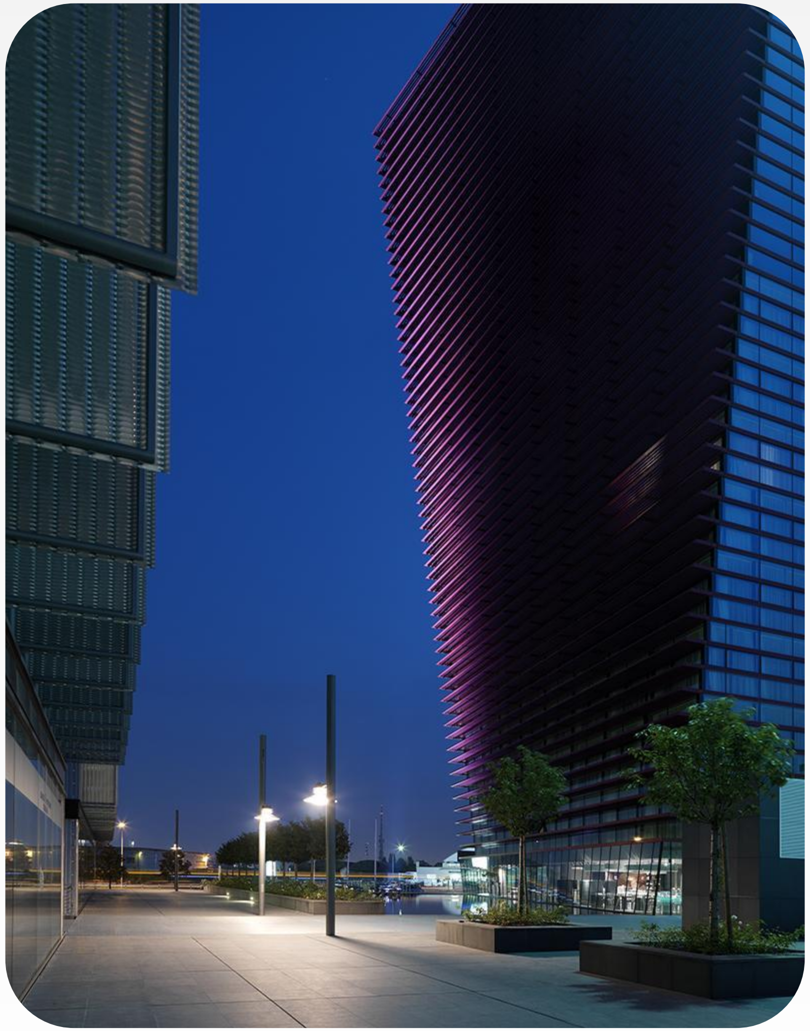
IT CLUB FVG

Securing OT/ICS plants

NGS - Next Gen Solutions

info@nextgensolutions.it

NGS - Next Gen Solutions is specialised in high-level, next-generation IT infrastructures with focus on Cyber Security, IT/OT security, system integration and automation. The team implements IT infrastructure projects, integrating the best technologies and offering high design, configuration and service expertise in the Enterprise, Industrial and Maritime sectors.



The main sectors in which we operate

Enterprise

Security solutions designed for distributed companies and large-scale distribution

Industry

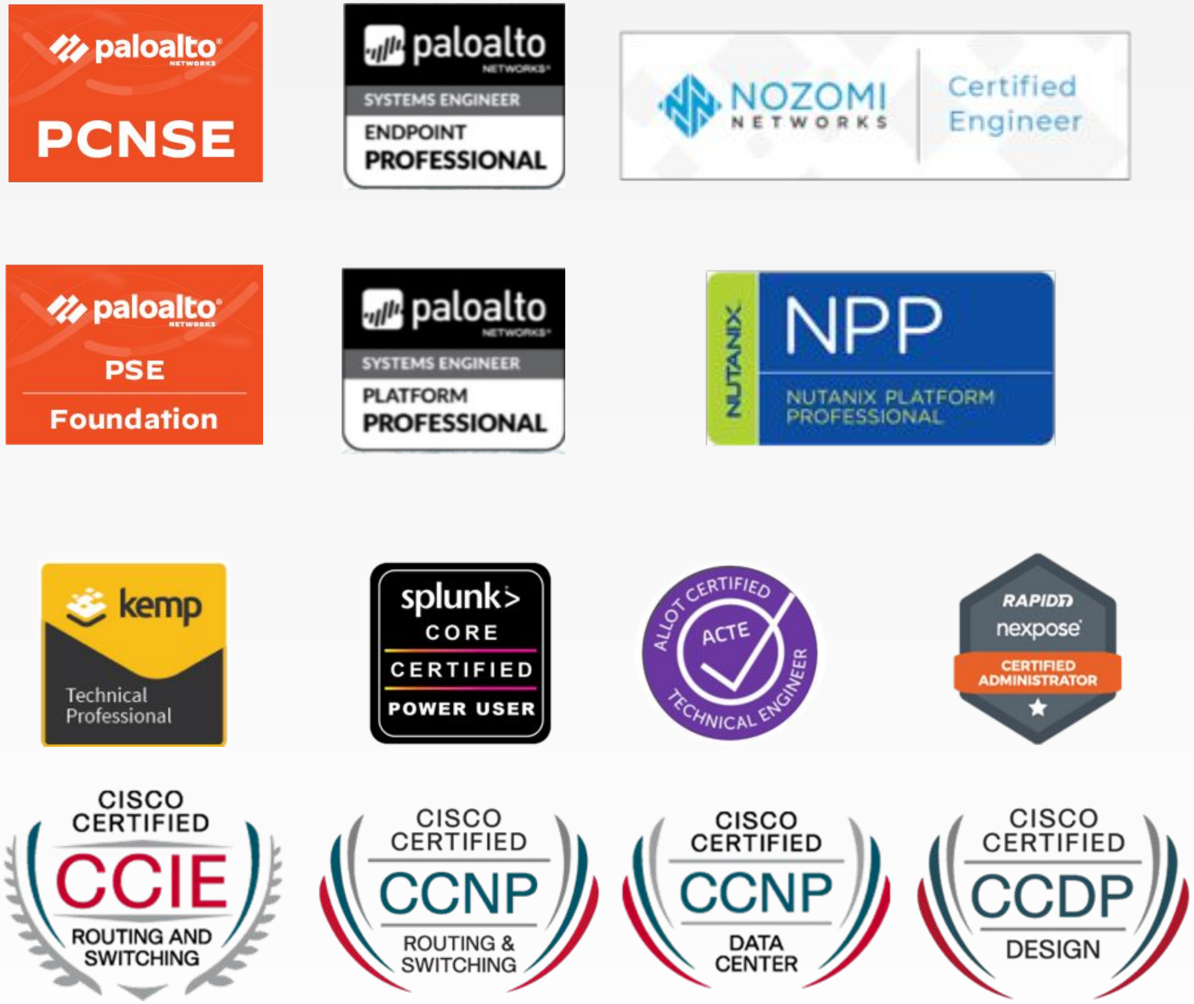
Protection of connected systems designed for Industry 4.0

Maritime

Security and integration designed for cruise and cargo ships and port infrastructure.

Our team

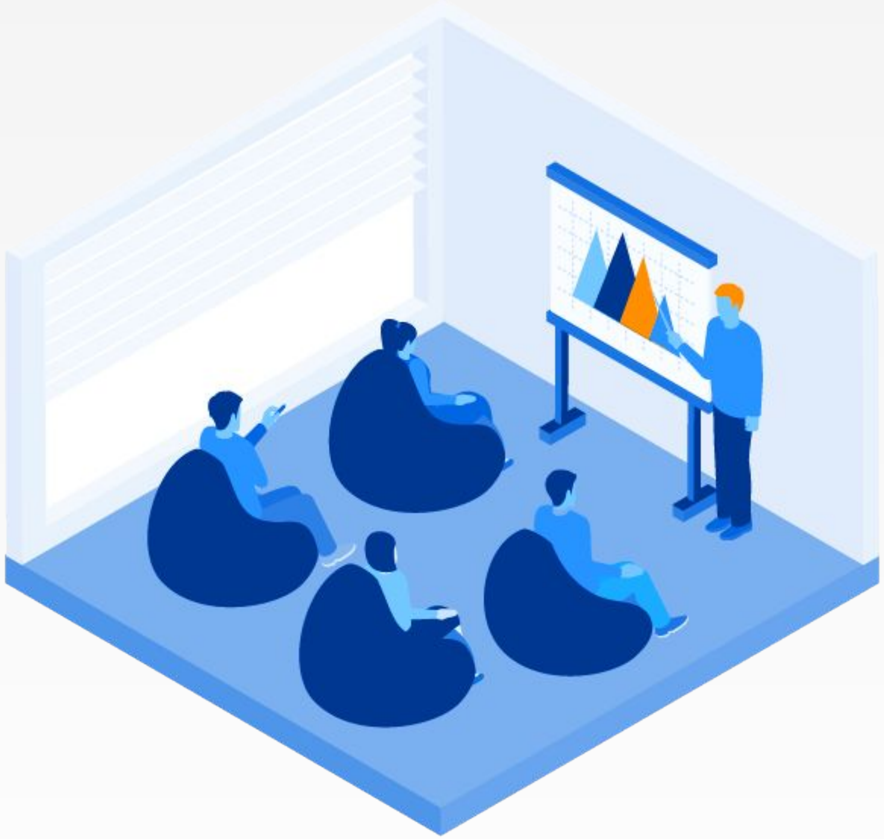
NGS presents itself on the market by offering cross-sectional and interdisciplinary skills thanks to a team of qualified and certified professionals engaged in constant training, research and development of ideas.



