VERSIVO
ACTIVE CYBER DEFENSE

Approaching OT/ICS Security

Cybersecurity from the Attacker's point of view

www.versivo.it

VERSIVO: Active Cyber Defence

VERSIVO operates in order to **make Cyberspace a SAFE place** where companies and their people can integrate, interconnect and use technology without worry.

VERSIVO, moreover, tends to upset cost/benefit advantages of cyber threats, depriving them naturally and implicitly of any advantage.

The vision that guides **the future of VERSIVO** is to **create a culture for the correct handling of Cyber Risk as a competitive advantage** in the business market and civic **value in boosting sensitivity to built-in/by design** Cybersecurity in the consumer market, thus triggering a virtuous and self-powered process.

# whoami

Andrea Dainese - vCISO

- Senior Network & Security Architect with 15+ years' experience in securing complex IT infrastructures
- Focused on cyber security strategies, GDPR/ISO27001 compliance and Automation
- VERSIVO Incident Response Team
- Cisco (CCIE), VMware, Red Hat… certified
- Privacy and digital security evangelist – expert counselor-mediator in Cyberbullying (https://adainese.it)

andrea.dainese@versivo.it

# whoami

Rocco Sicilia - Ethical Hacker

- Senior Cloud & Security Architect with 15+ years' experience in management of complex IT infrastructures
- Focused on offensive security strategies and system hacking
- VERSIVO Red Team
- Cyber Security Researcher (https://roccosicilia.com)

rocco.sicilia@versivo.it

AGENDA

Agenda

- > Cybercrime and Industry 4.0
- > Peculiarities of OT/ICS devices
- > Risk Analysis and Management
- > Supply Chain
- > Where to start from: a security roadmap

Agenda

Issues

- Shadow OT
- Weak protocols
- Sensitive communications
- Certified environment
- Remote maintenance
- Removable storage

Solutions

- Asset discovery & inventory
- Secure programming
- Industrial networks availability
- Malware prevention, patching, virtual patching and backup
- Isolation and secure access

OBJECTIVES

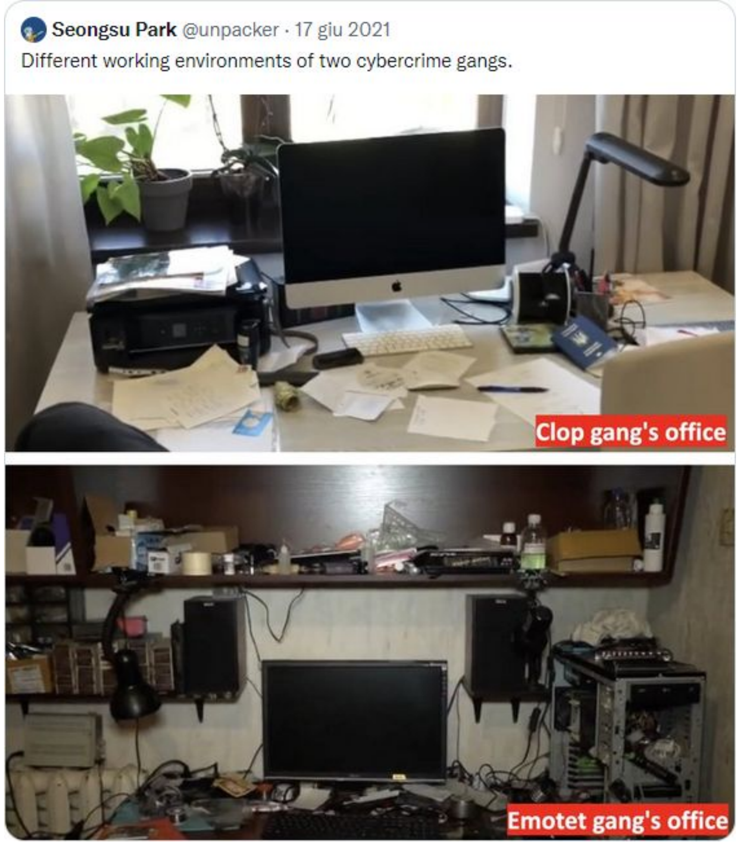
Objectives

Knowledge:

- Threat actors, business models and attack vectors.
- Current Cyber attacks targeting IT and OT.
- OT and IT peculiarities.
- Regulations, standard and guidelines.
- Security measures, tools and strategies.
- Approaching Cybersecurity with a continuous improvement risk based approach.

CYBERCRIME

Working Environments



Seongsu Park @unpacker · 17 giu 2021

Different working environments of two cybercrime gangs.

