Das Defense Center zum Schutz von Produktionsanlagen

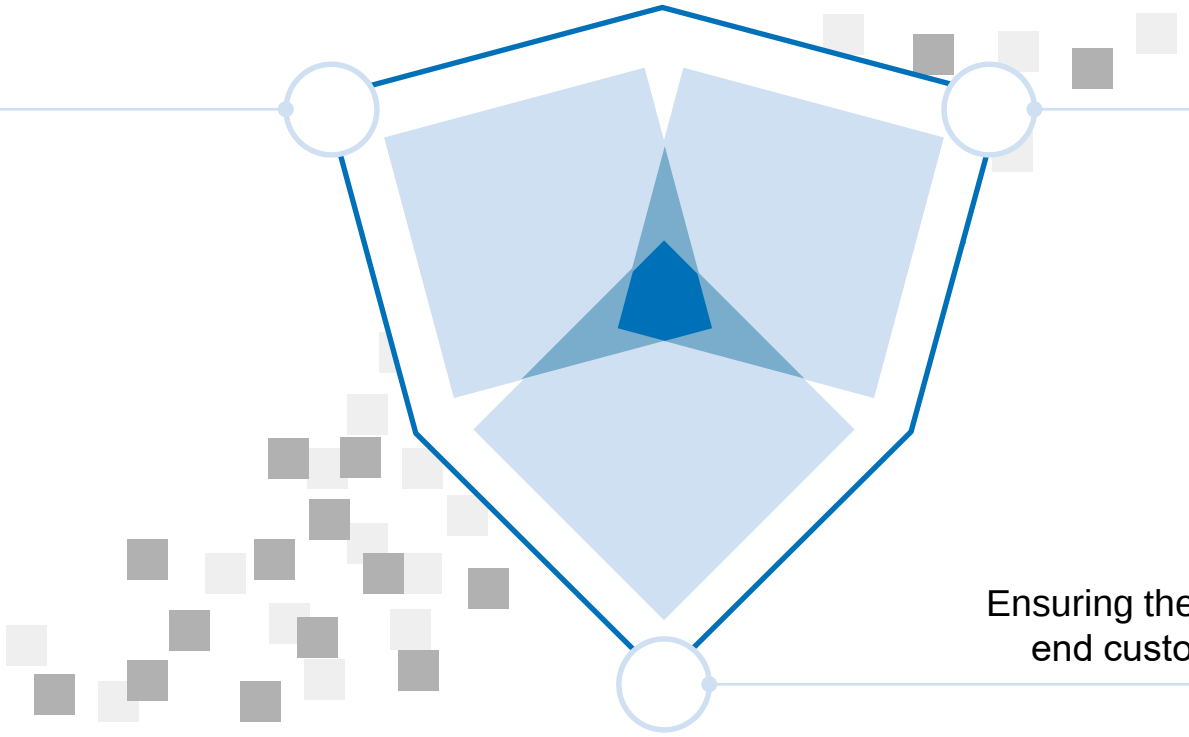
Wolfgang Kiener

Global Head, Advanced Threat Center of Excellence

TÜVRheinland®
Precisely Right.

Securing today. Safer tomorrow.

Cybersecurity as a baseline for safety and privacy



Safety

Protection of the environment against the IoT product.

Cybersecurity

Protection of the IoT product against cybercriminals.

Privacy

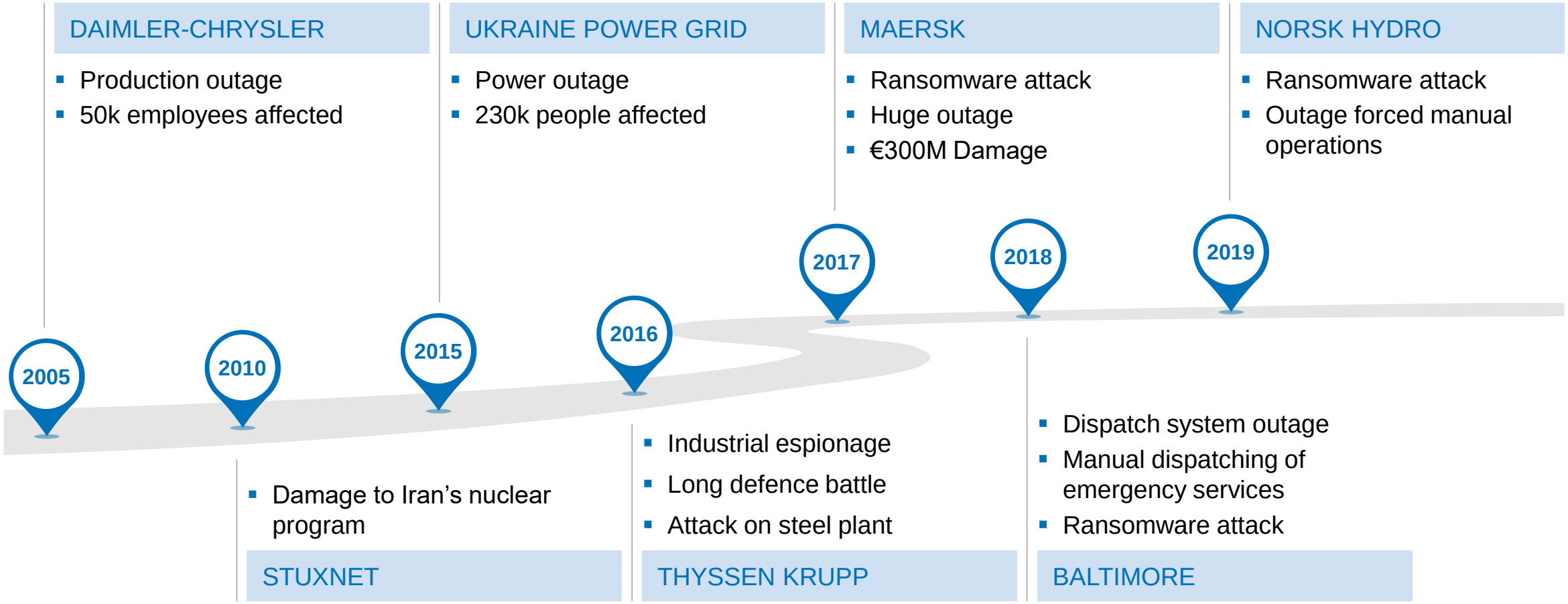
Ensuring the informational self-determination of the end customer and protection of customer’s data.