Andrea Dainese (CSO)

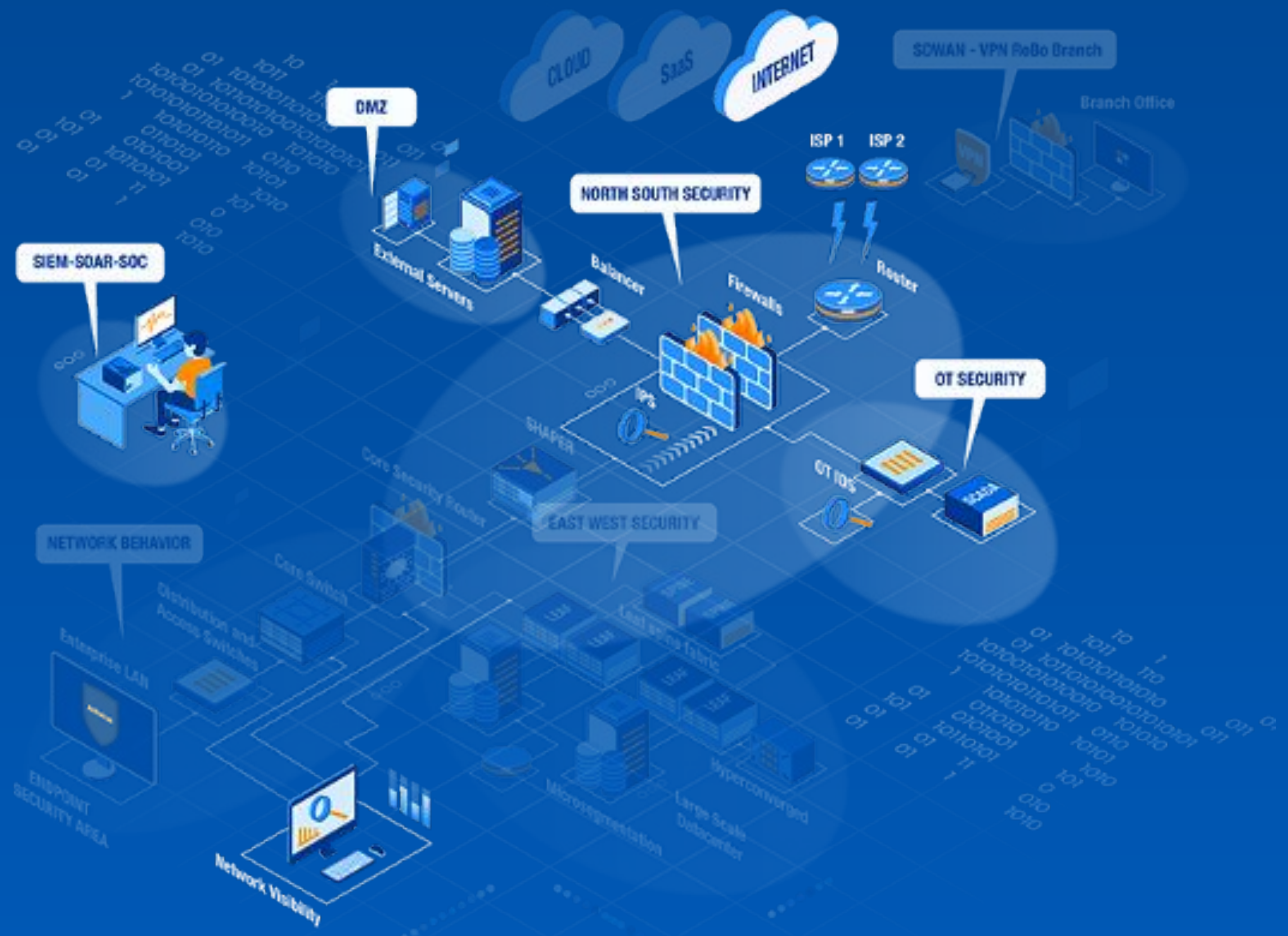
andrea.dainese@nextgensolutions.it

- Senior Network & Security Architect with 15+ years' experience in management of complex IT infrastructures
- Focused on cyber security strategies, GDPR/ISO27001 compliance and automation
- Member of Cyber Incident Response Team
- Cisco (CCIE), VMware, Red Hat… certified
- Privacy and digital security evangelist – expert counselor-mediator in Cyberbullying



Industry

Protecting connected plants in Industry 4.0 era



Industry 4.0

Industry 4.0 (a.k.a. Connected Enterprise, Smart manufacturing…) promotes the computerization of manufacturing interconnecting machines, devices, sensors, and people.
Industry 4.0 integrates processes across the entire organization.
On the other side, plant components were designed to be placed in a protected environment, thus they are extremely static and vulnerable.

Agenda

- Brief history of cyberattacks against critical infrastructure
- Examples of today OT/ICS exposed infrastructure
- Particularity of OT/ICS infrastructures
- Attacking an OT/ICS plant
- Defending an OT/ICS plant
- Demo
- Q&A

Brief history of cyberattacks against critical infrastructure

Stuxnet (2010)

USA - Israel

Stuxnet is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.

Stuxnet

Highlights

- Exploit 4 Zero Day Vulnerabilities
- Developed for Air Gapped targets
- Supply Chain attack

How it works

- Spreads via USB Keys
- Detects Siemens ICS plants
- Compromises only specific devices
- Alterates centrifuges spin
- Provides false feedback to monitors

BlackEnergy (2015)

Russia

On December 23 2015, 230,000 people in Ukraine were left in the dark for six hours after hackers compromised several power distribution centres which provide electricity to residents in Ukraine.

BlackEnergy

Highlights

- Disabled 50 substations (135MW)
- Destroyed SCADA Hard Drives, battery backups and access to controllers

How it works

- Spreads via phishing emails with infected documents (Excel, Word...),TeamViewer…
- Communicate with C&C servers
- Steal credentials
- Propagate to the ICS network

Wannacry & NotPetya (2017)

North Korea - Russia

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

WannaCry ransomware attack

Highlights

- Exploit Zero Day Windows RCE
- Millions of infected computers
- Deactivated by a Kill Switch

Timeline

- A Long Time Ago: EternalBlue by NSA
- 14/03: Microsoft Security Bulletin
- 15/04: Shadow Brokers release
- 12/05: #WannaCry Patient Zero

Triton (2018)

North Korea

Triton is malware first discovered at a Saudi Arabian petrochemical plant in 2017. It can disable safety instrumented systems, which can then contribute to a plant disaster. It has been called "the world's most murderous malware."

New ICS Attack Framework “TRITON”

Highlights

- Attack framework
- Interact and reprogram SIS (Safety Instrumented Systems) controllers

Attack Options

- Use the SIS to shutdown the process
- Reprogram the SIS to allow an unsafe state
- Reprogram the SIS to allow an unsafe state – while using the DCS to create an unsafe state or hazard

LockerGoga (2019)

The systems of Norwegian aluminum manufacturing company Norsk Hydro were reportedly struck [...], by LockerGoga ransomware. [...] Norsk Hydro noted their “lack of ability to connect to the production systems causing production challenges and temporary stoppage at several plants.

[About the LockerGoga Ransomware]

Highlights

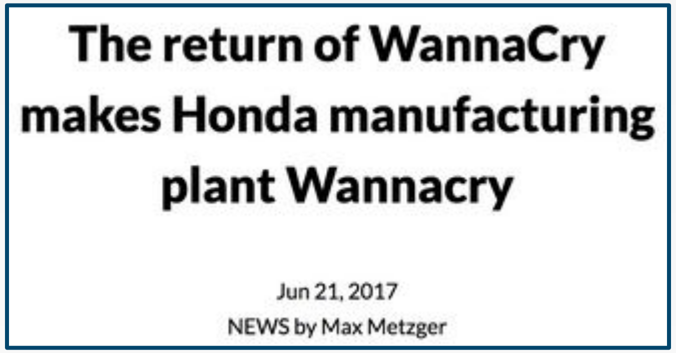
- Targeted for Norsk Hydro plants
- Signed by valid certificates
- No C&C

How it works

- Deployed on compromised network
- Modifies user accounts
- Logoff connected users
- Disconnect the system (Wifi, Wired)
- Crypt (destroy) files

Financial Impact of NotPetya & WannaCry

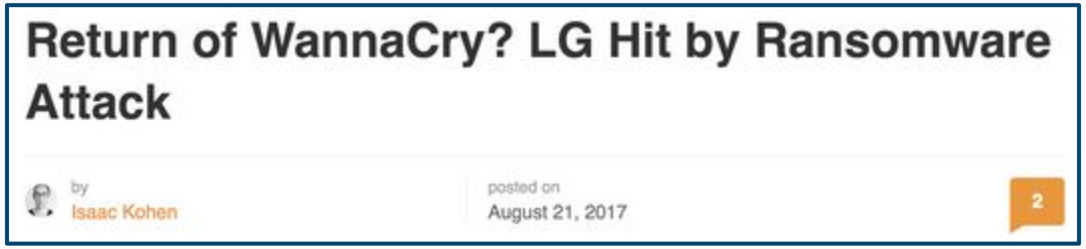
- Merck (Pharma) **$870M**
- FedEx (Logistics) **$400M**
- [Maersk (Logistics) **$300M**]
- Honda, Nissan, Renault forced to stop production plants



