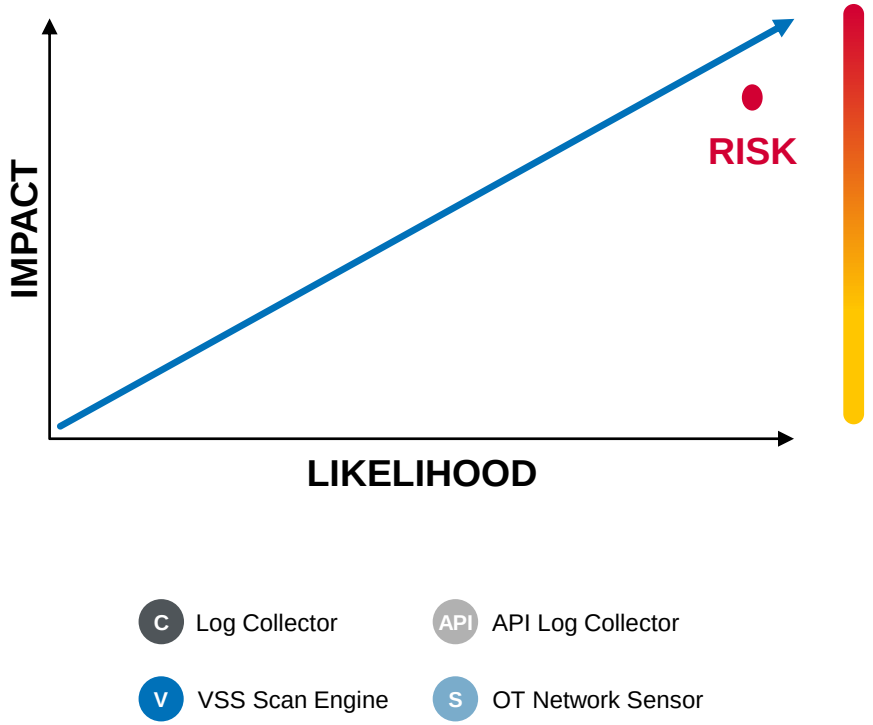
SOC – Defense Center

TÜVRheinland®
Precisely Right.

More visibility and threat detection across IT and OT.

Collectors, Sensors, and Scanners on all levels (Purdue Model)





TÜVRheinland®
Precisely Right.

Live Hacking Session

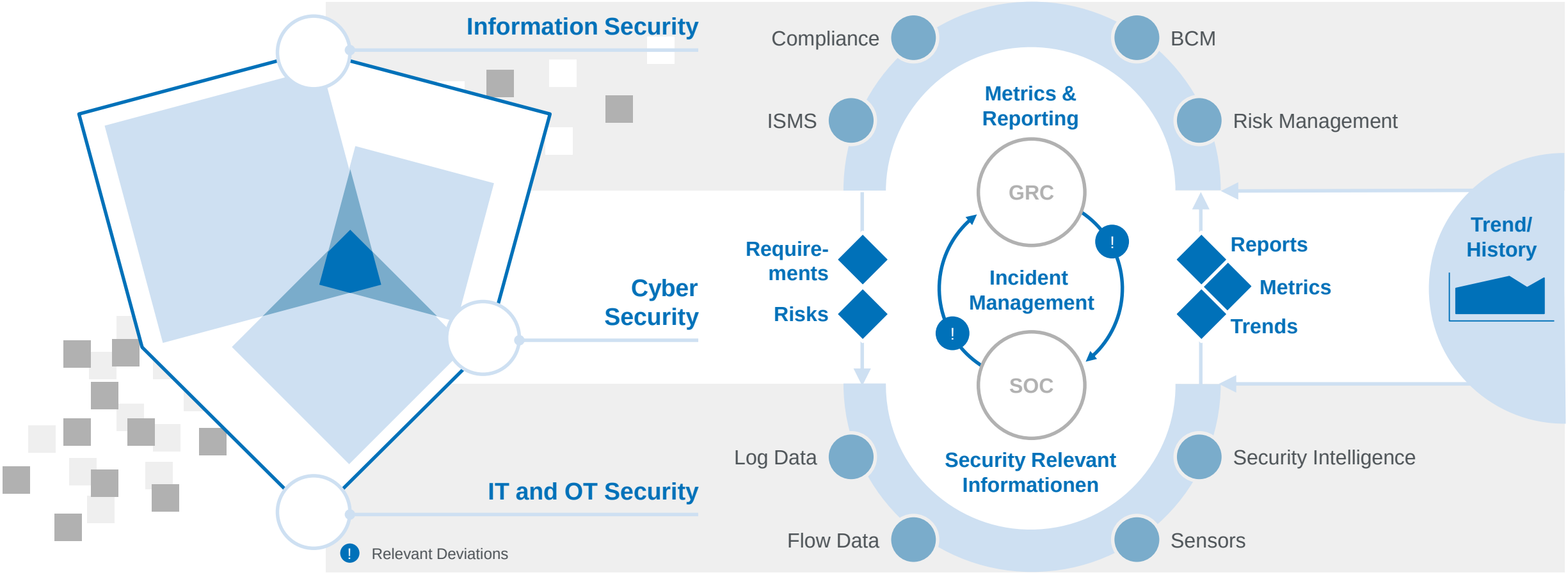
Watch live offense and defense in OT at booth 9

