

Industrial Cybersecurity Challenges

Andreas Reiter RC-AT DI FA DH-GRAZ SAS
andreasreiter@siemens.com



IT

- Dynamic
- Full spectrum of technologies
- Well connected
- Confidentiality, Integrity, Availability
- **Data is King**

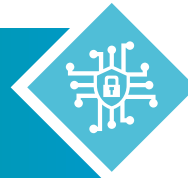
- Control production floor processes
- Process oriented
- Safety/Availability, Integrity, Confidentiality
- **Process is King**



OT

IT - OT Challenges

Information Technology



Operational Technology

3-5 years

Asset lifecycle

20-40 years

Forced migration

Software lifecycle

Usage as long as spare parts
available

Well integrated IAM

Requirements on
Identities

Long living identities
(static accounts?)

High

Options to add
security SW

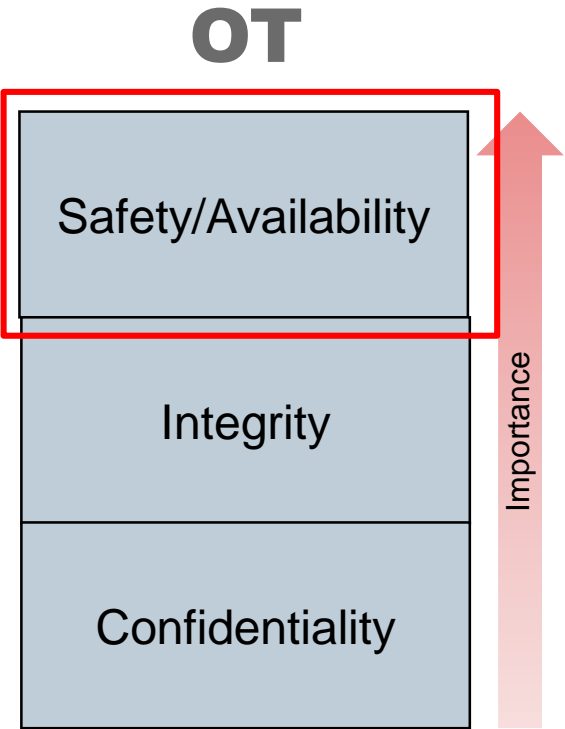
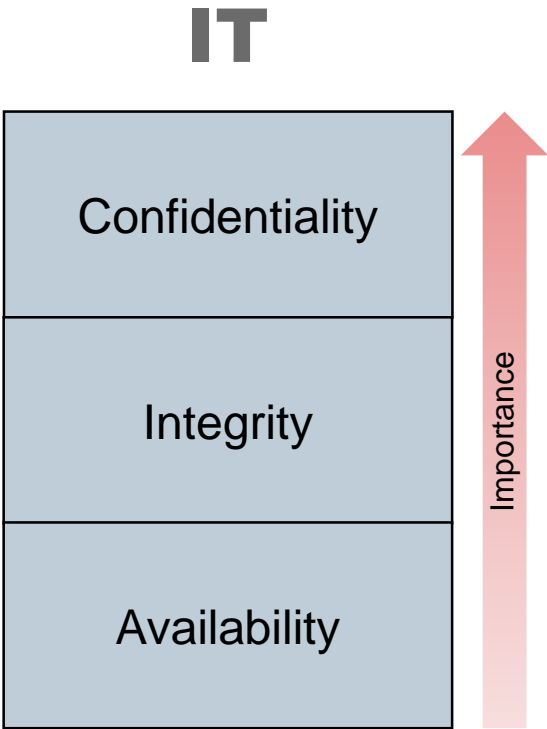
Low