The return of WannaCry makes Honda manufacturing plant Wannacry

Jun 21, 2017

NEWS by Max Metzger

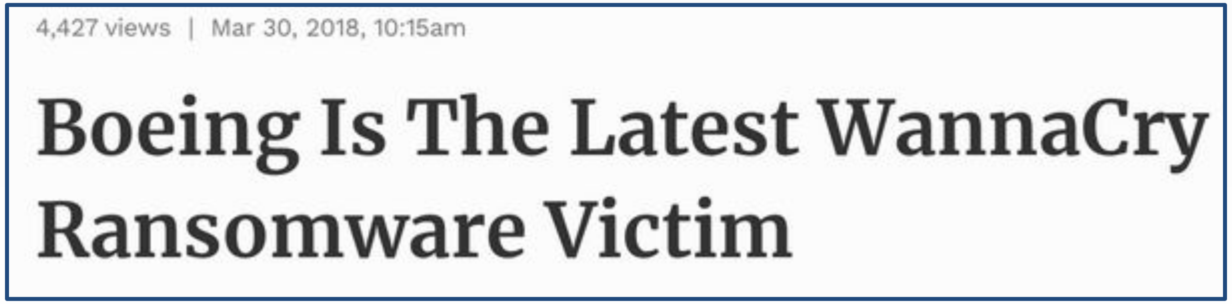


Return of WannaCry? LG Hit by Ransomware Attack

by Isaac Kohen

posted on August 21, 2017

2



4,427 views | Mar 30, 2018, 10:15am

Boeing Is The Latest WannaCry Ransomware Victim

EKANS (2020)

Car manufacturer Honda has been hit by a cyber attack, according to a report published by the BBC, and later confirmed by the company in a tweet. Another similar attack, also disclosed on Twitter, hit Edesur S.A., one of the companies belonging to Enel Argentina which operates in the business of energy distribution in the City of Buenos Aires.

EKANS Ransomware and ICS [...]

Honda and Enel impacted by [...]

Impact on

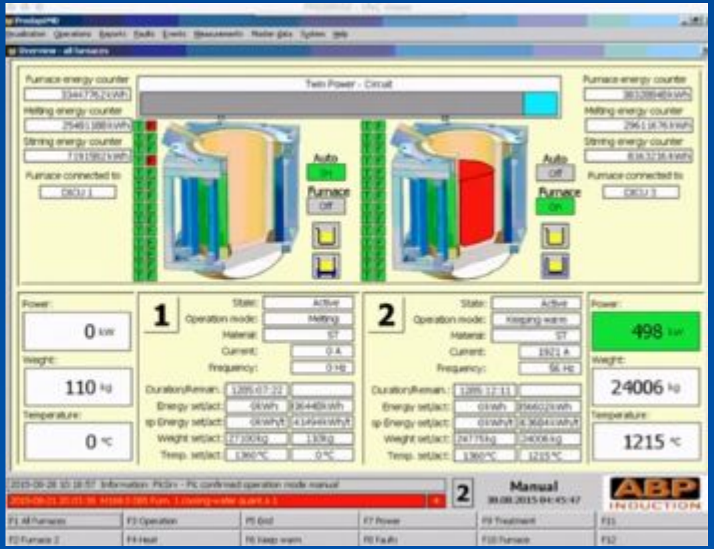
- Production sites (Honda)
- Customer care (Enel)
- ICS-specific processes (capabilities)

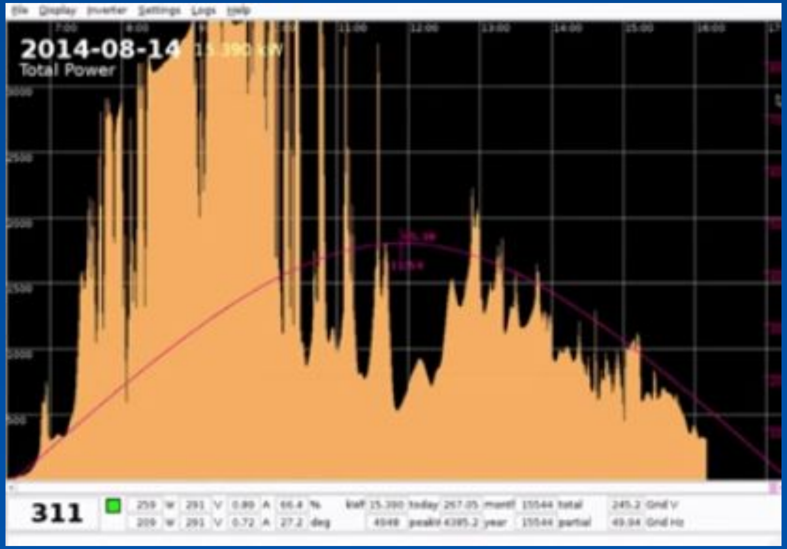
Attack Vectors

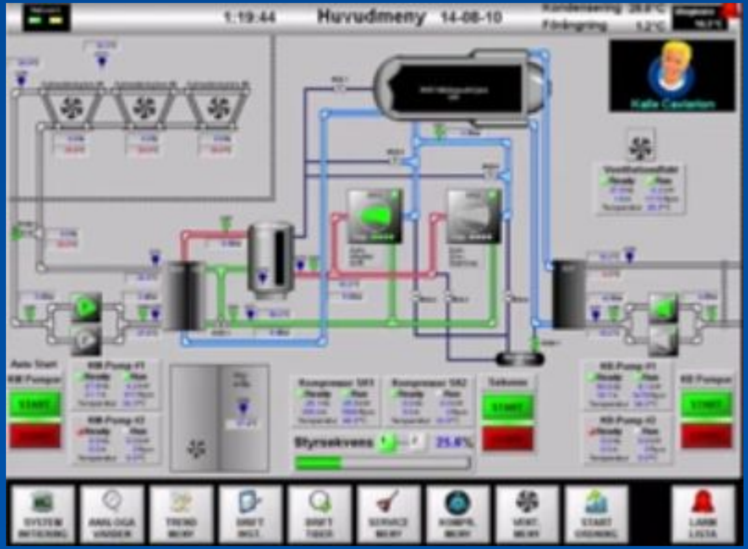
- Remote Desktop Protocol (RDP) access publicly exposed
- Recently discovered SMB RCE (SMBleed)
- Phishing
- Compromised Infrastructures

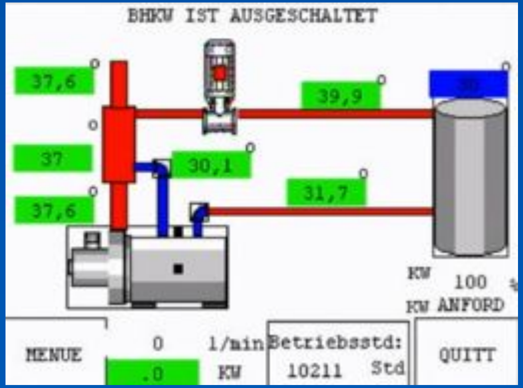
Examples of today OT/ICS exposed infrastructure

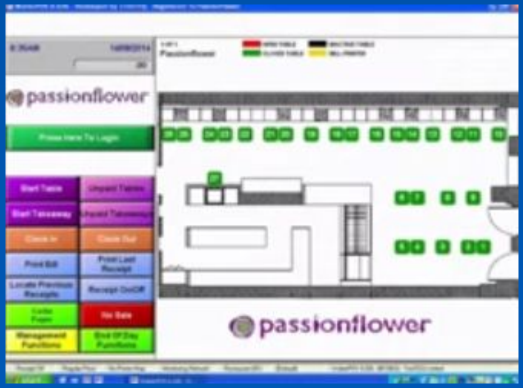
Examples of today OT/ICS exposed infrastructure