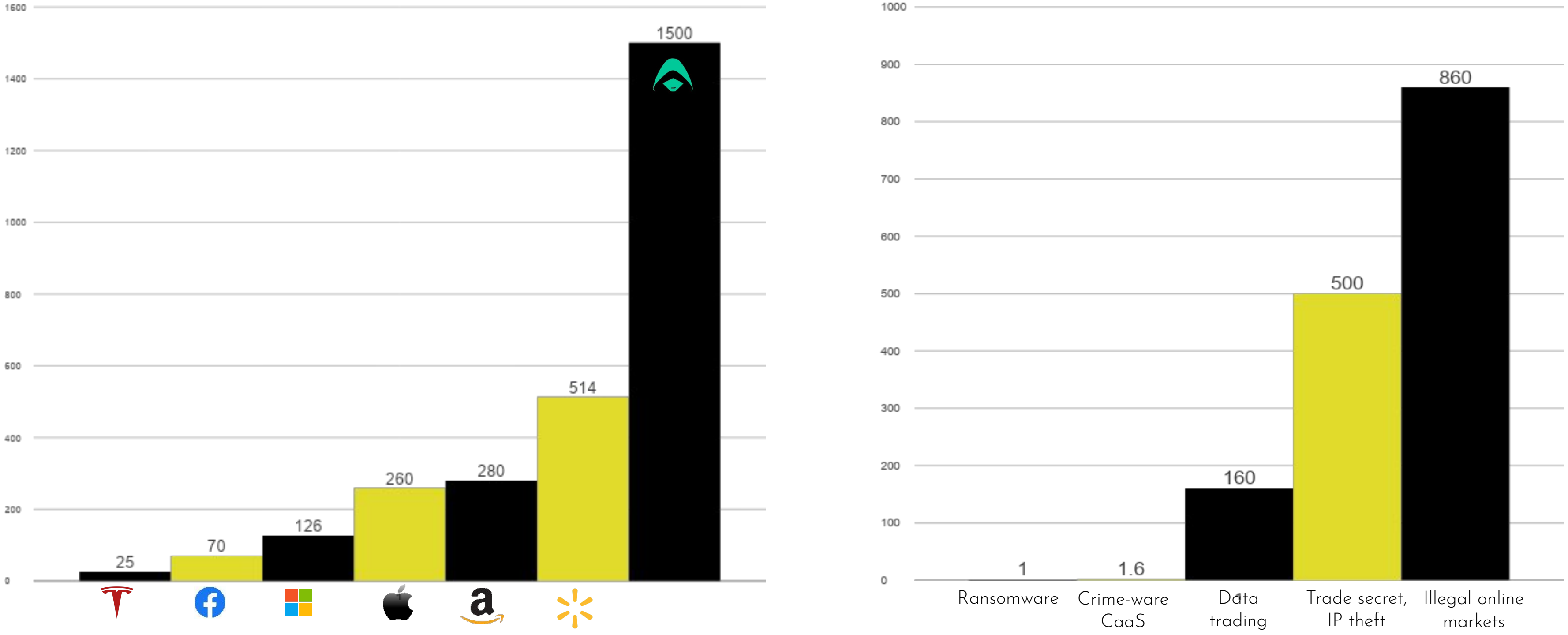
https://twitter.com/malwaretechblog/status/1405632693874823168

Threat actor examples

Actor	Goal	Target	Budget
State-Sponsored Actors	Espionage, theft, sabotage	People, Corporations, critical services	Very High
Cyber Terrorists	Sabotage	Critical services	High
Cybercriminals (organized)	Financial gain (extortion)	People, Corporations	Medium to High
Hacktivists	Sabotage, exposing data	Anyone/anything	Low to Medium
Insiders	Sabotage, financial gain	Same organization	Low with privileged access

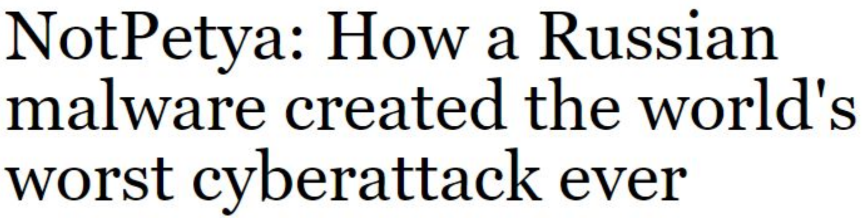
Cybercrime revenue

2019 Companies and Cybercrime annual revenue in billions USD



https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times-bigger-than-walmarts

Famous Cyber Attacks



NotPetya: How a Russian malware created the world's worst cyberattack ever

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

Boeing Is The Latest WannaCry Ransomware Victim

The return of WannaCry makes Honda manufacturing plant Wannacry

Jun 21, 2017
NEWS by Max Metzger

Maersk: Springing back from a catastrophic cyber-attack

Rae Ritchie — August 2019

- Exploit SMBv1 vulnerability (Ethernalblue)
- Data encryption
- Spread out to other systems (worm)

Famous Cyber Attacks

How Stuxnet worm took out key Iranian nuclear facility in 2010

By Mark Saunokonoko • Senior Journalist | 2:58pm Apr 12, 2021

- Exploit 4 Zero Day Vulnerabilities
- Developed for Air Gapped targets
- Supply Chain attack
- Alterates centrifuges spin
- Provides false feedback to monitors

How hackers attacked Ukraine's power grid: Implications for Industrial IoT security

The December 2015 cyberattacks on Ukranian power utilities were rare in that actual damage was inflicted. But there's ample evidence of widespread infiltration into organisations' operational systems.

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

Threat Research Blog

Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure

December 14, 2017 | by Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer

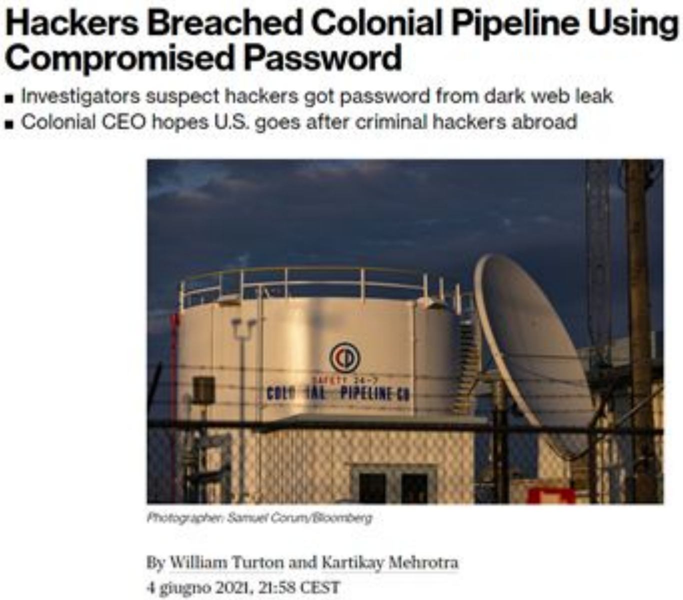
- Attack framework (development kit)
- Reprogram the SIS to allow an unsafe state
- Reprogram the SIS to allow an unsafe state – while using the DCS to create an unsafe state or hazard