Low

Heterogeneity

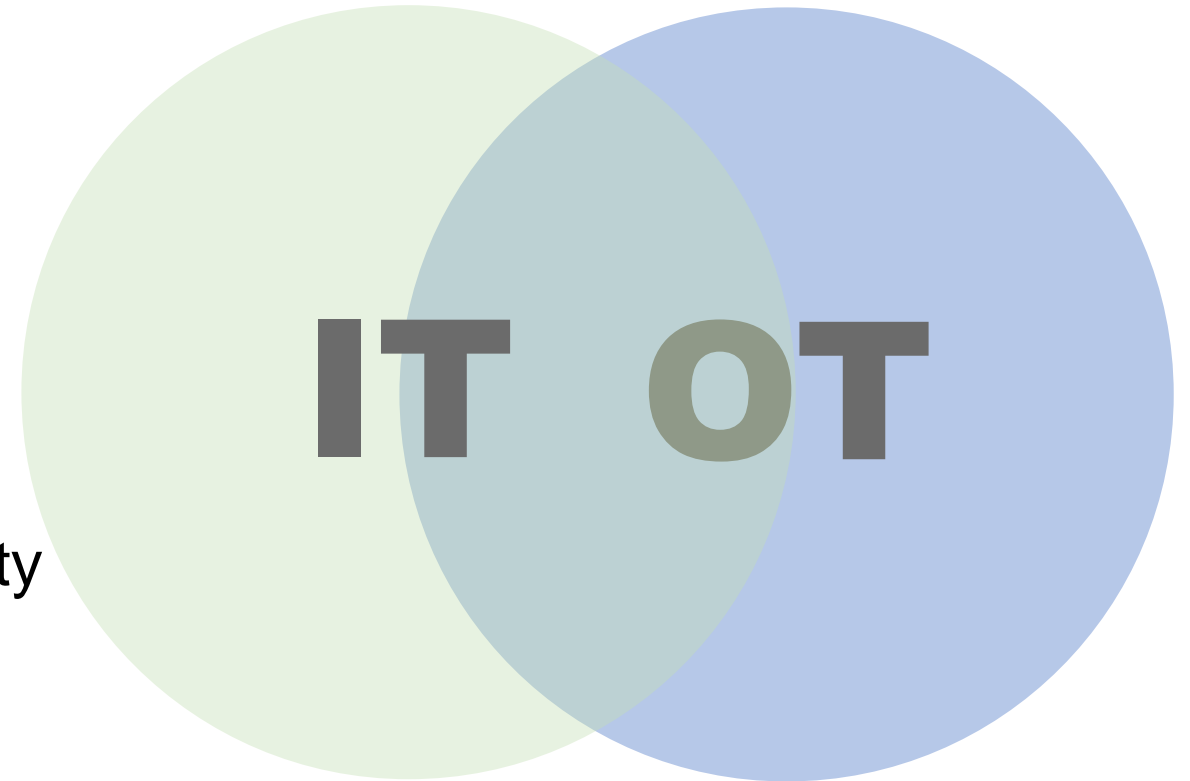
High

Priorities



IT – OT?

- Massive data generation
- Big data analytics capabilities
 - Real-time decisions
 - Predictive maintenance
- Increased efficiency and productivity
- Create new revenue streams



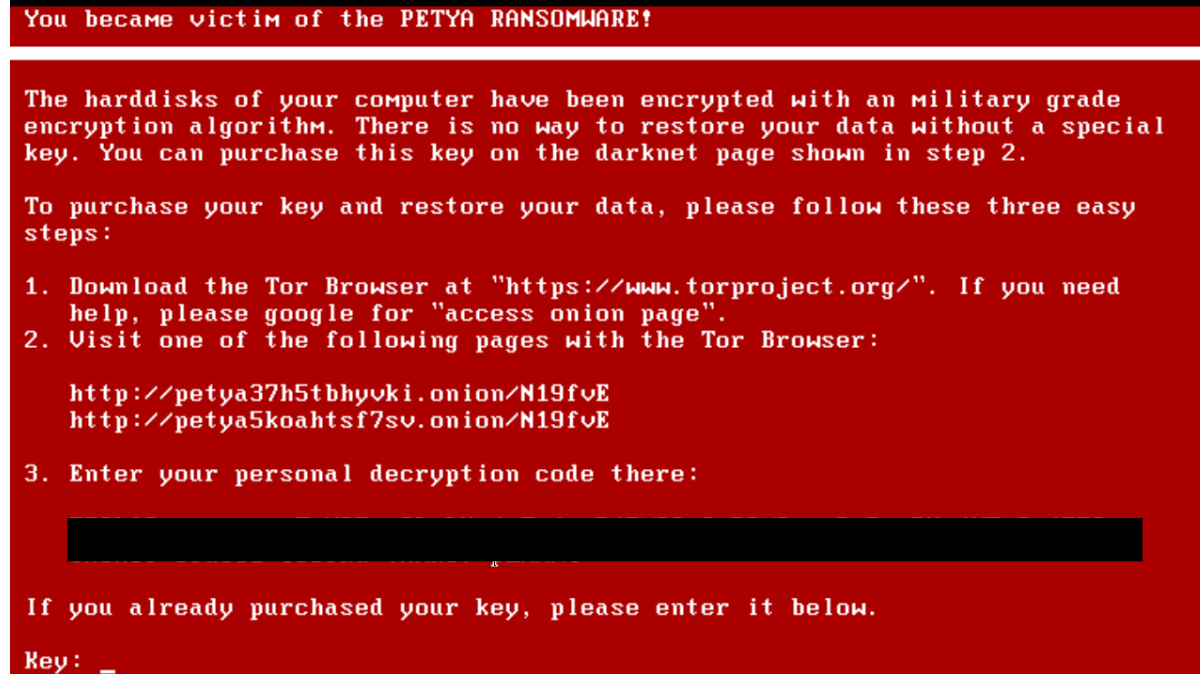
73% are aware that their attack surface increases