1 **Monitor** 2 **Detect** 3 **Protect**

TÜVRheinland®
Precisely Right.

A holistic Cybersecurity approach in OT and IT

Tie in Security Operations into Security Management and measure it.

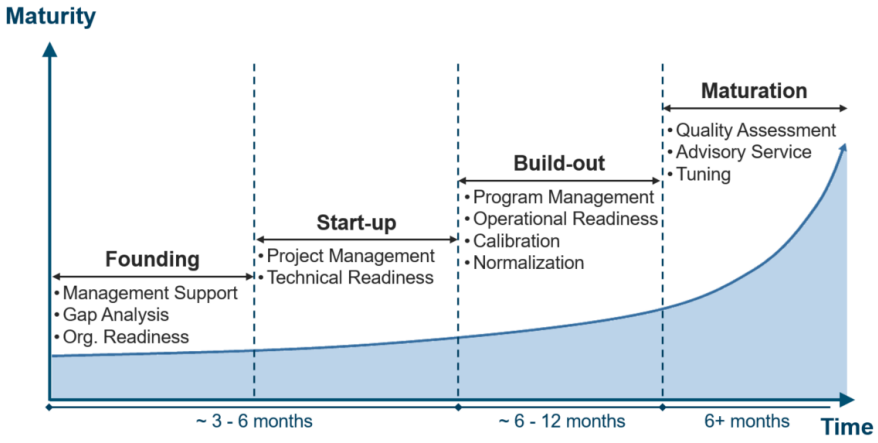


TÜVRheinland®
Precisely Right.

Make or buy a Cyber Defence Centre?

Different models for different requirements.

	In-house	Hybrid	Outsourced
Team	Client Provider Co-sourcing	Provider	Provider
Policy, Processes, Procedures	Client	Provider	Provider
Use Cases, Threat Intelligence	Client	Provider Client	Provider Client
Technology Platforms	Client	Provider Client	Provider
Investment	High CAPEX High OPEX	Medium CAPEX Medium OPEX	Low CAPEX Predictive OPEX
Deployment Time	High	Medium	Low



SOC Roles and Profiles	FTE	Coverage
Tier I Security Analyst	*	24x7
Tier II Security Analyst	*	
Tier III Security Analyst and Advisor	*	8x5
SOC Manager and Advisor	*	8x5
Platform Engineer	*	8x5

* FTE depending on local labor laws (e.g. working hours, rest times)

Shift Times Example

- **Shift 1:** 6am – 2pm: 2 analysts
- **Shift 2:** 2pm – 10 pm: 2 analysts
- **Shift 3:** 10pm – 6am: 1 analyst

* Two analysts for peaks during business hours
* Weekend shifts mean recoup time
* Vacation, public holiday, labro laws

Tier I Security Analyst Responsibilities (extract)

