Complex Systems & Security Laboratory
www.coseritylab.it

Ministero delle imprese e del made in Italy

Scuola Superiore di Specializzazione in Telecomunicazioni Sicurezza

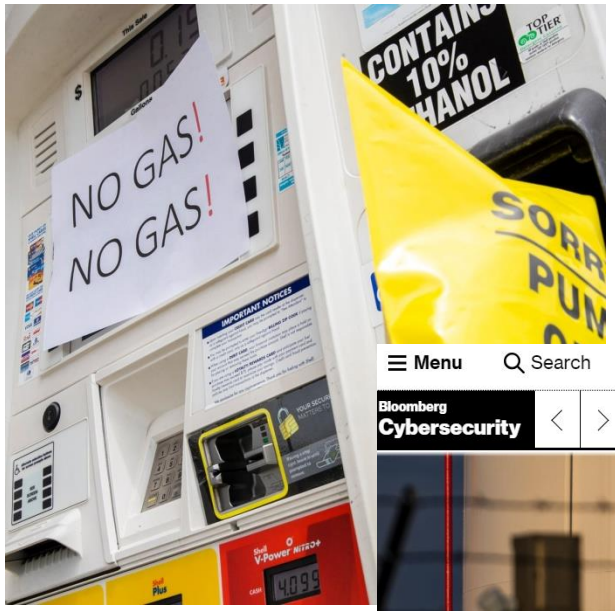
Cybersecurity delle Operational Technologies (OT): minacce e contromisure

Prof. Roberto Setola

r.setola@unicampus.it

Università Campus Bio-Medico di Roma
Via Alvaro del Portillo, 21
00128 Roma
Italy

Roma, 19 Aprile 2023



Menu Search **Bloomberg** Sign In **Subscribe**

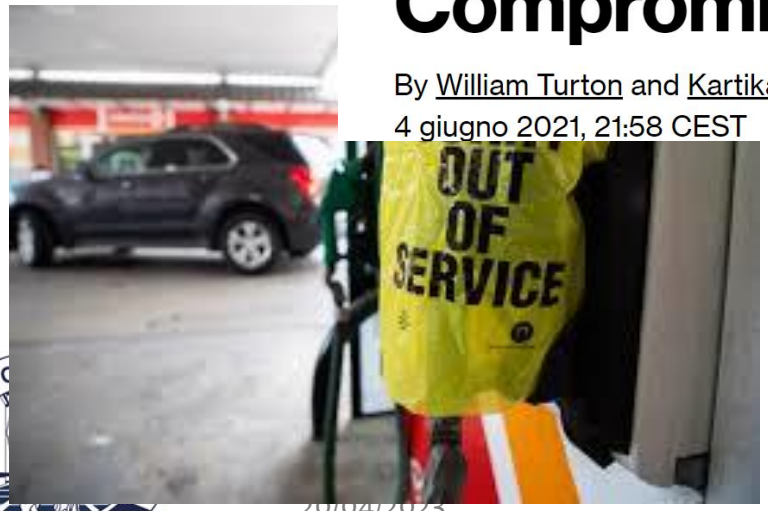
Bloomberg Cybersecurity | Cybersecurity Provider Exclusive Networks to Seek Paris List... | Apple Delays Launch of Feature That Would Scan Photos for Ch... | Juniper Breach Mystery Starts to Clear With New Details on H...

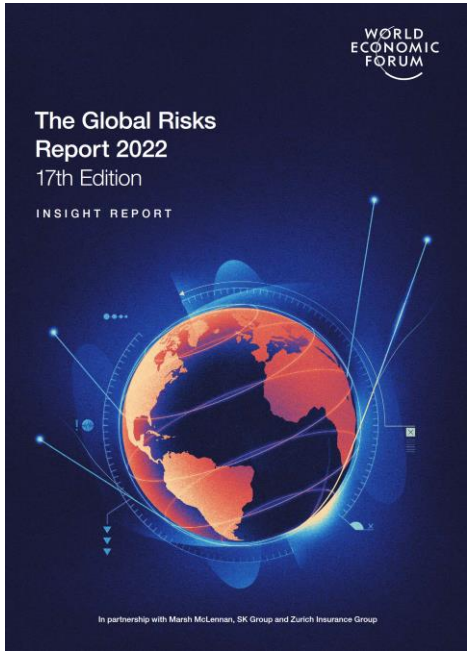
Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

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

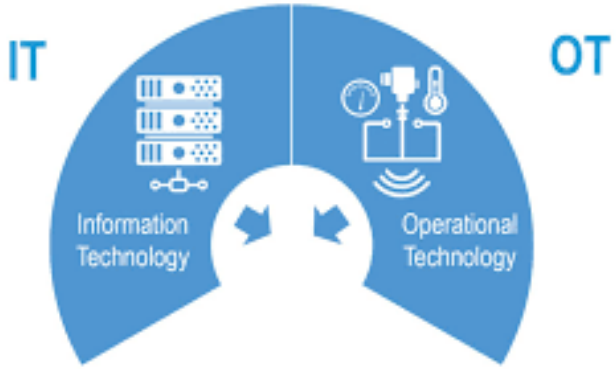


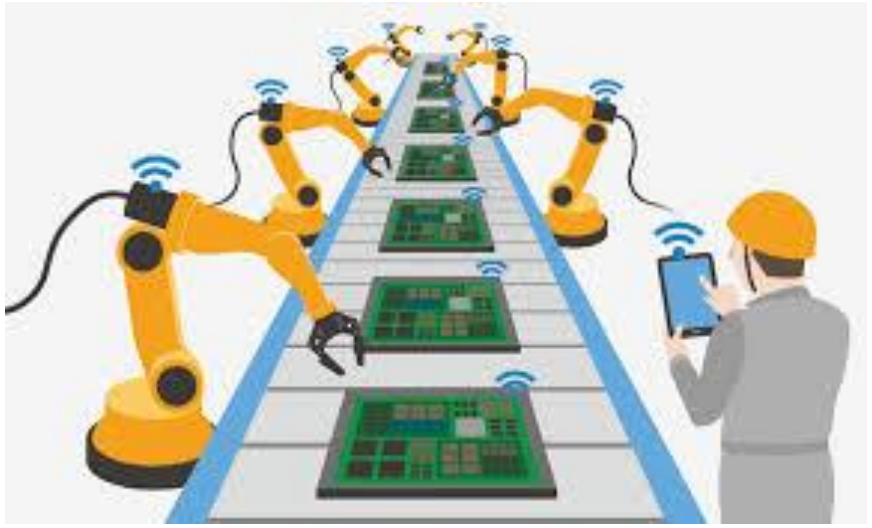


"*Attacks on large and strategic systems will carry cascading physical consequences across societies, while prevention will inevitably entail higher costs*".

L'evoluzione dei sistemi **ICS/SCADA** e il progressivo aumento delle possibilità di gestione e controllo in remoto delle attività produttive esporrà, verosimilmente, il settore manifatturiero al rischio di crescenti compromissioni cyber, finalizzate ad **alterare i dati operativi di processo**, con potenziali impatti di ordine non solo economico ma anche **cinetico**.

