your cybersecurity partner for innovation

Introduction to Industrial Control System Security

Federico Turrin

Advanced Topics in Computer and Network Security
University of Padova

11/10/2023

About me

Short bio:

- **Ph.D.** & **Post Doc** @ University of Padova
  - Supervisor: Prof. **Mauro Conti**
- Abroad experiences
  - Student @ Grenoble Institute of Technology, France (2017)
  - Visiting researcher @ SUTD, Singapore (2022)
- **Currently:** Cyber Security Engineer @ SPRITZ Matter

Contacts:

- Mail: federico.turrin@spritzmatter.com
- Website: https://www.math.unipd.it/~turrin/
  (moving soon)

Research Interests:

- Cyber-Physical System Security
- Industrial Control System Security
- Vehicles Security
- Anomaly and Intrusion detection

Presentation outline

- Introduction to Industrial Security Security
  - Definition and Architecture
  - Why should we care about
  - Difference from IT systems

- Are ICS really exposed?
  - The Shodan case
  - Our measurement

- How we protect?

Introduction to Industrial Security Security

Cyber-Physical Systems

Cyber-Physical Systems (CPSs) interconnect:

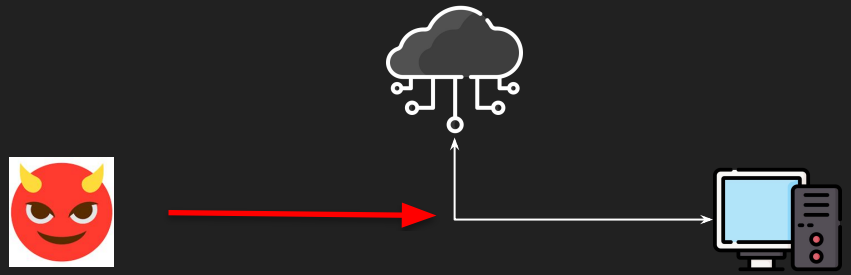
- Physical Processes, or Operational Technology (OT)
- Information Technology (IT)

Some Example:

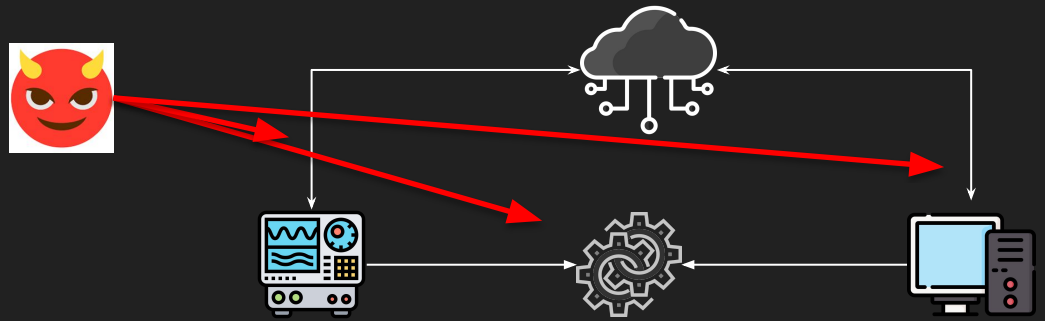
- *Smart Grid*
- *Smart Cars*
- *Industrial Control Systems*
- *e-Health Devices*

Attack Surfaces

Traditional IT Systems



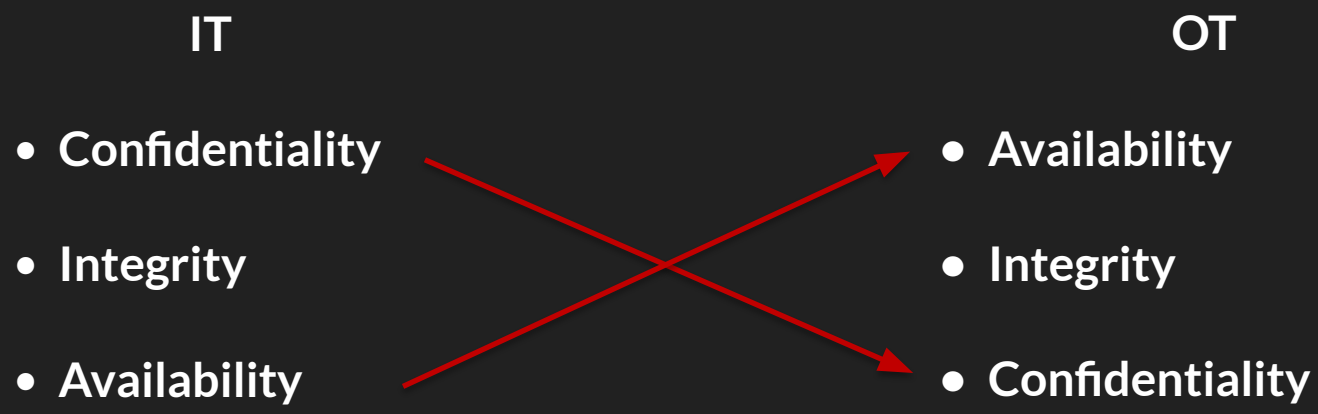
Cyber-Physical Systems



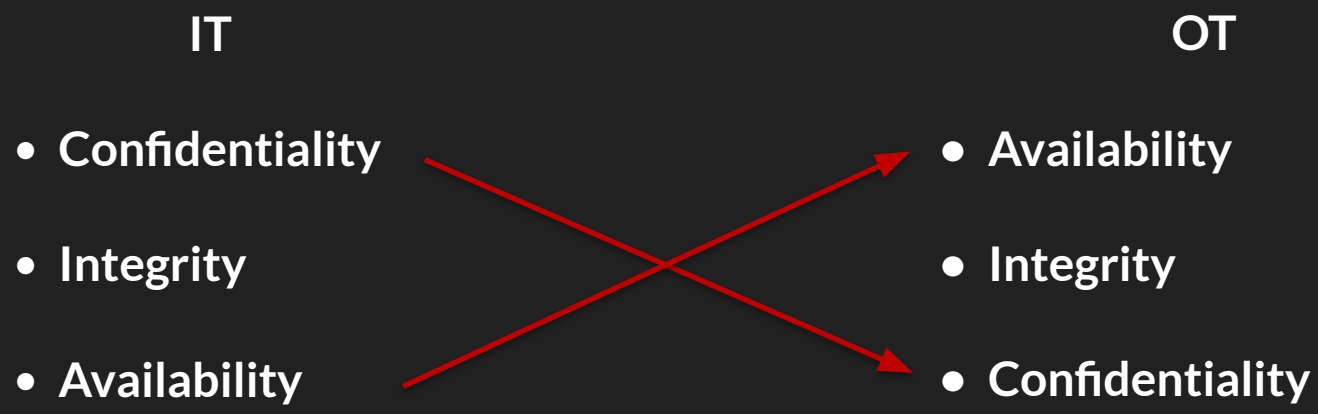
Confidentiality, Integrity, and Availability (CIA)

IT	OT
• Confidentiality	• ?
• Integrity	• ?
• Availability	• ?

Confidentiality, Integrity, and Availability (CIA)



Confidentiality, Integrity, and Availability (CIA)



What if we lose Availability of nuclear plants monitoring data?

Confidentiality, Integrity, and Availability (CIA)

IT

- Confidentiality
- Integrity
- Availability

OT

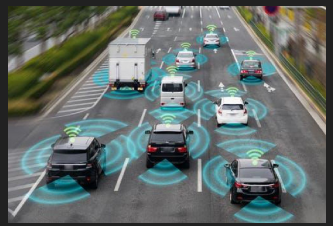
- Availability
- Integrity
- Confidentiality

What if we lose Availability of nuclear plants monitoring data?

Smart Cars Security

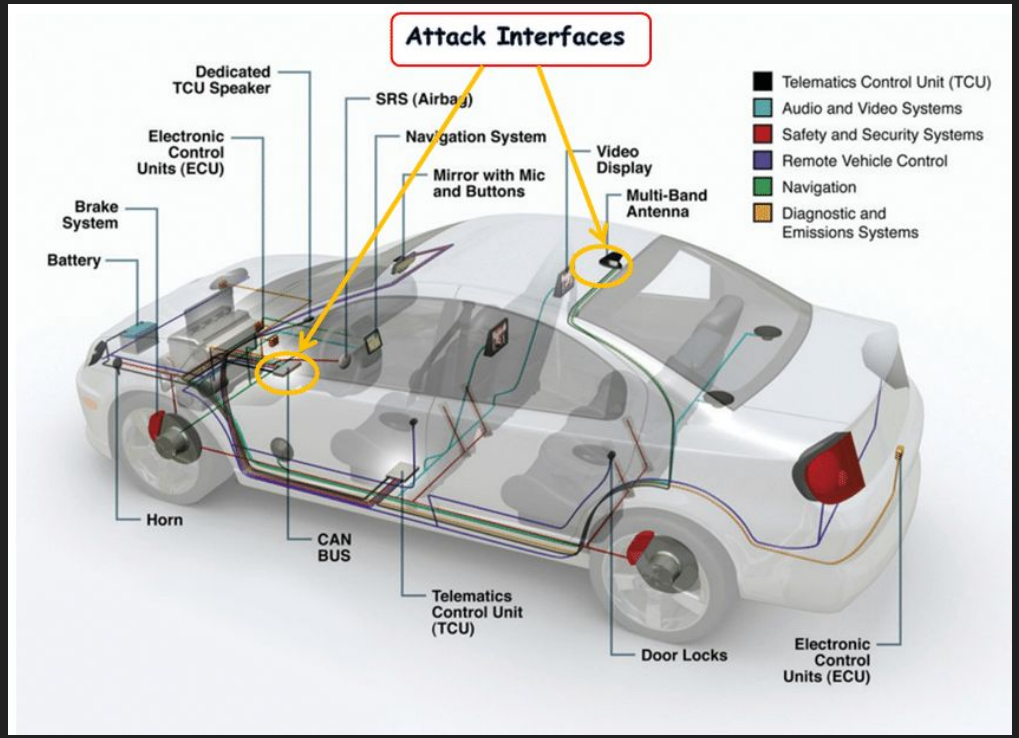
- Today's vehicle networks are truly distributed electronic systems.