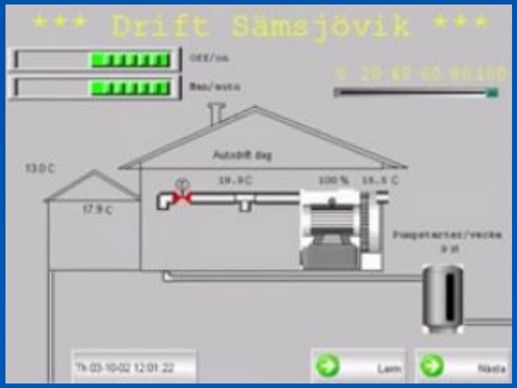


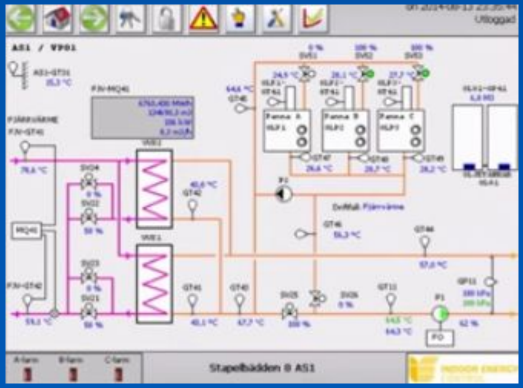




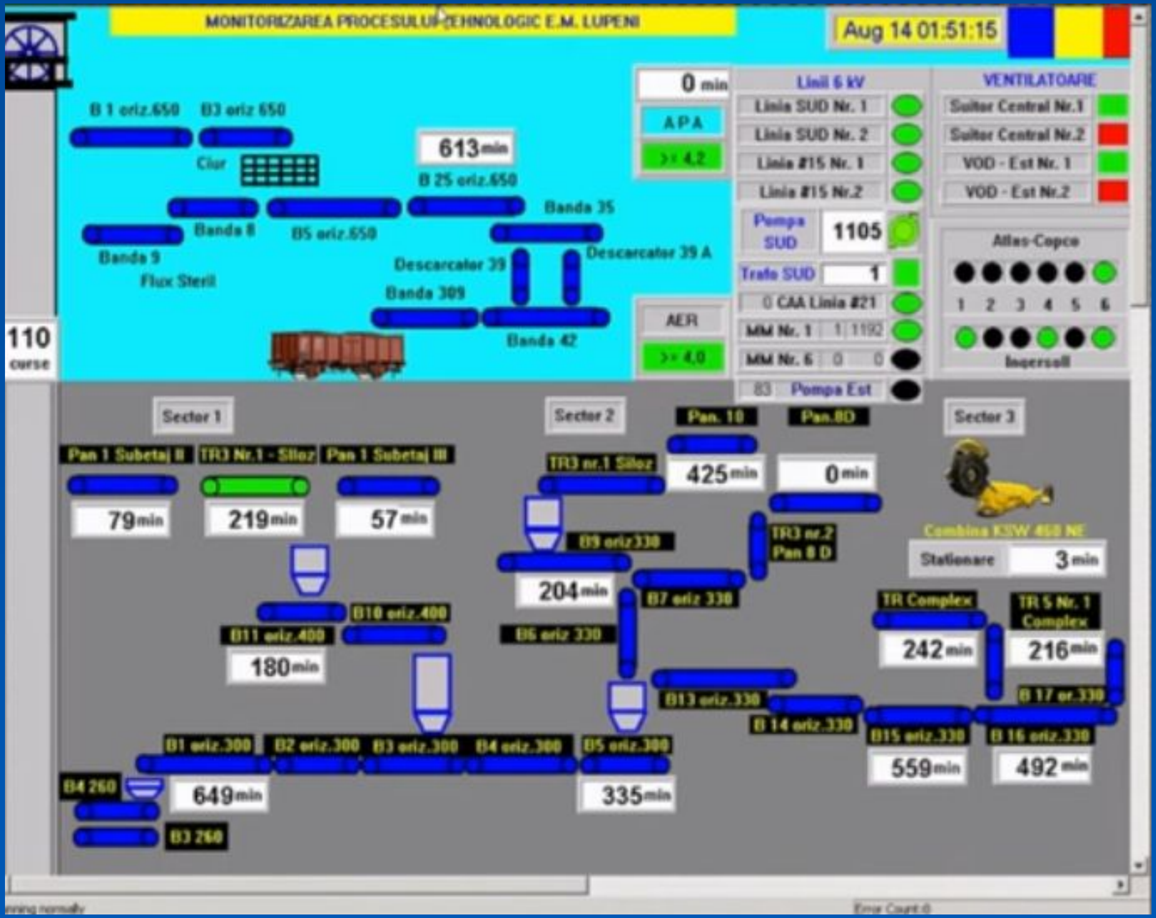


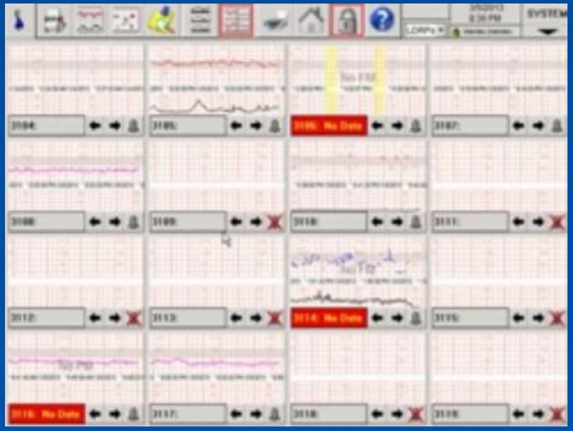


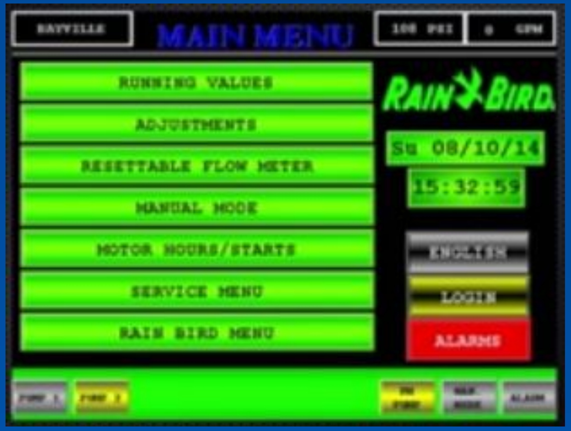


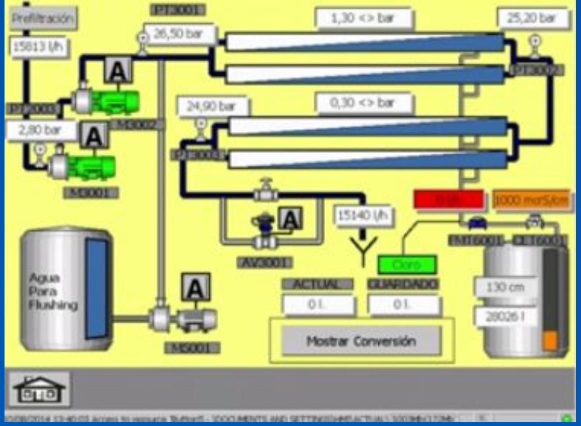


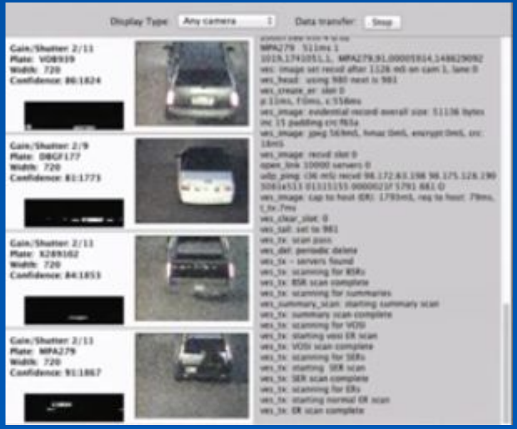
Examples of today OT/ICS exposed infrastructure











Gain/Shutter: 2/11
Plate: VDB939
Width: 720
Confidence: 86:1824

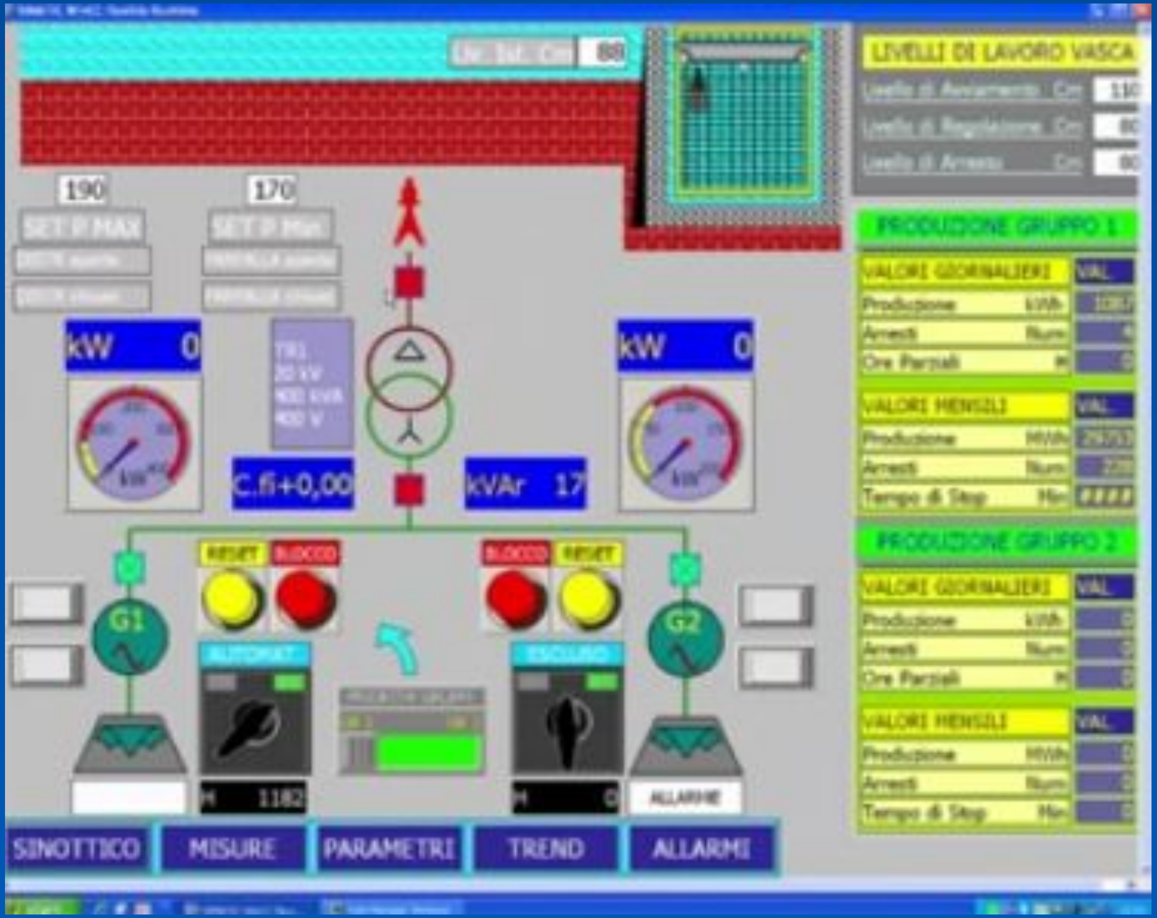
Gain/Shutter: 2/9
Plate: DBGF177
Width: 720
Confidence: 81:1773