Operational Technology





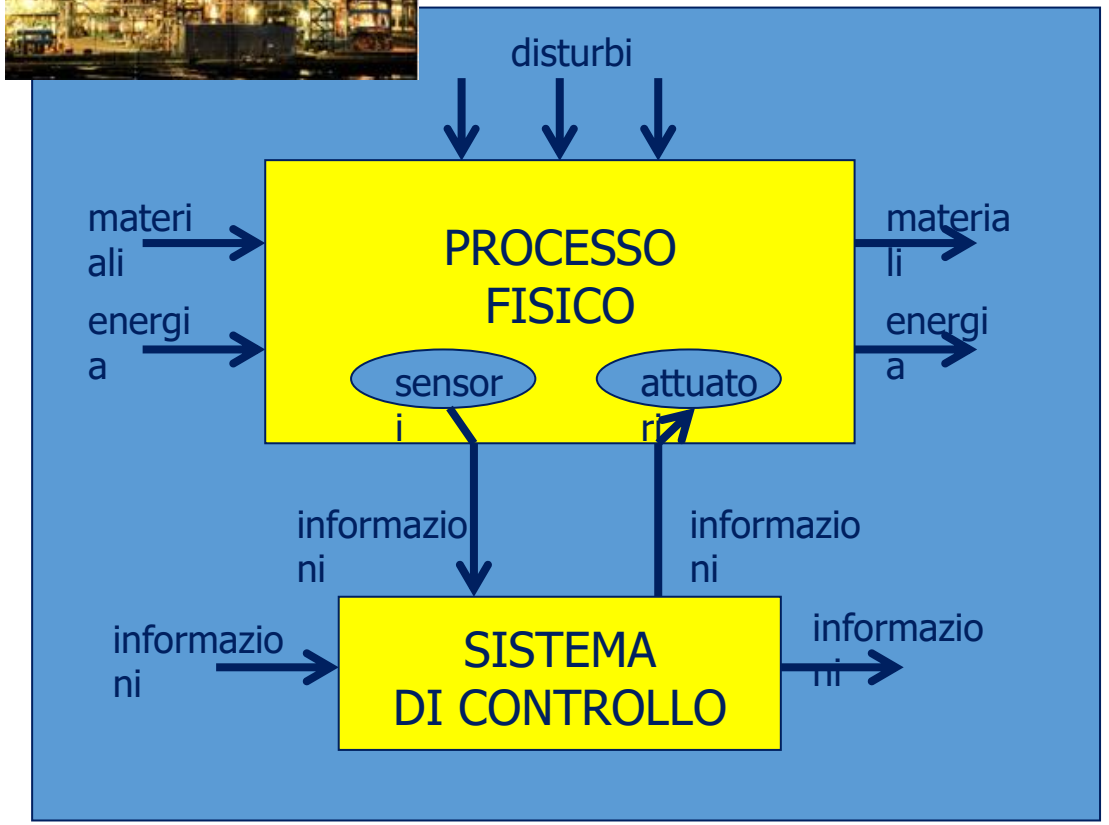
Industrial Control System

Plant (sensor)

Plant (actuators)

RTU (Remote Terminal Unit)

Control room
(MTU – Master Terminal Unit)