Very critical
- x-by-wire
- steering aids, ABS, ESP(DSC)
- remote window and lock control
- engine control
- airbag control
- navigation systems
- entertainment systems



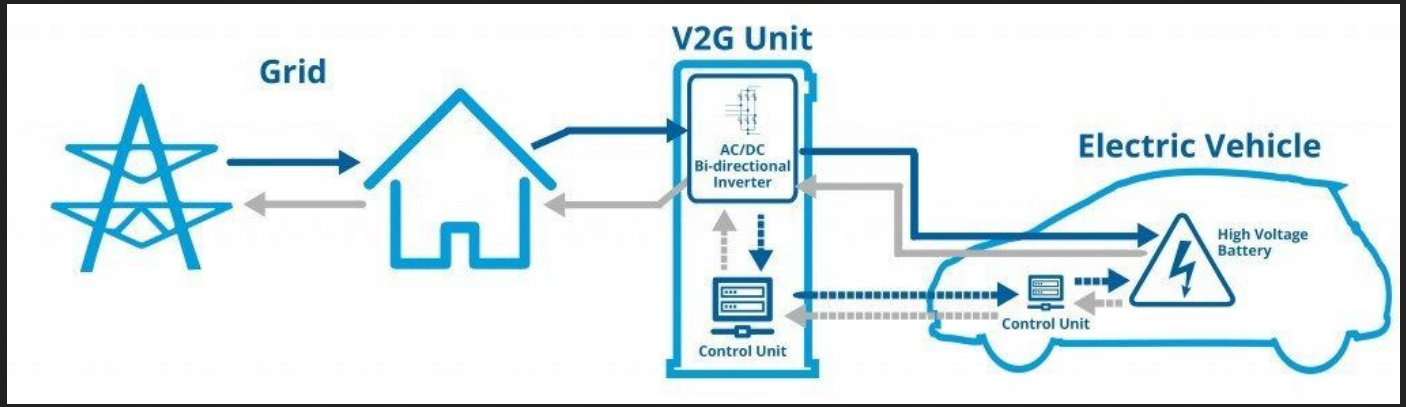
- The CAN bus is standard in automotive communication
  - Very simple protocol, 8 byte payload
  - No security features

CAN Bus


Attack Interfaces
Dedicated TCU Speaker
SRS (Airbag)
Navigation System
Electronic Control Units (ECU)
Mirror with Mic and Buttons
Video Display
Multi-Band Antenna
Brake System
Battery
Horn
CAN BUS
Telematics Control Unit (TCU)
Door Locks
Electronic Control Units (ECU)
Telematics Control Unit (TCU)
Audio and Video Systems
Safety and Security Systems
Remote Vehicle Control
Navigation
Diagnostic and Emissions Systems

Vehicle-to-Grid (V2G)

- Wide spreading of Electric Vehicles (EVs)
  - Increasing energy demand
- V2G enables communication between EV and the Supply Equipment
- Bi-directional power supply



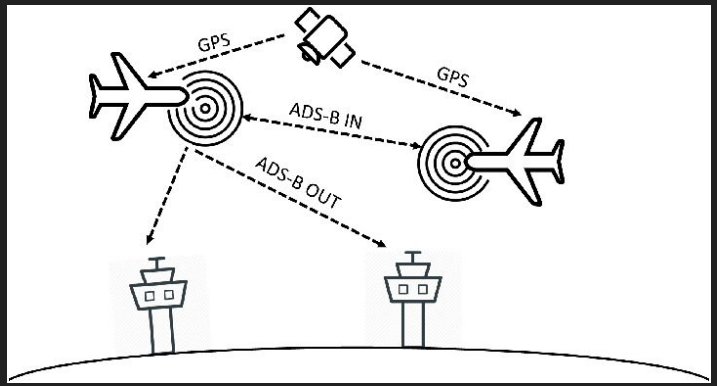
Air – Ground Communications

Automatic Dependent Surveillance–Broadcast (ADS-B)

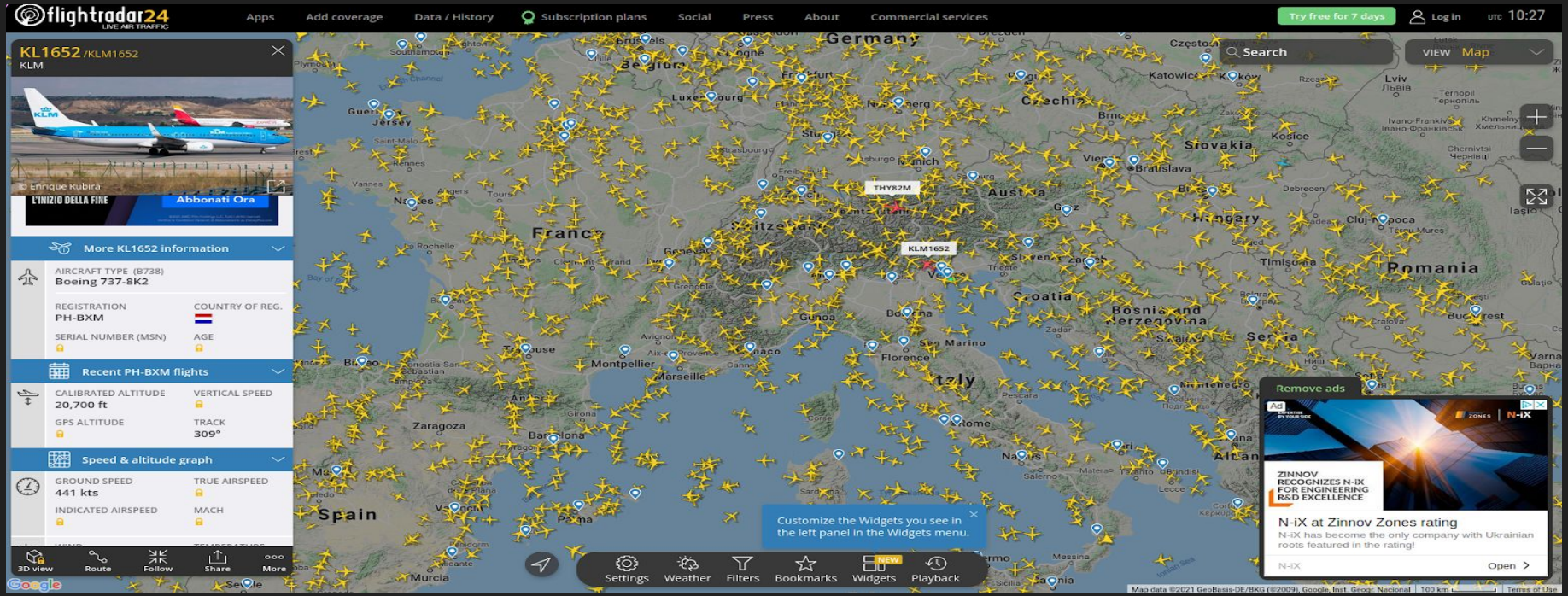
-> No Security **At All**

Implications:

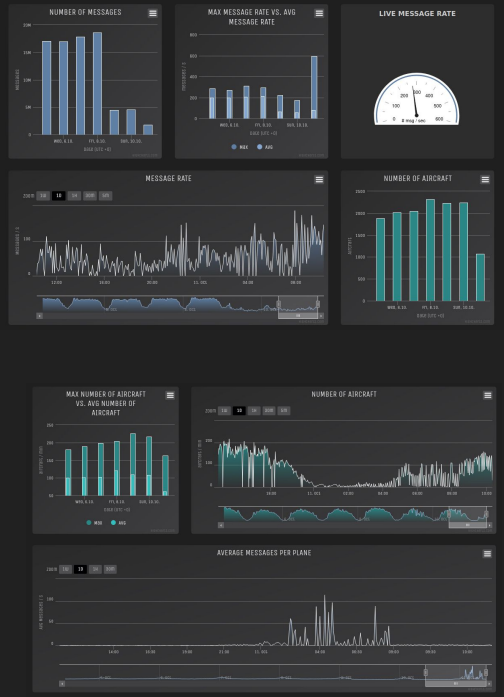
- Confidentiality: Eavesdropping
- Integrity: Message Deletion/Modification
- Availability: Jamming/Flooding
- Authentication: Message Injection



