IT-Security im Industrieumfeld

Wie passt IT mit OT zusammen?

ÖVIA Kongress 2018

BearingPoint®


ngriff auf ein deutsche
Stahlwerk
2014


Angriff auf ein
Stromnetz
in der Ukraine
2015

Angriff auf ein Kläranlagensystem „KWC“ 2016

Pet

77% aller Industrieunternehmen waren in den letzten 12 Monaten Opfer von Cyber Attacken

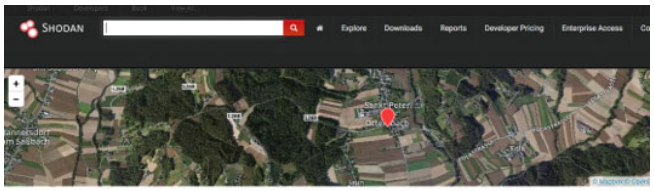
71% sehen Cyber Risiken als strategisches Risiko, 79% diskutieren CS auf C-Level

24% haben kein dediziertes CS Budget, bei Fam.Unternehmen haben 37% kein dediz. Budget

21% der größeren Unternehmen ist nicht bekannt, ob sie betroffen sind oder nicht

10% des IT Budgets sollte für Cyber Security verwendet werden, sagen 18% der Unternehmen

KPMG Studie 2018: Cyber Security in Österreich (Mai 2018)



195.3.81.196

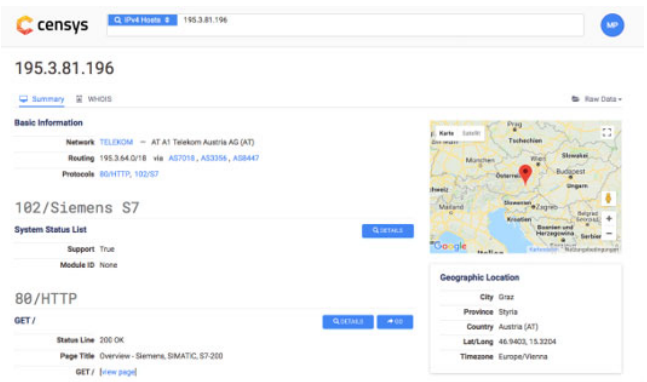
City	Sankt Peter Am Ottersbach
Country	Austria
Organization	Telekom Austria
ISP	Telekom Austria
Last Update	2018-06-11T14:00:35.174069
ASN	AS8447

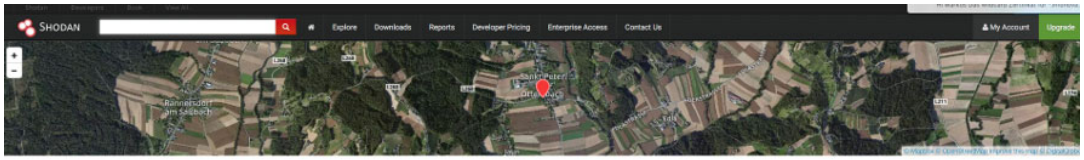
Ports

161

Services

161 snmp — Siemens, SIMATIC, S7-200





195.3.81.196

City	Sankt Peter Am Ottersbach
Country	Austria
Organization	Telekom Austria
ISP	Telekom Austria
Last Update	2018-06-17T12:04:42.977590
ASN	AS8447