Gain/Shutter: 2/11
Plate: X289102
Width: 720
Confidence: 84:1853

Gain/Shutter: 2/11
Plate: MPA279
Width: 720
Confidence: 91:1867

```
MPA279  511ms 1
1019,174105 1,1, MPA279,91,00005914,1486290[illegible]
ves: image set recod after 1126 mS on cam 1, lane 0
ves_head: using 980 next is 981
ves_create_er: slot 0
p 11ms, f 0ms, c 558ms
ves_image: evidential record overall size: 51136 bytes
inc 15 padding crc f63a
ves_image: jpeg 563mS, hmac 0mS, encrypt 0mS, crc
18mS
ves_image: recod slot 0
open_link 10000 servers 0
udp_ping: (36 mS) recvd 98.172.63.198 98.175.126.190
3061a513 01315155 0000021F 5791 881 0
ves_image: cap to host (ER): 1793mS, req to host: 79ms,
t_tx 7ms
ves_clear_slot: 0
ves_tail: set to 981
ves_tx: scan pass
ves_del: periodic delete
ves_tx - servers found
ves_tx: scanning for BSRs
ves_tx: BSR scan complete
ves_tx: scanning for summaries
ves_summary_scan: starting summary scan
ves_tx: summary scan complete
ves_tx: scanning for VOSI
ves_tx: starting vosi ER scan
ves_tx: VOSI scan complete
ves_tx: scanning for SERs
ves_tx: starting SER scan
ves_tx: SER scan complete
ves_tx: scanning for ERs
ves_tx: starting normal ER scan
ves_tx: ER scan complete
```

Examples of today OT/ICS exposed infrastructure



LIVELLI DI LAVORO VASCA

Livello di Avviamento	Cm	110
Livello di Regolazione	Cm	80
Livello di Arresto	Cm	80

PRODUZIONE GRUPPO 1

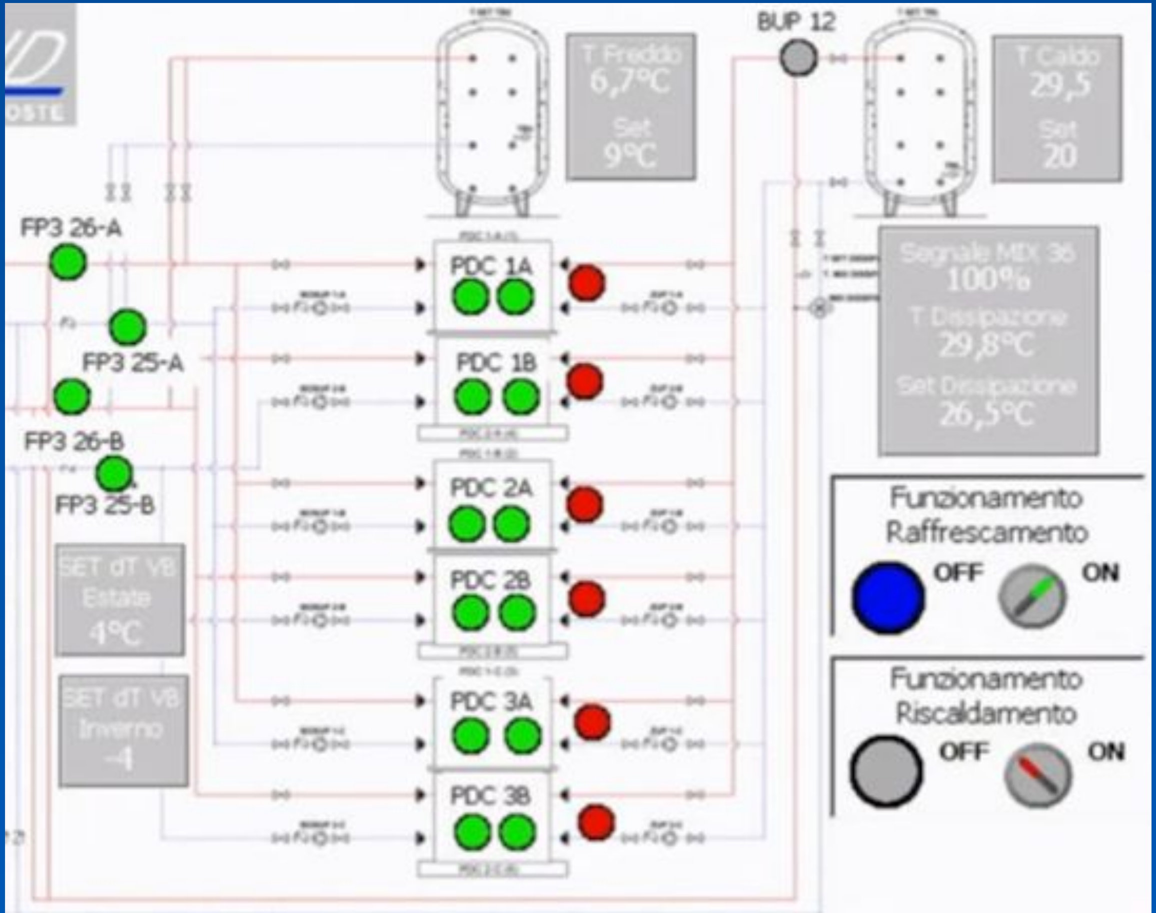
VALORI GIORNALIERI		VAL
Produzione	kWh	1083
Arresti	Num	4
Ore Parziali	H	0