*55% have no plans invest, or plan to invest in
cybersecurity in the next 12 months*

*91% are aware that OT security can only be tackled
together with IT*

(Not)Petya (2017)

- Maersk: Petya infected IT infrastructure
- Gates did not open (no data)
- Trucks were locked out



Ransomware is here to stay

Technology

Ransomware attack takes US maritime base offline

BBC



On Monday January 13, 2020, Picanol Group fell victim to a massive ransomware attack. The attack is causing a serious disruption to activities in Ypres, Romania, and China.

Open Industrial Control Systems

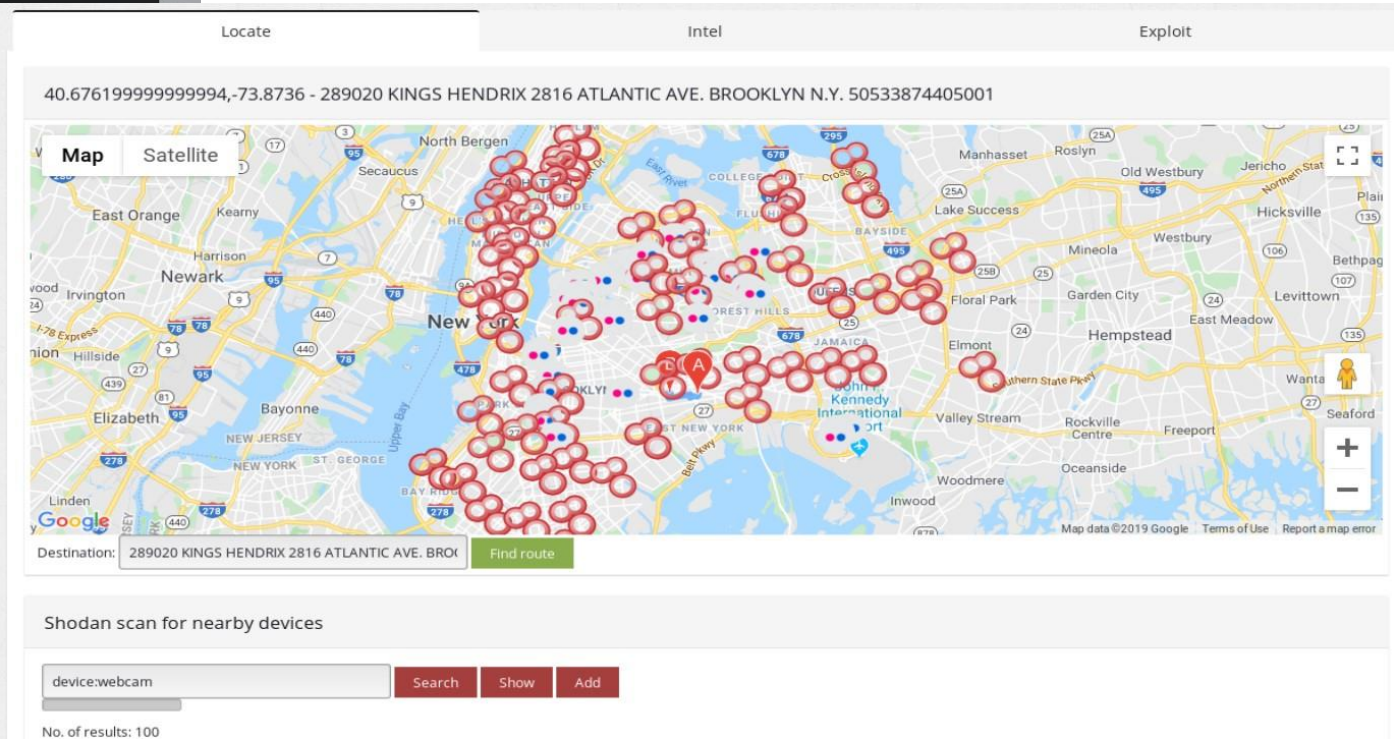
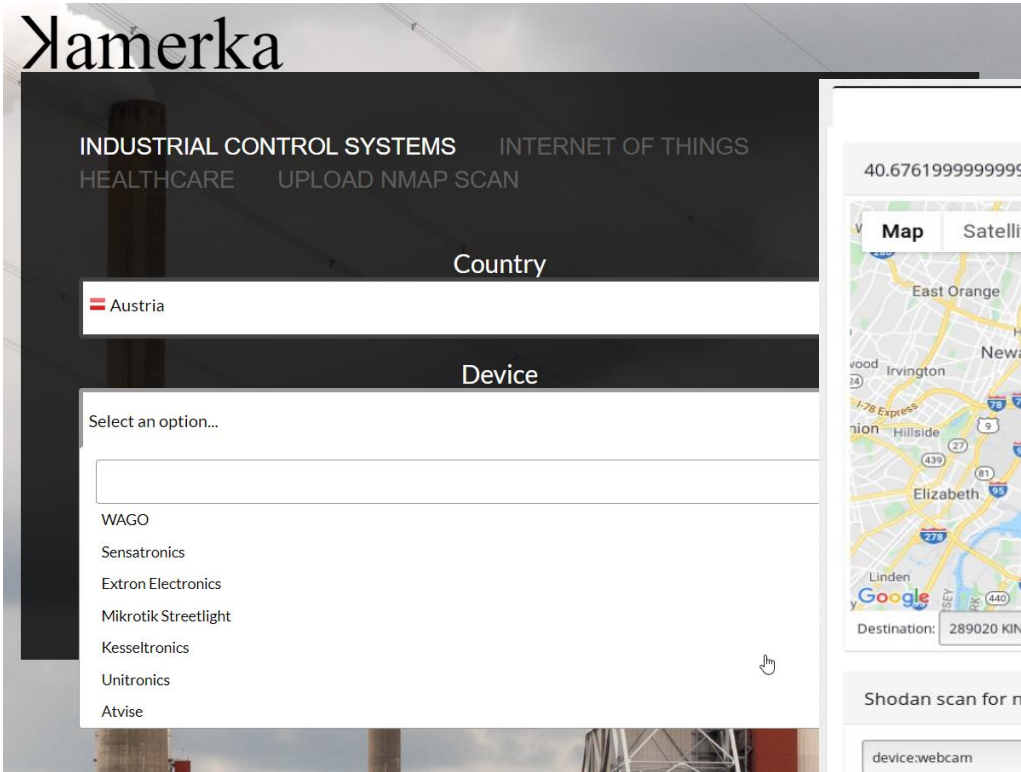