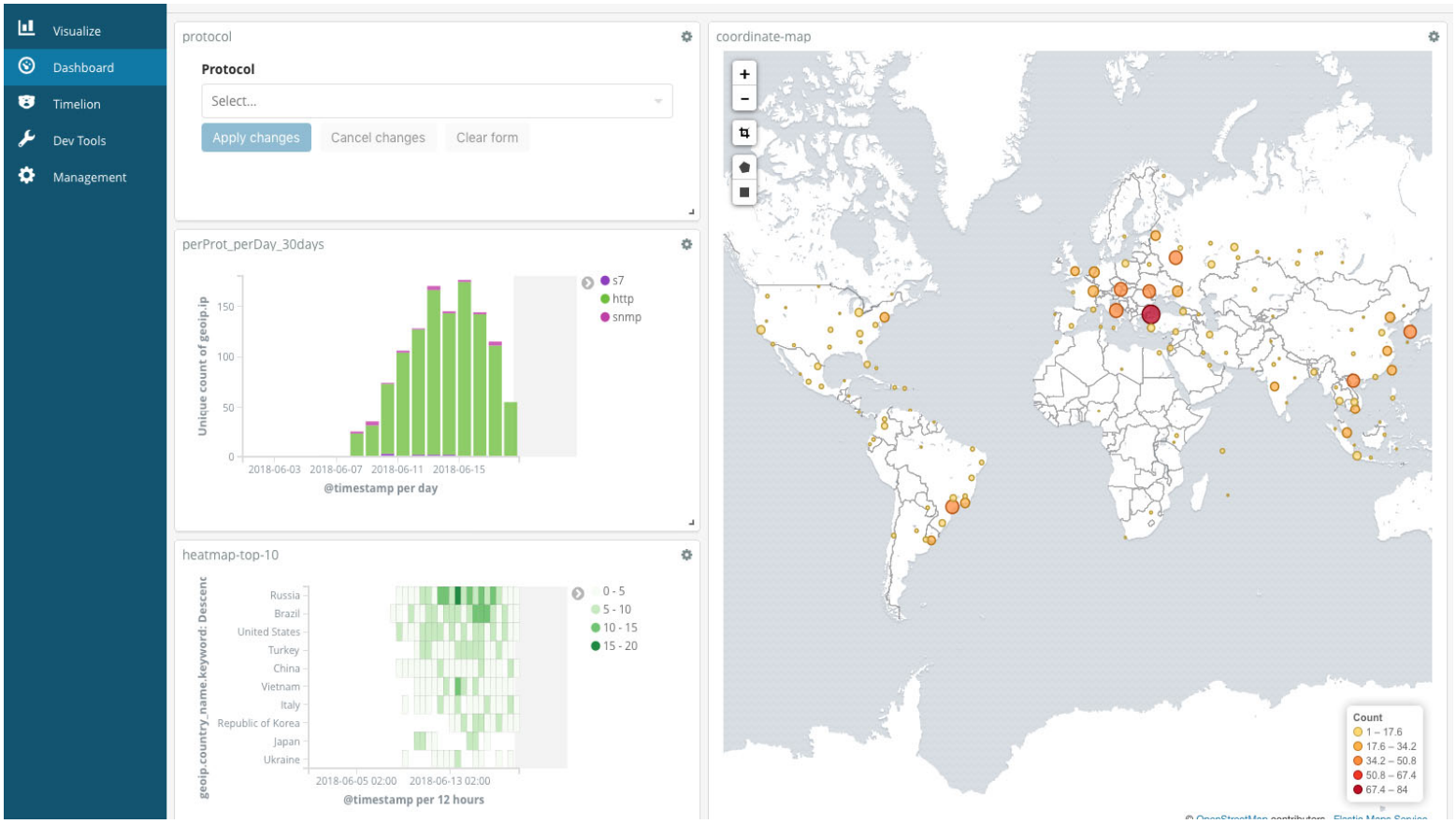
Ports

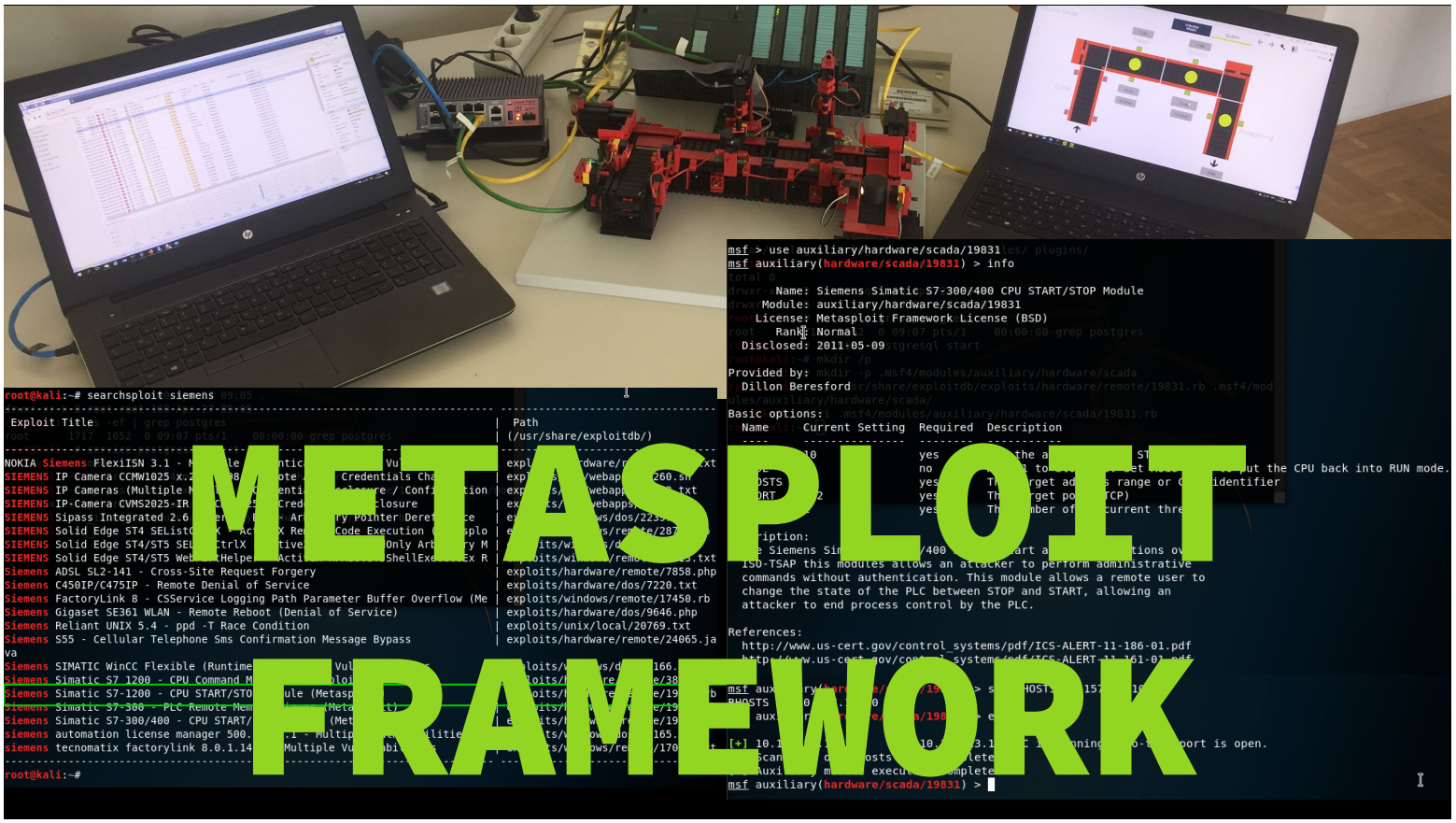
80 161

Services

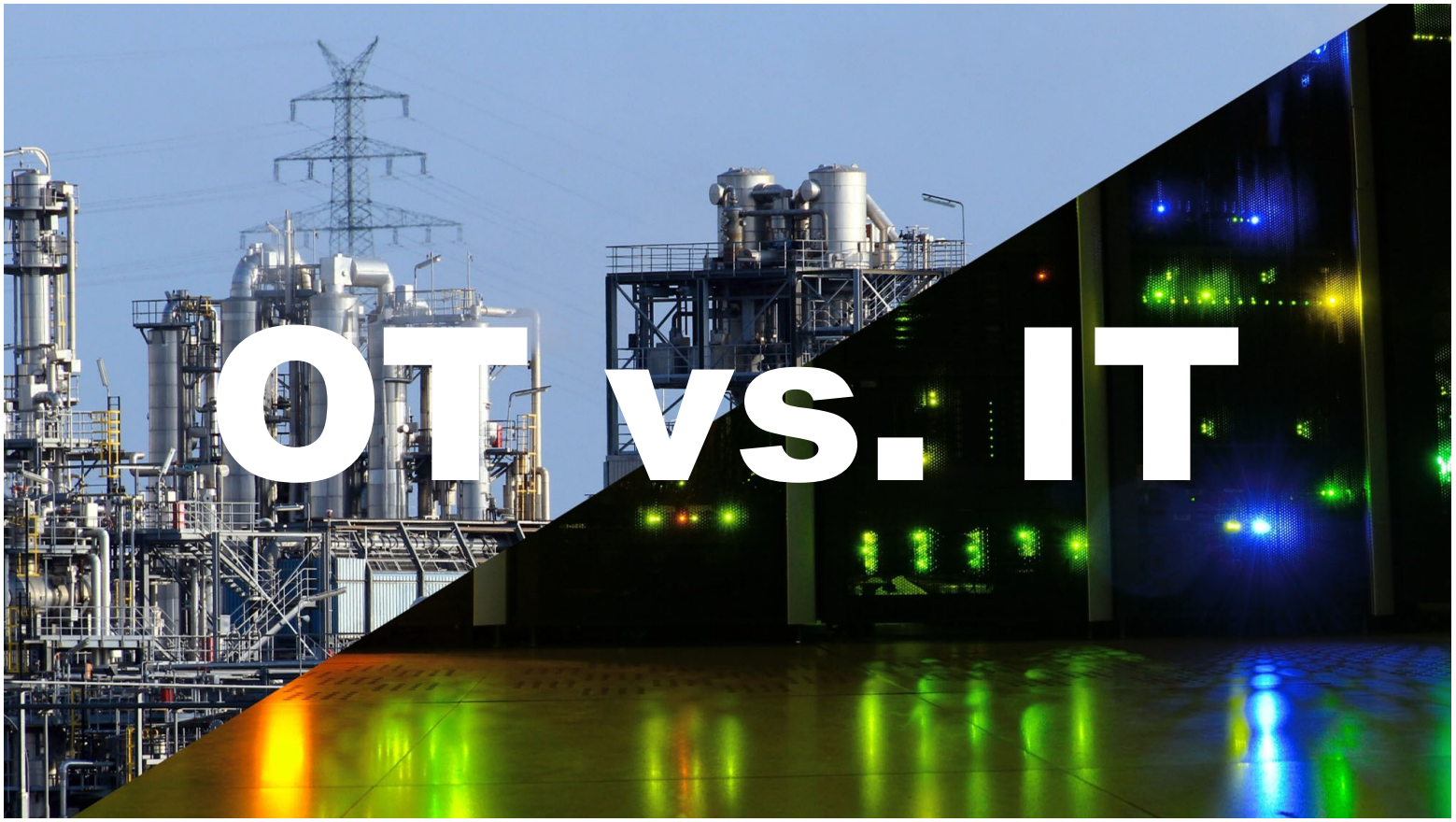
80 http — HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 13:35:40 GMT
Last-Modified: Tue, 19 May 1993 09:00:00 GMT
Content-Type: text/html
Set-cookie: path=/
Content-Length: 579

161 snmp — Siemens, SIMATIC, S7-200





METASPLOIT FRAMEWORK



OT vs. IT

Die Evolution der Cyber-Angriffe

Generation V

Gen. 5: 2017 tauchen in kurzer Abfolge hintereinander, mehrere große, globale Cyber Attacken in den Medien auf (WannaCry, Petya, etc.), die unterschiedlich, teils komplexe Angriffsvektoren und Tools verwenden, um von Unternehmen als auch Privatpersonen Geld zu erpressen oder größtmöglichen Schaden anzurichten.

Advanced Threat Prevention

Generation IV

Gen. 4: Um das Jahr 2010 nehmen immer mehr gezielte Attacken zu, die sich selbst verändernde Inhalte (polymorphe Payloads) verwenden, um von Signatur basierten Schutztechnologien (Anti Virus, IPS, etc.) nicht erkannt zu werden.

Sandboxing and Anti-Bot

Generation III

Gen. 3: Zu Beginn der 2000er Jahre kommen die ersten Exploits auf, die Schwachstellen in Applikationen ausnutzen, um Unternehmen zu schaden.

Intrusion Detection and Prevention

Generation II

Gen. 2: Mit zunehmender Vernetzung, tauchen Mitte der 90er Jahre erste Angriffe aus dem Internet auf. Erste Firewall Technologien werden geschaffen.