- Providing real-time security monitoring in a 24x7 environment
- Performing level 1 assessment of incoming alerts (validating the confidence and criticality of the alert) and escalating High Confidence critical alerts in compliance with the appropriate service levels
- Coordinate with Tier-2 Analyst for further investigation of suspicious alerts/incidents

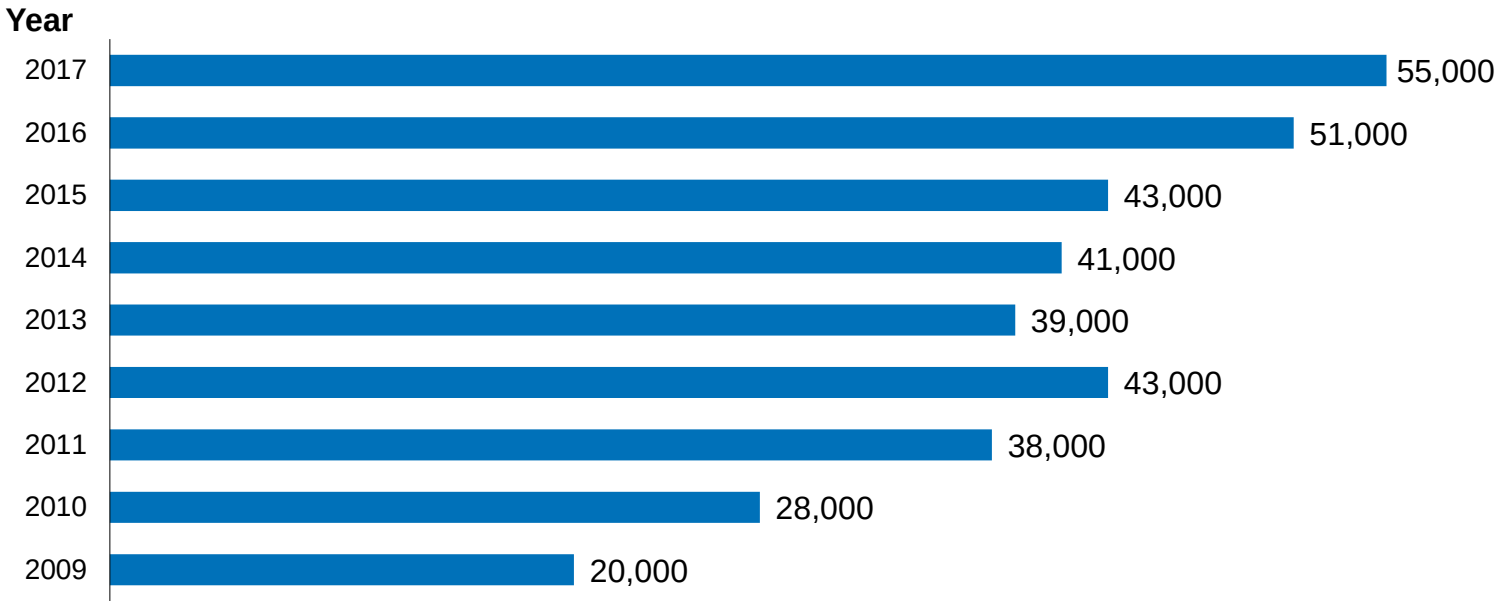
SOC Org. Chart Example

TÜVRheinland®
Precisely Right.

Make or buy a Cyber Defense Centre?

The resource gap in cybersecurity is increasing

OPEN IT POSITIONS IN GERMANY



Source: Bitkom Research 2017

Cybersecurity specialists demand reached 20% of all open IT positions in Germany.

Source: Bitkom Research 2017

One million cybersecurity job openings in 2016 … projected shortfall of two million by 2019.

Source: Cisco and ISACA

Average cybersecurity salary for experts is at €76k and increasing (Germany).

