Sichere Produktion

Cybersecurity in der vernetzten Fertigung

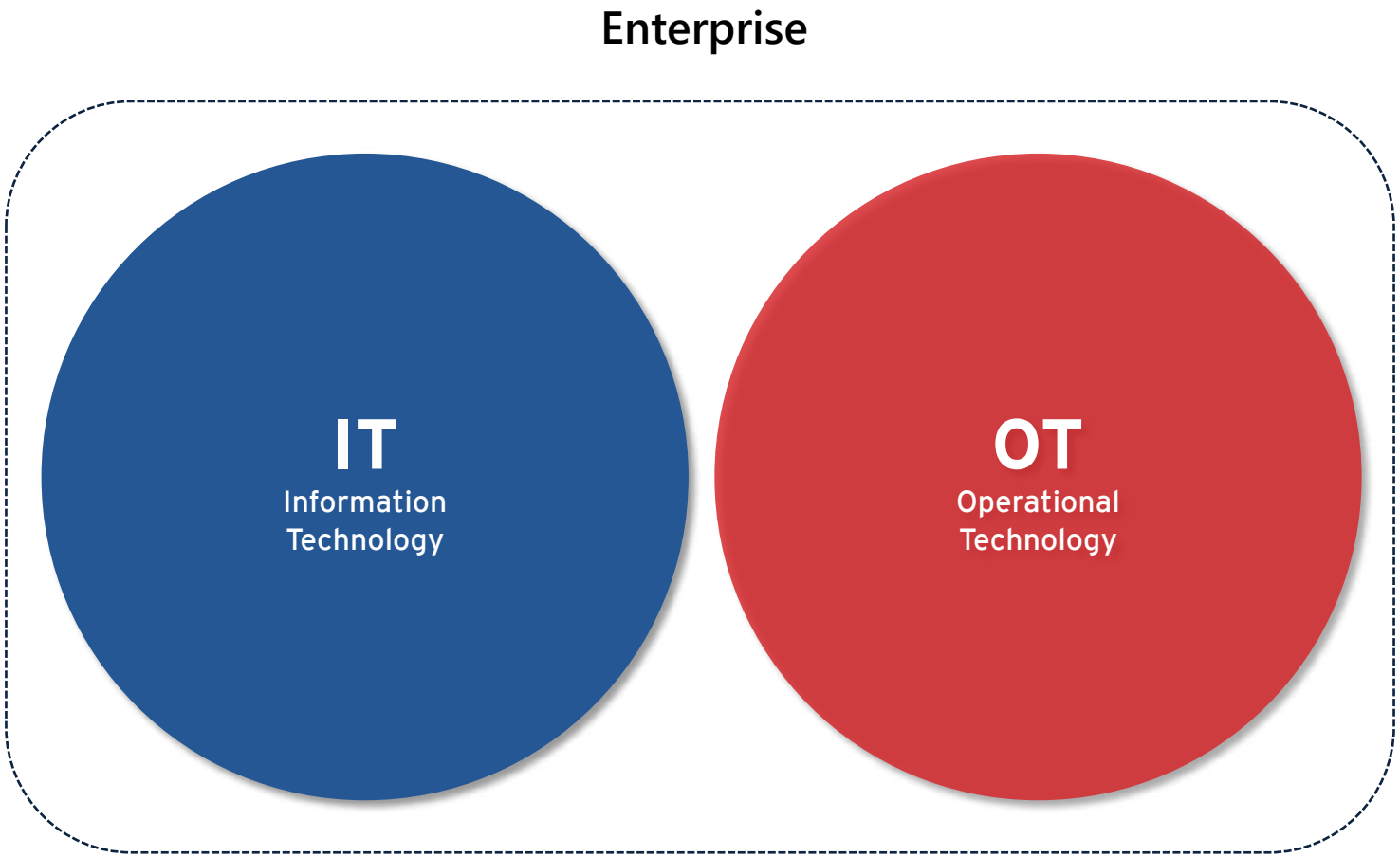
Falk Trümner / DriveLock SE