Firewall Technologien

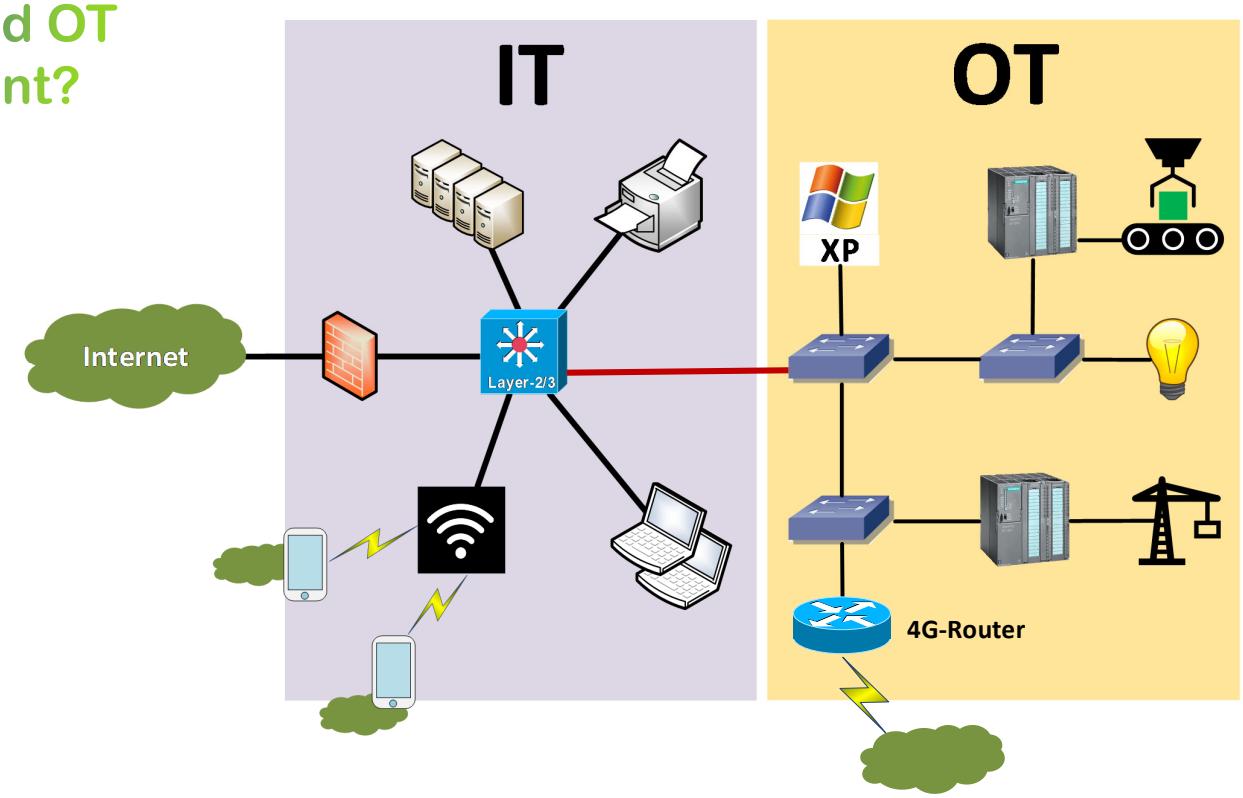
Generation I

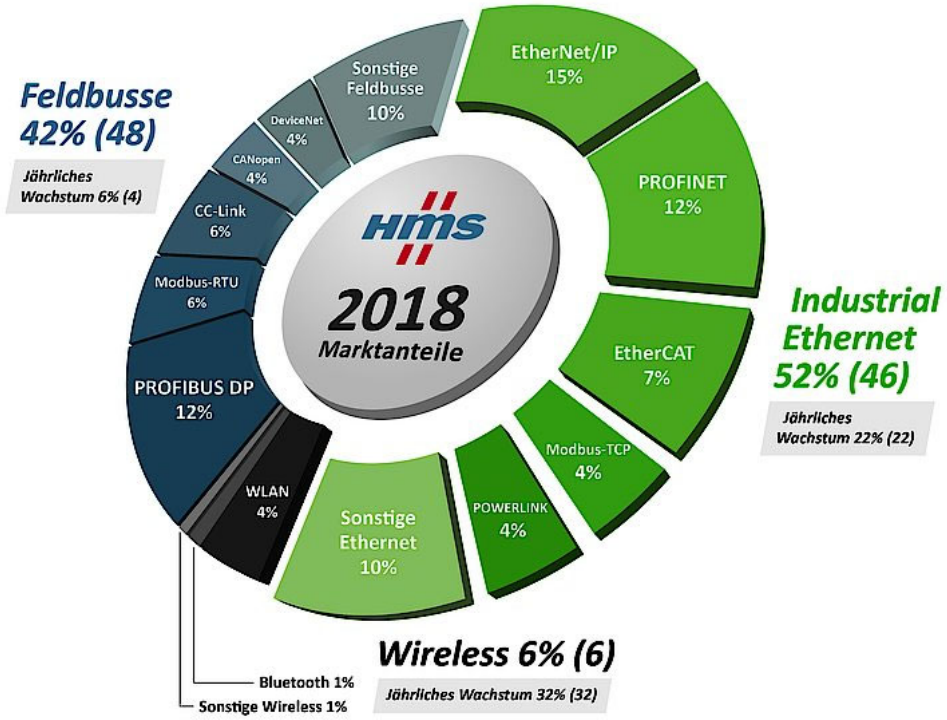
Gen. 1: Ende der 80er Jahre, erste Virus Attacken auf Stand-Alone PC's, mit Schaden fürs Business. Erste Anti-Viren Programme werden entwickelt.