Tassonomia dei sistemi OT

SCADA

DCS

PLC

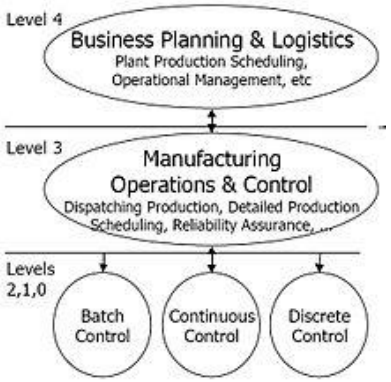
Micro-controller

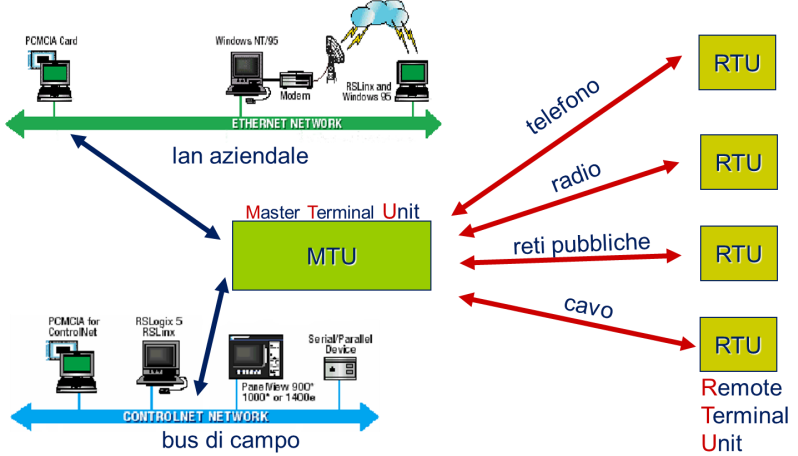
IIoT

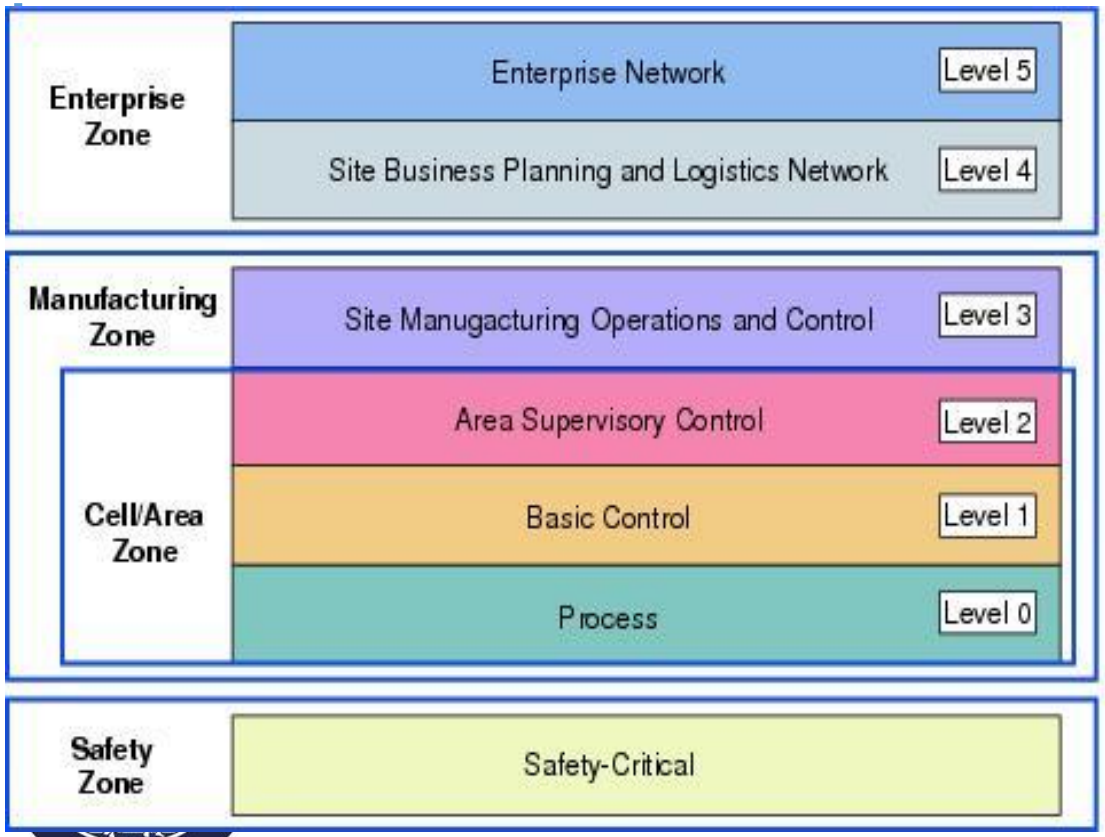
Smart meter

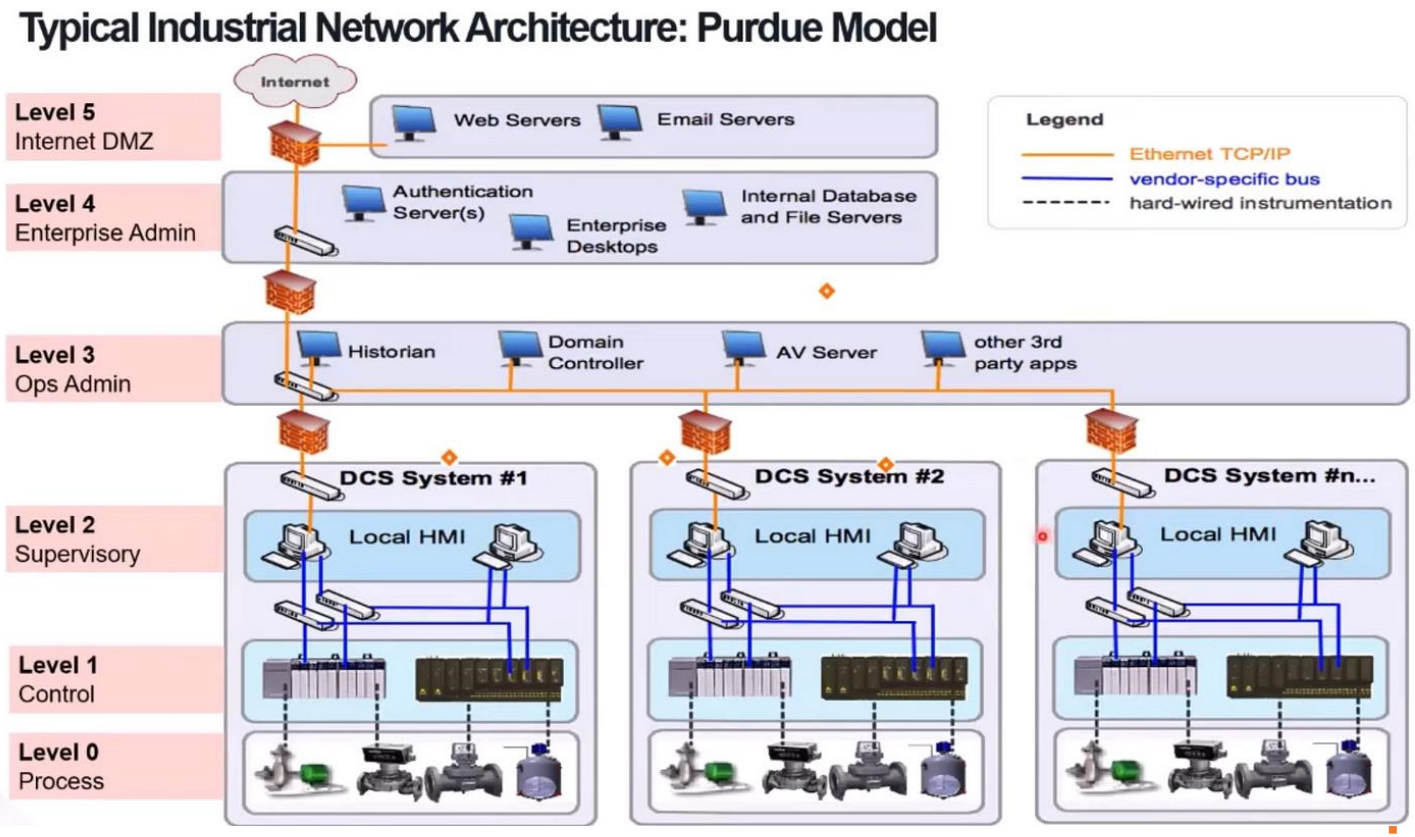
Computerized Numerical Control

Purdue Model









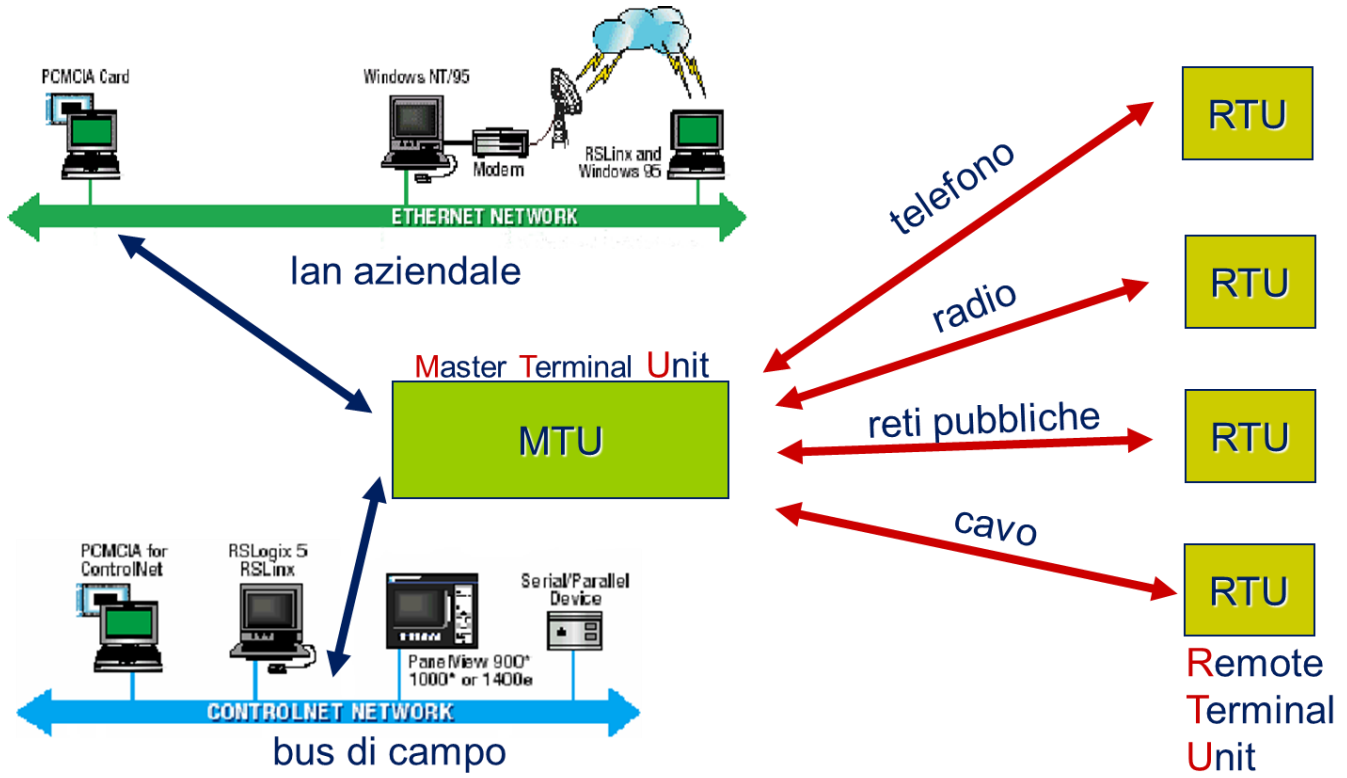
Operational Technologies

Fino alla fine degli anni '90, i sistemi OT erano essenzialmente isolati dalla rete IT aziendale, utilizzavano ambienti e protocolli proprietari e scambiavano informazioni su reti dedicate.