Air – Ground Communications



Opensky network



- SPRITZ is part of the OpenSky Testbed

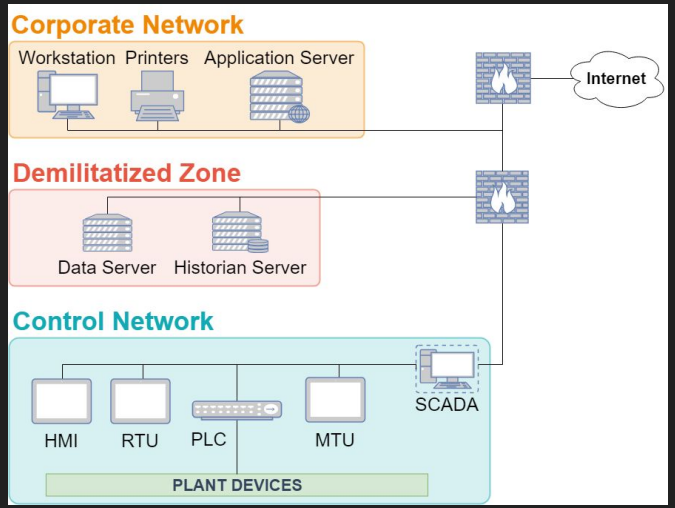
Industrial Control Systems

- Monitor and control industrial processes
- Sometimes categorized as *Critical Infrastructures*

  (e.g., nuclear power plant, water treatment systems)
- Unavailability or failure have serious consequences
  - Business
  - Environment
  - Human lives

Reference model for the ICS Architecture

The **Purdue model** divides ICS network into logical segments



Corporate Network (IT): applications used to support Enterprise Business and User Goals

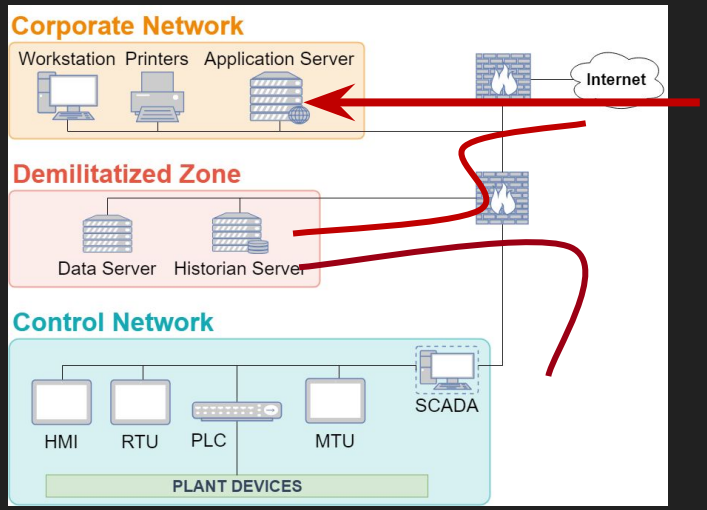
DMZ: avoid direct communication between Corporate Network and Control Network.

Control Network (OT): managing the operations environment and the real-time control system

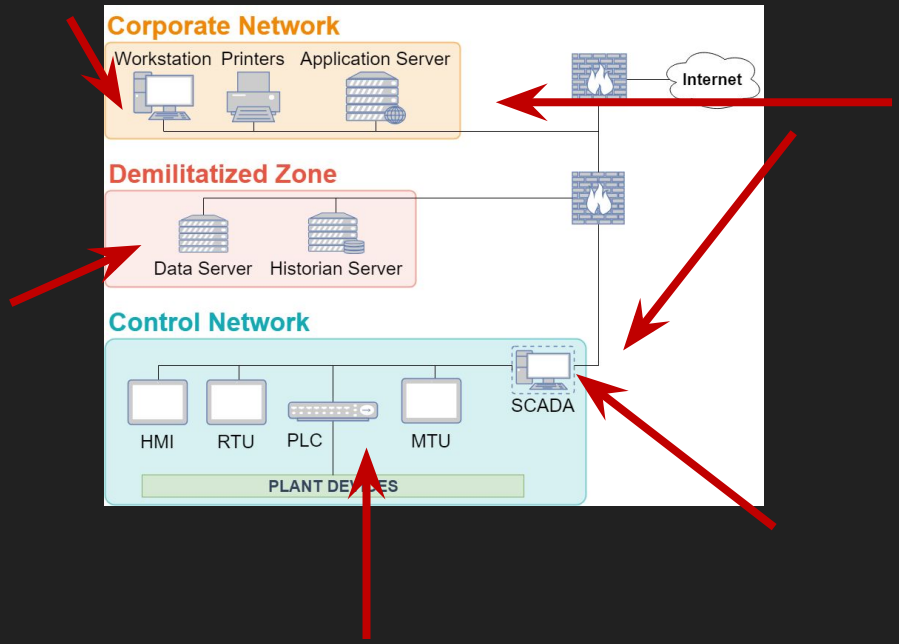
Obregon, Luciana. "Secure architecture for industrial control systems." *SANS Institute InfoSec Reading Room* (2015).

Theory vs Reality

How it should be

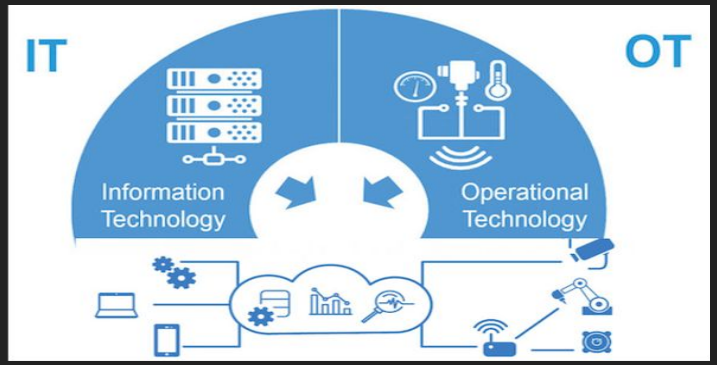


How it actually is



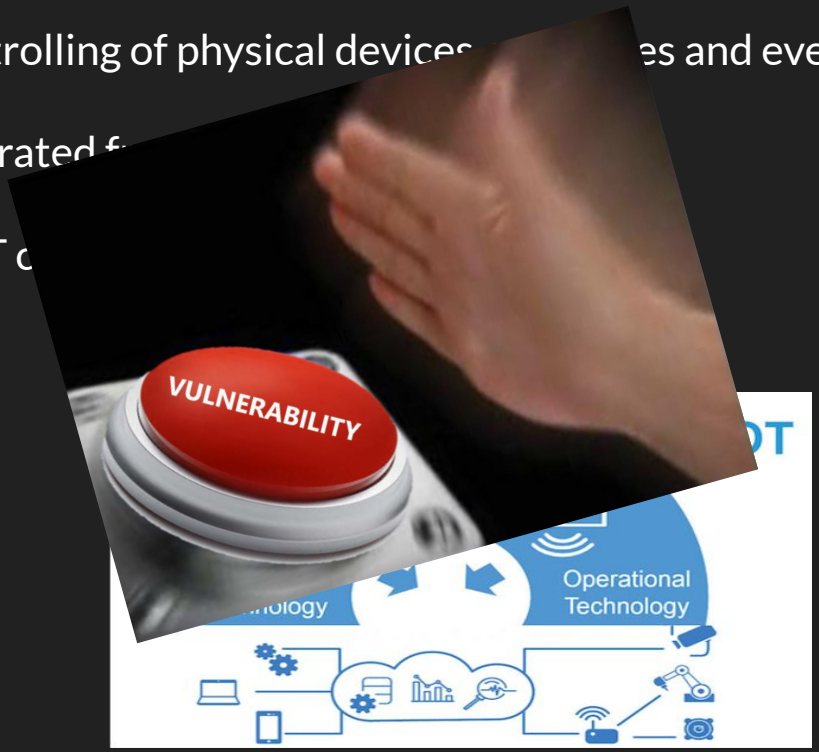
Operational Technology (OT)

- Monitoring and controlling of physical devices, processes and events.
- Historically OT separated from IT network
- Nowadays IT and OT coexist in the same network



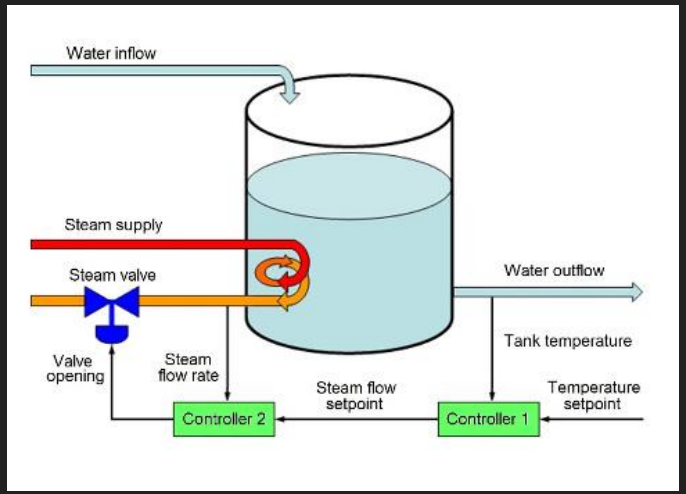
Operational Technology (OT)

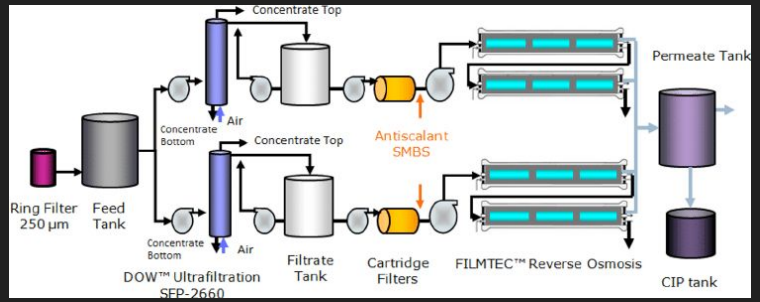
- Monitoring and controlling of physical devices and events.
- Historically OT separated f
- Nowadays IT and OT c