! Our business is highly affected by the dependencies between Safety, Cybersecurity and Privacy.

TÜVRheinland®
Precisely Right.

Attack frequency and impact is increasing

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



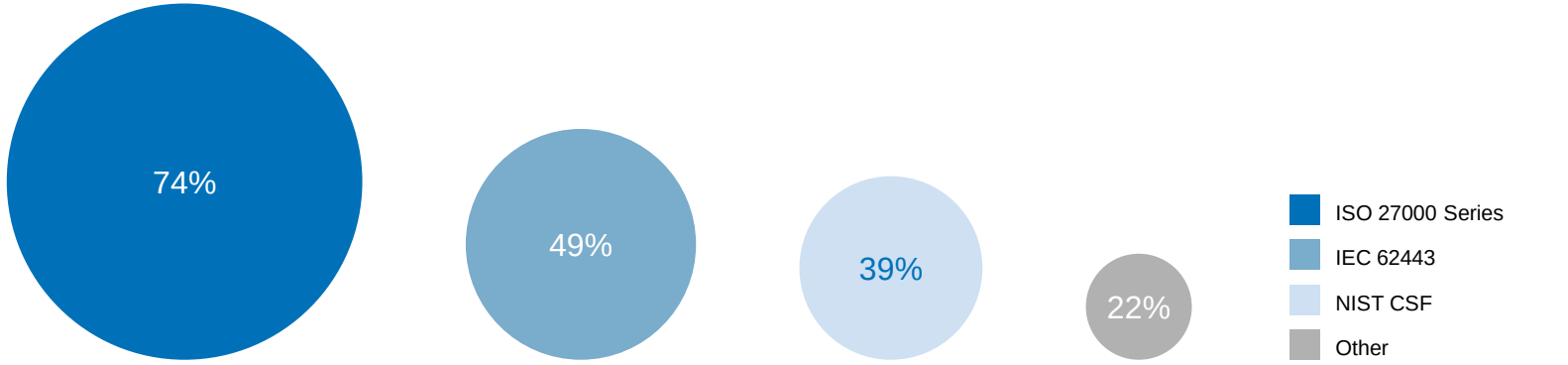
TÜVRheinland®
Precisely Right.

TÜV Rheinland Industrial Security Survey 2019

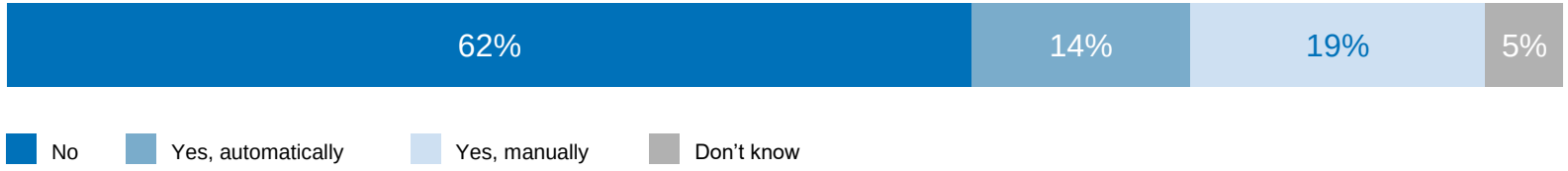
What frameworks do you use and do you know your OT assets?

https://www.tuv.com/ot-security19

WHAT FRAMEWORKS OR STANDARDS DID YOU USE FOR THE [CYBERSECURITY RISK] ASSESSMENT? (MULTIPLE SELECTIONS POSSIBLE)



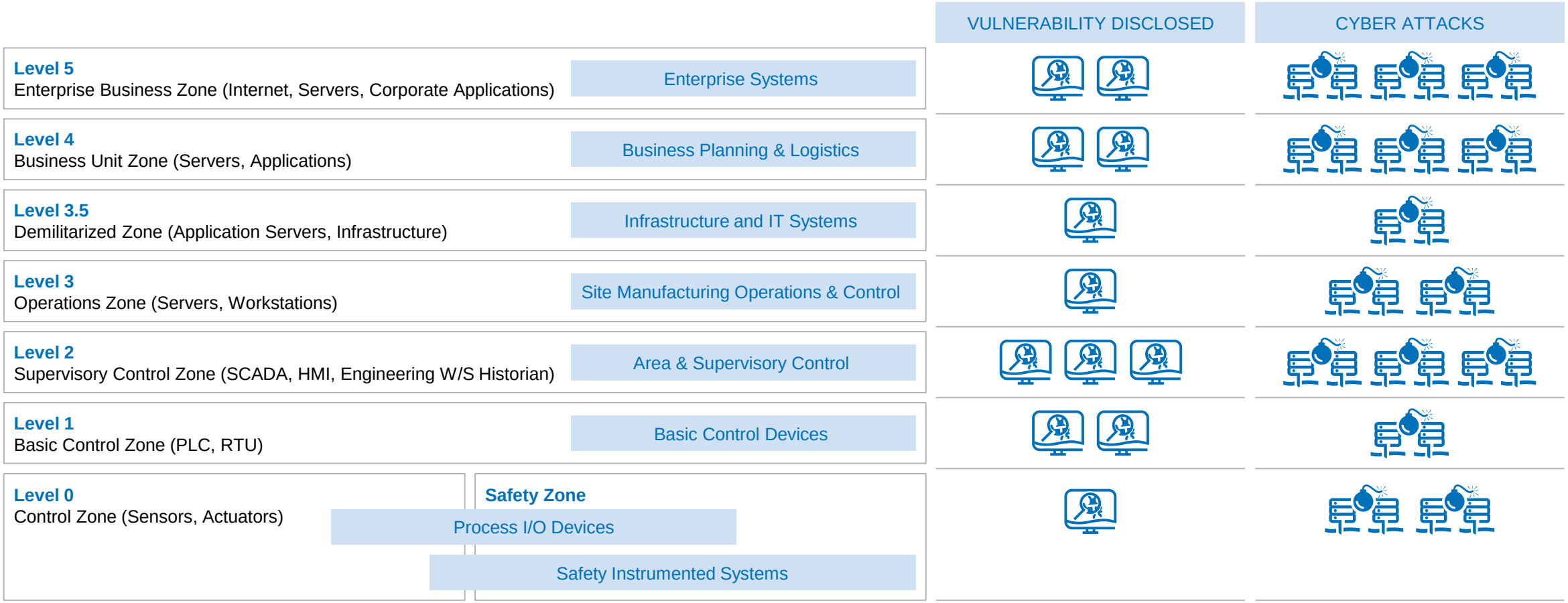
ARE YOU ABLE TO DETECT ALL THE ENDPOINTS ON YOUR OPERATIONAL TECHNOLOGY NETWORK?