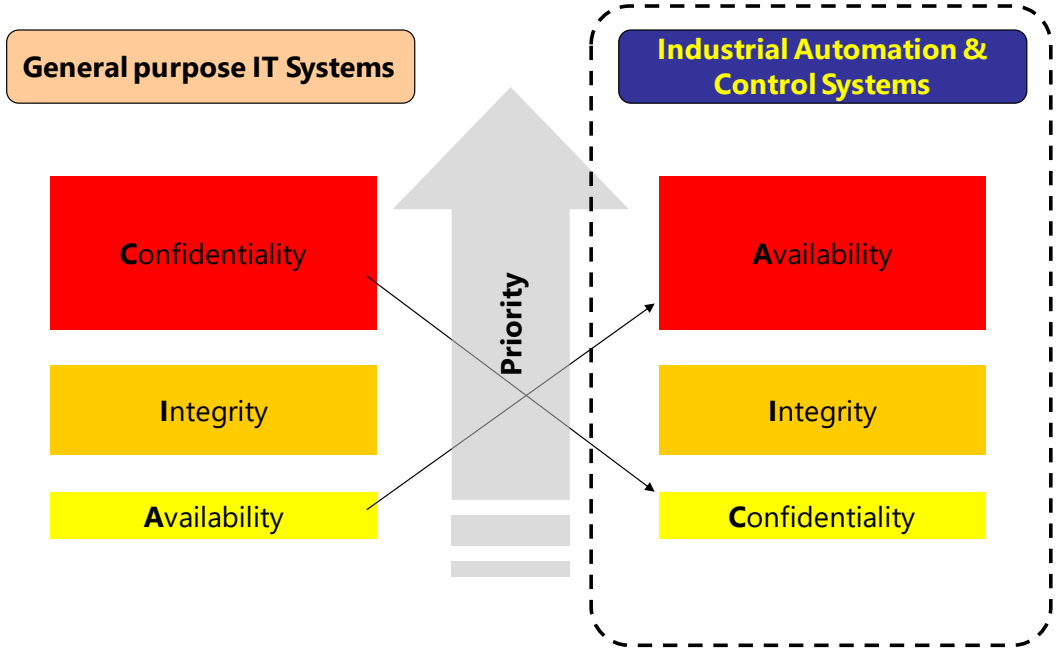
Oggi utilizzano software e protocolli off-the-shelf, sono integrati con le reti IT e fanno ampio uso di dispositivi mobili e IIoT (Industrial Internet of Thing).

Ciò espone i sistemi OT alle stesse classi di minacce dei sistemi IT.

Le peculiarità dei sistemi OT non rendono disponibili tutti gli strumenti di contrasto per l'IT



IT vs OT Cyber security priorities



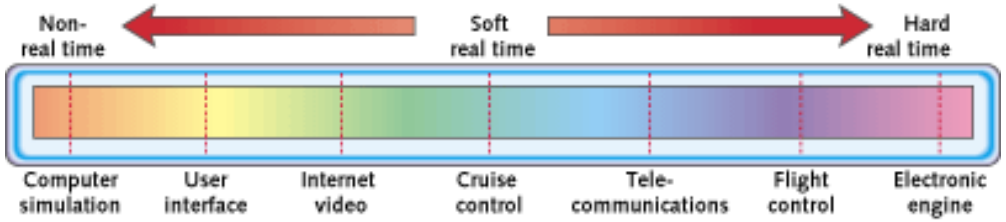
Source: ANSI/ISA–99.00.01–2007
Security for Industrial Automation and Control Systems

Availability is a crucial requirement

I sistemi *OT* presentano diverse peculiarità:

- Sono caratterizzati da un gran numero di connessioni di **I/O**
- Molti messaggi di **pochi byte** (il loro numero aumenta nel caso di situazioni anomale)
- Operano **24/7/365** all'anno
- Hanno dei **lifetime** di 10 – 20 anni
- Hanno bisogno di requisiti di **Hard real-time** (vs soft real time)

Figure 1: The real-time spectrum



Conseguenze di un attacco cyber

Un attacco cyber a un sistema OT può produrre:

- Danni fisici/distruzione delle apparecchiature
- Potenziali impatti sulla salute dei lavoratori/popolazione
- Problemi di inquinamento
- Effetti a cascata su altre infrastrutture/sistemi
- Lunghi tempi di recupero

Idaho National Laboratory **Aurora** Test in 2007
https://www.youtube.com/watch?v=fJyWngDco3g

Intentional or «accidental» sabotage

Un cyber attack compromette il normale funzionamento del sistema. Ciò può avvenire in due modi diversi.

- L'azione cyber è tale da interferire con il funzionamento del sistema OT rallentando le comunicazioni, cancellando i file di configurazione, rendendo inaccessibili alcune risorse, ecc. Eventi che inducono il sistema a porsi (automaticamente) in una condizione di sicurezza bloccando l'erogazione del servizio.

- L'azione cyber "costringe" il processo a operare in condizioni diverse da quelle nominali, inducendo un comportamento che altera il modo in cui il sistema è progettato per funzionare.

«accidental» sabotage

«intentional» sabotage

2000 – Maroochy Shire

Source

An ex-employer used a wireless Internet connection to penetrate into SCADA of sewage treatment plant

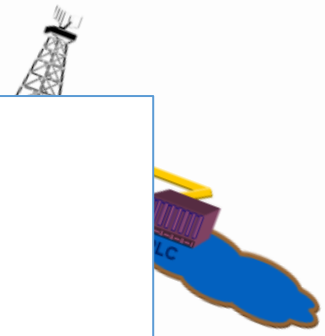
Consequences

- 47 "abnormal" accidents in January-April 2000
- 1.200.000 liters of raw sewage dispersed in the environment
- Potable water compromised in the area

How did he do it?

- On April 23, 2000 Vitek was arrested with stolen radio equipment, controller programming software on a laptop and a fully operational controller.