In Florida city, a hacker tried to poison the drinking water

By FRANK BAJAK February 8, 2021

- Compromised Wordpress website
- Lateral movement to OT network
- Manual control HMI via TeamViewer
- Raise NaOH from 100 to 1100ppm

Famous Cyber Attacks



Hackers Breached Colonial Pipeline Using Compromised Password

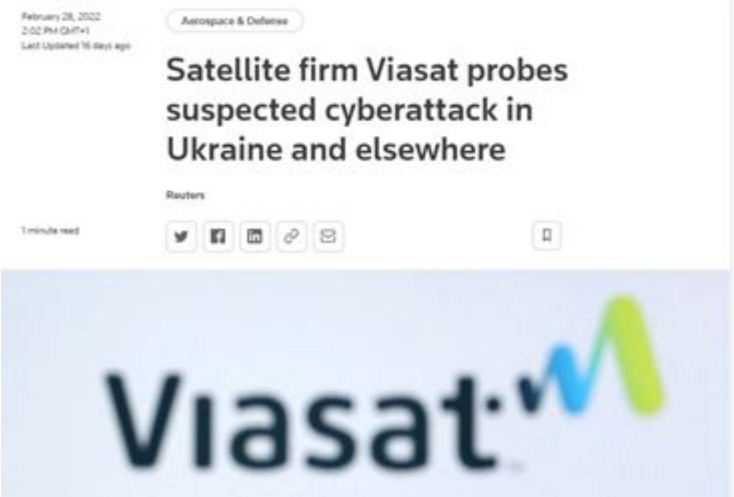
- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

Photographer: Samuel Corum/Bloomberg

By William Turton and Kartikay Mehrotra
4 giugno 2021, 21:58 CEST

- Databreach + Password reuse
- Known vulnerable VPN (CVE-2021-20016)
- Ransomware attack type
- OT shutted down for precautions
- Kick back attack

https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked...