Agenda

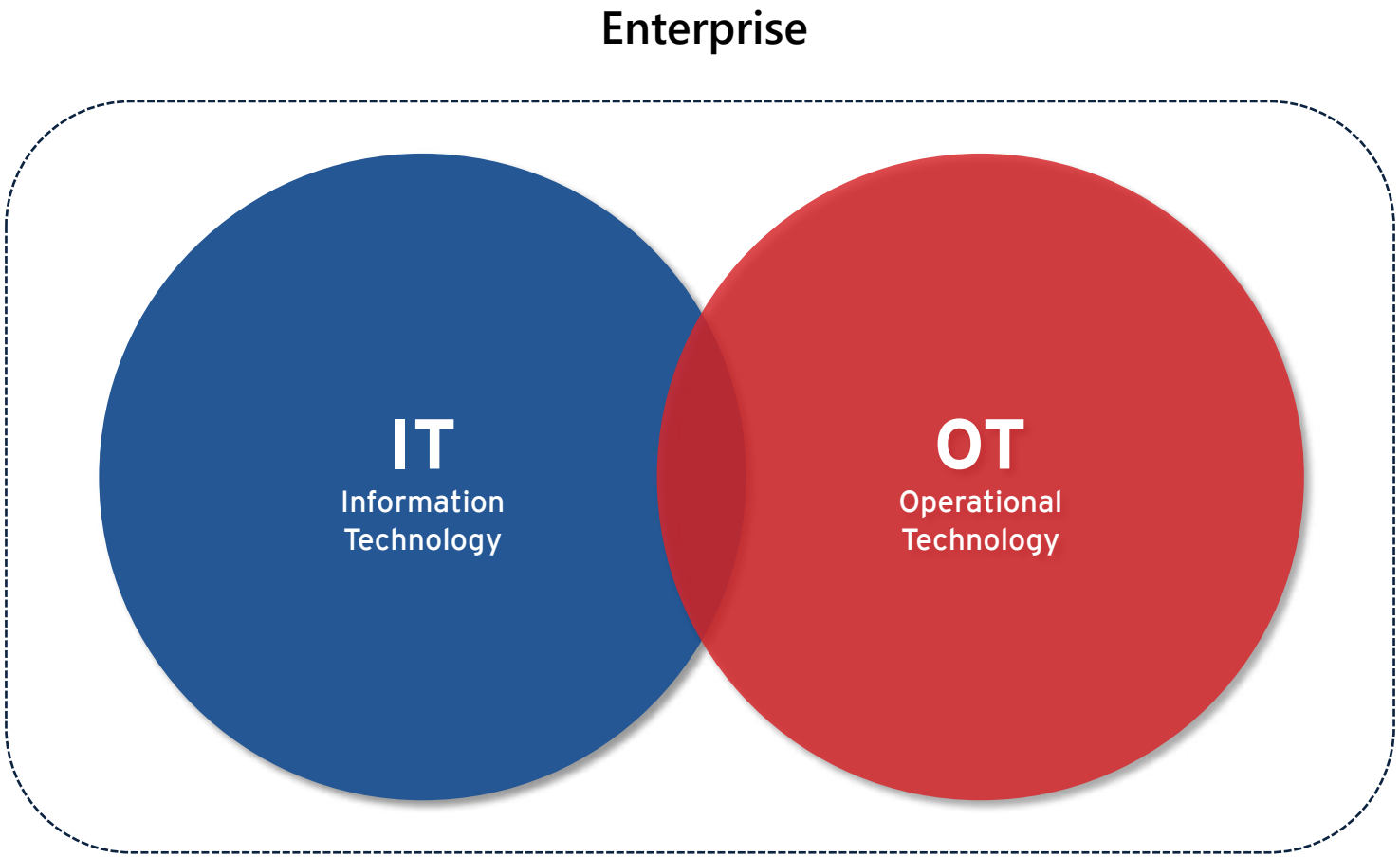
- IT vs. OT
- Industrial Control Systems
- Threats
- Countermeasures