Vitek is now in jail…



…acker jailed for revenge sewage attacks

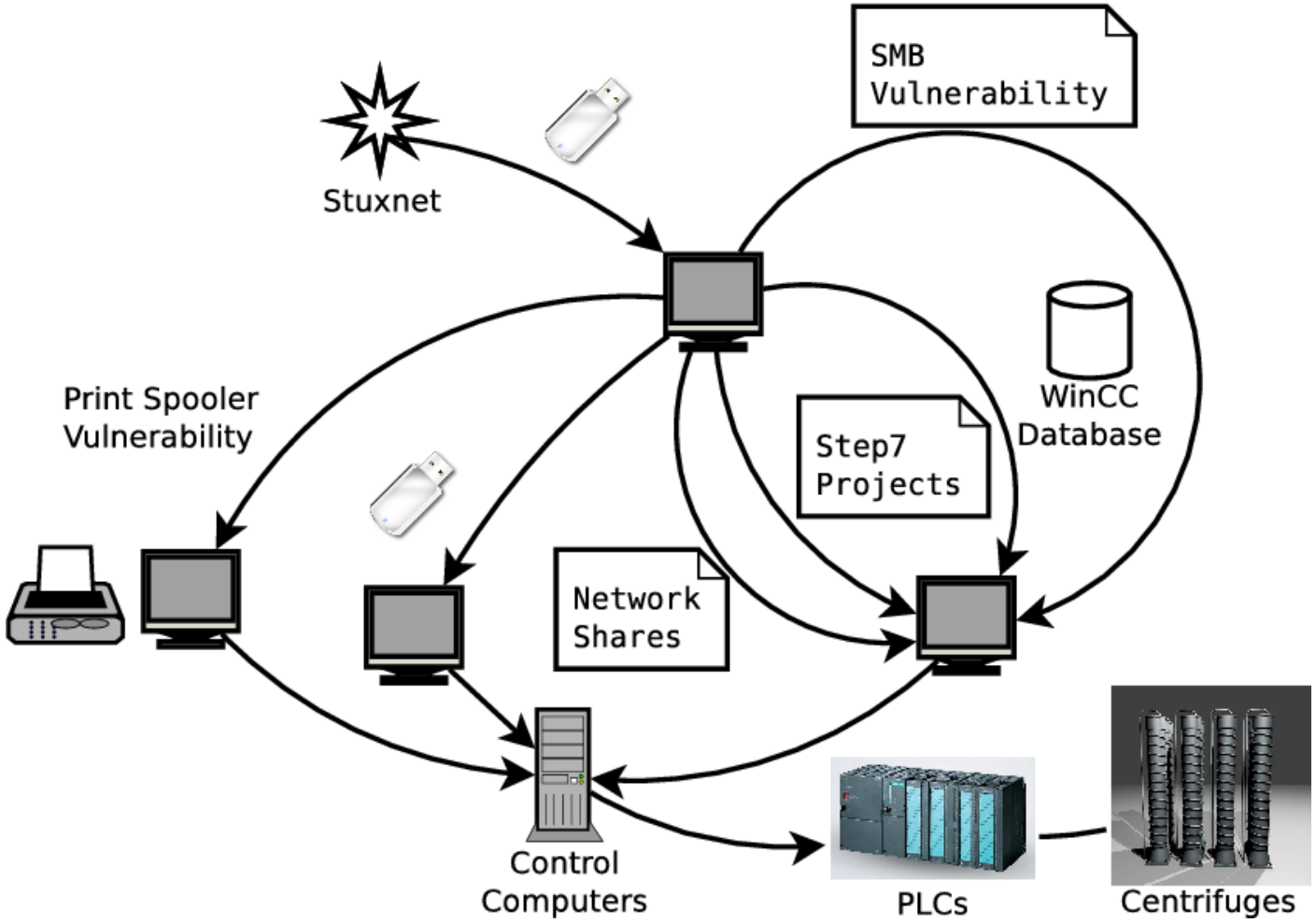
Job rejection caused a bit of a stink

By Tony Smith 31 Oct 2001 at 15:55 SHARE ▼

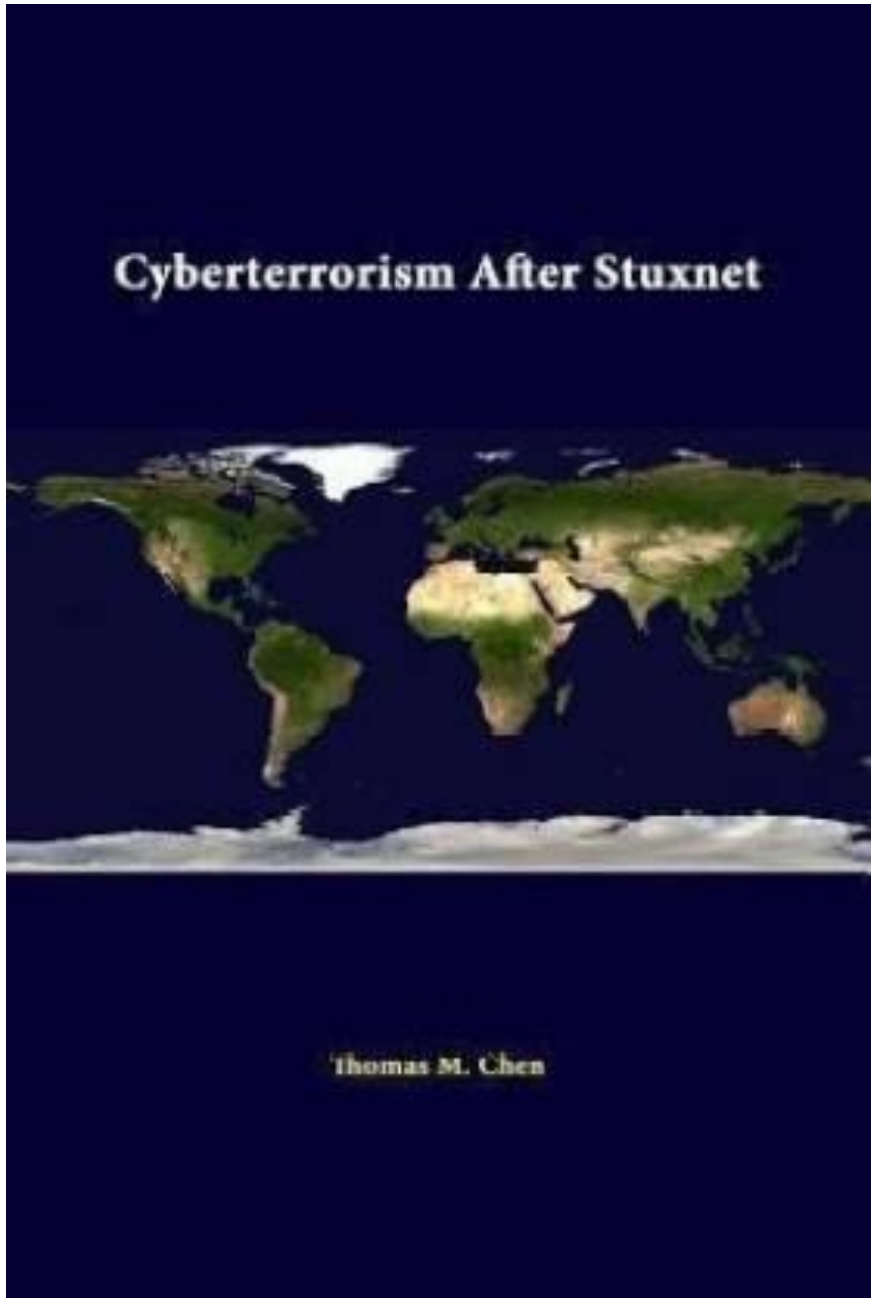
An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

2010 - La svolta !