TÜVRheinland®
Precisely Right.

Vulnerability and Attack Trends Analysis

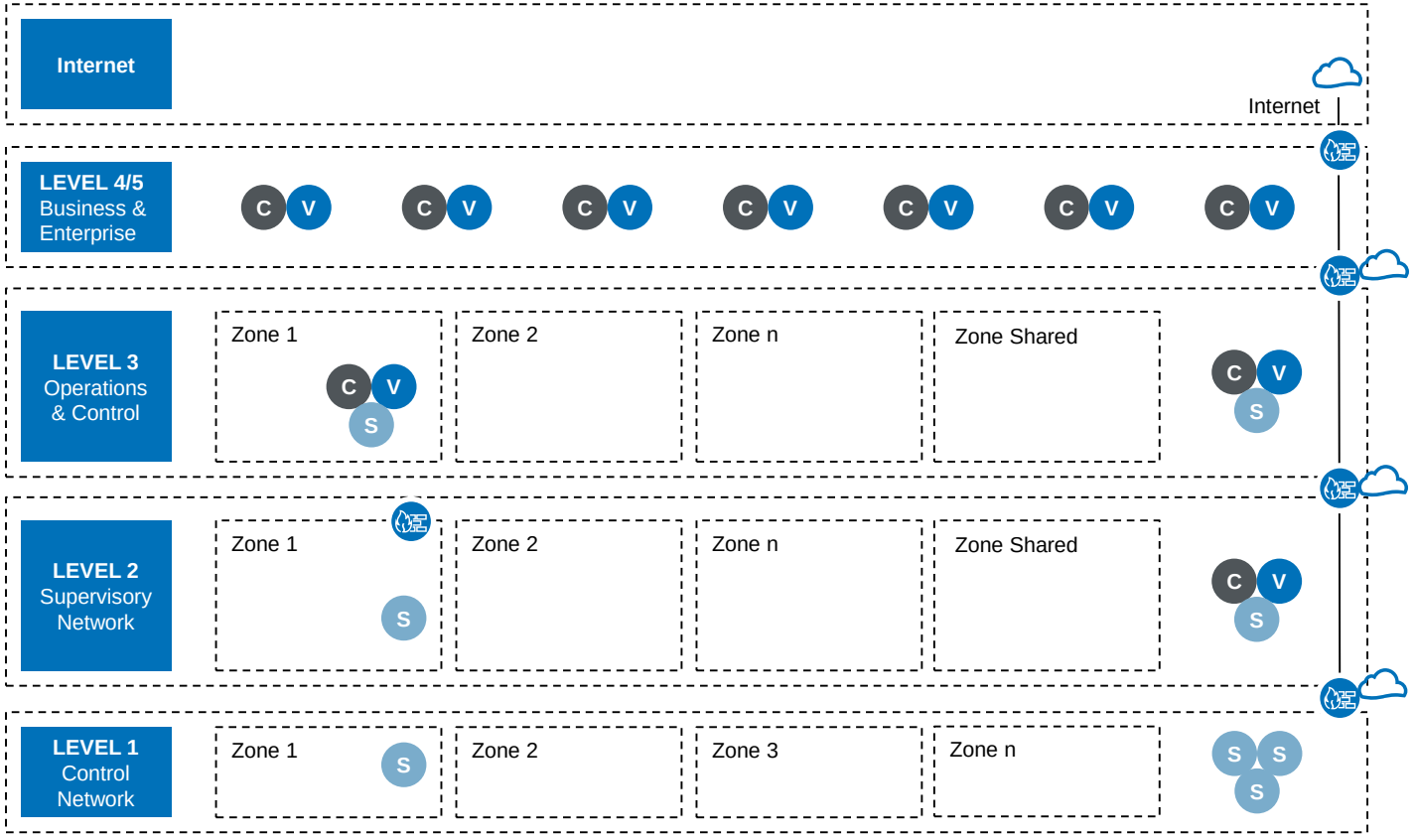
Comparing vulnerability and attack trends indicate corporate systems see most attacks; providing access for threat actors to exfiltrate data and infiltrate industrial networks

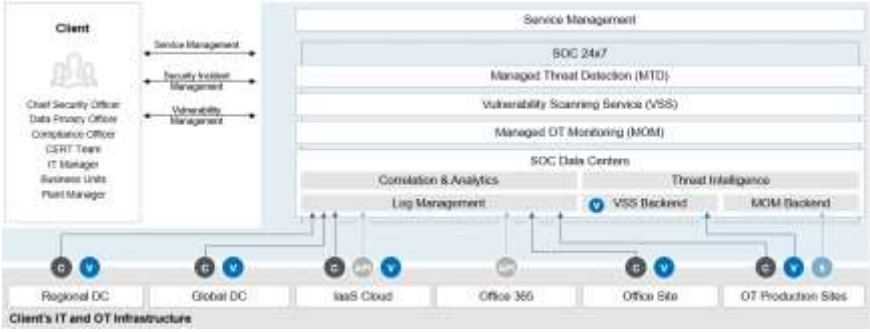


TÜVRheinland®
Precisely Right.