IT vs. OT

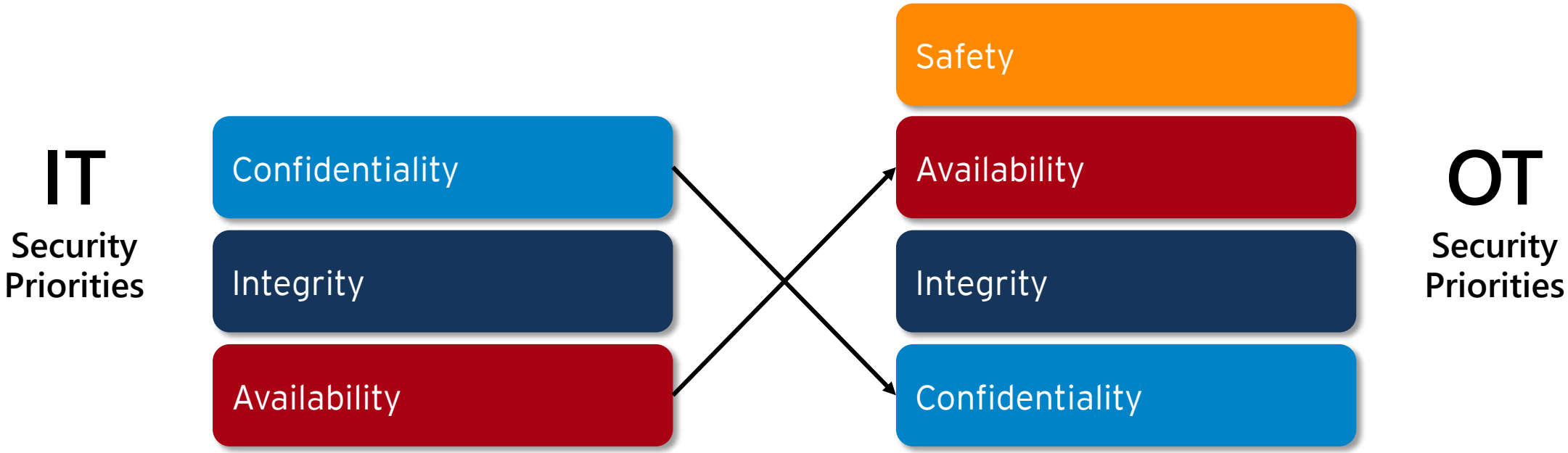
IT/OT Convergence



IT/OT Convergence



Priorities



1000% availability

Industrial Control Systems

Mission Critical Devices

- Supervisory Control and Data Acquisition (SCADA)
- Human Machine Interfaces (HMIs)
- Engineering Workstations (EWSes)
- PC-based controllers
- Database servers
- Fixed-function devices
- Industrial IoT devices

ICS Functions

Control

Control values, motors and other components.

This function may be automatically driven by changes in logic states e.g. of sensors.