VALORI MENSILI		VAL
Produzione	MWh	29753
Arresti	Num	220
Tempo di Stop	Min	####

PRODUZIONE GRUPPO 2

VALORI GIORNALIERI		VAL
Produzione	kWh	0
Arresti	Num	0
Ore Parziali	H	0

VALORI MENSILI		VAL
Produzione	MWh	0
Arresti	Num	0
Tempo di Stop	Min	0



T Freddo 6,7°C Set 9°C

T Caldo 29,5 Set 20

Segnale MIX 3B 100%

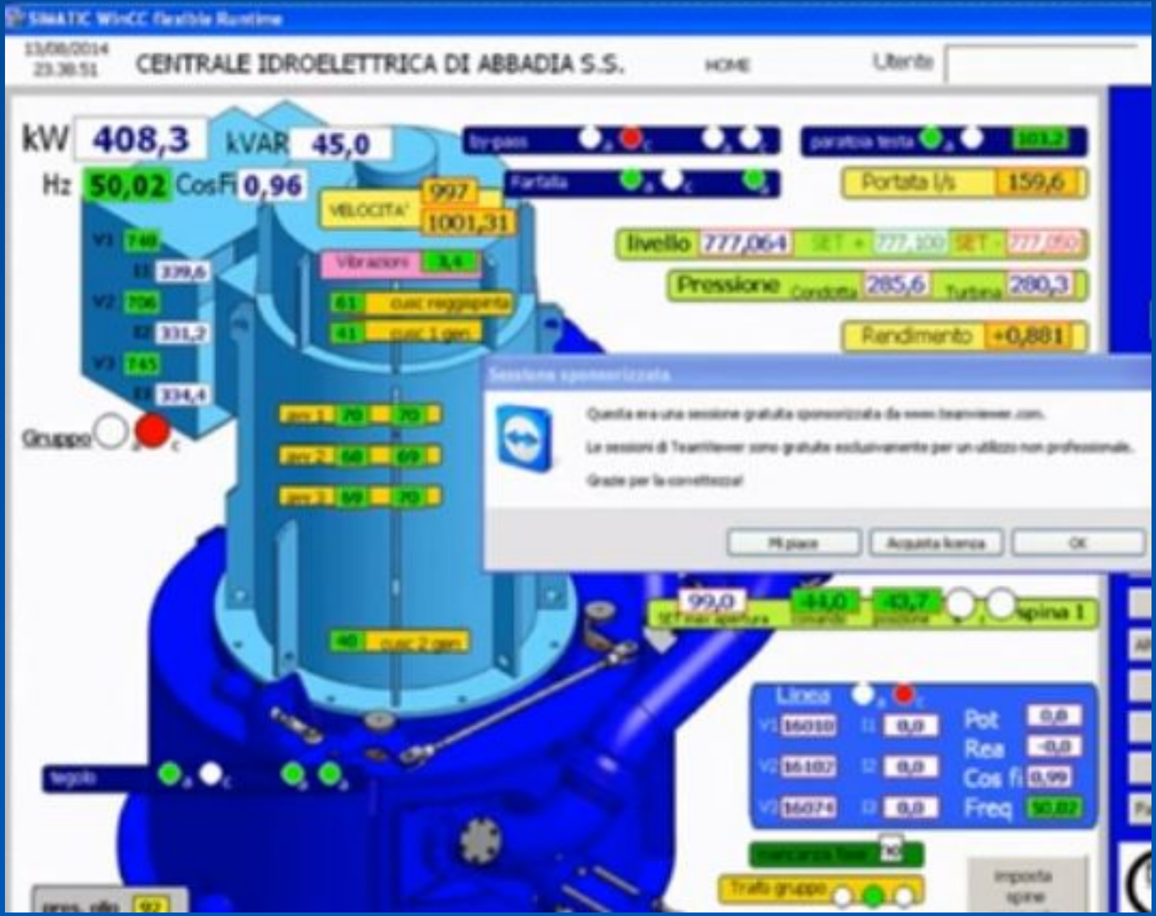
T Dissipazione 29,8°C

Set Dissipazione 26,5°C

SET dT VB Estate 4°C

SET dT VB Inverno -4

Examples of today OT/ICS exposed infrastructure

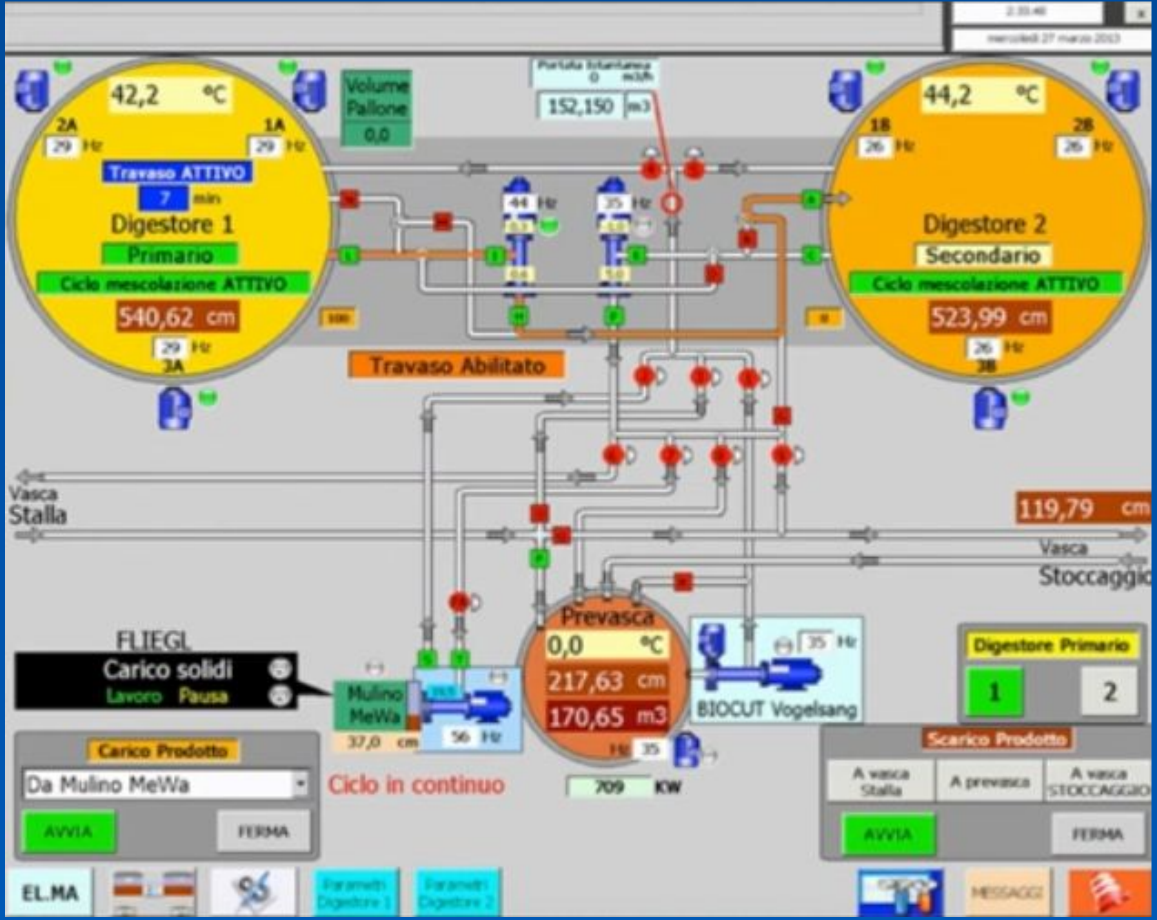


Sessione sponsorizzata

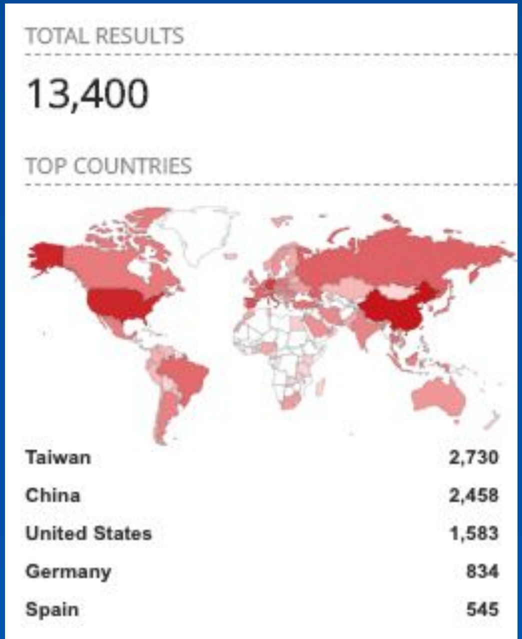
Questa era una sessione gratuita sponsorizzata da www.teamviewer.com.

Le sessioni di TeamViewer sono gratuite esclusivamente per un utilizzo non professionale.

Grazie per la correttezza!



Finding OT/ICS exposed infrastructure (Siemens S7)

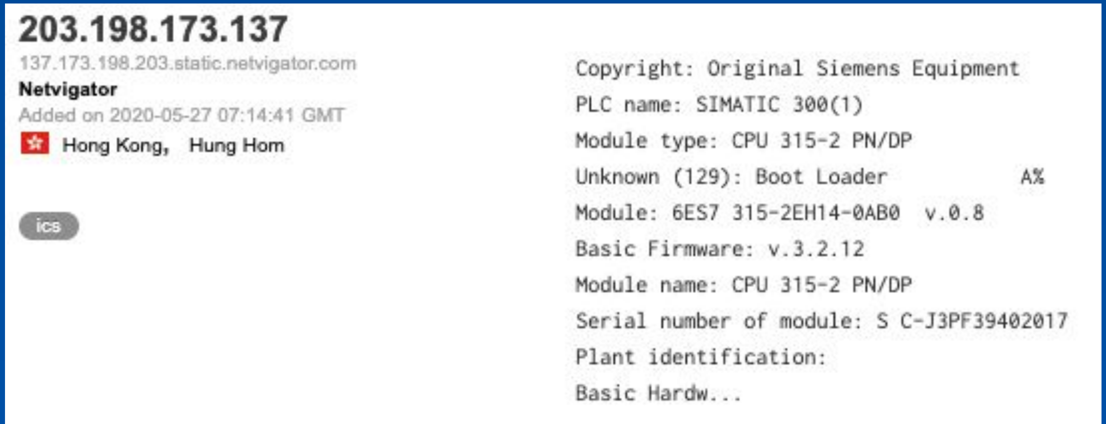


TOTAL RESULTS

13,400

TOP COUNTRIES

Taiwan	2,730
China	2,458
United States	1,583
Germany	834
Spain	545



203.198.173.137

137.173.198.203.static.netvigator.com

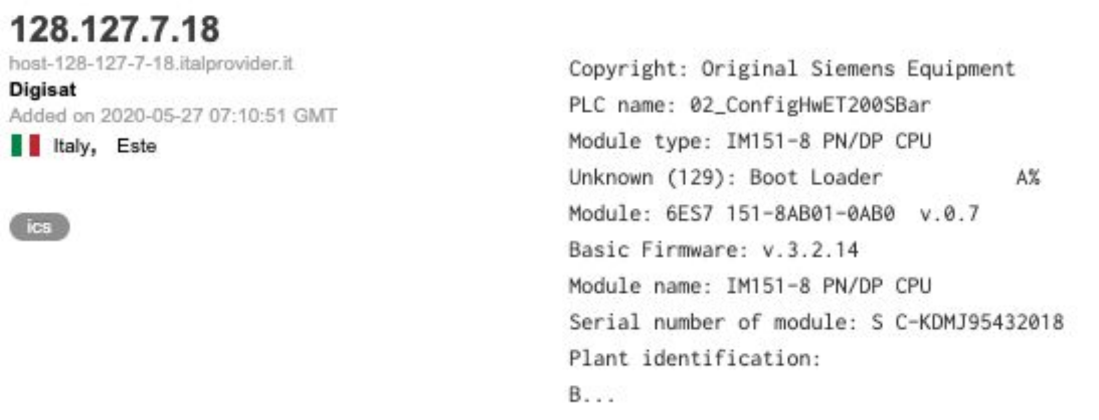
Netvigator

Added on 2020-05-27 07:14:41 GMT

Hong Kong, Hung Hom

ics

```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 315-2 PN/DP
Unknown (129): Boot Loader           A%
Module: 6ES7 315-2EH14-0AB0  v.0.8
Basic Firmware: v.3.2.12
Module name: CPU 315-2 PN/DP
Serial number of module: S C-J3PF39402017
Plant identification:
Basic Hardw...
```