Anti-Virus Software

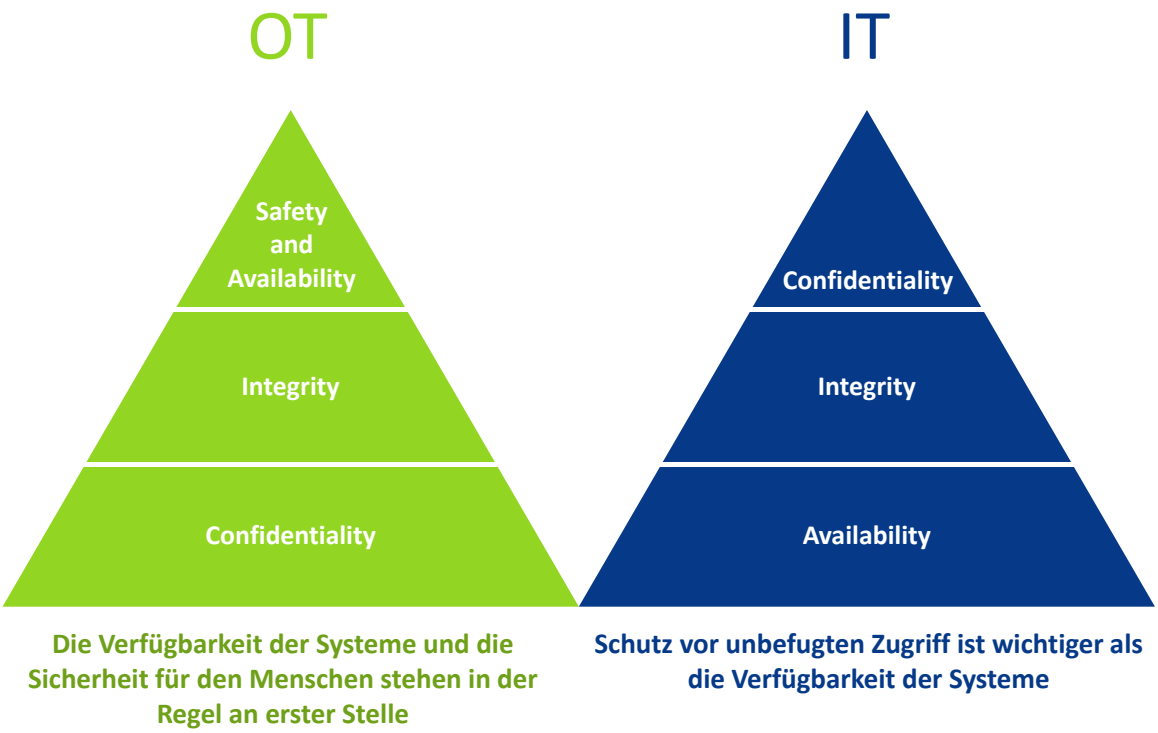
1990 2000 2010 2017

IT und OT vereint?



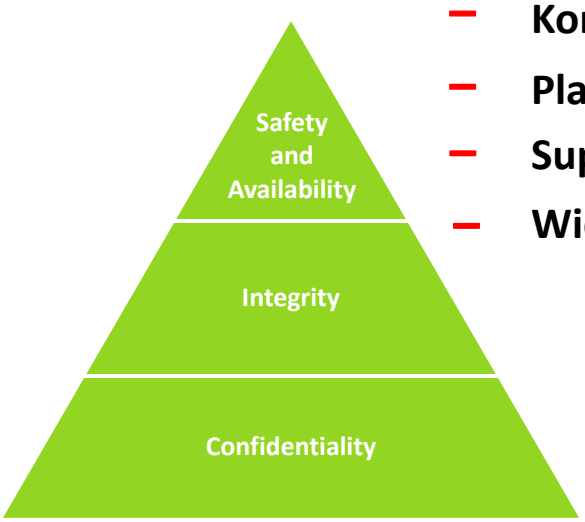


Marktanteile Feldbus versus Industrial Ethernet und Wireless (Bild: HMS)



Management von Sicherheits-Updates

OT



? Testen möglich? +

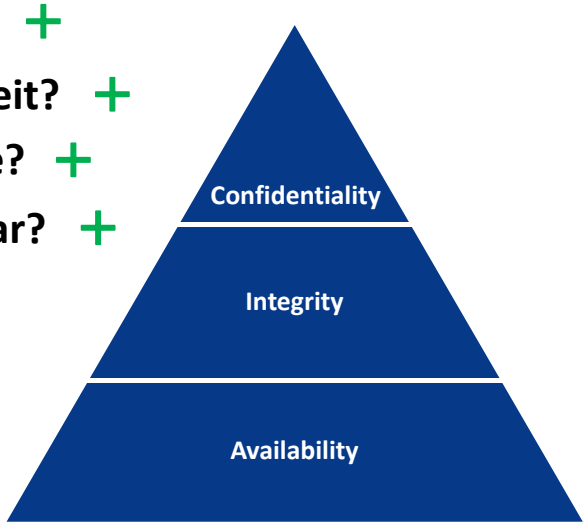
– Kompatibilität? +

– Planungssicherheit? +

– Support Lifecycle? +

– Wiederherstellbar? +

IT




Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Web Security
Messaging Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Fraud Prevention / Transaction Security
Cybersecurity Landscape
Threat Intelligence
Specialized Threat Analysis & Protection
Data Security
Mobile Security
Identity & Access Management
Cloud Security
Industrial / IoT Security


PERIMETER SECURITY
Firewalls
IPS / IDS
WiFi Sec.
DDoS Protection
VPN / SSL
DMZ
DDoS
NETWORK SECURITY
Firewalls
IPS / IDS
Filtering
WAF
Segmentation
SIEM
APT
ENDPOINT SECURITY
Anti Virus
Disk Encryption
(Firmware) Update Mangement
Anti Malware
Access and Identity Management
Mobile Device Management
Malware
APPLICATION SECURITY
Clean and Secure Coding
Penetration Testing
Security by Design
CRM
php
Encryption
Interface Authentication
Rules and Permissions Management
DATA SECURITY
Encryption
Data Loss Prevention
Access Rights Management
BearingPoint.