View

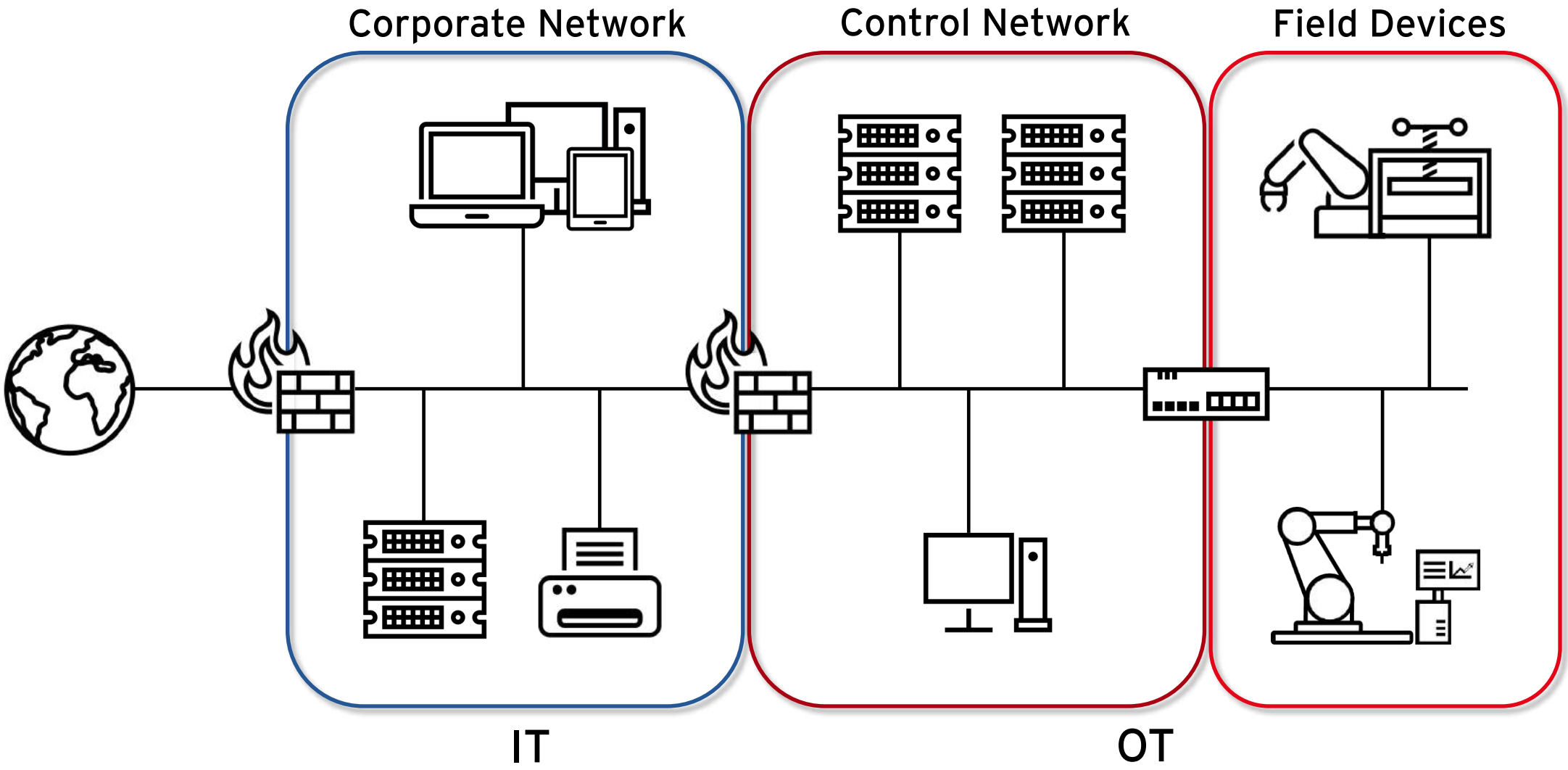
Visualize and watch the current state of the process in order to make decicions.

Monitor

Monitors the currect state of the process. E.g. fluid level, valve positions, feed rates, speed or temperature.