Da potenziale minaccia a rischio effettivo



After Stuxnet



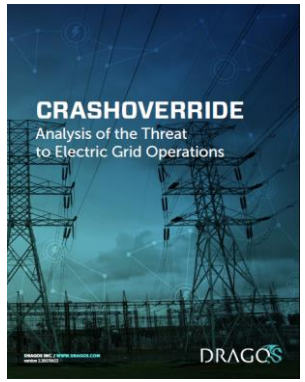
Alcuni episodi

IRONGATE
(2014)

Dragonfly/HAVEX
(2016)

BLACKENERGY 2
(2014)

CrashOverride
(2016)



BLACKENERGY 3
(2015)

"external interference from the computer network"
Ukrenergo

TRITON
(2017

Target: Safety Instrumented System (**SIS**) controllers

Ukrainian black-out 2015

The cyberattack on Ukraine's power grid is a warning of what's to come

On December 23, 2015 100,000 people in and around the Ukrainian city of Ivano-Frankivsk were left without power for six hours.

Power companies experienced unscheduled power outages. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors.

Phishing E-mails

BlackEnergy 3

VPN & Credential Theft

Network & Host Discovery

Malicious Firmware Development

SCADA Hijack (HMI/Client)

Breaker Open Commands

UPS Modification
Firmware Upload
KillDisk Overwrites

Power Outage(s)

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEA

ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING

Alert (ICS-ALERT-14-281-

Ongoing Sophisticated Malware Campaign Compromising ICS (Update

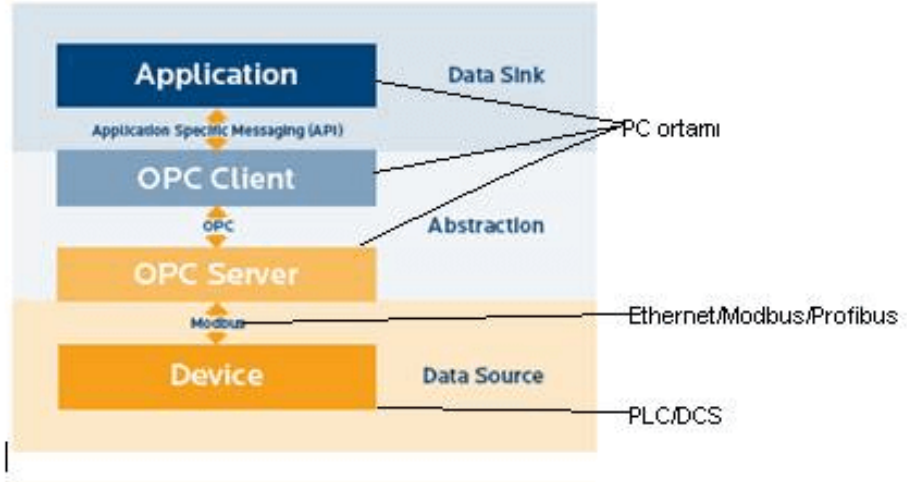
- ICS-CERT has identified a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing **since at least 2011**. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs).
- ICS-CERT has not been able to verify if the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. The malware is highly modular and not all functionality is deployed to all victims.

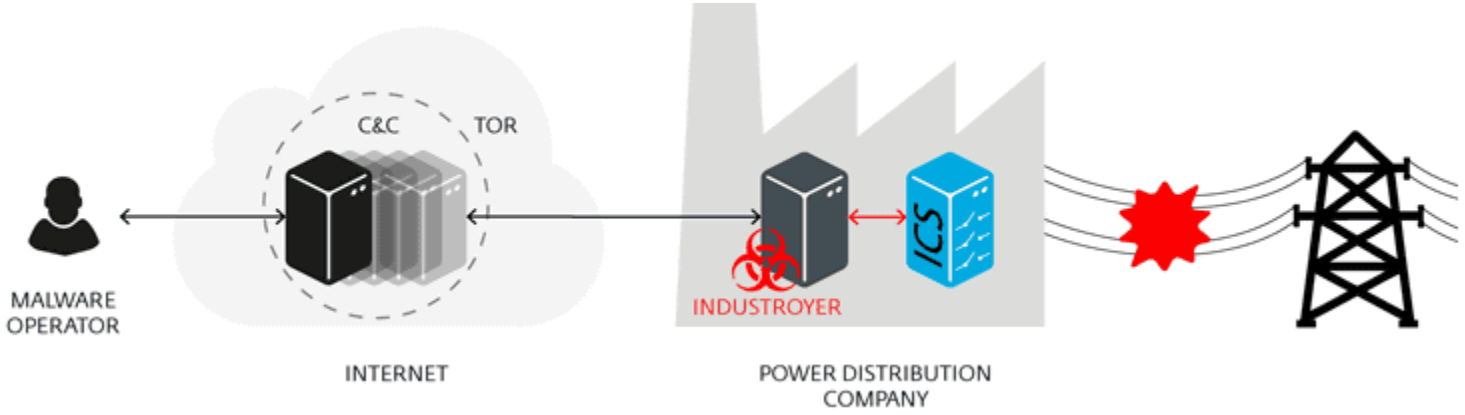
2016 Industroyer (ESET) o CRASHOVERRIDE (Dragos)

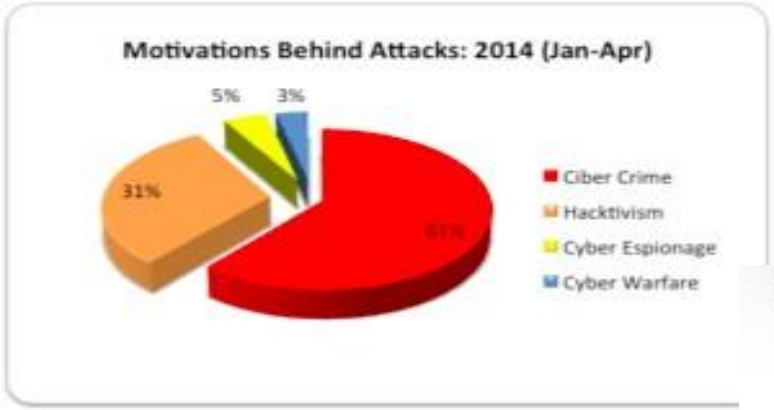
- It does not exploit vulnerabilities or 0-days
- It leveraged the OPC protocol to help it map the environment and select its targets.
- It targeted the libraries and configuration files of HMIs to understand the environment further and leveraged HMIs
- It is a platform to conduct attacks against grid operations systems in various environments and **not confined to work only on specific vendor platforms** (even if it contains specific elements to attack and destroy ABB components)