More visibility and threat detection across IT and OT.

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





C Log Collector

API API Log Collector

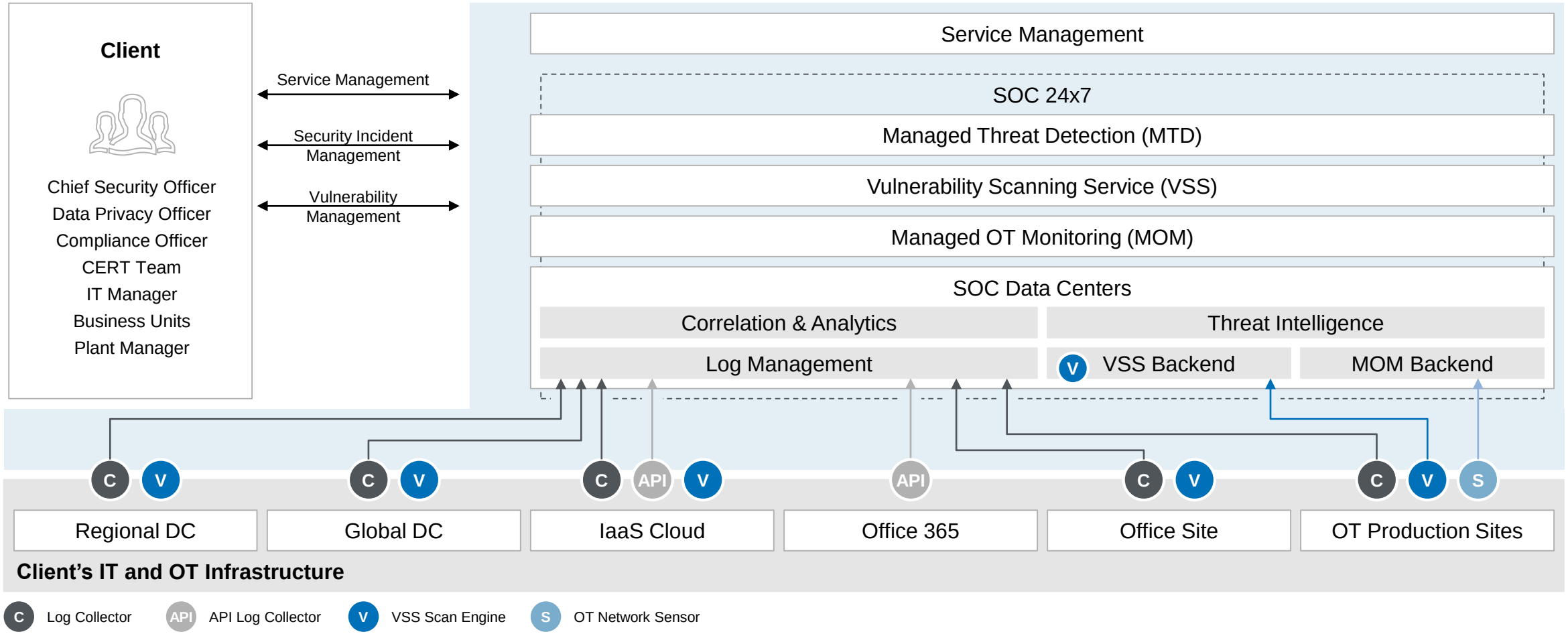
V VSS Scan Engine

S OT Network Sensor

TÜVRheinland®
Precisely Right.

The Defense Center for more visibility and threat detection IT and OT.