CIS Controls™

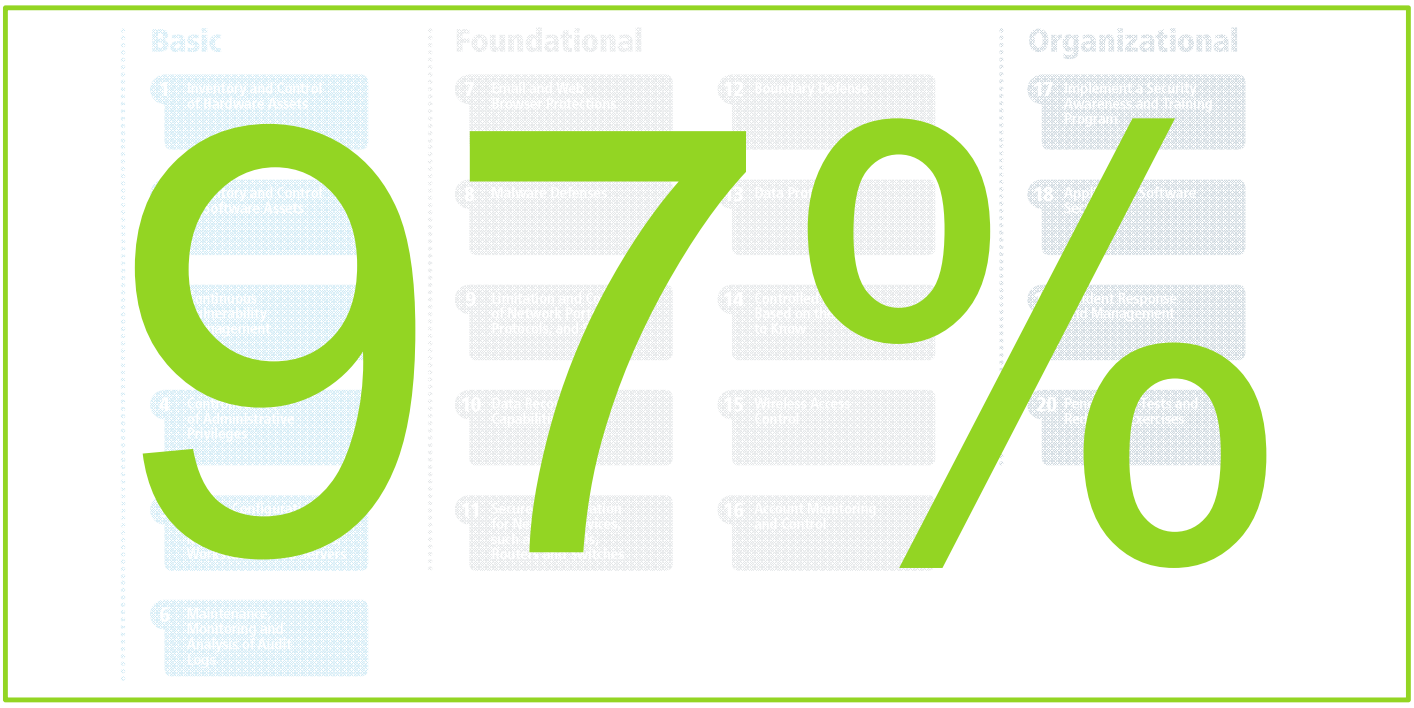
Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