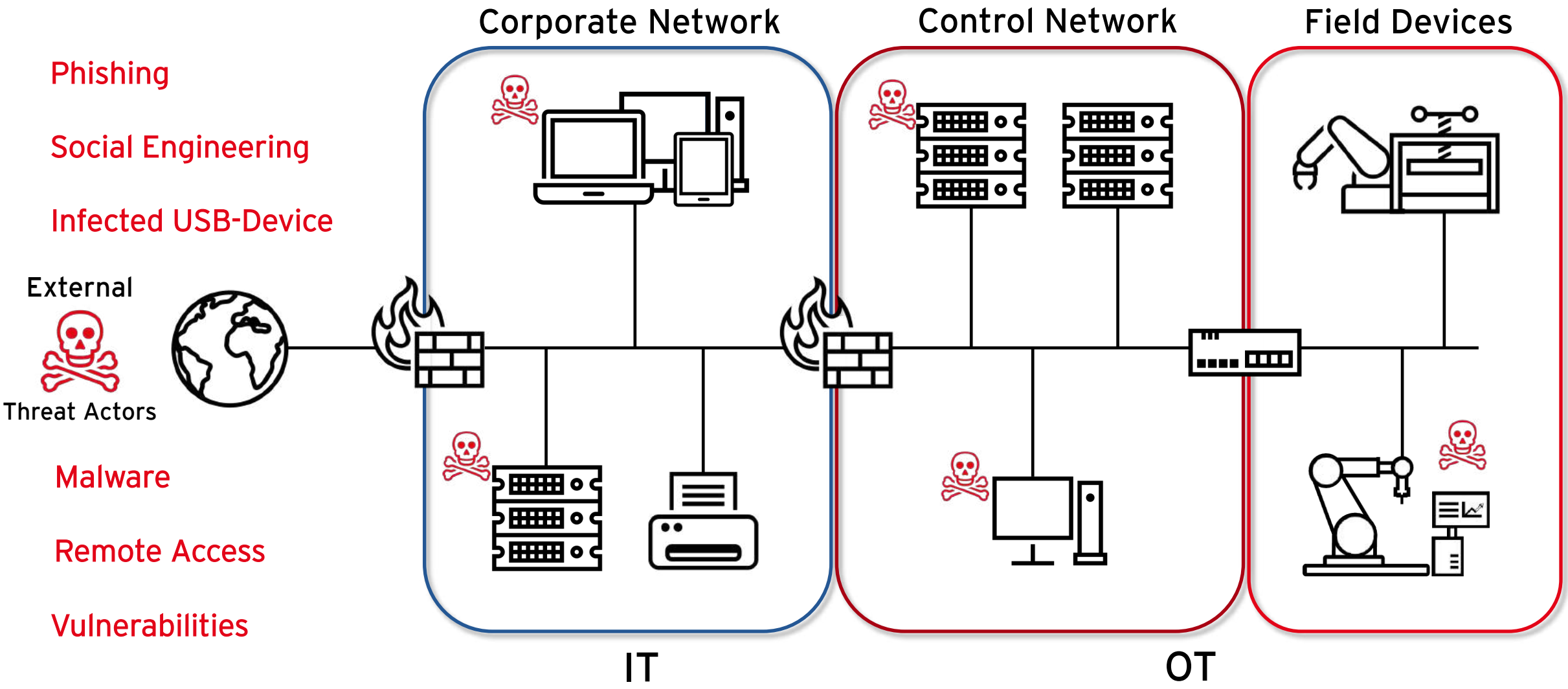
In contrast to viewing, monitoring includes alerting, event conditions, and warning of adverse process conditions.