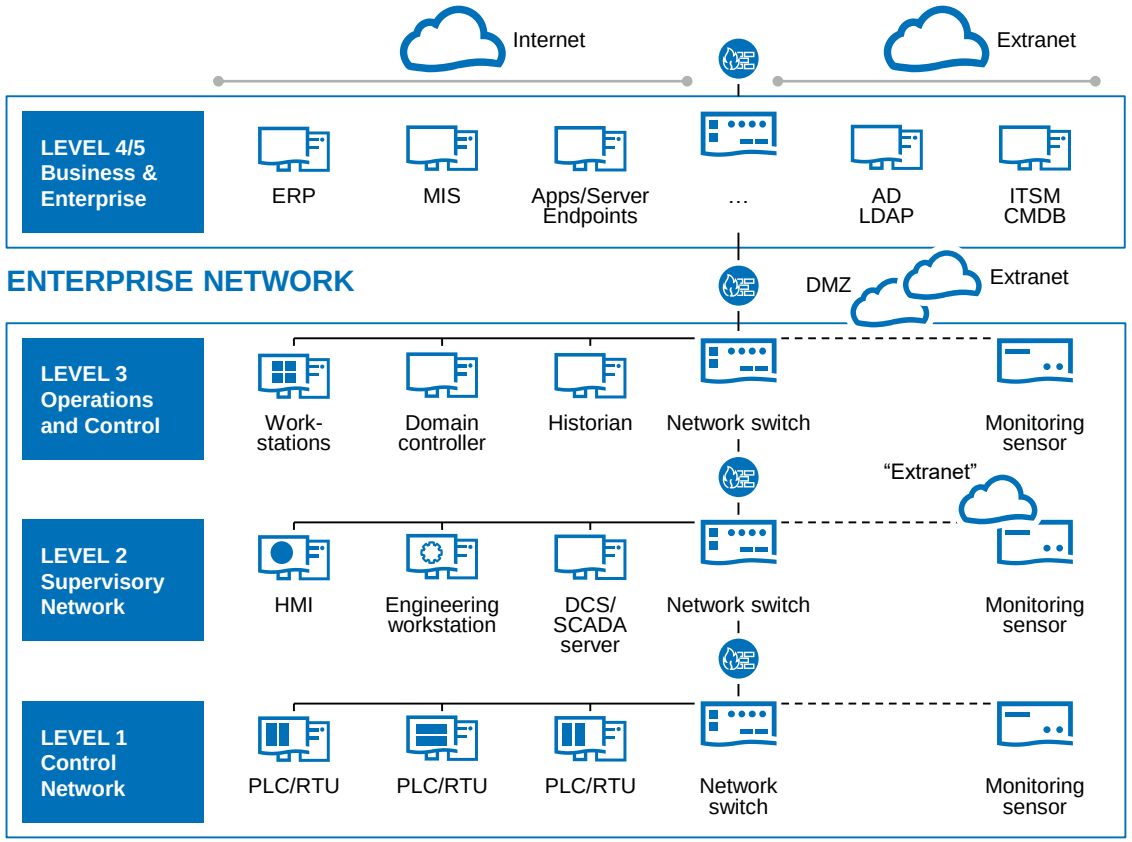
TÜV Rheinland's Defense Center



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

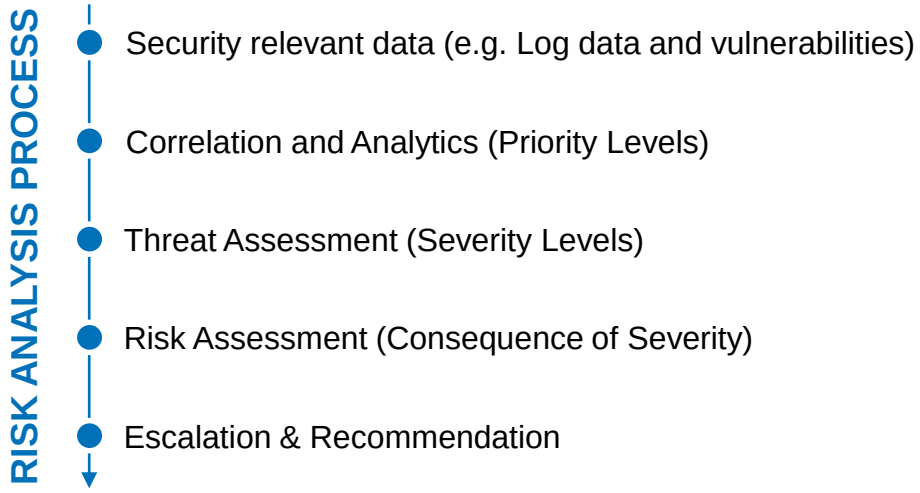
Efficient Compliance

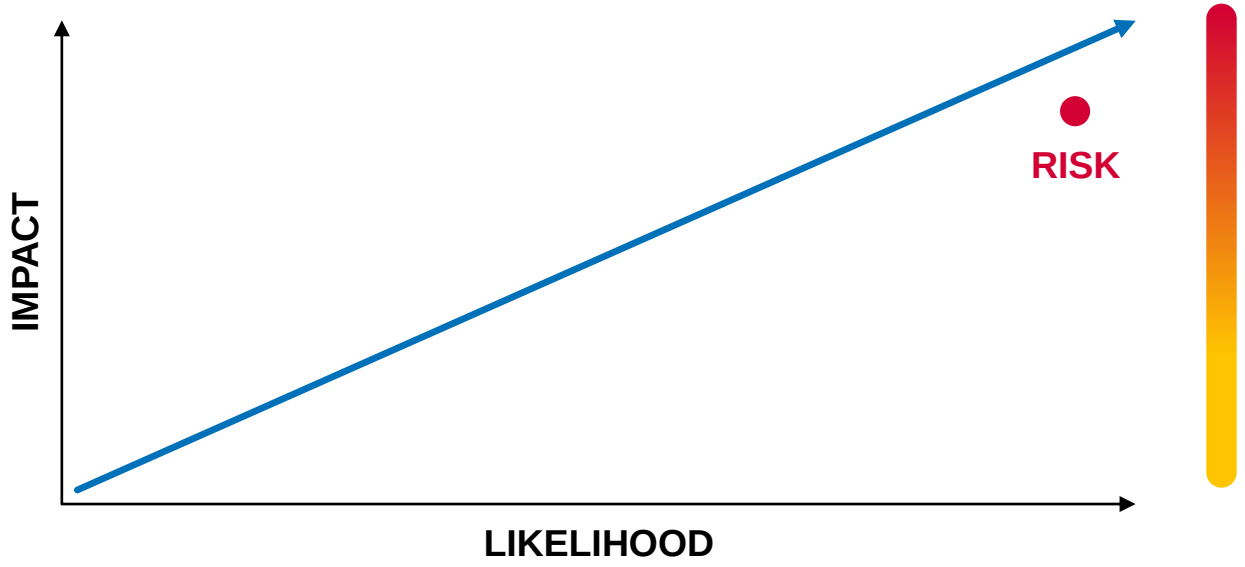
SOC – Defense Center

TÜVRheinland®
Precisely Right.

How does TÜV Rheinland approach Cyber Defense?