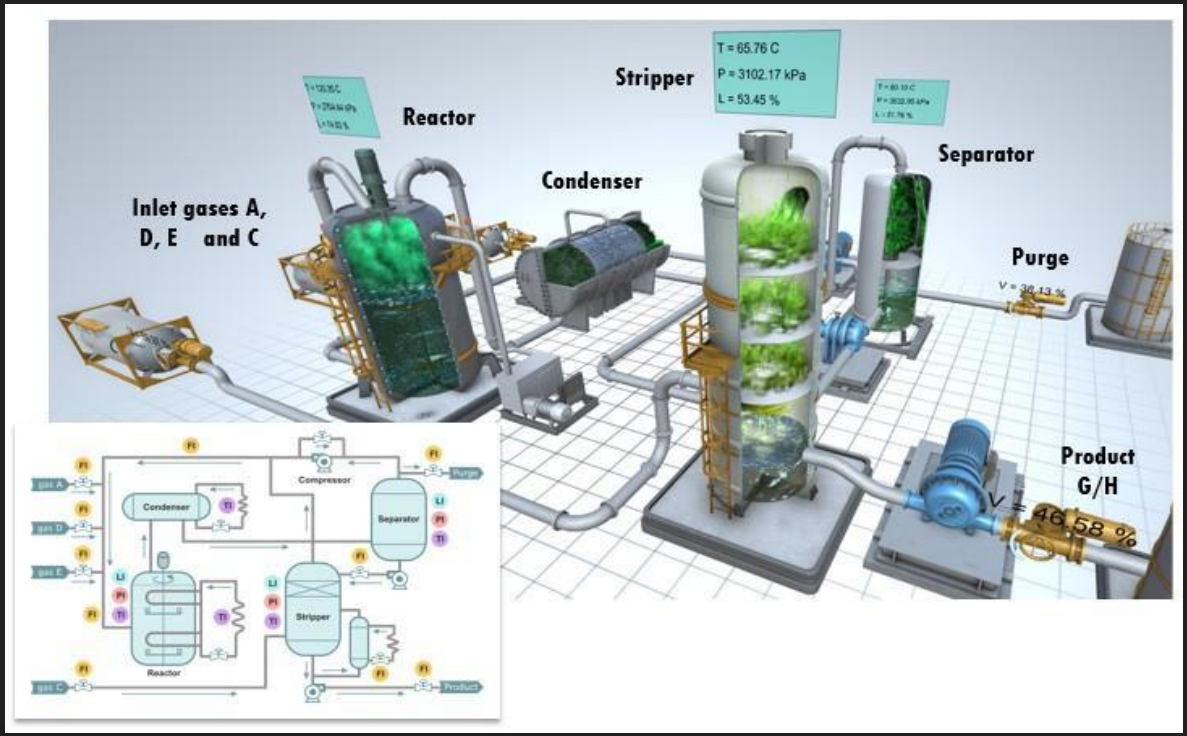
Only reality....

Some Example



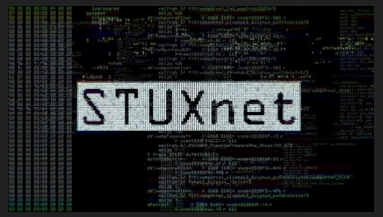


Some Example



Attack History of ICS

- Maroochy Shire (2000)
- **Stuxnet** (2010)
- ...
- German Steel Meel (2014)
- IRONGATE (2015)
- Ukrainian Power Grid (December 2015)
- Crash Override (2016)
- TRITON (December 2017)
- GreyEnergy (2018)
- Colonial Pipeline (2021) !!
- Florida Water System (2021) !!



TRITON

More dangerous scenario…

LockBit Ransomware Gang Claims Italian Winery Cantina Tollo as Victim

The perpetrators have left a warning for Cantina Tollo, threatening to publicly release all confidential information unless their demands for ransom are met.

IL CASO

Sassicaia, tentata estorsione da 150mila euro in bitcoin

Home › Cyber Security

Faenza, grosso incendio alla cantina Caviro. Un dipendente: "Il botto mi ha fatto fare un salto di un metro"

di Marco Bettazzi

Nessuna persona risulta coinvolta. Evacuate 530 persone, che rientrano in serata a casa. I sindacati chiedono incontro urgente all'azienda. L'Arpae: nessun inquinante nell'aria

«Cianuro nell'acqua e nel vino», aziende italiane minacciate dagli hacker: «30 mila euro o avveleniamo le bottiglie»

Vinomofo data breach: 500,000 customers at risk after wine dealer hit by cyber-attack

Vinomofo warns customers to remain alert to scam activity after the hack

Home / Commercial /

HALF A MILLION CUSTOMERS AT RISK AFTER AUSSIE WINE RETAILER HIT BY CYBER ATTACK

by Reporter 18 October 2022 | 1 minute read SHARE THIS ARTICLE

"Miracolo" nel Modenese: dai rubinetti di casa esce il Lambrusco

CURIOSITÀ - Modena

A causa di un guasto nell'impianto idrico di una cantina, il vino è iniziato a fuoriuscire dai rubinetti delle abitazioni

Il Gazzettino

Ettolitri di vino versati nel fiume per la valvola rotta in cantina: è strage di pesci

Ok but…why should we care?

Allianz classifies Cybersecurity Risk a the most important business risk

The most important business risks in 2023: global

Ranking changes are determined by positions year-on-year, ahead of percentages.

Rank		Percent	2022 rank	Trend
1	Cyber incidents *(e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)*[1]	34%	*1 (44%)*	→
2	Business interruption *(incl. supply chain disruption)*	34%	*2 (42%)*	→
3	Macroeconomic developments *(e.g. inflation, deflation, monetary policies, austerity programs)*	25%	*10 (11%)*	↑
4	Energy crisis *(e.g. supply shortage/outage, price fluctuations)*	22%	NEW	↑
5	Changes in legislation and regulation *(e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)*[2]	19%	*5 (19%)*	→

Top 10 risks in Italy

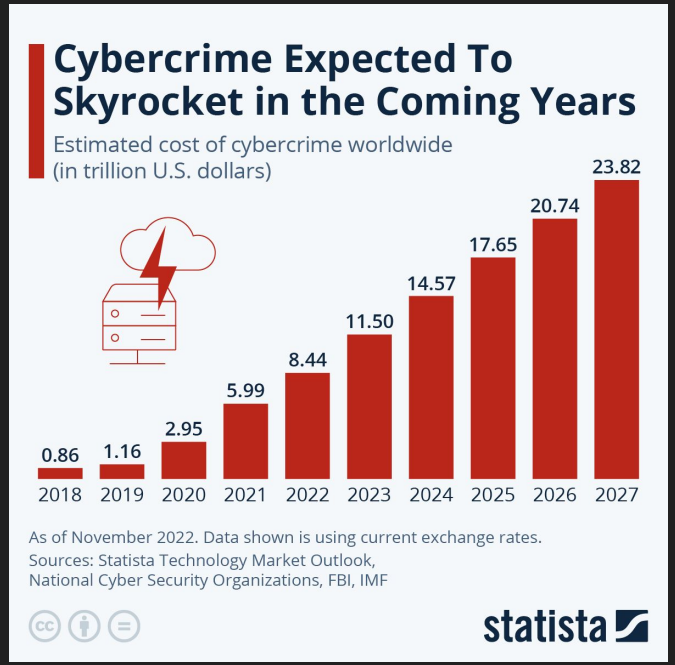
Source: Allianz Global Corporate & Specialty

Figures represent how often a risk was selected as a percentage of all responses for that country
Respondents: 38. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2022 rank	Trend
1	Cyber incidents *(e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)*	47%	*1 (52%)*	→
2	Business interruption *(incl. supply chain disruption)*	37%	*2 (45%)*	→
3	Energy crisis *(e.g. supply shortage/outage, price fluctuations)*	32%	NEW	↑
4	Macroeconomic developments *(e.g. inflation, deflation, monetary policies, austerity programs)*	21%	*10 (10%)*	↑
5	Climate change *(e.g. physical, operational and financial risks as a result of global warming)*	18%	*8 (13%)*	↑
6	Changes in legislation and regulation *(e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	16%	*4 (23%)*	↓
7	Natural catastrophes *(e.g. storm, flood, earthquake, wildfire, extreme weather events)*	13%	*3 (33%)*	↓
8	Fire, explosion	11%	NEW	↑
8	Market developments *(e.g. intensified competition/new entrants, M&A, market stagnation, market fluctuation)*	11%	*5 (16%)*	↓
8	Political risks and violence *(e.g. political instability, war, terrorism, civil commotion, strikes, riots, looting)*	11%	NEW	↑