Source: Heise Medien

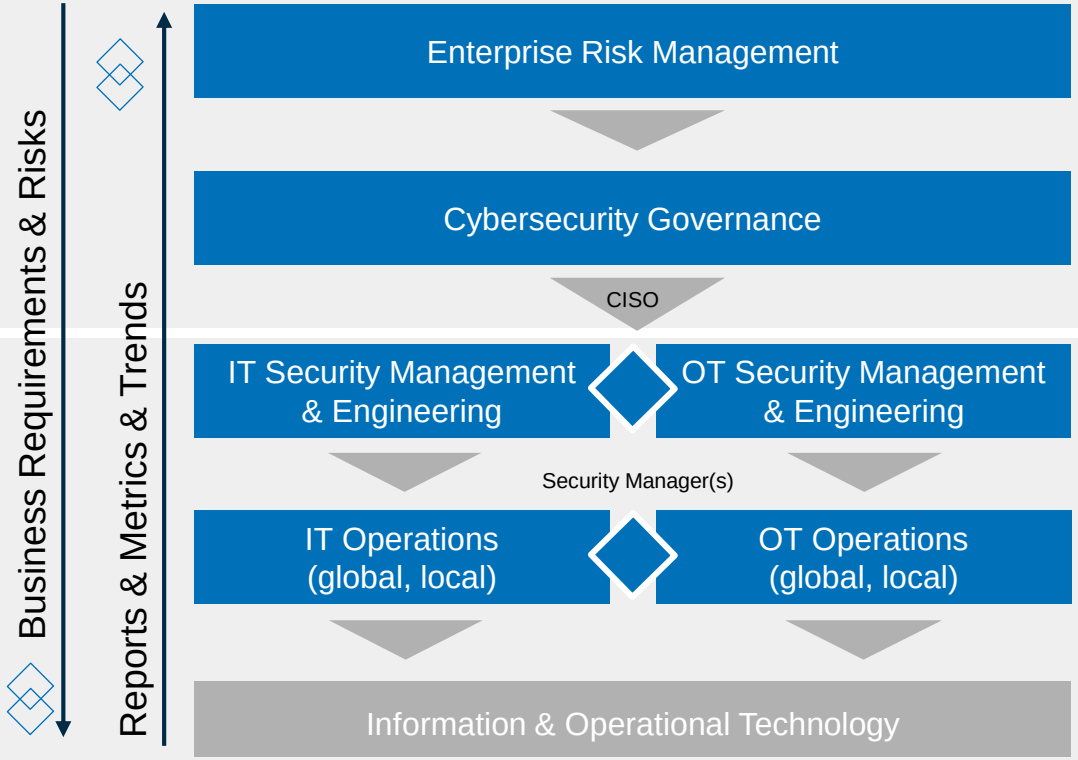
! The Resource Gap is the biggest challenge in Cybersecurity right now and in future.

TÜVRheinland®
Precisely Right.

TÜV Rheinland Cybersecurity & Safety

Protect digital manufacturing processes.

Envisioned Client Operating Model



TÜV Rheinland OT Cybersecurity Offering (extract)

- Industry 4.0 Cybersecurity Strategy
- Business Continuity Management
- IT-OT Integrated Risk Management
- IT-OT ISMS and Awareness
- IT-OT Risk & Threat Modeling
- IT-OT Risk Assessments
- OT Security Awareness Program
- OT Plant Blueprint Consulting
- OT Architecture Review
- OT Vulnerability Assessments
- OT Security & Inventory Monitoring
- Threat Detection & Response
- Incident Response & Recovery
- Secure Maintenance Access

Consulting Services

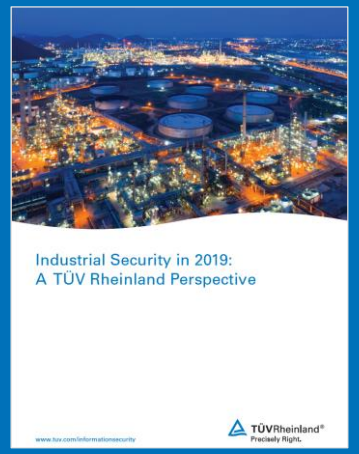
Testing Services

Managed Services

TÜVRheinland®
Precisely Right.

Questions?

Wolfgang Kiener
Global Head Advanced Threat Center
Phone: +49 174 1880217



Industrial Security in 2019: A TÜV Rheinland Perspective

www.tuv.com/ot-security19

Cybersecurity Trends 2019

www.tuv.com/cybersecuritytrends2019

TÜVRheinland®
Precisely Right.