Vulnerability Information is most important for prioritization of threats





RISK = LIKELIHOOD (THREAT × VULNERABILITIES × COMPENSATING CONTROLS) × **IMPACT** (ASSET VALUE/CRITICALITY)

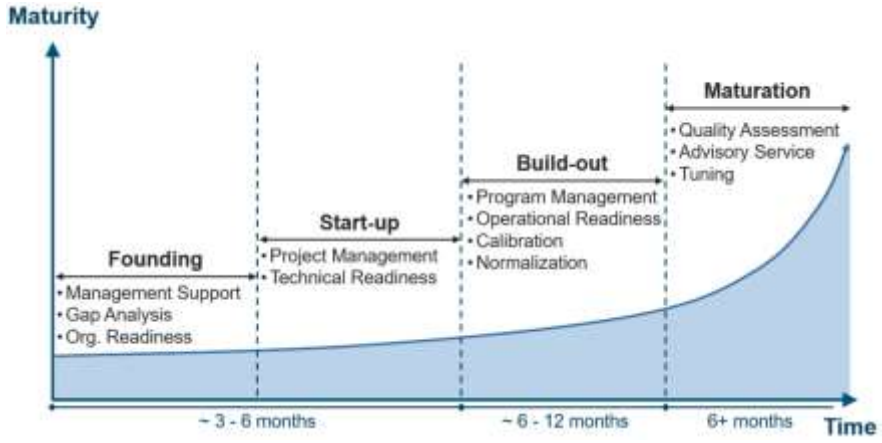
Prioritized security incidents enable smart/focused budget and resource allocation.

TÜVRheinland®
Precisely Right.

Make or buy a Cyber Defense 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

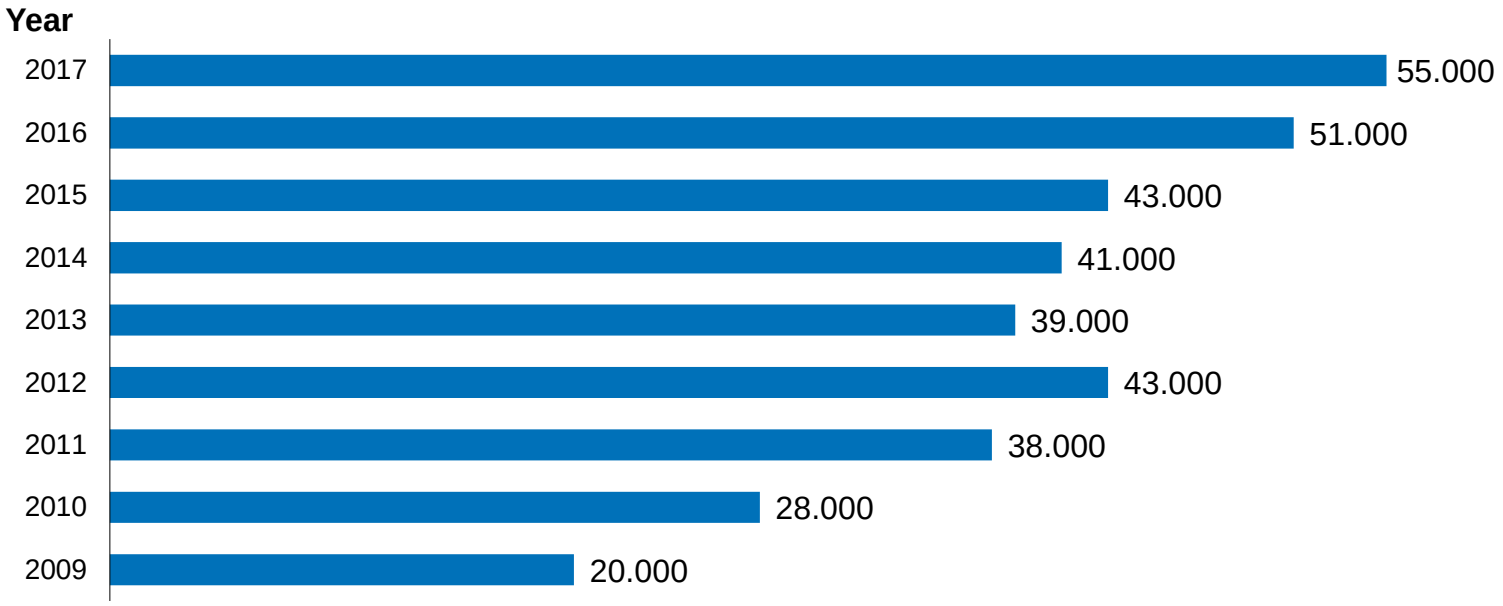
SOC Org. Chart Example

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).

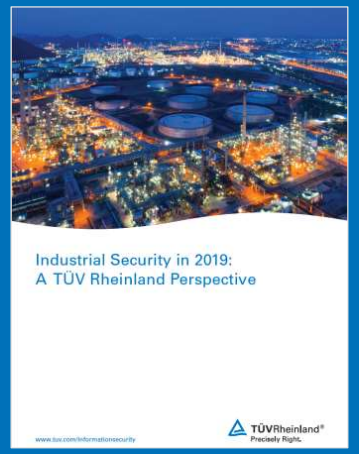
Source: Heise Medien

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

TÜVRheinland®
Precisely Right.

Thank you.

Wolfgang Kiener
Global Head of 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.

TÜV Rheinland. Who are we?

TÜVRheinland®
Precisely Right.

- $2.3 Billion
- Privately Held
- 144 Years Old
- 500 Locations
- 69 Countries
- 19,320 people

Protecting society since 1872

Industry 1.0
Mechanical Production

Industry 2.0
Mass Production & Electricity

Industry 3.0
Electronic & IT Systems

Industry 4.0
Cyber-physical Systems, Social, Mobile, Analytics, Cloud

! The digital transformation will be defined by the use of “cyber-physical” systems.

TÜVRheinland®
Precisely Right.

TÜV Rheinland. Your partner in IT and OT Cybersecurity.