Growth of Cyber Attacks

World



Italy

Impact of Cyber Attack on Industrial Systems

Operational Disruption

- production delays or shutdown
- significant financial losses

Loss of Sensitive Data

- Enable industrial espionage
- Intellectual Property Loss

Compromise Worker Safety

Environmental Impacts

- Public health or community safety

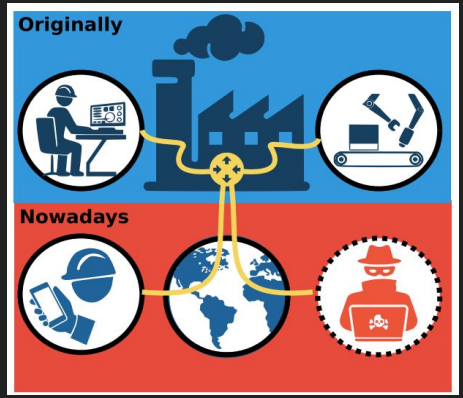
Financial and Reputational Losses

- Halted business
- Repair damages
- Rebuild customer trust

Exposure to Sanctions and Legal Liability

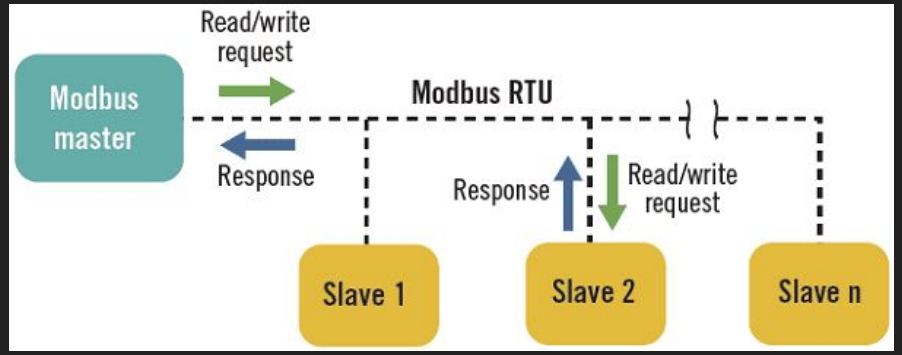
What is happening to ICS?

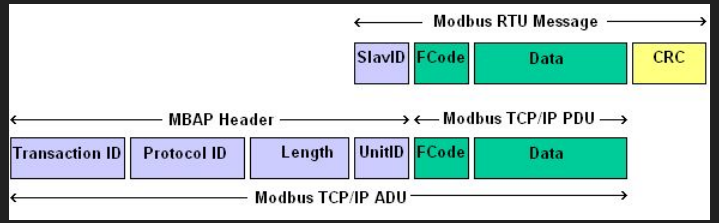
- Protocols designed to operate in air-gap environments
  - No Authentication
  - No Encryption
  - No Integrity protection
- Adapted over TCP/IP communication
- Connection of legacy devices to the Internet



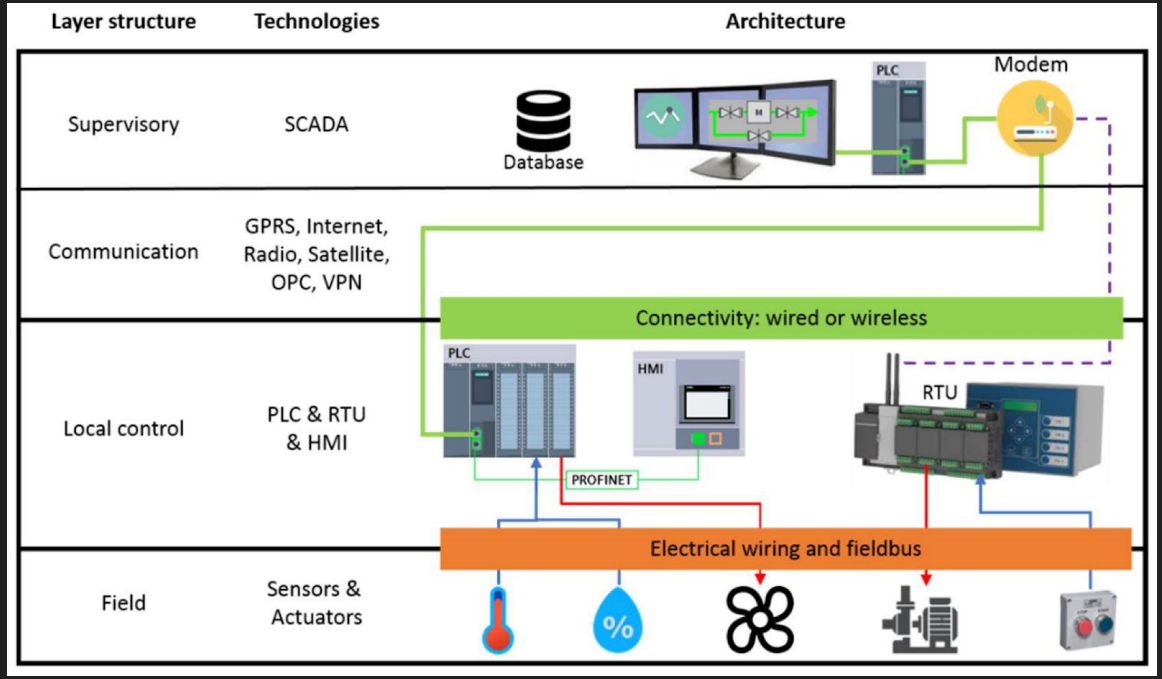
Protocol example: Modbus

- Simple Master/Slave communication
  - Read/Write operations
- Different versions
  - Serial
  - RTU
  - TCP
- No security by design



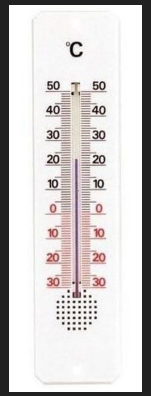


SCADA Hierarchy



Field Level

- **Sensor:**
  - Measuring physical
  - Generally continuous domain values
    (e.g., Temperatures, water level)

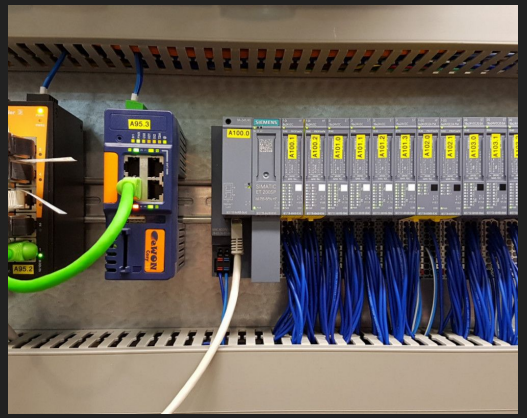


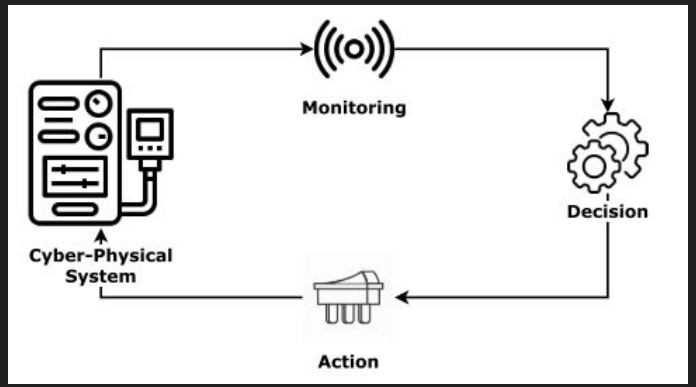
- **Actuator:**
  - Perform an “Action” on the system
  - Generally categorical values
    (e.g., Open/Close, ON/OFF)

Programmable Logic Controller (PLC)

- Receive **Input** and compute **Output**

- Ladder logic programming:
  - Instruction list
  - Function block diagram
  - Structured text
  - Sequential function charts





Human Machine Interface (HMI)

- Graphical Interface of the system
  - General used by field operators
- Report information about the system
  - System state
  - Alarms
  - Errors
  - …
- May also allow input

Supervisory Control And Data Acquisition (SCADA)

- Higher level of the ICS hierarchy
- Monitor and control acquired from field sites
- Manage the communication between the various devices
- Connection point for the remote operators

Differences from IT

- Patching and frequent updates are **not** well suited for control systems
- **Real-time availability**
- **Legacy systems** (Often no authentication or encryption)
- **Simpler network dynamics** (Fixed topology, regular communication, limited number of protocols,…)

Typical ICS Vulnerabilities

- **Communication links lack security features**
  - No encryption or authentication
    - Transmissions in plaintext

- **Lack of physical protection**
  - PLCs and RTUs easily accessible to tamper

- **Industrial components can have a long lifespan** (30+ years)
  - Range of different technological generations in one system

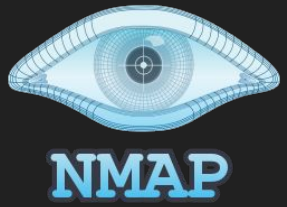
Are ICS really exposed?