Smart Factory



Threats

Many Roads Lead to Rome



Consequences of a Cyberattack

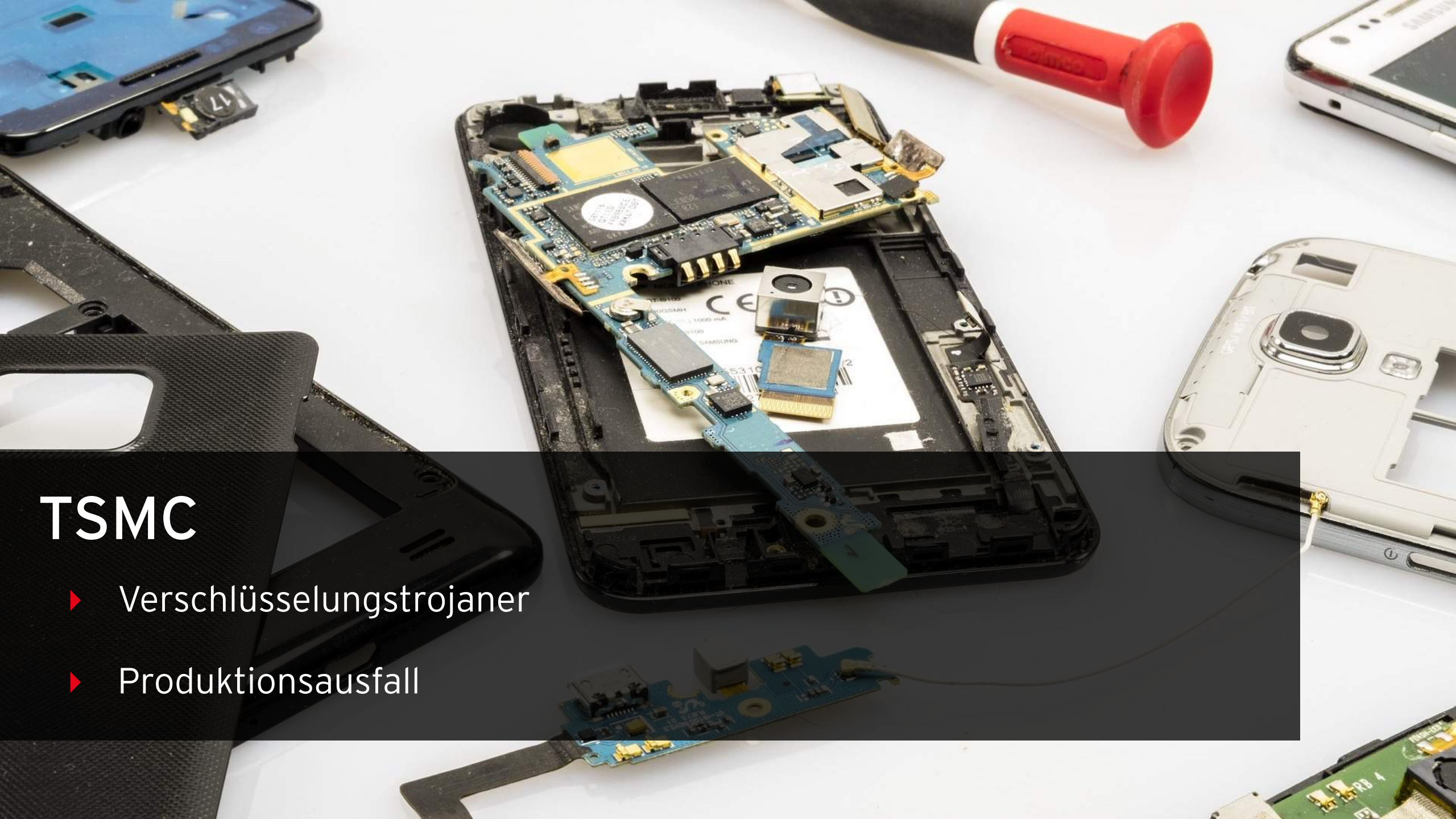
- Loss of availability of the ICS / loss of production
- Causing physical damage to equipment
- Triggering of safety procedures or impairment of safety systems
- Reduction of product quality
- Data leakage / loss of know-how (intellectual property)

Top Threats for Industrial Control Systems

Infiltration of malware via removable media and external hardware

Infection with malware via Internet and Intranet

Human error and sabotage



TSMC

- Verschlüsselungstrojaner
- Produktionsausfall

Countermeasures

Protective Measures

Restrictive use of removable media and mobile devices

Protection from malware

Raising awareness and employee training

Monitoring, logging and detection

Protective Measures

Restrictive use of removable media and mobile devices

Protection from malware

Raising awareness and employee training

Monitoring, logging and detection

USB flash drive as a social engineering tactic

An employee inserts a found USB memory stick into a company computer

- Control access rights
- Block executable content
- Scan external drives

Protective Measures

Restrictive use of removable media and mobile devices

Protection from malware

Raising awareness and employee training

Monitoring, logging and detection

400.000

Neue Varianten von Schadsoftware
...pro Tag!

Application Whitelisting?

Australian Government
Department of Defence

„Application whitelisting is one of the **most effective mitigation strategies** in ensuring the security of systems.“

„Application Whitelisting is the **number one mitigation** from the NSA's Information Assurance Top 10“

„In fact, application whitelisting is the **most effective way** to significantly reduce the impact of malware in today's environments.“

CIS Center for Internet Security®

„Application whitelisting is a basic security control. Utilize this technology on all assets **to ensure that only authorized software executes** and all unauthorized software is blocked from executing on assets.“

Protective Measures

Restrictive use of removable media and mobile devices

Protection from malware

Raising awareness and employee training

Monitoring, logging and detection

Endpoint Detection & Response (EDR)