February 28, 2022
2:02 PM GMT+1
Last Updated 16 days ago

Aerospace & Defense

Satellite firm Viasat probes suspected cyberattack in Ukraine and elsewhere

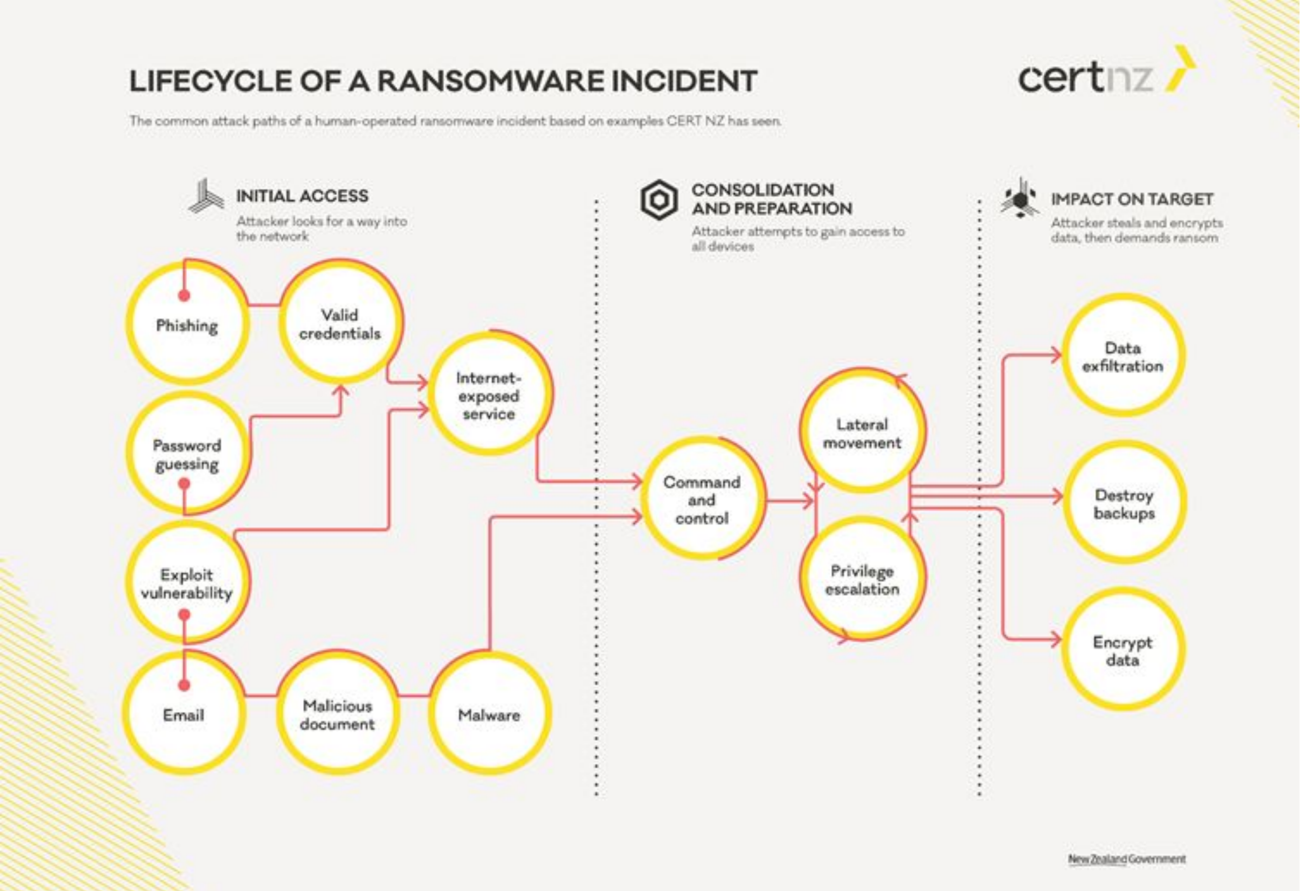
Reuters

1 minute read

- Tens of thousands of terminals are offline
- Impact on civil satellite network (neither maritime nor aviation)
- Misconfiguration in the "management section"
- Hackers remote access into the modems
- Affected devices need to be manually reprogrammed

https://www.reversemode.com/2022/03/satcom-terminals-under-attack...

Attack Vectors



LIFECYCLE OF A RANSOMWARE INCIDENT

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.

certnz

INITIAL ACCESS
Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices

IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom

New Zealand Government

https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

How ransomware happens and how to stop it:

- This diagram shows the common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen. The diagram is split into three phases.
- Get initial access via phishing, vulnerable systems, credential theft, supply chain.
- Lateral movement to interesting networks.
- Execution

WHY

VERSIVO
ACTIVE CYBER DEFENSE

Cyberspace

- Provides tools, methods and interactions to get more opportunities
- It is considered the fifth theater of warfare

The remedy

- Find the correct proportion between freedom, even unconscious, and security

PECULIARITIES OF OT/ICS DEVICES

Peculiarities of OT/ICS devices

Weaknesses of OT/ICS devices:

- Designed for «availability»
- Extremely sensitive to Ethernet disruptions and overloads.
- Communications do not guarantee confidentiality, integrity, and availability (unauthenticated clear text protocols).
- Long term life
- Not subject to the same life cycle as IT components (outdated vulnerable and unpatchable software)

Peculiarities of OT/ICS devices

Common issues:

- Shadow OT
- Weak protocols
- Sensitive communications
- Long term life devices
- Certified environment
- Remote maintenance
- Removable storage

Common issues: shadow OT

Known (maybe)

- PLC & HMI
- IoT & sensors
- SCADA Networks
- Maintenance links

Unknown

- Network communications
- Field network
- Embedded Wifi features
- Undeclared remote access devices (4G, Dialup, Internet VPN)
- Cloud based telemetry
- Forgotten devices
- Passwords (weak/default)
- Vulnerabilities
- …
- **Risk (unmanaged)**

Common issues: weak and sensitive protocols

Designed for

- "Availability"
- Real Time communications
- Long term life

Weakness

- Sensible to network disruptions
- Expose sensitive data (registry)
- Unauthenticated
- No data integrity check
- Well known vulnerabilities
- …
- **Unexpected behaviours**

Common issues: long term life

IT

- Cheap (relatively)
- 3-7 years life span
- Frequent OS updates
- +30 years of experience in attacking and securing
- …
- **Reliable and secure**

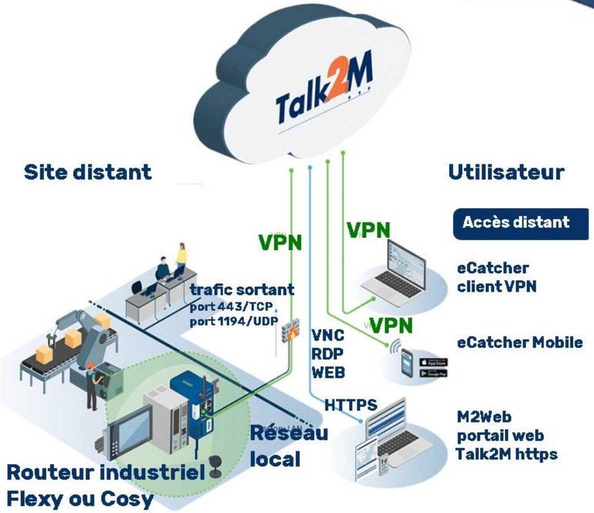
OT/ICS

- Expensive
- 10-20 years life span
- “do-not-touch” policy (certified installation)
- IT attacks can be reused
- …
- **Legacy, weak and harmful**