The vulnerable ICS landscape

- ICS are continuously under scanning
  - Important to be aware
- Generally the first step to compromise a system
- Looking for industrial ports/services exposed
  - Leveraging tools *(e.g., nmap, zmap)*
  - Leveraging public available information *(e.g., Shodan, Censys)*
- This estimation may not be accurate
  - Exposed ≠ Operating
  - Limited information

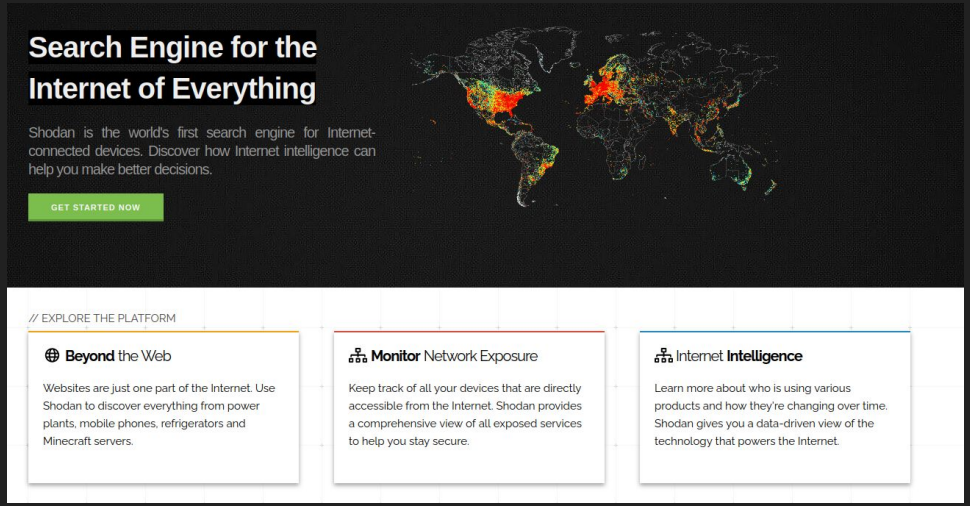
Are them enough?

- Active scanning influenced by
  - NAT
  - Firewall
  - other source-based filtering rules
- Active scanning can just identify exposed ports
- ICS using insecure communications may not be detected
- Results may be outdated
- Presence of Honeypot

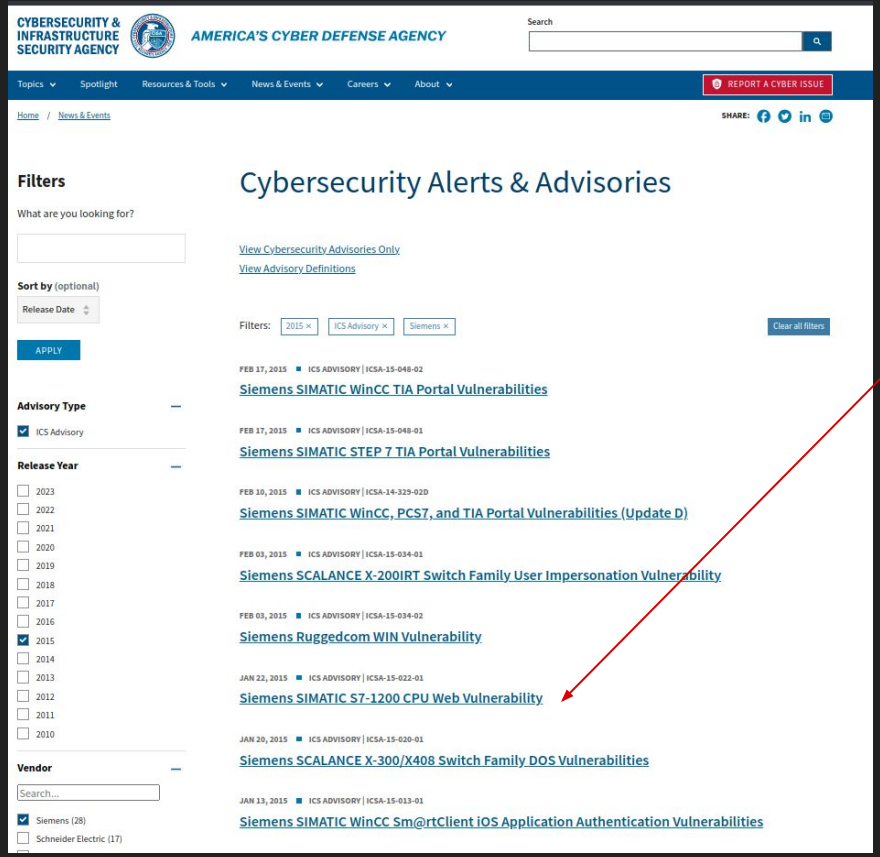


Shodan

- Most famous port scanner & Threat Intelligence Tool
- Many queries already implemented (link1, link2)
- Free student licence



ICS Vulnerabilities



ICS ADVISORY

Siemens SIMATIC S7-1200 CPU Web Vulnerability

Last Revised: August 29, 2018 **Alert Code:** ICSA-15-022-01

OVERVIEW

Siemens has identified an open redirect vulnerability in the SIMATIC S7-1200 CPU family. This vulnerability was reported directly to Siemens by Ralf Spenneberg, Hendrik Schwartke, and Maik Brüggemann from OpenSource Training. Siemens has produced an update that mitigates this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

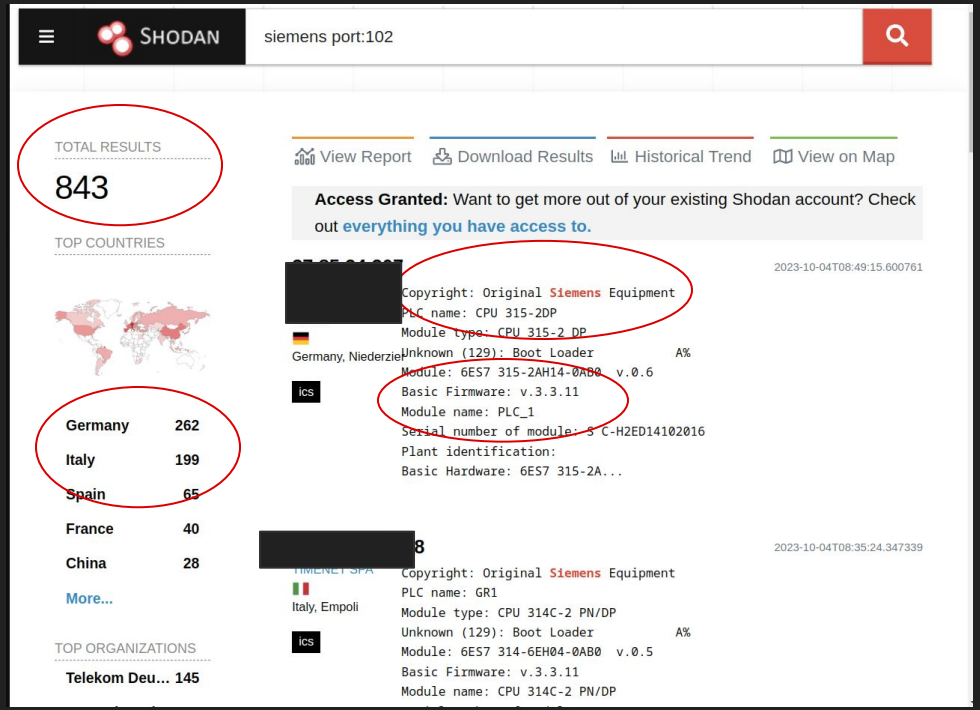
The following Siemens SIMATIC S7-1200 CPU family versions are affected:

- SIMATIC S7-1200 CPU family: All versions prior to V4.1

ICS Exploration

Common ICS ports

port 102	Siemens S7
port 502	Modbus
port 789	Red Lion
port 20000	DNP3
port 34980	EtherCAT
port 34962	PROFINET
port 44818	EtherNet/IP
port 47808	BACnet/IP