Monitor endpoints

Detect dangers

Respond to incidents

Protective Measures

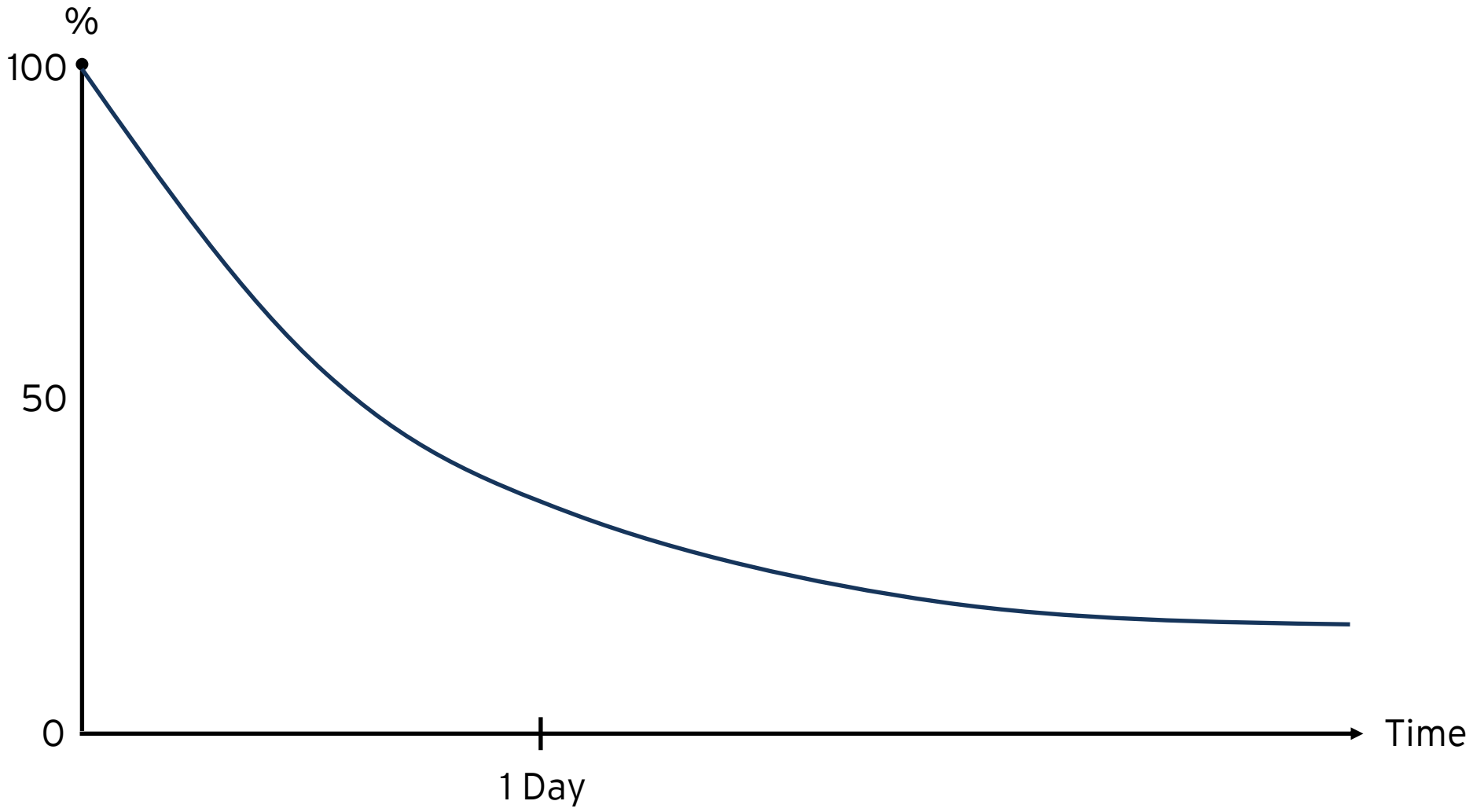
Restrictive use of removable media and mobile devices