Common issues: remote maintenance

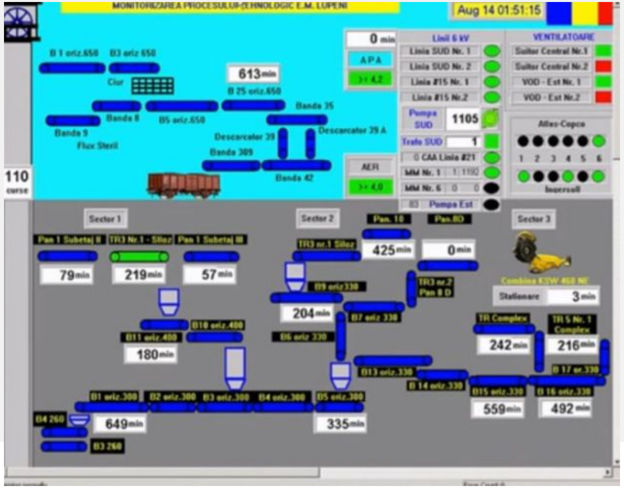
Blackbox VPN devices

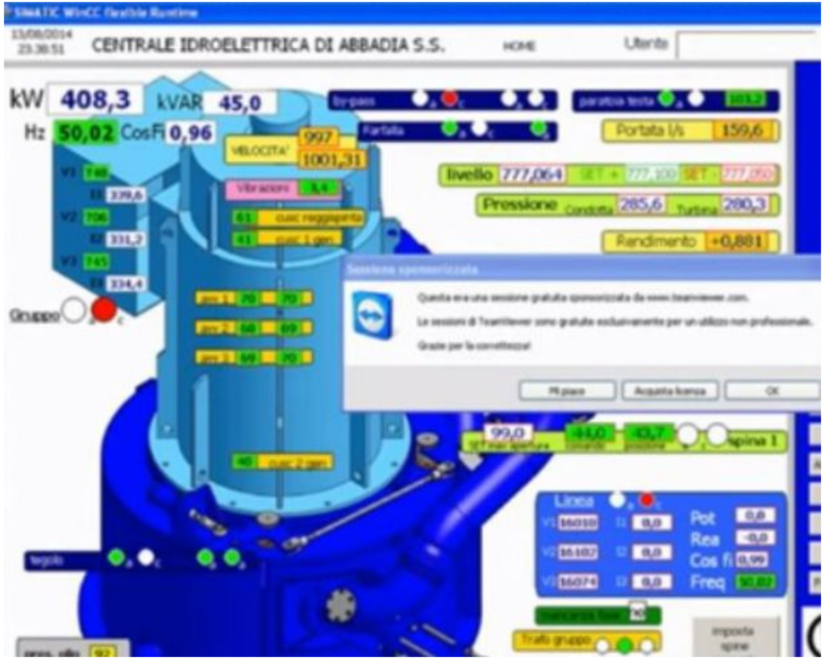
- Remote maintenance
- Uncontrolled access
- Supply chain attack



Common issues: home made remote maintenance

- Remote assistance (Team Viewer)
- Exposed (vulnerable) HMI (RDP, VNC)





Sessione sponsorizzata

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

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

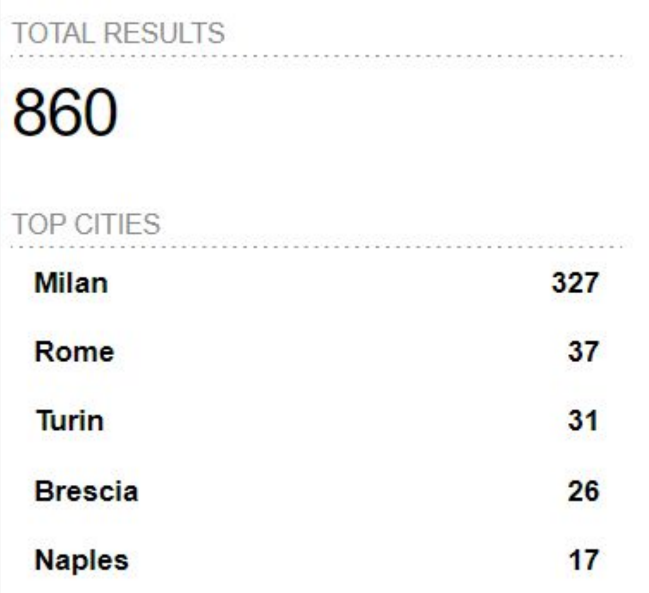
Grazie per la correttezza!

https://www.youtube.com/watch?v=hMtu7vV_HmY

Finding OT/ICS devices

Siemens S7 devices

```
port:102 country:"IT"
```



TOTAL RESULTS

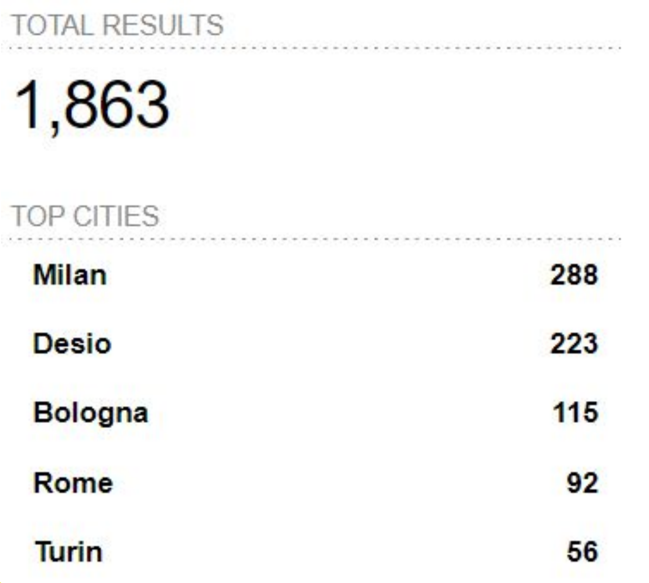
860

TOP CITIES

Milan	327
Rome	37
Turin	31
Brescia	26
Naples	17

Modbus devices

```
port:502 country:"IT"
```



TOTAL RESULTS

1,863

TOP CITIES

Milan	288
Desio	223
Bologna	115
Rome	92
Turin	56

Common issues: removable storage

USB storage:

- Infected devices
- Unauthorized devices
- Malicious devices

Risks for OT/ICS devices

Risks

- **Espionage:** theft of information, patents, production methods, recipes.
- **Sabotage:** systems tampering, damage to people or things, modification to the production cycle.
- **Estorsion:** theft and seizure of data and systems.
- **Compliance:** Cyber-Insurance exclusion, law violation.
- **Physical security:** disruptions and attacks can lead to physical damages.

Threat Actors

- **Governments/Terrorists:** financing through extortion, espionage, and sabotage..
- **Cyber criminals:** business models based on commissioned theft, extortion.