69 Countries **>500** Locations **19,924** Employees

Businesss Unit Cybersecurity

~400 Cybersecurity Experts

€ 140 Mio. € Revenue

~180 Cybersecurity Experts in Germany

Cologne	60	Gelnhausen	35	Hanover	8
Munich	44	Saarbrücken	16	Hamburg	17

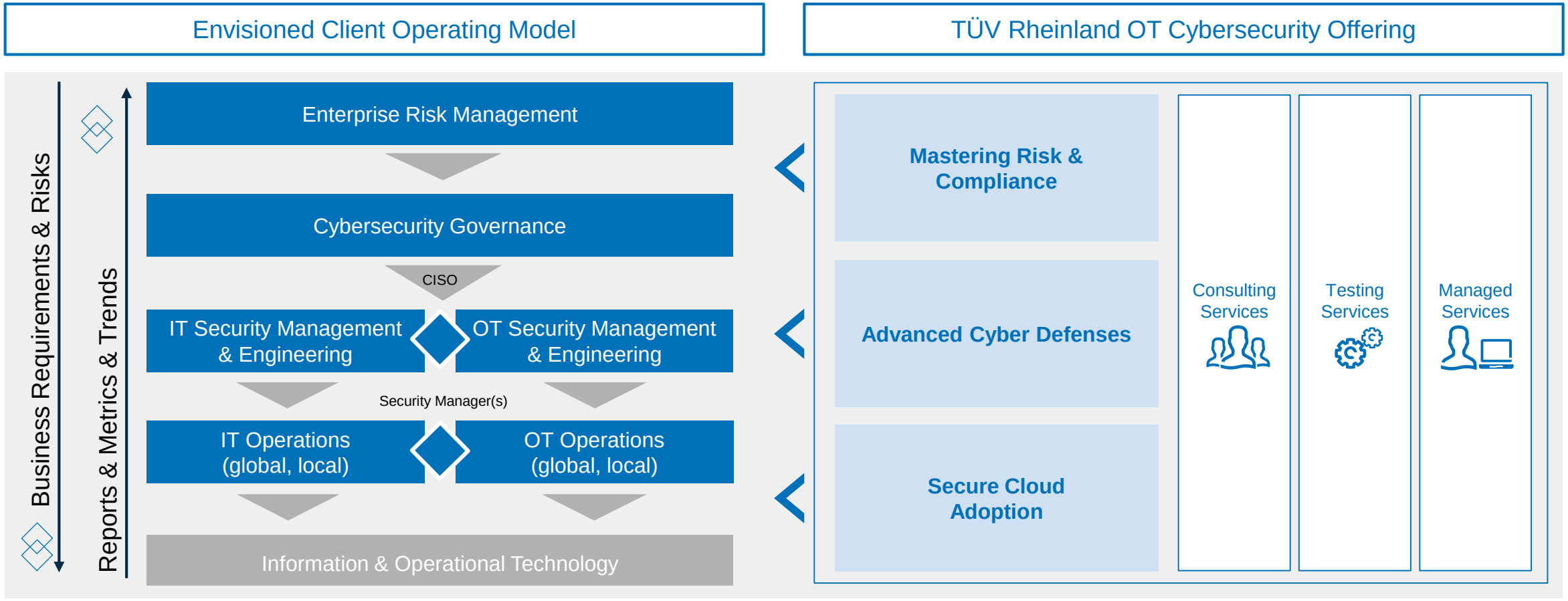
Consulting Services | Testing Services | Managed Services

TÜV Rheinland Cybersecurity Unit is focused on consult, build, run, and test cybersecurity solutions.

TÜVRheinland®
Precisely Right.

TÜV Rheinland Industrial Cybersecurity

Protecting the digital operational processes

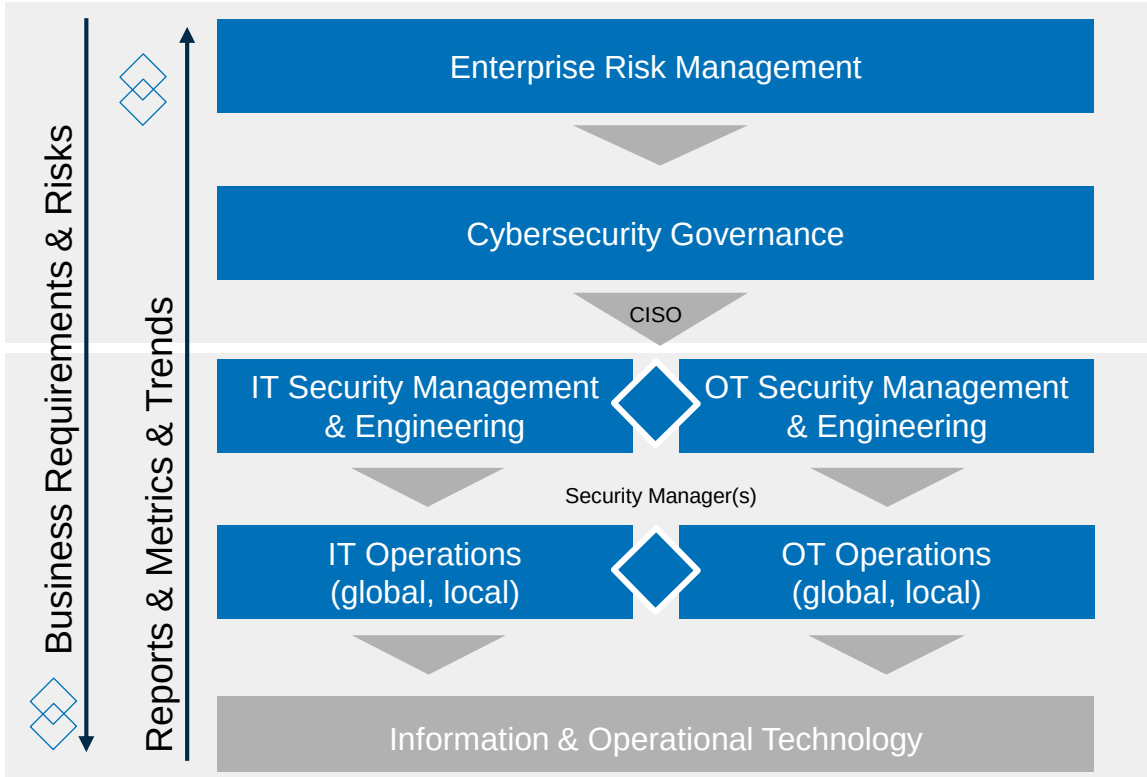


TÜVRheinland®
Precisely Right.