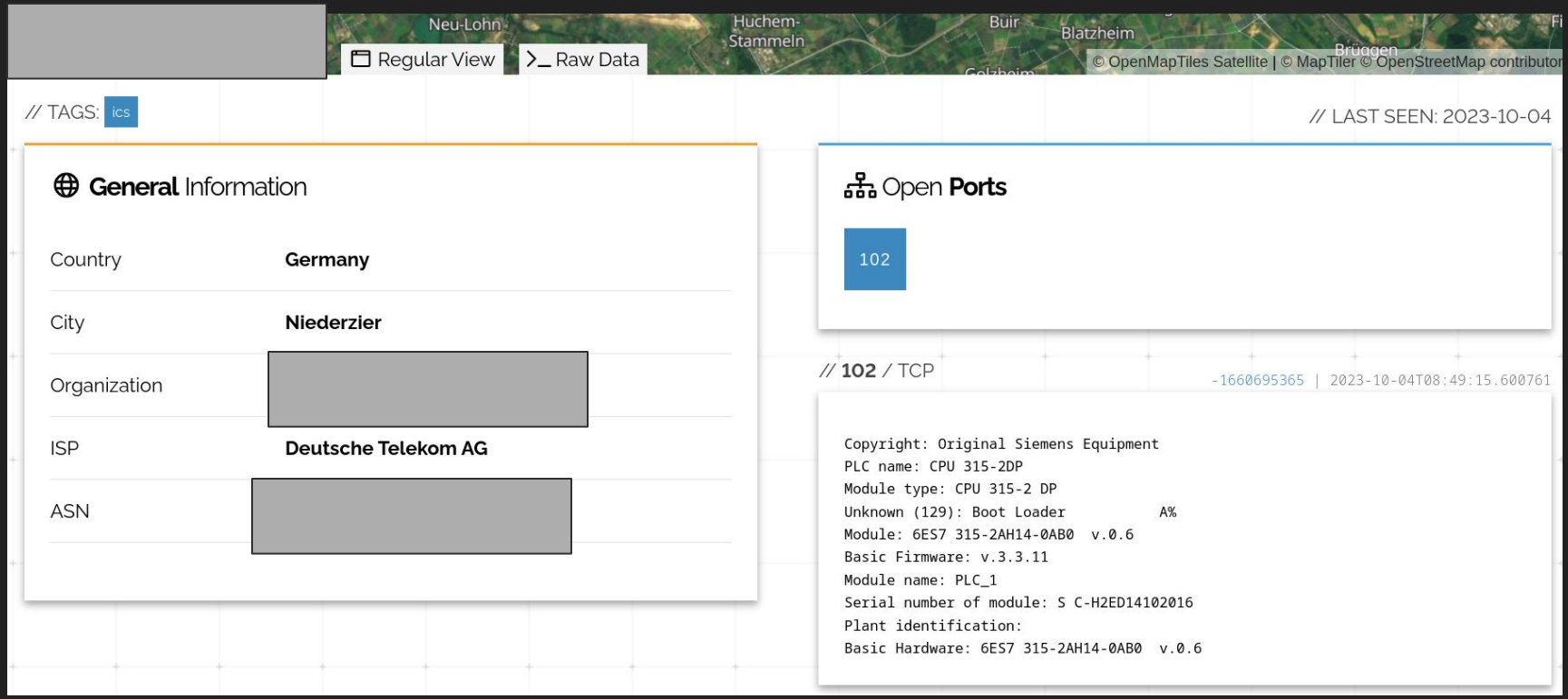


ICS Exploration

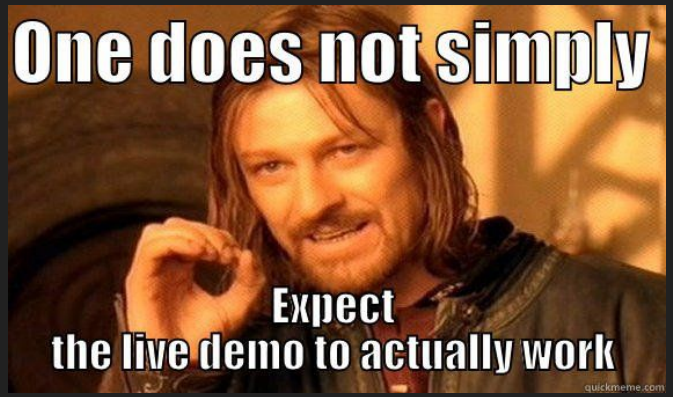
Common ICS ports

port 102	Siemens S7
port 502	Modbus
port 789	Red Lion
port 20000	DNP3
port 34980	EtherCAT
port 34962	PROFINET
port 44818	EtherNet/IP
port 47808	BACnet/IP

ICS Exploration



Demo time!


One does not simply
Expect
the live demo to actually work
quickmeme.com

Research Questions (2019)

RQ1) How often (insecure) ICS protocols are used over the Internet?

RQ2) How often are ICS services exposed to third parties?

RQ3) Is active-scanning based enumeration of hosts a good estimator of (vulnerable) industrial traffic use on the Internet?

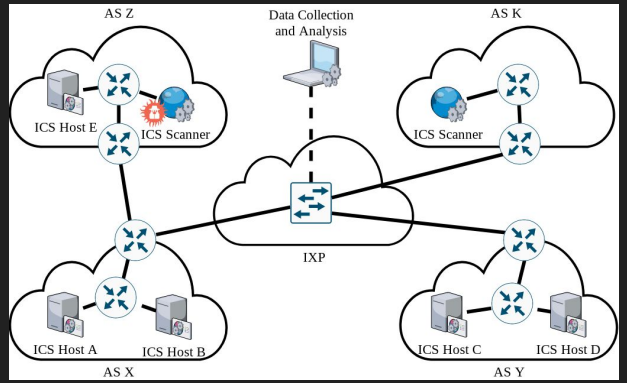
Traffic Analysis

Goal:

1) Measuring **unprotected Industrial Traffic** exposed over the Internet
2) Measuring **malicious activities** targeting Industrial Systems

- Traffic Collection at VSIX for 31 days
  (i.e., ~189GB and ~1.6B packets)

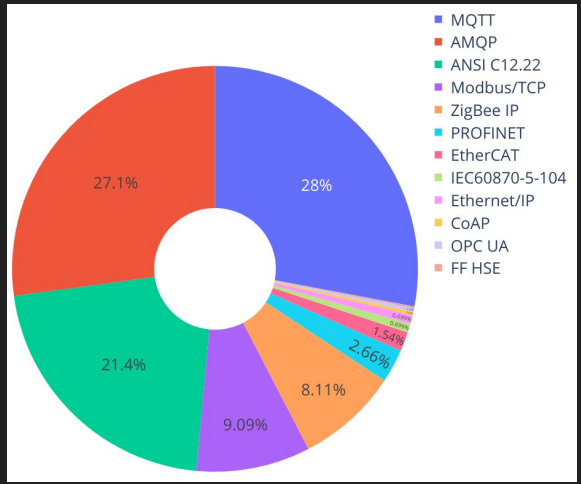
- 5094 Industrial packets
  - 86% Scanning Activities
  - 14% Legitimate Traffic



Legitimate Industrial Traffic

RQ1) *How often (insecure) ICS protocols are used over the Internet?*

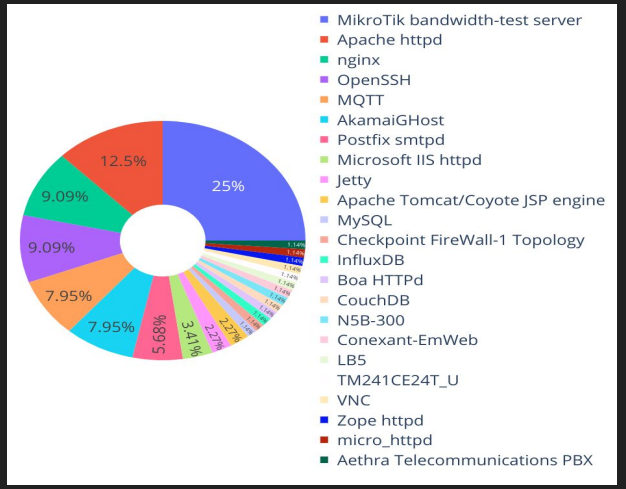
- 168 ICS hosts detected
  - 8 using two differents ICS protocols
- 12 different ICS protocols detected
  - 6 of which does not have any security feature
  - 59 hosts use such insecure protocols
  - **75.6% of the hosts leverage insecure communication**

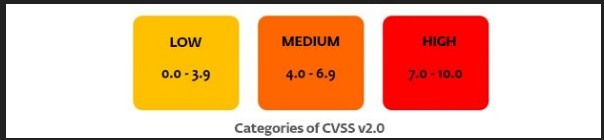


Exposure to Third-Parties

RQ2) *How often are ICS services exposed to third parties?*

- Detected ICS hosts queried on *Shodan*
- 7% of the hosts detected have ICS ports exposed
- 64.3% of the hosts detected have IT ports exposed
  - IP-cameras, routers, alarm systems, energy monitoring
  - 11 hosts with at least one known vulnerability (CVE)
  - 9 of them have one CVE with a CVSS greater than 7.0





Comparison with Shodan

RQ3) *Is active-scanning based enumeration of hosts a good estimator of (vulnerable) industrial traffic use on the Internet?*

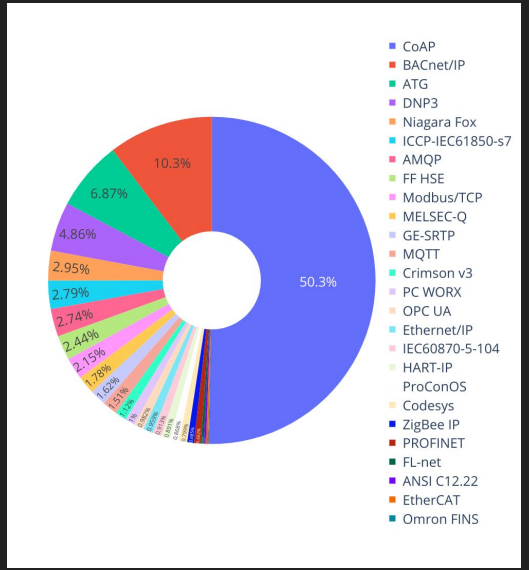
- Collection from *Shodan* of the ICS hosts belonging to an AS connected to the IXP
  - Gathered all italian ICS hosts indexed
  - Filtered out the ones that do not belong to an AS directly connected to the IXP
- Shodan detected 440 hosts compared to 168
- The traffic-based approach detected more hosts than Shodan for 6 ICS protocols
- Just 1.2% of the hosts exchanging ICS traffic were also detected by Shodan