SUPPLY CHAIN RISKS

Supply Chain Risks

Supply Chain Attacks:

- **Connected suppliers:** attackers can move from a compromised supplier to the Organization (information theft, lateral movement)
- **Material supplier:** attacks targeting suppliers can impact the business of the Organization (reflected attack).
- **Outsourcing:** attacks targeting partners can impact the business of the Organization (reflected attack).

Examples:

- Attackers can use the remote assistance connections to spread out into the Organization.
- Attacks targeting the material supplier con stop the supply of raw materials.
- Attacks targeting the outsourced warehouse can stop sales.

HOW

VERSIVO
ACTIVE CYBER DEFENSE

« he who knows his enemy and knows himself can face a hundred battles without fear »

Sun Tzu, **The Art of War**

STANDARDS, FRAMEWORKS AND REGULATIONS

VERSIVO
ACTIVE CYBER DEFENSE

Standards and Frameworks

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

[Framework for Improving Critical Infrastructure Cybersecurity (NIST)](#)

CIS®

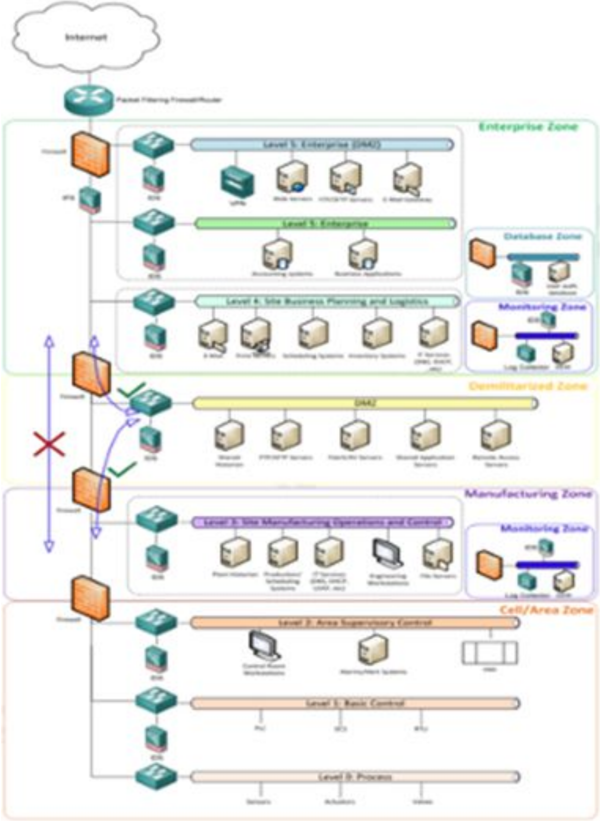
[CIS Controls](#)

International Organization for Standardization
ISO
31000
Risk-Management

UNI ISO 31000:2018 Risk management – Guidelines

NIST
National Institute of Standards and Technology

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations ([800-171](#) & [172](#))



[Secure Architecture for Industrial Control Systems (Purdue Model)](#)

Regulations

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

- Directive (UE) 2016/1148 (NIS Directive)
- Regulation (EU) 2019/881 (EU Cybersecurity Act)
- NIS2 Directive (in progress)
- MSC-FAL.1/Circ.3 Guidelines (IMO)
- Resolution MSC.428(98) (IMO)

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

Cybersecurity Act lays 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.)

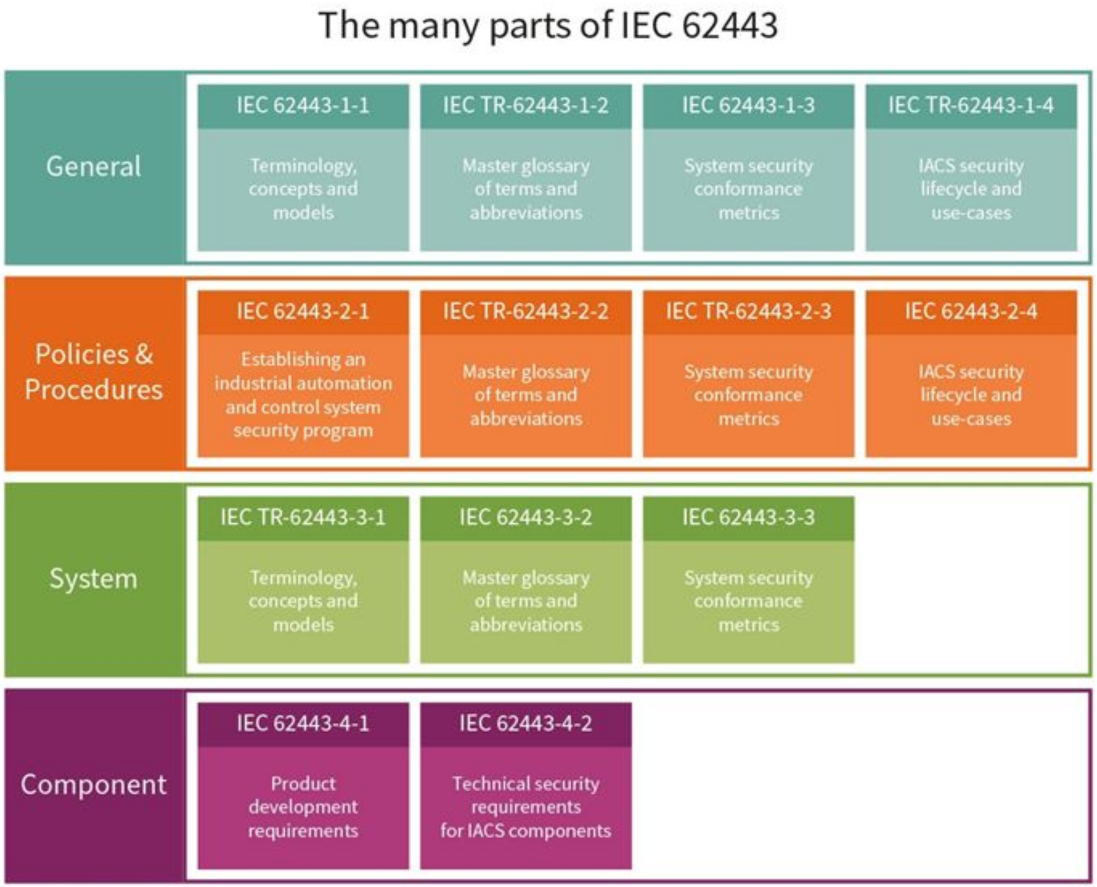
The ISO/IEC 15408/18045 Common criteria and evaluation methods, IEC 62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components, EN 303-645 cybersecurity for consumer IOT can constitute the basis for all cybersecurity evaluation.