128.127.7.18

host-128-127-7-18.italprovider.it

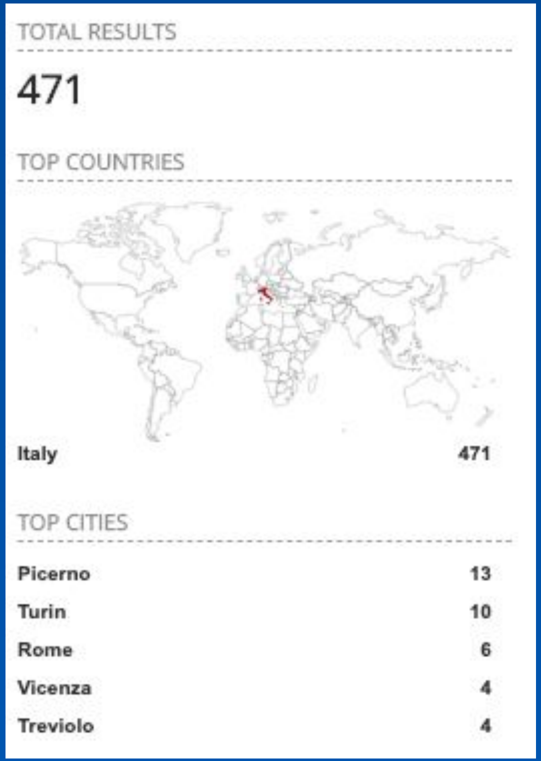
Digisat

Added on 2020-05-27 07:10:51 GMT

Italy, Este

ics

```
Copyright: Original Siemens Equipment
PLC name: 02_ConfigHwET200SBar
Module type: IM151-8 PN/DP CPU
Unknown (129): Boot Loader           A%
Module: 6ES7 151-8AB01-0AB0  v.0.7
Basic Firmware: v.3.2.14
Module name: IM151-8 PN/DP CPU
Serial number of module: S C-KDMJ95432018
Plant identification:
B...
```



TOTAL RESULTS

471

TOP COUNTRIES

Italy	471

TOP CITIES

Picerno	13
Turin	10
Rome	6
Vicenza	4
Treviolo	4

Particularity of OT/ICS infrastructures

OT/ICS devices

OT/ICS devices were designed to solve a complex problem under deterministic circumstances. With the advent of Internet protocols and Industry 4.0, OT/ICS devices are now interconnected to IP networks and usually exposed to external systems, users.
Vendors usually require remote access to OT/ICS devices for maintenance.

Designed for:

- "availability"
- real time communications
- long term life

Weakness:

- sensible to ethernet disruptions
- exposed sensitive data (registry)
- unauthenticated
- no data integrity check
- well known vulnerabilities

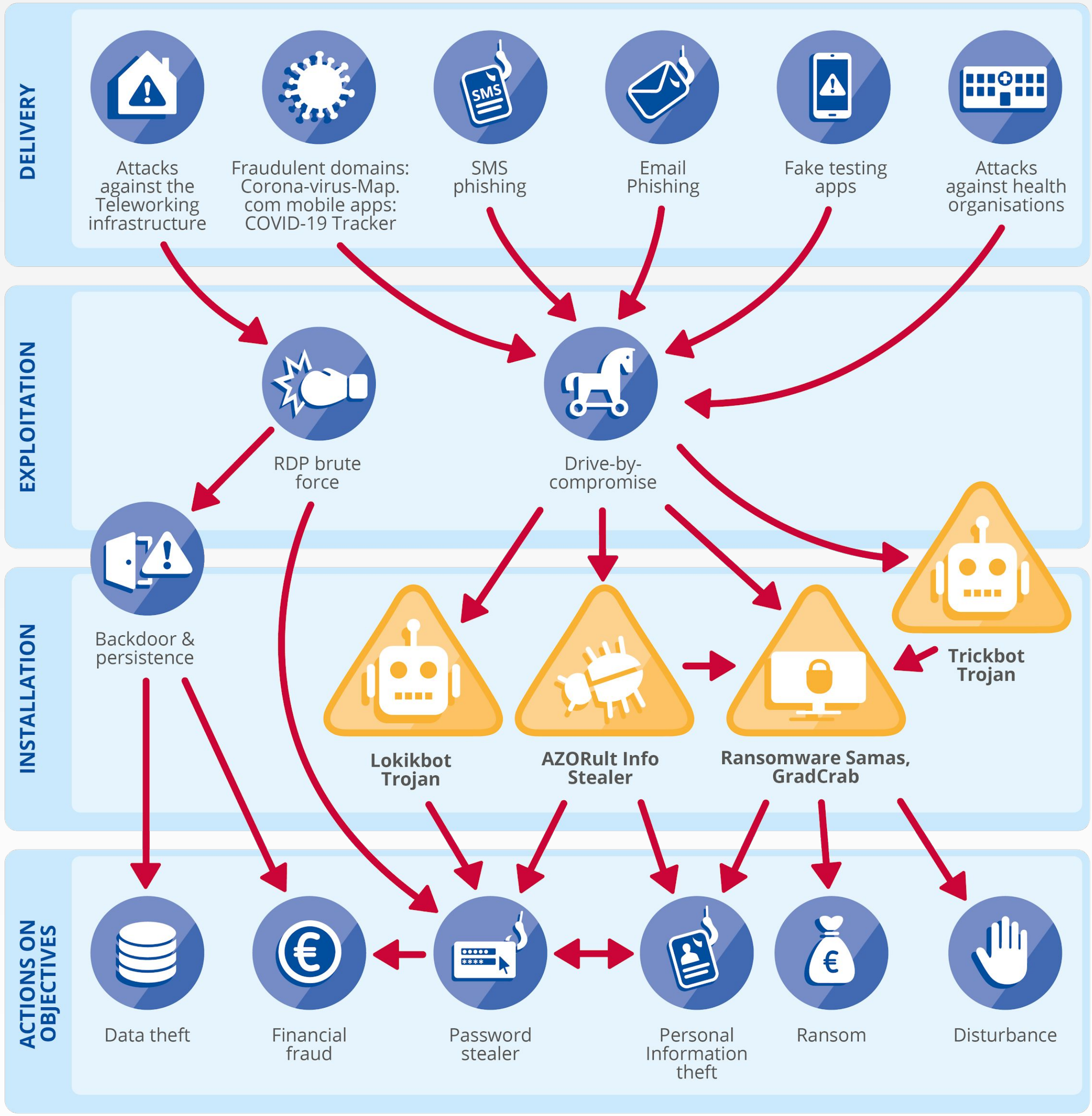
Attacking an OT/ICS plant

Threat Landscape Mapping

The ENISA Threat Landscape (ETL) provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends.

[ENISA Threat Landscape](#)

[Cyber Kill Chain®](#)



Attacking an OT/ICS plant

Firewall/IDS/IPS evasion

Gain access to an inside system, directly or indirectly. Exposed Windows SCADA systems is the fastest way, other vulnerable systems could lead to the target.

Lateral movement

Move from the compromised system to an internal system and gain direct access to industrial plants.

Abusing OT/ICS protocols

Understand plant topology, abuse memory registers to break plant components or to change plant behaviour.