TÜV Rheinland OT Cybersecurity

Industrial security goes beyond protecting technology. Integrated risk management and governance enables smarter investment to reduce risk in a converging OT and IT technology landscape.

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.

How does TÜV Rheinland approach Cyber Defence?

Achieving a complete picture across OT and the entire enterprise.

MANAGED SERVICES: FROM MSS TO MDR

Cybersecurity Program Management | CERT | Incident Response & Forensics

Operational Interlock: Automation & Orchestration

Managed Threat Detection incl. Remote Response

- Managed Endpoint Protection
- Vulnerability Scanning Service
- APT Defense Service
- Managed OT Monitoring

Operational Interlock: Automation & Orchestration

Information and Operational Technology Infrastructure

CONSULTING AND TESTING SERVICES

- SOC Build Consulting
- Maturity Assessment (Detection, Response, Intel)
- Make or Buy Workshop and Consulting
- Use Case Workshop
- Architecture Review/Assessment/Workshop
- CERT Build Consulting
- Incident Response
- Forensics
- Threat Modeling
- Red and Blue Team Testing
- Threat Hunting

FASTER DETECTION

FASTER RESPONSE

TAILORED RESPONSE

RESPONSE PARTICIPATION

TÜVRheinland®
Precisely Right.

OT Monitoring and Threat Detection

OT Cybersecurity Risk Assessment

PREPARATION

2 weeks

- Prepare & plan
- Kick-Off workshop
- Install sensors and management station

MONITOR

2 – 12 weeks

- Platform training
- Monitor network traffic
- Analyze traffic flows
- Detection & analysis

FINAL EVALUATION

2 weeks

- Test use cases
- Create report
- Debriefing workshop and next-steps

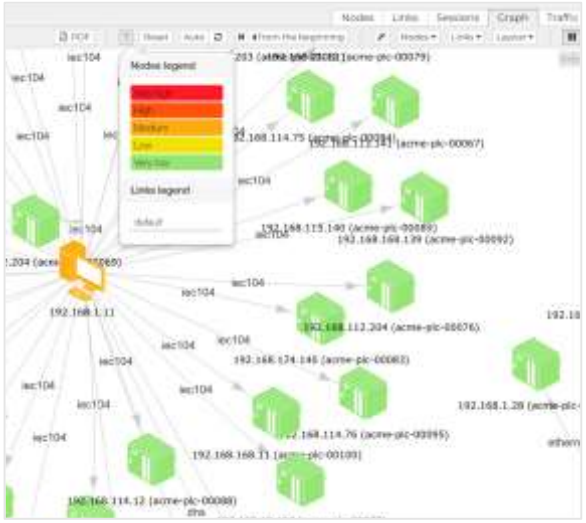
DISENGAGE

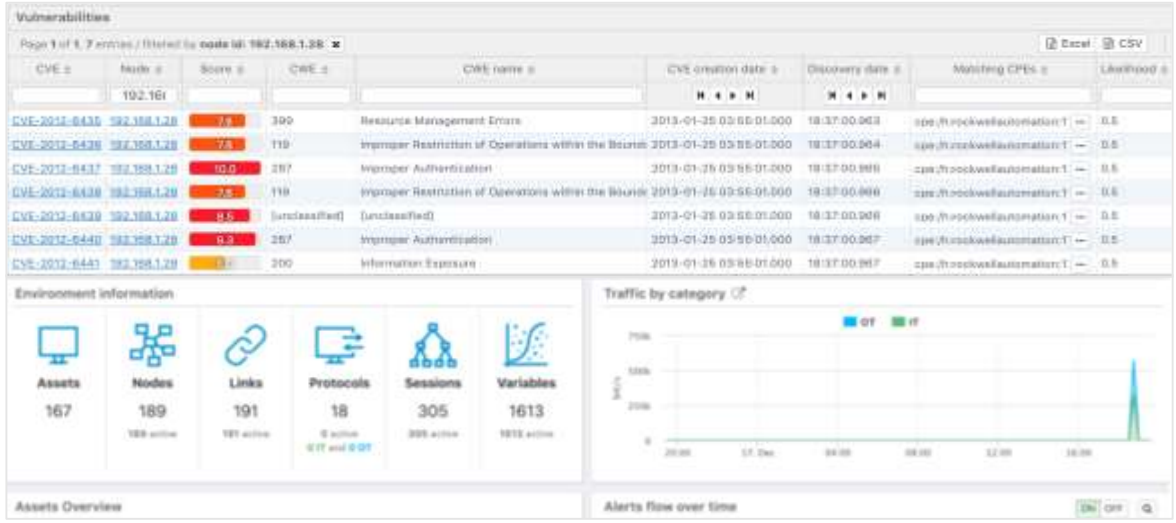
2 days

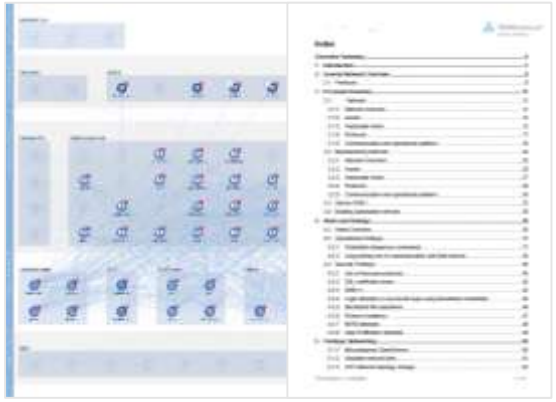
- Erase data
- Remove equipment

DELIVERABLES

- Comprehensive Report
- Asset inventory & communication profile
- Asset Vulnerabilities
- Risk and threat identification
- Recommendations
- Benchmark







TÜVRheinland®
Precisely Right.