- Cybersecurity Maturity Model Certification (CMMC)

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

VERSIVO
ACTIVE CYBER DEFENSE

IEC62443 Standard



The many parts of IEC 62443

General	IEC 62443-1-1 Terminology, concepts and models	IEC TR-62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC TR-62443-1-4 IACS security lifecycle and use-cases
Policies & Procedures	IEC 62443-2-1 Establishing an industrial automation and control system security program	IEC TR-62443-2-2 Master glossary of terms and abbreviations	IEC TR-62443-2-3 System security conformance metrics	IEC 62443-2-4 IACS security lifecycle and use-cases
System	IEC TR-62443-3-1 Terminology, concepts and models	IEC 62443-3-2 Master glossary of terms and abbreviations	IEC 62443-3-3 System security conformance metrics	
Component	IEC 62443-4-1 Product development requirements	IEC 62443-4-2 Technical security requirements for IACS components		

VERSIVO
ACTIVE CYBER DEFENSE

IEC62443 Standard

IEC 62443 is a set of security standards for the secure development of Industrial Automation and Control Systems (IACS).

It provides a thorough and systematic set of cybersecurity recommendations. It's used to defend industrial networks against cybersecurity threats.

Security Levels

- 0: No specific requirements or security protection are necessary.
- 1: Protection against unintentional or accidental misuse..
- 2: Protection against intentional violation using simple means.
- 3: Protection against intentional violation using sophisticated means.
- 4: Protection against intentional attacks with sophisticated means with extended resources..

Requirements (controls depends on SL)

- 1. Identification and Authentication Control: Identify and authenticate all users.
- 2. Use Control: Enforce the assigned privileges of an authenticated user to perform the requested action.
- 3. System Integrity: Ensure the integrity of the IACS to prevent unauthorized manipulation.
- 4. Data Confidentiality: Ensure the confidentiality of information on communication channels and in data repositories.
- 5. Restricted Data Flow: Segment the control system via zones and conduits to limit the unnecessary flow data.
- 6. Timely Response to Events: Respond to security violations.
- 7. Resource Availability: Ensure the availability of the control system against the degradation or denial of essential services.

Additional guidelines:

- CWE
- SEI CERT
- OWASP
- DISA STIG
- PLC Security

WHAT

Security measures

Organizational measures

- Physical and logical audit
- Risk based thinking
- Awareness & Education
- Subcontractor requirements (i.e. ISO27001)
- Subcontractor audit (GDPR Art.28)

Technical measures

- Asset discovery & inventory
- Secure programming
- Industrial networks availability
- Malware prevention, patching, virtual patching and backup
- Isolation and secure access

OT/ICS Assessment

> **Physical and logical audit**
> **Asset discovery & inventory**
> **Network communication assessment**

1. Identify devices (name, version, vulnerabilities…)
2. Identify running network protocols
3. Risk assessment (define impact and likelihood)
4. Automate the process

> Awareness & Education

1. One to one interview
2. Identify risky behaviour (include physical risk)
3. Define policies, procedures and guidelines
4. Educate

Subcontractors and suppliers

- > **Subcontractor requirements (i.e. ISO27001)**
- > **Subcontractor audit (GDPR Art.28)**

1. Regularly audit subcontractors and suppliers
2. Analyze risk
3. Include them in the business continuity plan

Technical measures and caveats

- **Secure programming:** https://plc-security.com/
- **Ethernet networks:** fail by design (STP convergence)
- **Protect industrial networks:**
  - Anti malware solutions (for Windows based HMI)
  - Virtual patching (industrial firewall)
  - Network segregation and isolation (firewall and host based firewall)
  - Secure and monitor remote access (firewall + IPS)
- **The Purdue Model for Control Hierarchy (ISA-99)**
- **The Air Gap myth**

WHERE TO START FROM

IT/OT Convergence

IT: the CIA triage

- **C**onfidentiality: only authorized people can access data
- **I**ntegrity: data is trustworthy and free from tampering
- **A**vailability: data is available to authorized users

OT: the SRP+C triad

- **S**afety: ensure safety for people, facilities, operations.
- **R**eliability: consistent results, maintaining operations.
- **P**roductivity: optimal use
- **C**ustomization: there is no one size fits all

IT/OT Convergence

IT: the CIA triage

- **C**onfidentiality: onl authorized peo access data
- **I**ntegrity: data trustworthy and from tampering
- **A**vailability: da available to authorized user

Convergence Point

- Safety First
- Risk Appetite determines the needed actions
- Understand stakeholder needs and expectations

