

## INDUSTRIAL OT SECURITY NELL'ERA 4.0

---

Evoluzione degli attacchi informatici contro gli impianti industriali.



# HOW DO IT AND OT CYBER SECURITY DIFFER

(PRACTICAL WAY)



## OPERATION TECHNOLOGY (OT)

VS

## INFORMATION TECHNOLOGY (IT)

OT is hardware and software that detects or causes a change through the direct monitoring and control of industrial equipment, assets, processes, and events.

Specific equipment designed to operate in hostile environments (*vibrations, water, hot, cold...*)

Operating Systems and software designed for a precise purpose (simple features)

Leverages on legacy technologies and protocols, due to their long lifetime

An attack on OT could led to injury or loss of life, asset damage, or environmental impact.

IT covers the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services.

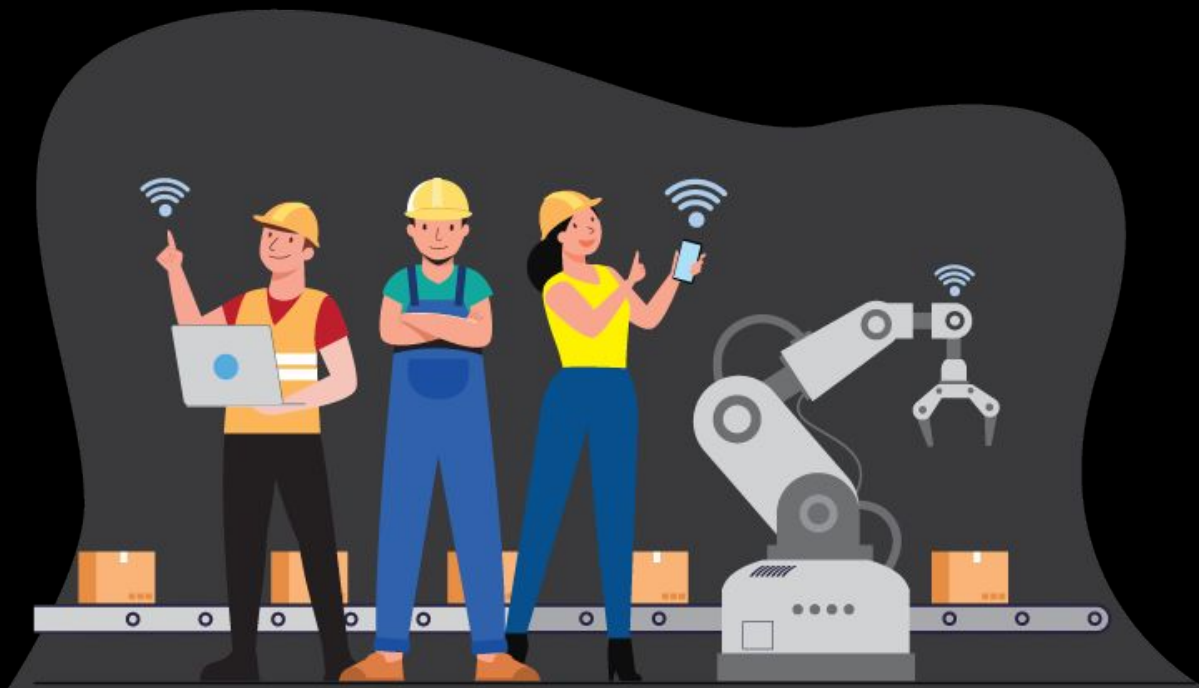
General purpose equipment (PCs, workstations)

General purpose Operating Systems and software (*Windows, Android, IE, Chrome, MS Outlook*)

Lifetime of few years (PCs can be substituted, software upgraded...)