Protection from malware

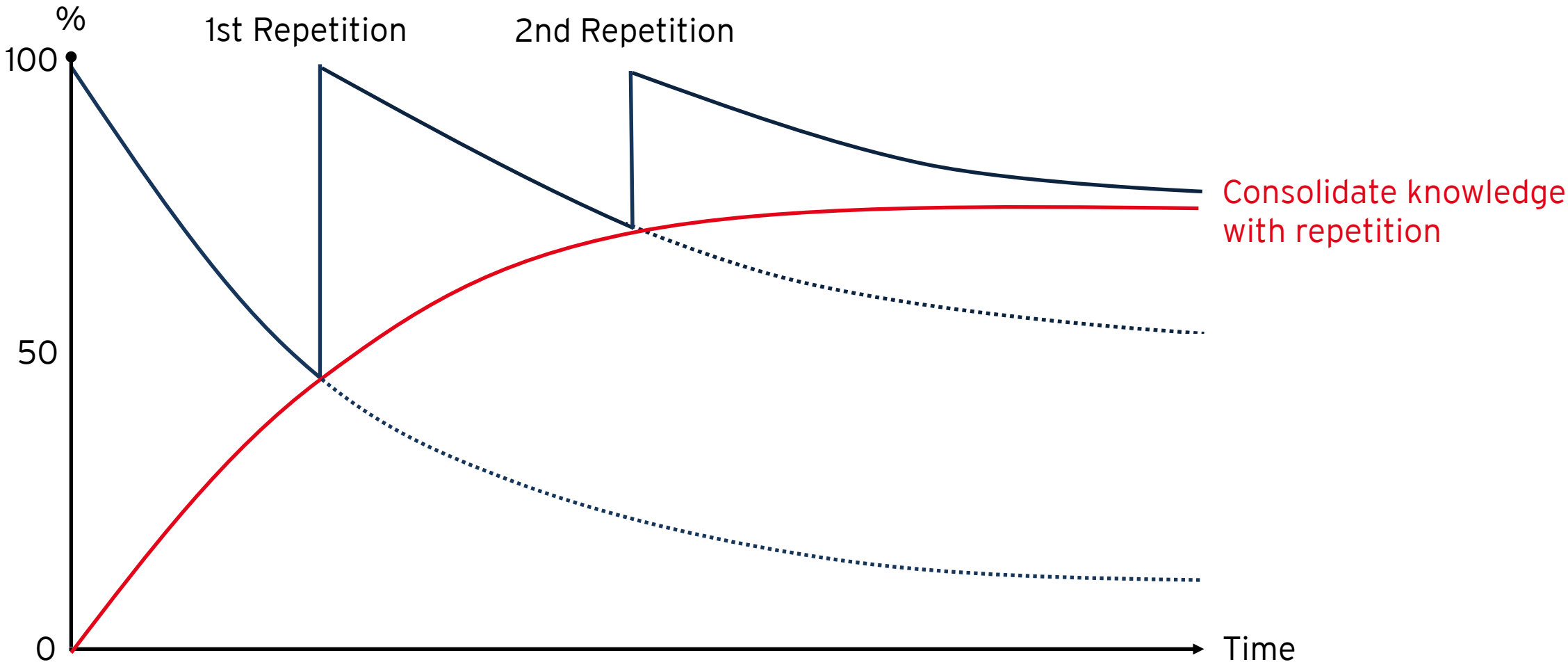
Raising awareness and employee training

Monitoring, logging and detection

Punctual IT security awareness trainings



Regular IT Security Awareness Trainings



Protective Measures

Restrictive use of removable media and mobile devices

Protection from malware

Raising awareness and employee training

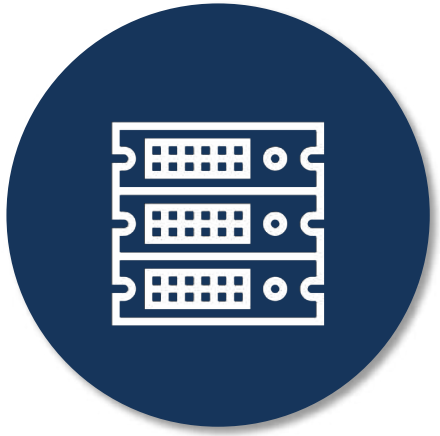
Monitoring, logging and detection

DriveLock Zero Trust Plattform

Cloud

&

On-Premises



Application Control

Device Control

Defender Management

Vulnerability Scanning

Firewall Management

Local User Management

Security Awareness

Encryption

Endpoint Detection & Response

With **cybersecurity** you create

innovation and growth

in your company.

Thank you!

Falk Trümner

falk.truemner@drivelock.com

Visit us!

Booth B2.534