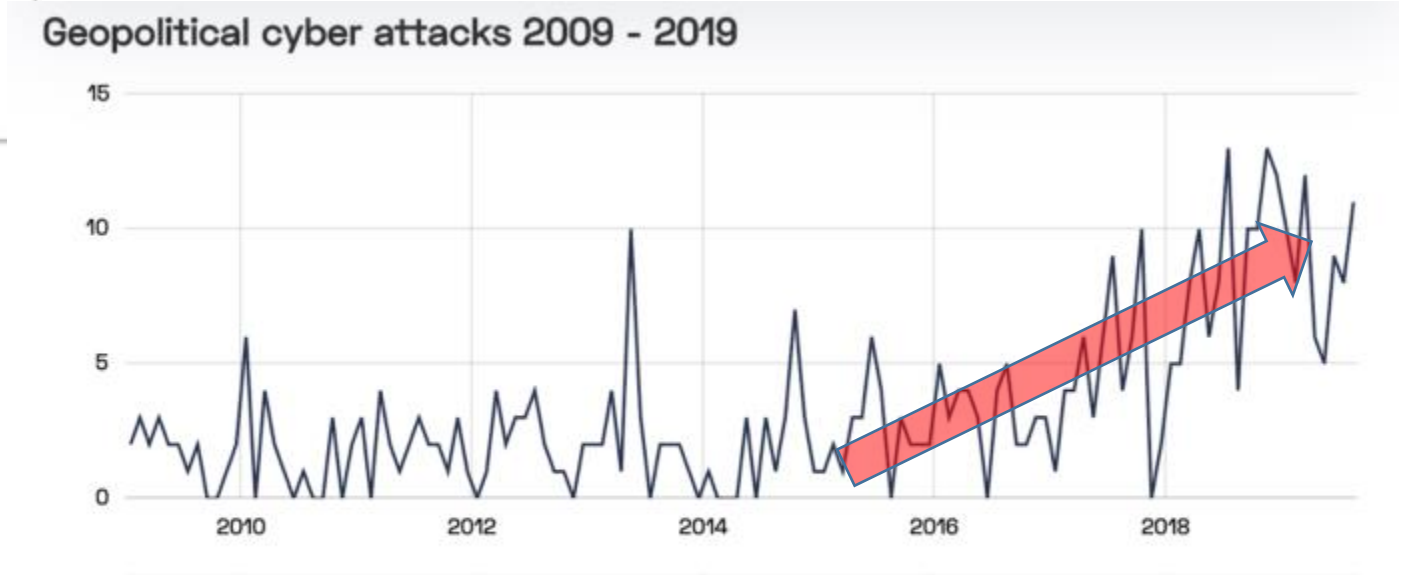
«interferenza esterna proveniente dalla rete informatica» Ukrenergo

17 dicembre 2016 **black out di 1 ora** che ha interessato il territorio Ucraino



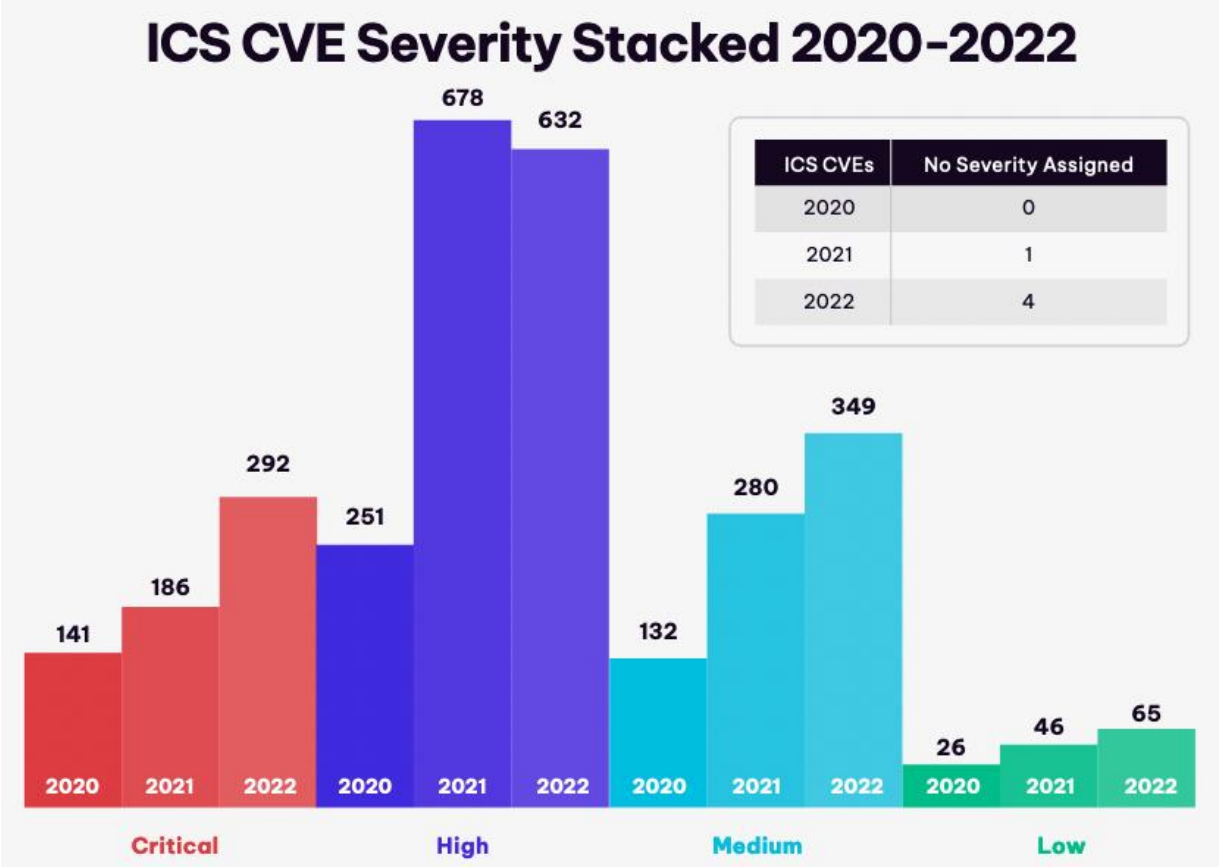






"World governments are investing more and more capital on both offense and defense-related cyber tools, tactics, and strategies"

https://www.fintechnews.org/is-cyberwarfare-as-threatening/



ICS/OT

Siemens Drives Rise in ICS Vulnerabilities Discovered in 2022: Report

More than 1,300 ICS vulnerabilities were discovered in 2022, including nearly 1,000 that have a high or critical severity rating.

https://www.securityweek.com/siemens-drives-rise-in-ics-vulnerabilities-discovered-in-2022-report/

FINANCIAL TIMES

Israel-Iran attacks: 'Cyber winter is coming'

Suspected online assaults on water plant and port offer clues to next stage of rivalry

Two Israeli officials said striking at Iranian civilian infrastructure was an escalation taken at the behes
acting defence minister, who wanted a visible response to a suspected attack on Israel's water statior

Illustrative: A worker at the Eshkol Water Filtration Plant in Northern Israel, operated by Israel's National Water Company Mekorot (photo credit: Moshe Shai/Flash90)

INDEPENDENT

NEWS INDEPENDENT TV CLIMATE SPORT VOICES CULTURE PREMIUM INDY/LIFE INDYBEST INDY100 MY INDEPENDENT VOUCHERS

Subscribe

Hackers attack train network to stop Putin moving troops from Russia to Ukraine

The hackers stopped trains in Minsk, Orsha, and Osipovichi by encrypting some systems, making it 'impossible to buy tickets'

The hacker group Anonymous has waged a cyber war against Russia.

https://theconversation.com/the-hacker-group-anonymous-has-waged-a-cyber-war-against-russia-how-effective-could-they-actually-be-178034