Scanning Activities

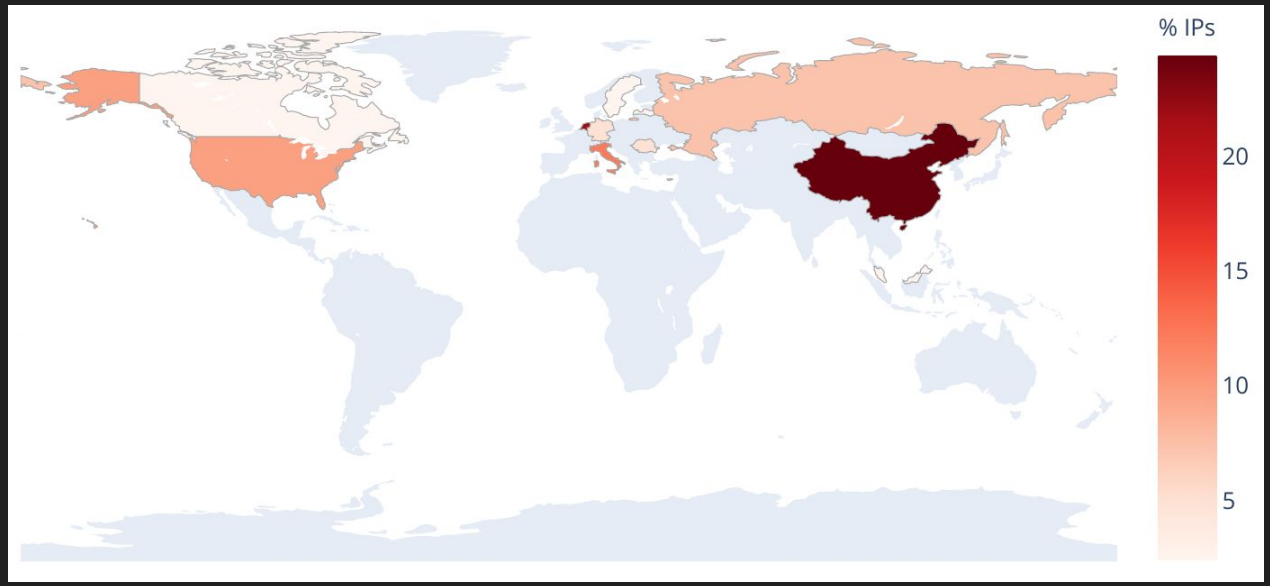
- All the ports of interest received at least one scan

- Almost 30% of the scan packets were crafted with protocol-specific requests
  - e.g., GET /.well-known/core for CoAP
  - The remaining were simple SYN packets

- 442 different IPs looking for exposed ICS ports
  - origin from 30 different Countries
  - 55.9% Benign (15 research companies)
  - 9.3% Malicious (e.g., a Mirai infected devices)



Scanning Activities Origin



How we protect?

Solution #1 - Security by Design

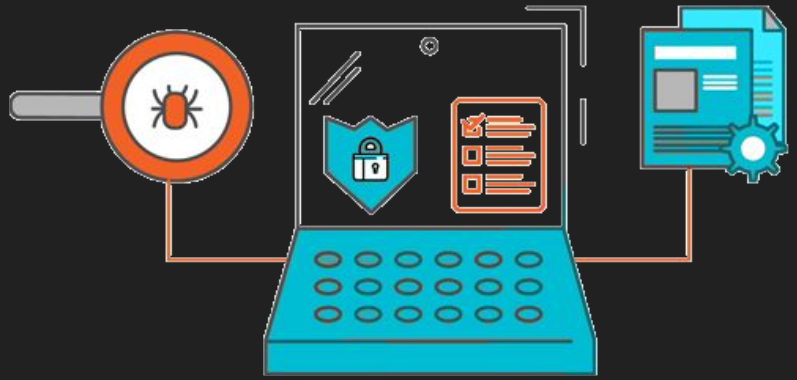
- Follow the security standard directives
  - ISA/IEC 62443, NIST, NERC
- Follow a reference architecture
  - e.g., Purdue model
- Implement all the security practices
  - Access control, data storage, secure communication

Challenges

- What about existing architectures (the majority)
- Not always suitable in all environments

Solution #2 - Continuous Security Assessment

- Perform Vulnerability Assessment
- Perform Penetration test
- Perform Assets Inventory
- Perform Risk Management

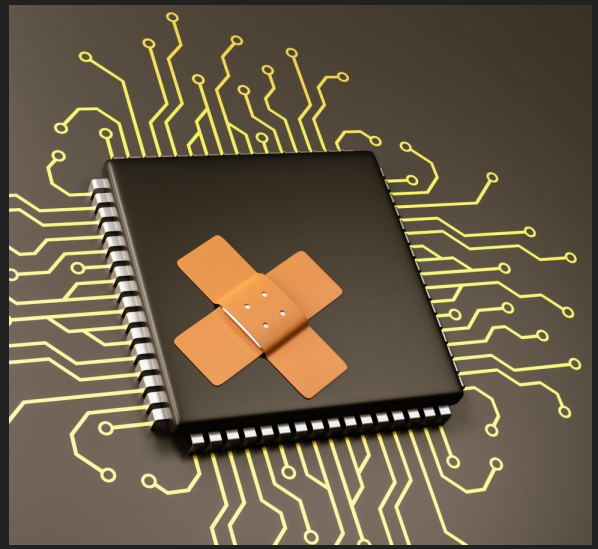


Challenges

- Risk of process interruption
- Require OT specific approaches (not so frequent)
- Valid only the day of the test

Solution #3 - Improving Security Robustness

- Patching vulnerabilities
- Securing the communication protocols
- Keep the system up to date

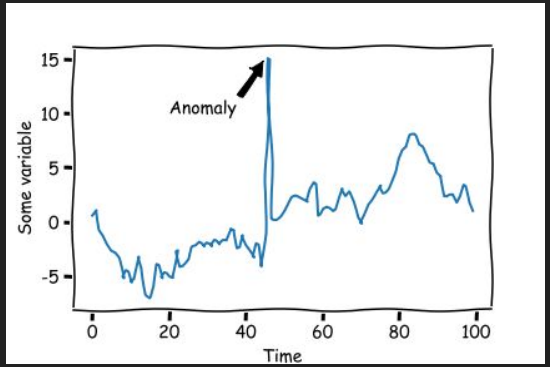


Challenges

- Upgrading or patching not always possible

Solution #4 - Leverage Solution on-top

- Implementation of Intrusion Detection Systems
- Implementation of Honeypot
- Implementation of proactive protection approaches



Challenges

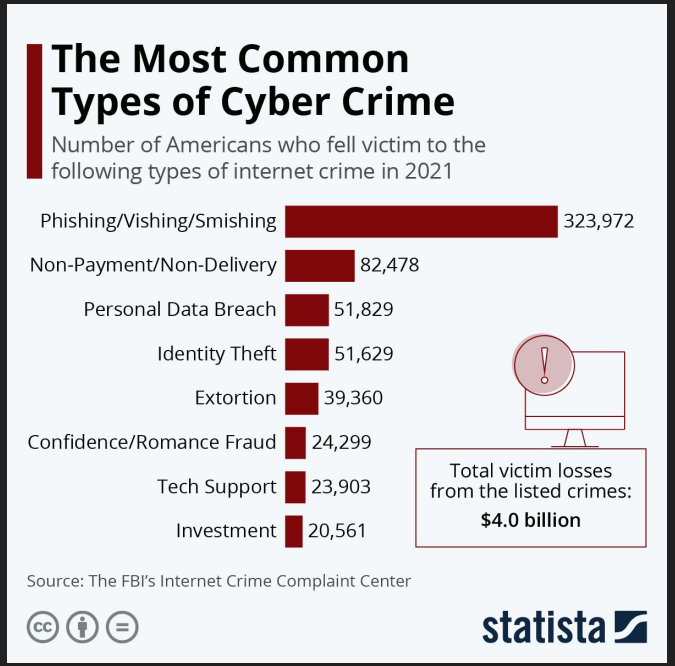
- Very complex solution
- May be costly and requires infrastructures modification

Solution #5 - Security Training

- Provide continuous education to employees
- Continuous test to assess employees awareness
  - Phishing campaigns
  - Password

Challenges

- Human factor will **always** be present
- Comprehension of complex arguments
- Things change very quickly



Lesson Learned

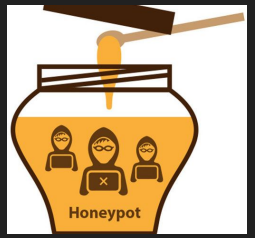
- Trend of Cyberattacks is growing
  - Industry represent a profitable target for attackers
- No solution will completely secure the system
  - Combination of them is important
  - Industrial security requires specific approaches
- Cybersecurity plays a key role in Industry business
  - Cyber security investments are necessary
- Better safe than sorry
  - “Prevenire è meglio di curare”

Thank you for your attention!

spritzmatter

your cybersecurity partner for innovation

Honeypot?

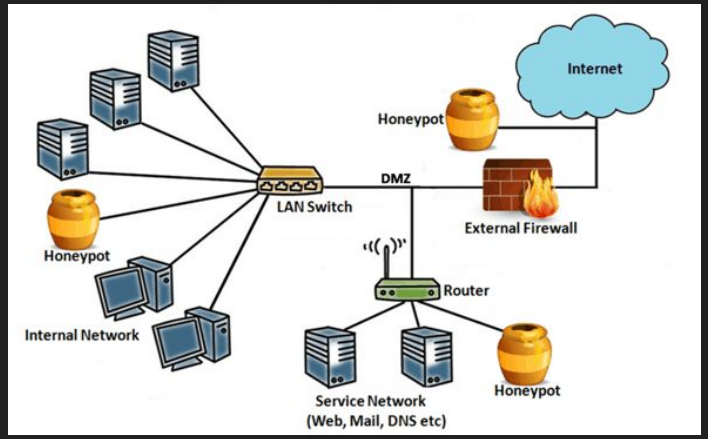


Multiple scopes:

- Deceive the attacker
- Collect data
- Catch suspicious activities

- Difficult to replicate a real system

- *Shodan Honeyscore* does not help



Vulnerability Assessment & Penetration Test (VAPT)

Vulnerability Assessment is a snapshot of the infrastructure vulnerabilities

- Identify CVEs and corresponding CVSS
- Analyze is known vulnerabilities apply on the assets
- Is followed by a risk management plan

Penetration test is an attack simulation

- Generally performed by red teams
- Goal is to see what an attacker can do
- Support the infrastructure robustness