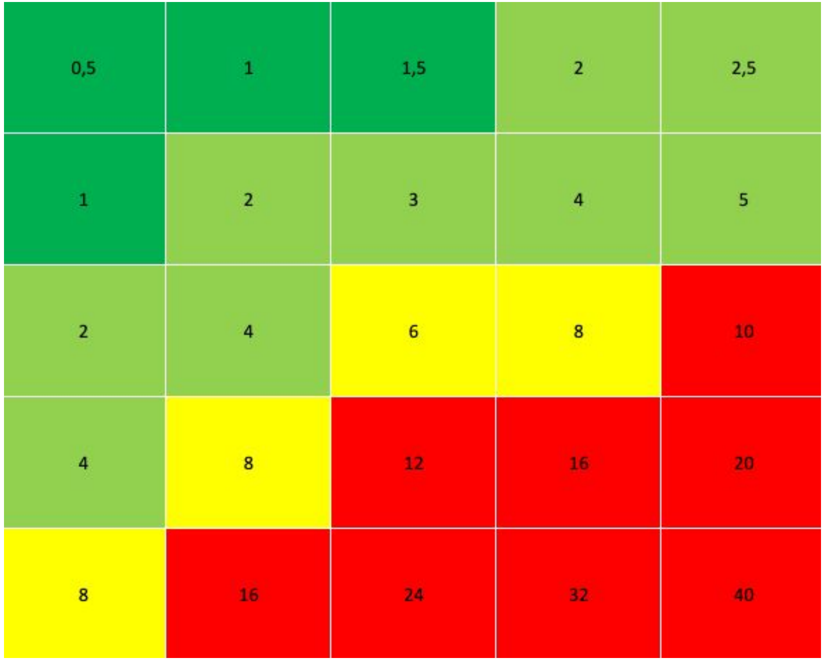
OT: the SRP+C triad

Safety: ensure safety people, facilities, erations.
iability: consistent ults, maintaining erations.
ductivity: optimal
stomization: there o one size fits all

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.

Risk management



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

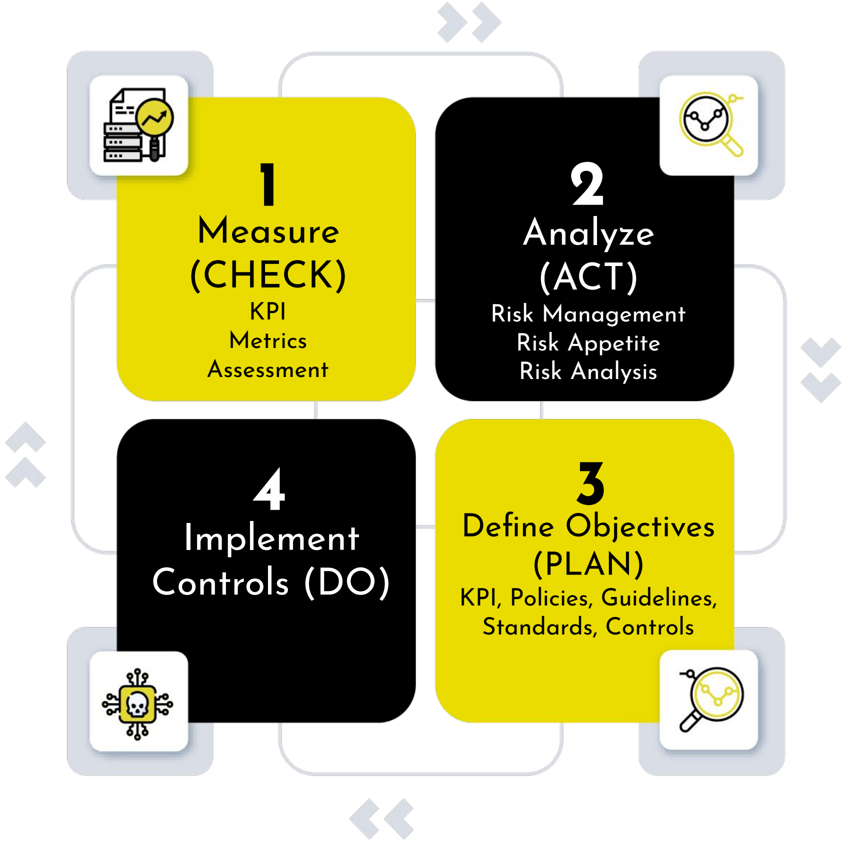
Cybersecurity Governance

Cybersecurity Governance:

- Security posture measure (asset discovery, vulnerability assessment…)
- Risk Analysis (Risk Management)
- Define a strategy (procedures, guidelines, standard, security controls and KPI)
- Implement and Govern

- Companies change
- The geopolitical context changes
- The regulations change
- Market perception and requirements change

Unplanned one-shot activities quickly lose their effectiveness



1
Measure
(CHECK)
KPI
Metrics
Assessment

2
Analyze
(ACT)
Risk Management
Risk Appetite
Risk Analysis

3
Define Objectives
(PLAN)
KPI, Policies, Guidelines,
Standards, Controls

4
Implement
Controls (DO)

VERSIVO

ACTIVE CYBER DEFENSE

« Find the correct proportion between freedom and security. »

« Make the attack anti-economic. »

VERSIVO

ACTIVE CYBER DEFENSE

« Security is a process, not a product »

Bruce Schneier, Information Security (2000)

Q & A

VERSIVO

ACTIVE CYBER DEFENSE

VERSIVO

Active Cyber Defense

Via Giovanni Felisati, 61
30171 Mestre-Venezia (VE) Italia
info@versivo.it
www.versivo.it