Defending an OT/ICS plant

(initial) Security Assessment

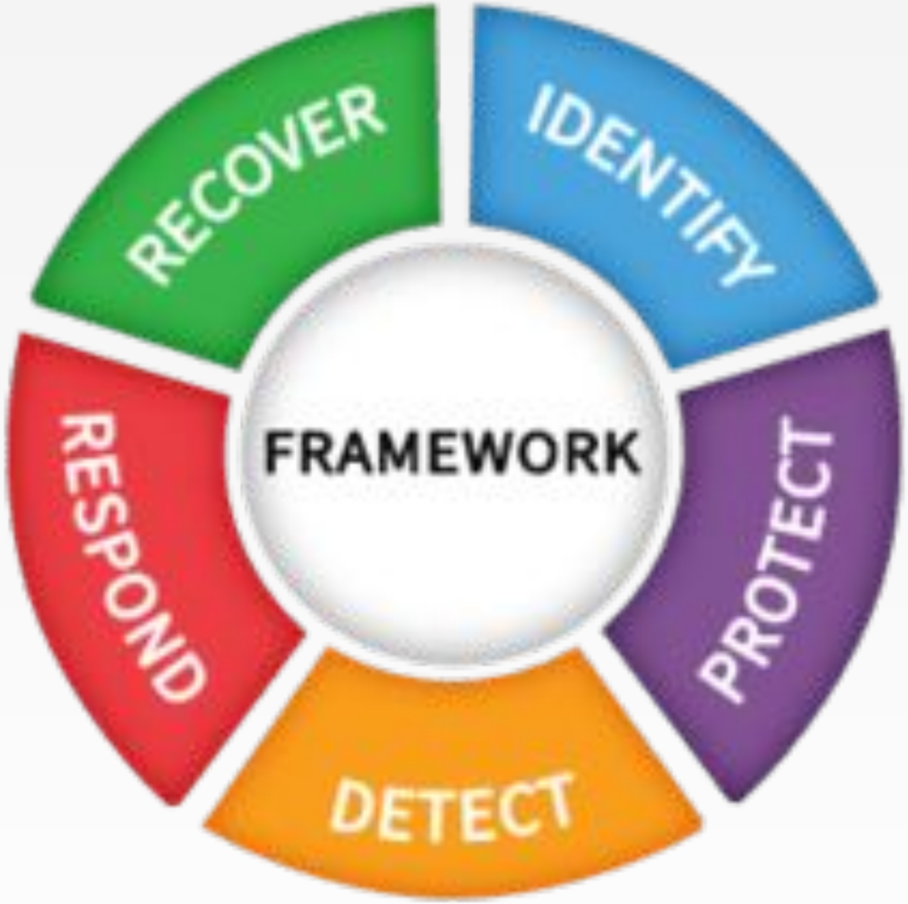
Initial Security Assessments identify vulnerabilities and potential threats. Exposing vulnerable applications can easily lead to compromise.

Attackers from all around the world are constantly looking for vulnerable servers to be exploited. Easy targets are compromised with ransomware attacks.

Approach: NIST 5 functions

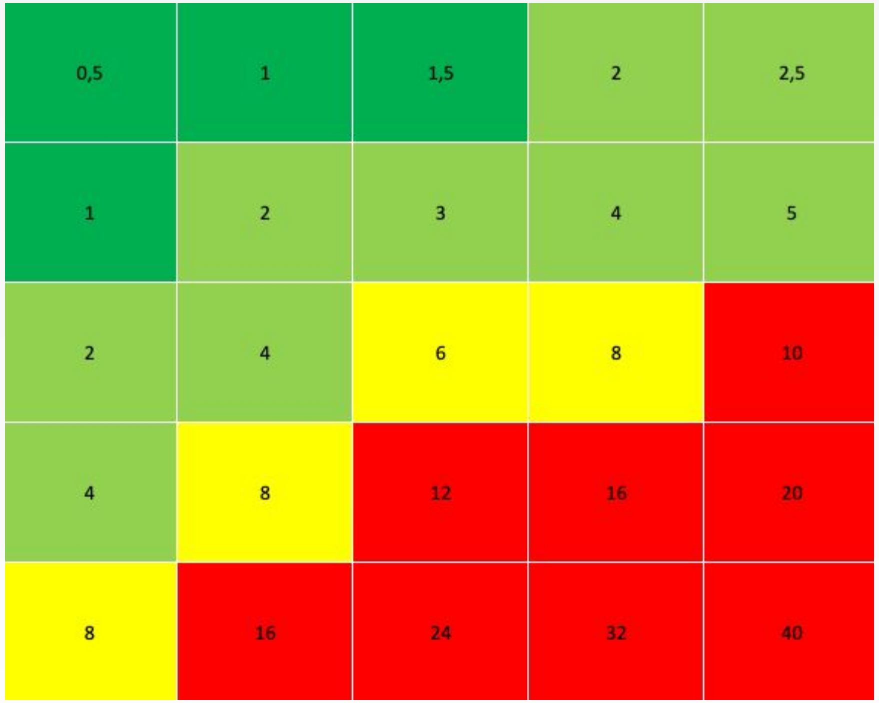
NIST Framework Core identifies 5 functions. These Functions are not intended to form a serial path or lead to a static desired endstate.Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

NIST Framework



Risk Based Thinking

Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of **uncertainty on objectives**) followed by coordinated and economical application of resources to minimize, monitor, and control the **probability** or **impact** of unfortunate events or to maximize the realization of opportunities.



0,5	1	1,5	2	2,5
1	2	3	4	5
2	4	6	8	10
4	8	12	16	20
8	16	24	32	40

Risk management

Threat Modeling

Threat modeling is a process by which potential threats [...] can be identified, enumerated, and mitigations can be prioritized. The purpose [...] is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.

Answers to

- Weak rings (personnel, supplier…)
- Exposed systems
- Critical systems

References

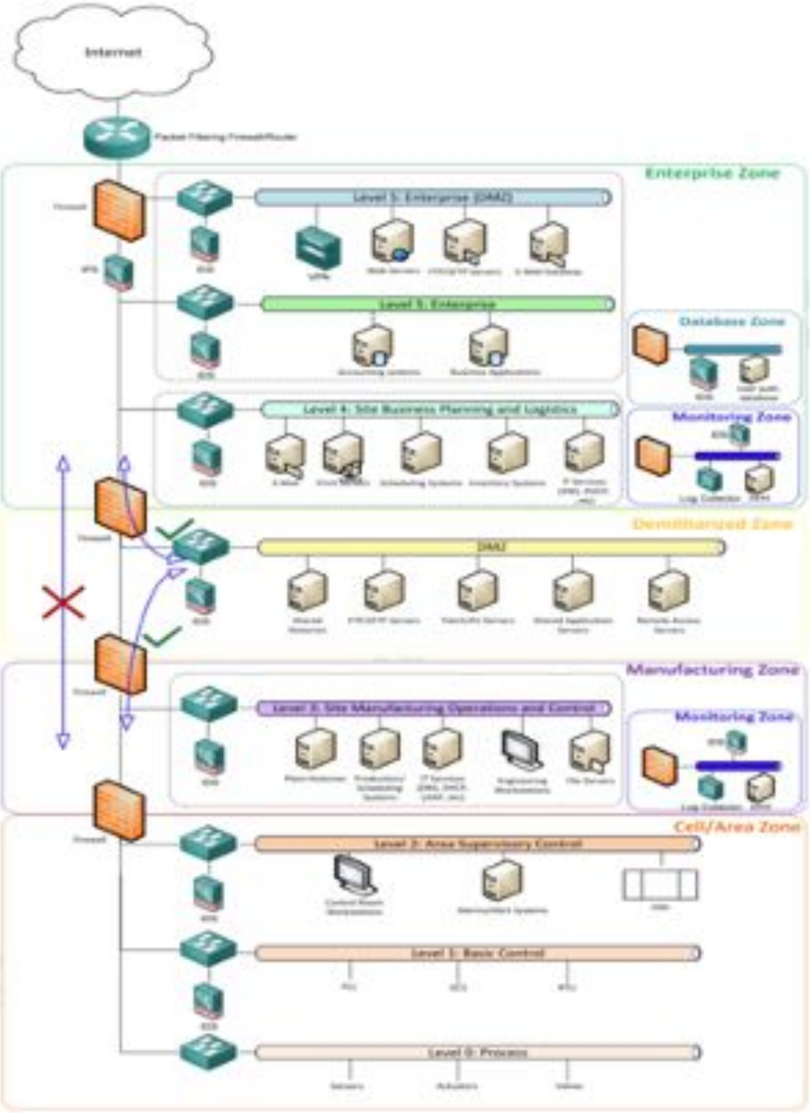
- Risk Centric Threat Modeling

The Purdue Model

for Control Hierarchy (ISA-99, 2004)

The Purdue Model for Control Hierarchy logical framework identify 6 levels (0-5) distributed in 5 zones: Enterprise (lvls. 5-4), Manufacturing (lvl. 3), Cell/Area (lvls. 2-0), Safety. Four security domains (access control, network security, log management, remote access) are applied to ICS network components.

[Secure Architecture for ICS]()



The Goal

Security is a process, not a target. No system can be 100% secure.
In other words a company can be compromised with sufficient resources.

Increasing the cost for a successful Cyber attack decreases the probability to become targeted.

Pay attention to

- Weak rings (personnel, supplier…)
- Exposed systems
- Critical systems

Optimize

- Implement risk based processes
- Automation and reporting
- Train personnel
- GDPR
- ISO27001

DEMO

Maritime Cyber risk

IMO 2021

The Maritime Safety Committee [...] adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

References

- Maritime cyber risk
- MSC-FAL.1/Circ.3 Guidelines
- Resolution MSC.428(98)
- Guidelines on Cyber Security
- NIST Framework

Cybersecurity Act (2019/881)

NIS Directive (2016/1148)

NIS Directive significantly affects digital service providers (DSPs) and operators of essential services (OESs). (Nis Dir.)

Cybersecurity Act lay down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT. (Cyb. A.)

References

- Directive (UE) 2016/1148
- Regulation (EU) 2019/881

Highlights

- Energy, Transport, Banking, Healthcare, Water supply, Digital Infrastructures…
- Incidents notified to national CSIRTs
- Risk Management
- Cybersecurity certification framework (products, services, processes)

When technologies and data are secure and instrumental to mankind, then people are free to follow their passions, achieve their desires and advance their company.

Q&A

End