TOTAL RESULTS

7,059



Open Industrial Control Systems



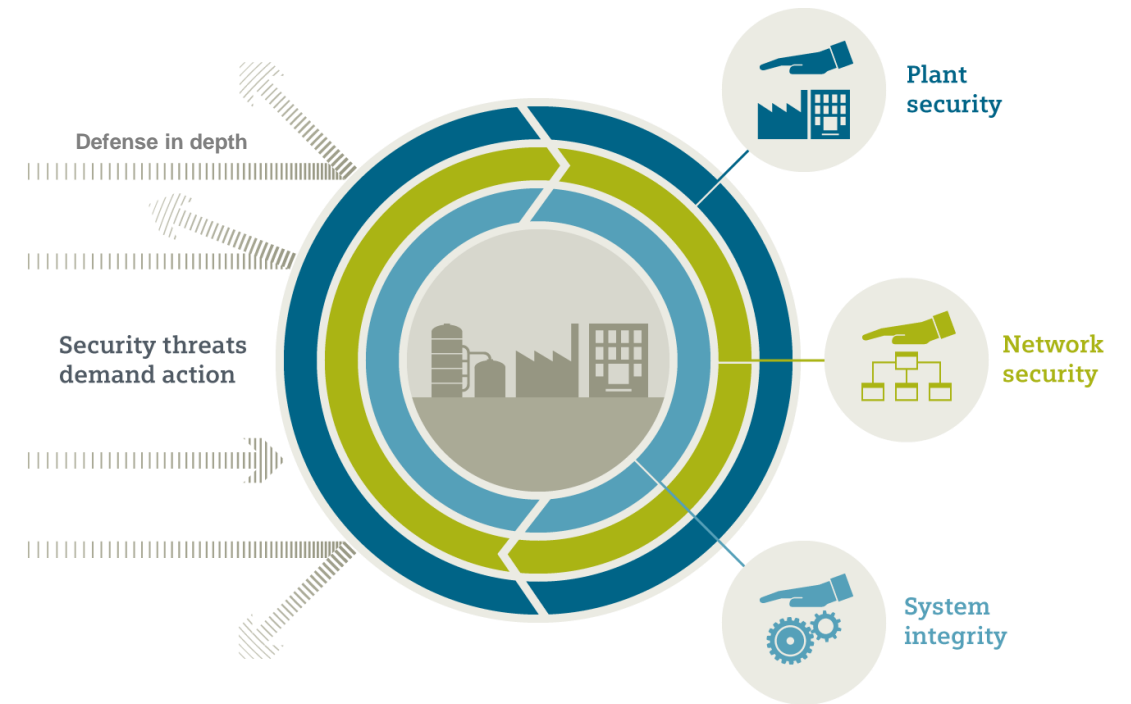
Strong Perimeter Security



- Analog to air gapping
- Firewalls
- Traffic analyzers
- Strong access management

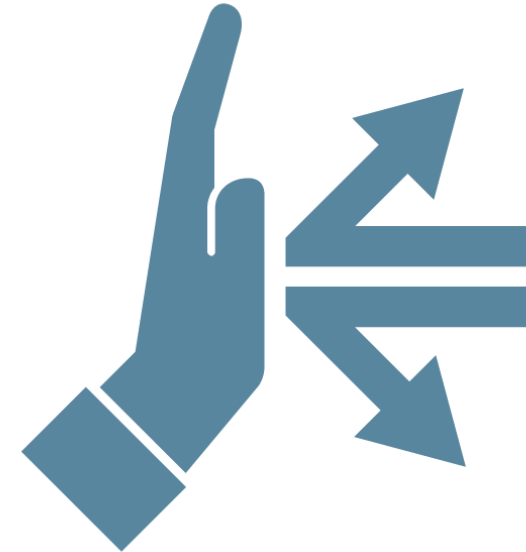
Defence in Depth

- Know what's going on in your network
 - Network monitoring
 - Log analysis
- “Castle approach”
 - Multiple lines of defense
 - Network segmentation
 - Device security
 - Common cryptographic principles
 - Security-by-design
 - ...

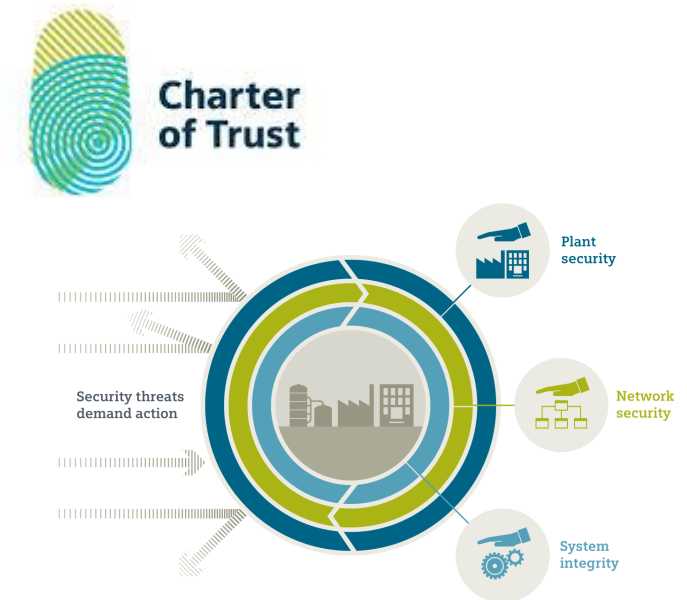


- Be proactive
- Not only scan IT, but also OT networks and components
- Check against known vulnerabilities
 - Open vulnerability databases
 - Vendor specific databases

- Security Event Management (SEM)
 - Near real-time security alarms and events
- Security Information Management (SIM)
 - Long-term storage of log data
- Patch management



- Founding member of the charter of trust
 - Holistic concepts
 - Think beyond products and services
- Plant Security Services
- Strong Security competence at DH-Graz
 - Security testing
 - International research projects
 - defense in depth
 - controlled access to production networks
 - certification



Your Takeaways

- IT and OT environments are converging
 - ...to make better use of data
 - ...to perform data analytics
- More attack vectors
- Be proactive in the definition of your security strategy



Andreas Reiter
RC-AT DI FA DH-GRAZ SAS

E-mail:
andreasreiter@siemens.com

<https://www.linkedin.com/in/anreiter/>

[siemens.com/industrialsecurity](https://www.siemens.com/industrialsecurity)