V7

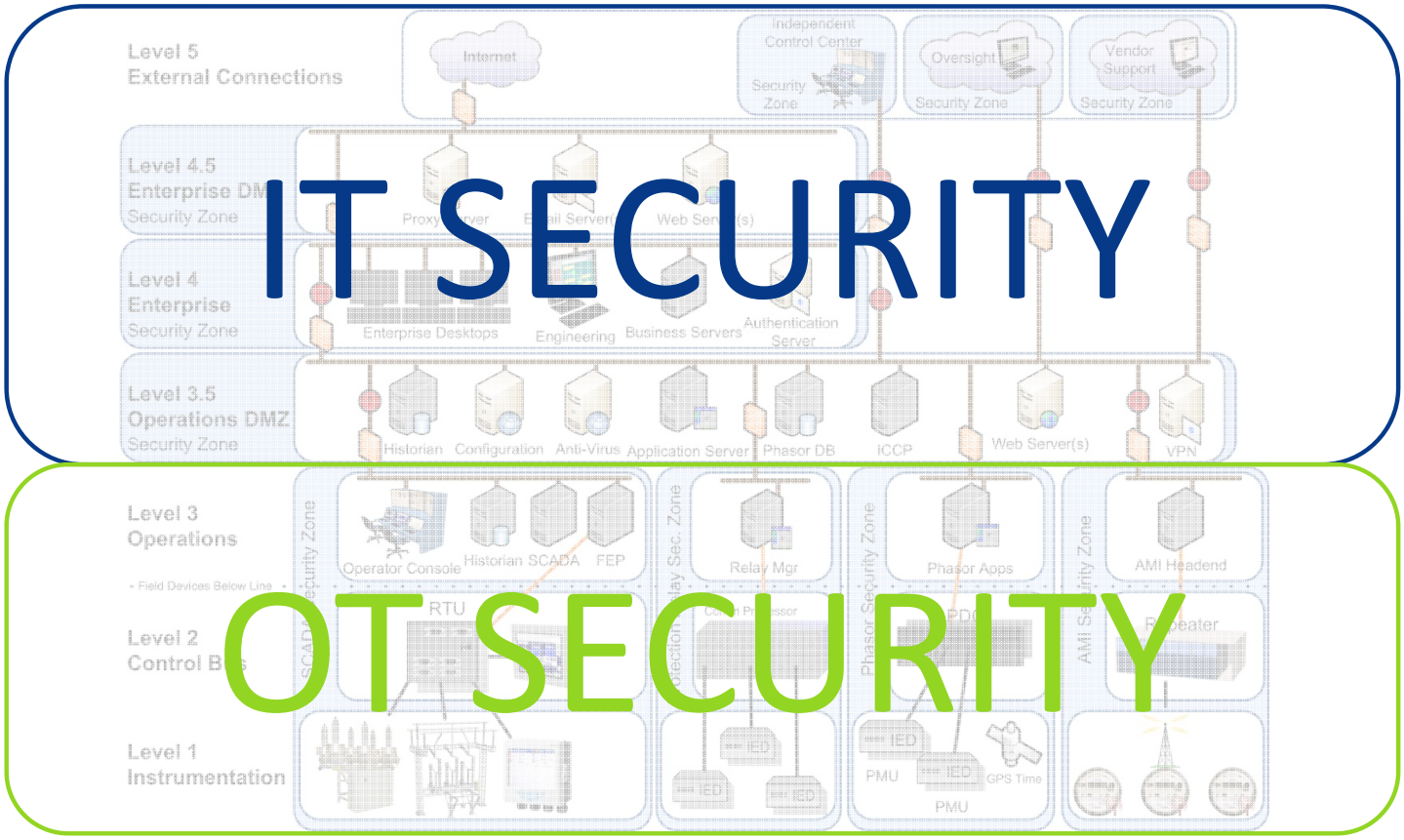
85%

CIS Controls™ V7

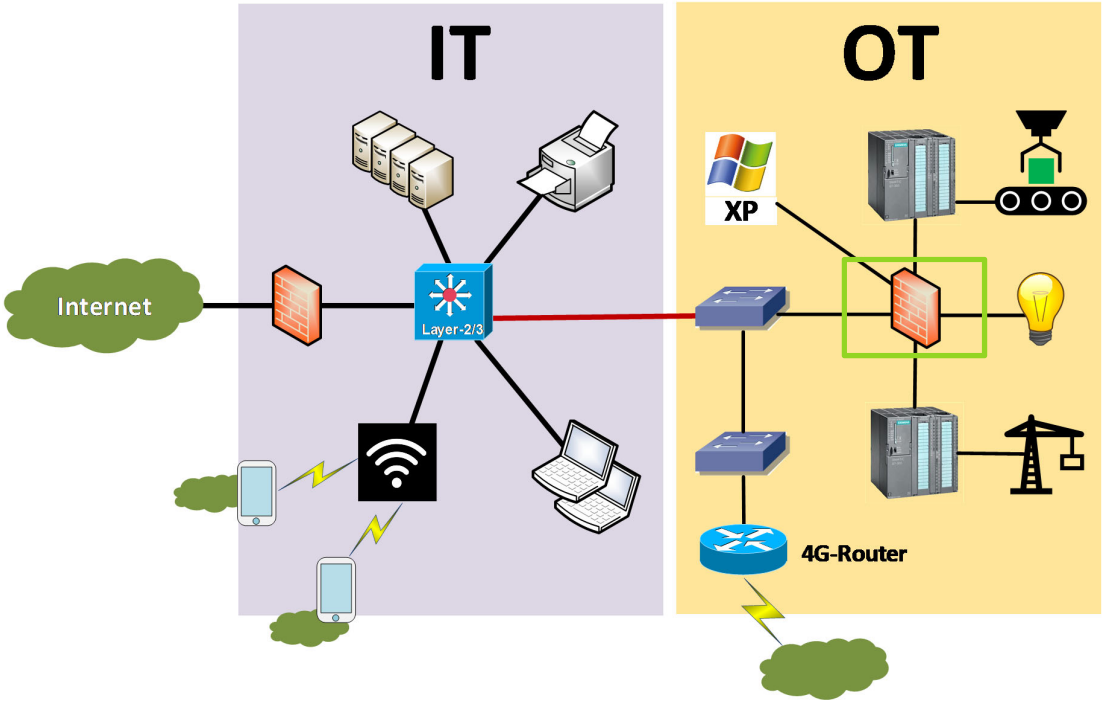


THE

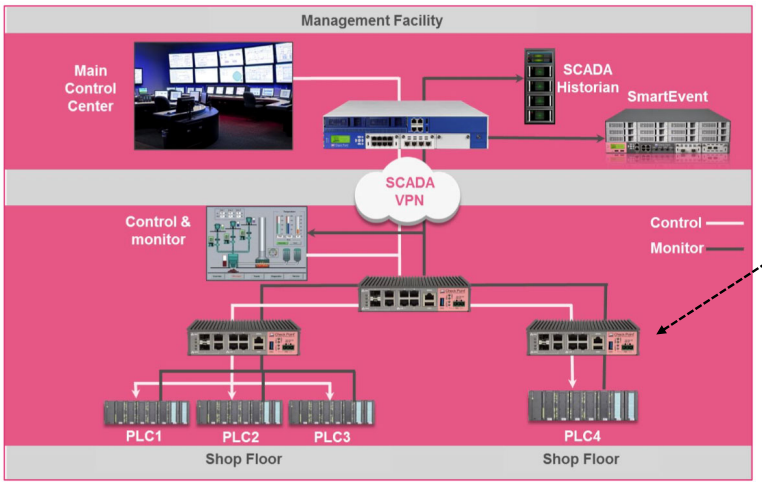
PURDUE Model



Segmentierung des Netzwerks

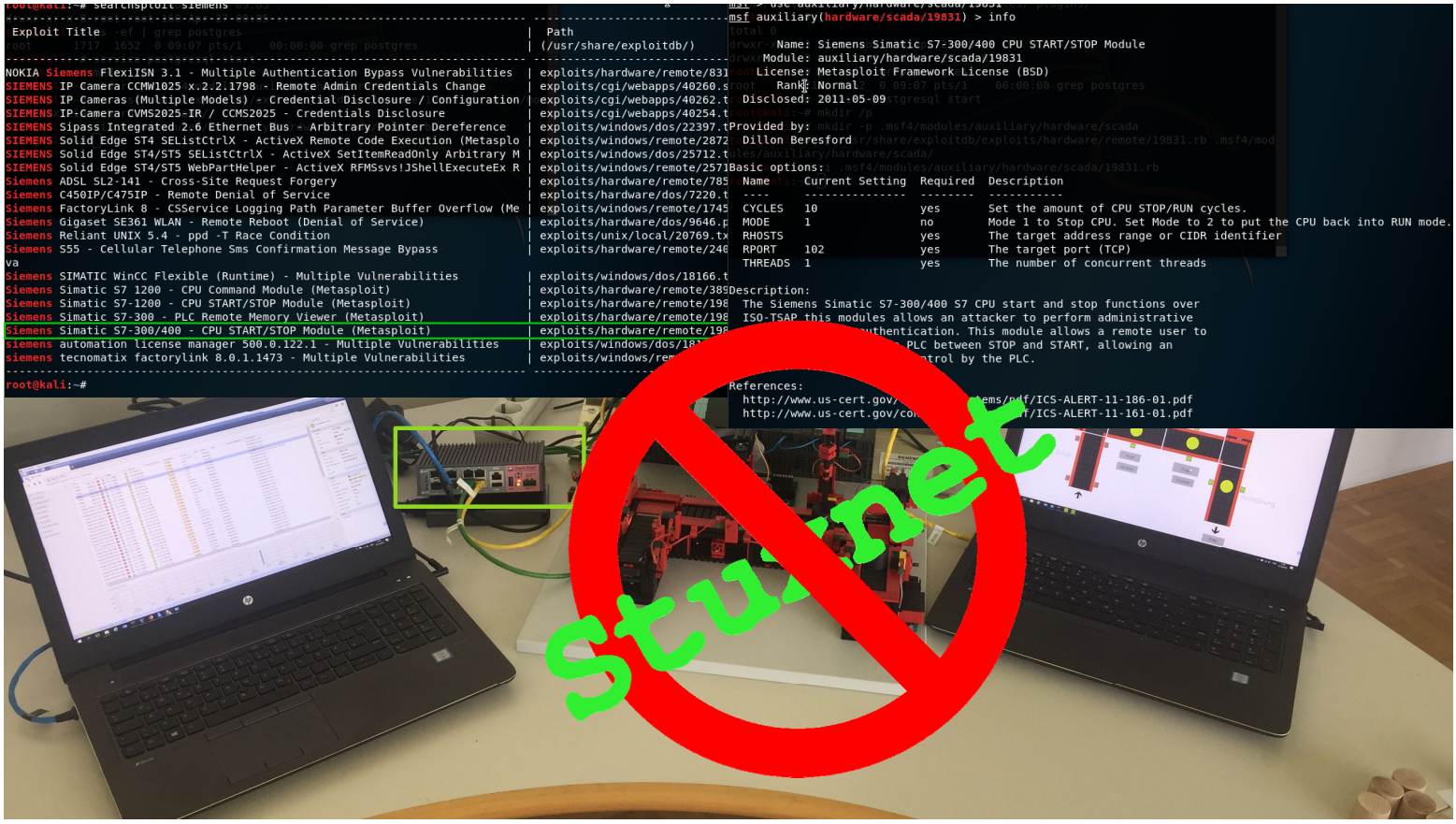


ICS - Protokollerkennung



Check Point 1200R Firewall

- Hardware für Industrieumgebungen
- Zentral verwaltbar
- Erkennt über 50 Industrieprotokolle
  - Profinet, Modbus, S7, etc.
  - ICS Kommandos und Wertebereich im Regelwerk definierbar



BearingPoint Technology

- **5.000** Mitarbeiter in Europa
- **350** Mitarbeiter in Graz
- **75** Mitarbeiter in Graz für IT Infrastrukturlösungen
- **20** Mitarbeiter im Netzwerk und **Cyber-Security** Bereich
- **Partner** führender Netzwerk- und Security-Hersteller
- **Kunden** in den Bereichen Telekommunikation, Finanzen und Industrie

Thomas Roßmann
thomas.rossmann@bearingpoint.com
https://besecure.bearingpoint.com/

BearingPoint®
Technology