An attack on IT could led to data theft

## OT | MACRO EVOLUZIONE TECNOLOGICA



**From anni '70....**

Dedicated systems and protocols



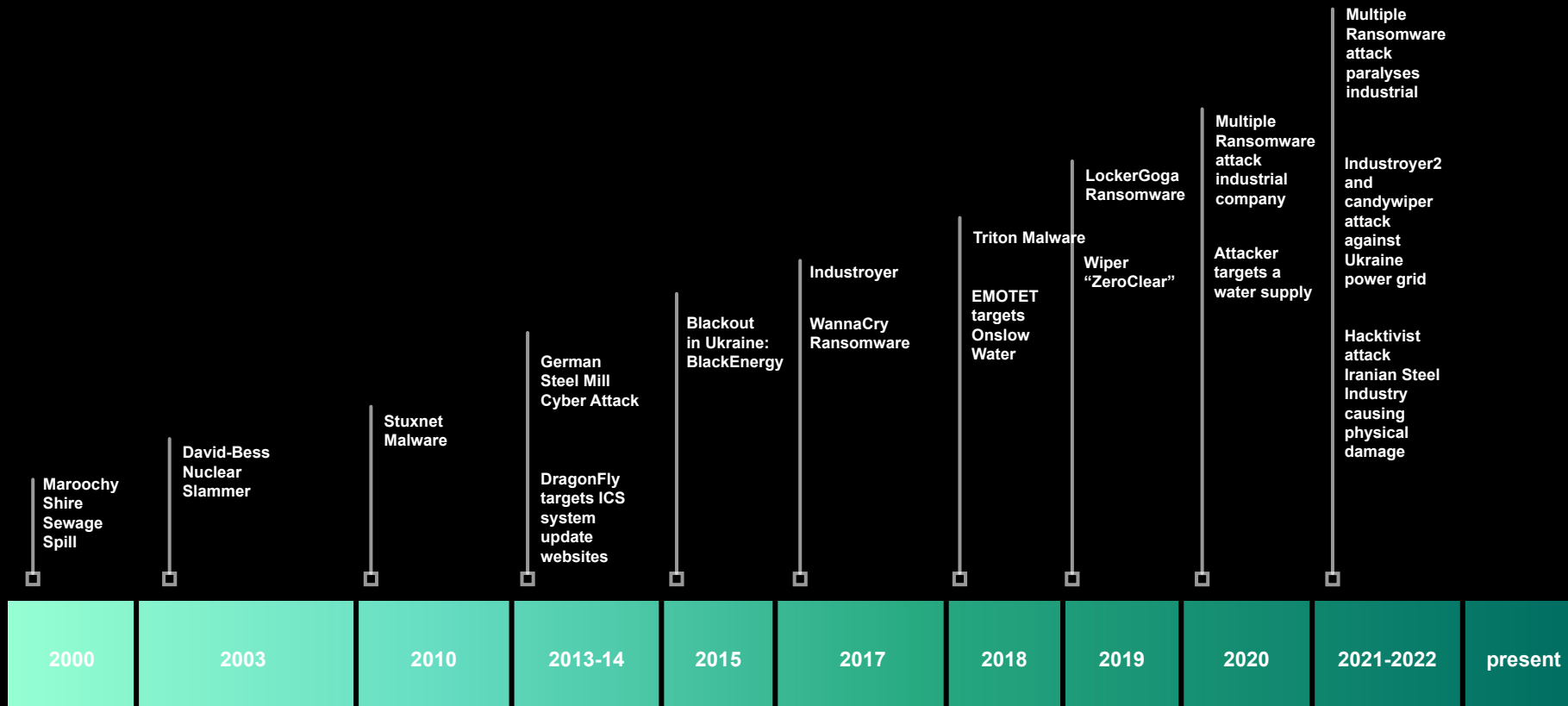
**fino al presente.**

Usage of TCP/IP  
and open-source OS

Completely Isolated Networks



Interconnected Networks



## PLC OSINT

Sample OSINT PLC on Shodan portal

SHODAN country:it 'Schneider Electric'

TOTAL RESULTS  
239

View Report Download Results Historical Trend View on Map

TOP CITIES

|         |    |
|---------|----|
| Rome    | 32 |
| Milan   | 29 |
| Turin   | 16 |
| Santena | 7  |
| Bologna | 5  |

More...

TOP PORTS

Unit ID: 0  
-- Device Identification: Schneider Electric  
-- CPU module: TM221CE24T V1

Italy, Veneto  
Unit ID: 1  
-- Device Identification: Schneider Electric  
ics

Unit ID: 255  
-- Device Identification: Schneider Electric

SHODAN country:it 'siemens:' 'Original Siemens Equipment Basic Fi'

TOTAL RESULTS  
161

View Report Download Results Historical Trend View on Map

TOP CITIES

|               |    |
|---------------|----|
| Milan         | 13 |
| Termini Im... | 13 |
| Potenza       | 12 |
| Rome          | 11 |
| Muro Luc...   | 10 |

More...

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

2023-02-16T08:...

Copyright: Original **Siemens Equipment**

PLC name: ...

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: ...

Plant identification: B...

TOP ORGANIZATIONS

## Medical Devices Exposed

Sample OSINT medical devices on Shodan portal

SHODAN country:it http.title:'XERO Viewer'

TOTAL RESULTS: 3

TOP CITIES:

|         |   |
|---------|---|
| Lecce   | 1 |
| Milan   | 1 |
| Saronno | 1 |

TOP PORTS:

|     |   |
|-----|---|
| 443 | 2 |
| 80  | 1 |

TOP ORGANIZATIONS:

**XERO Viewer** 2023-02-12

HTTP/1.1 200 OK  
Server: nginx  
Date: Sun, 12 Feb 2023 18:39:58 GMT  
Content-Type: text/html;charset=UTF-8  
Content-Length: 14964  
Connection: keep-alive  
Expires: 0  
Expires: 0  
Cache-Control: no-store, no-cache, must-revali  
Set-Cookie:

SHODAN html:'GlucoCare ige''

JavaScript Required 2023-02-01T21:35:05

**SSL Certificate**

HTTP/1.1 200 OK  
Date: Wed, 01 Feb 2023 21:35:05 GMT  
Server: Apache/2.4.54 (Amazon) OpenSSL/1.0  
Issued By: Last-Modified: Thu, 21 Dec 2017 18:42:03  
Name: ETag: "b7-560de0e54d4c0"  
|- Common  
Setigo: Accept-Ranges: bytes  
RSA  
Content-Length: 183  
Domain: Vary: Accept-Encoding  
Validation: Content-Type: text/html; charset=UTF-8  
Secure  
Server CA  
United States, San Jose  
|- Organization:



## Countermeasure pilar(s)

### PREVENTION

- **People awareness**
- Vulnerability management
- Assessment programs
- End point protection solutions
- Network segregation

### DETECTION

- End point protection solutions
- Intrusion Detection Systems
- SIEM infrastructures

### RECOVERY

- Containment procedures
- Backup and recovery solutions and procedures



[info@sicuranext.net](mailto:info@sicuranext.net)  
[www.sicuranext.com](http://www.sicuranext.com)