SUBJECT MATTER AREAS CYBERSECURITY INFORMATION TECHNOLOGY

Anonymous Claims Hacks on More Than 300 Russian Cyber Targets in 48 Hours, Including Gas Control System

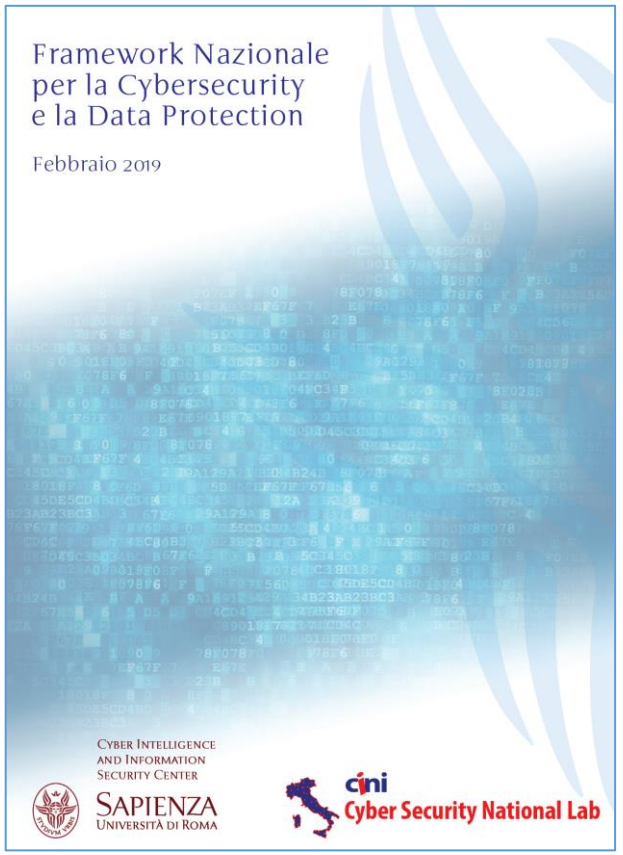
Hackers claimed bre... 200 gi...

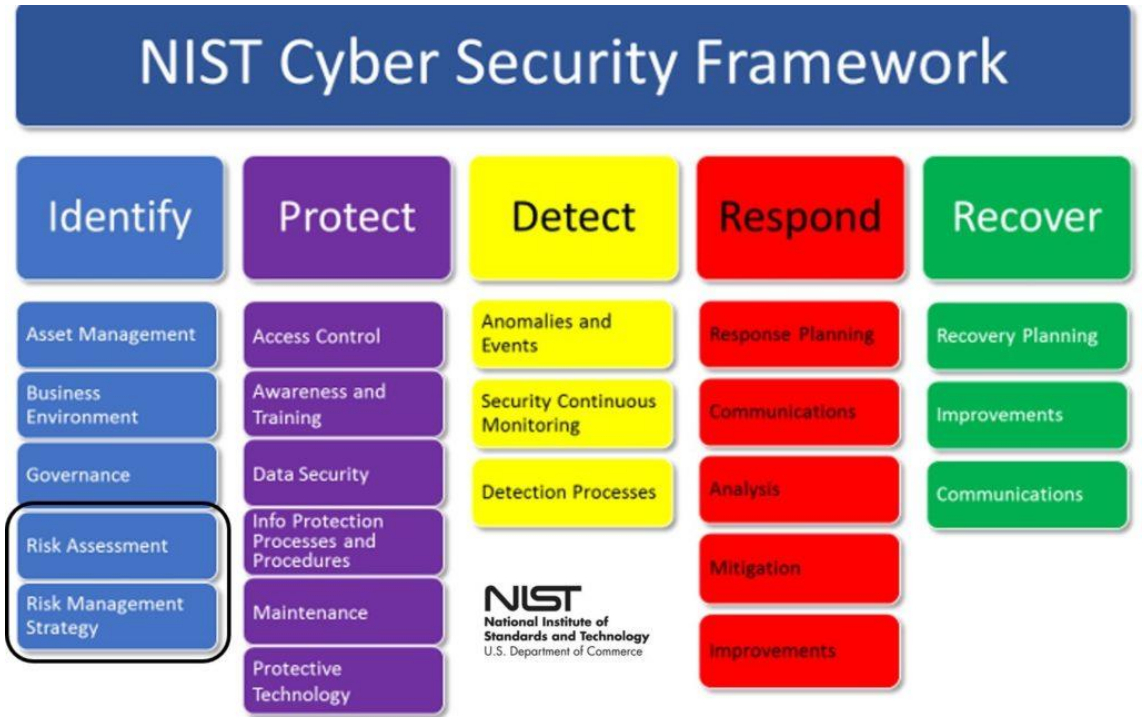
...efense manufacturer Tetraedr, obtaining more than ...tly leaking the data.

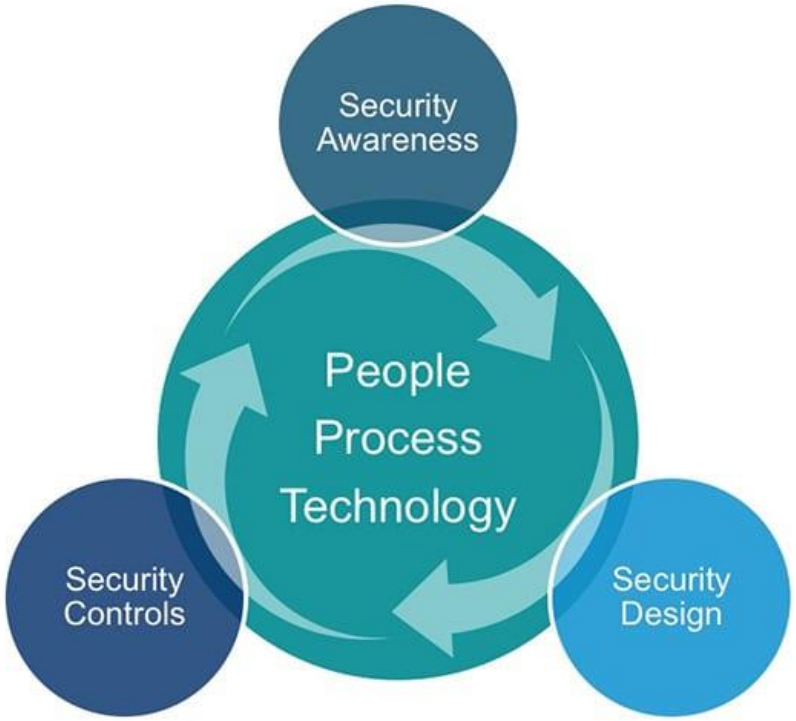
Ukrainian cyber resistance group targets Russian power grid, railways

By Joel Schectman, Christopher Bing and James Pearson

Strategie di difesa


Framework Nazionale
per la Cybersecurity
e la Data Protection
Febbraio 2019
Cyber Intelligence
and Information
Security Center
Sapienza
Università di Roma
cini
Cyber Security National Lab


NIST Cyber Security Framework
Identify
Protect
Detect
Respond
Recover
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Response Planning
Communications
Analysis
Mitigation
Improvements
Recovery Planning
Improvements
Communications
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

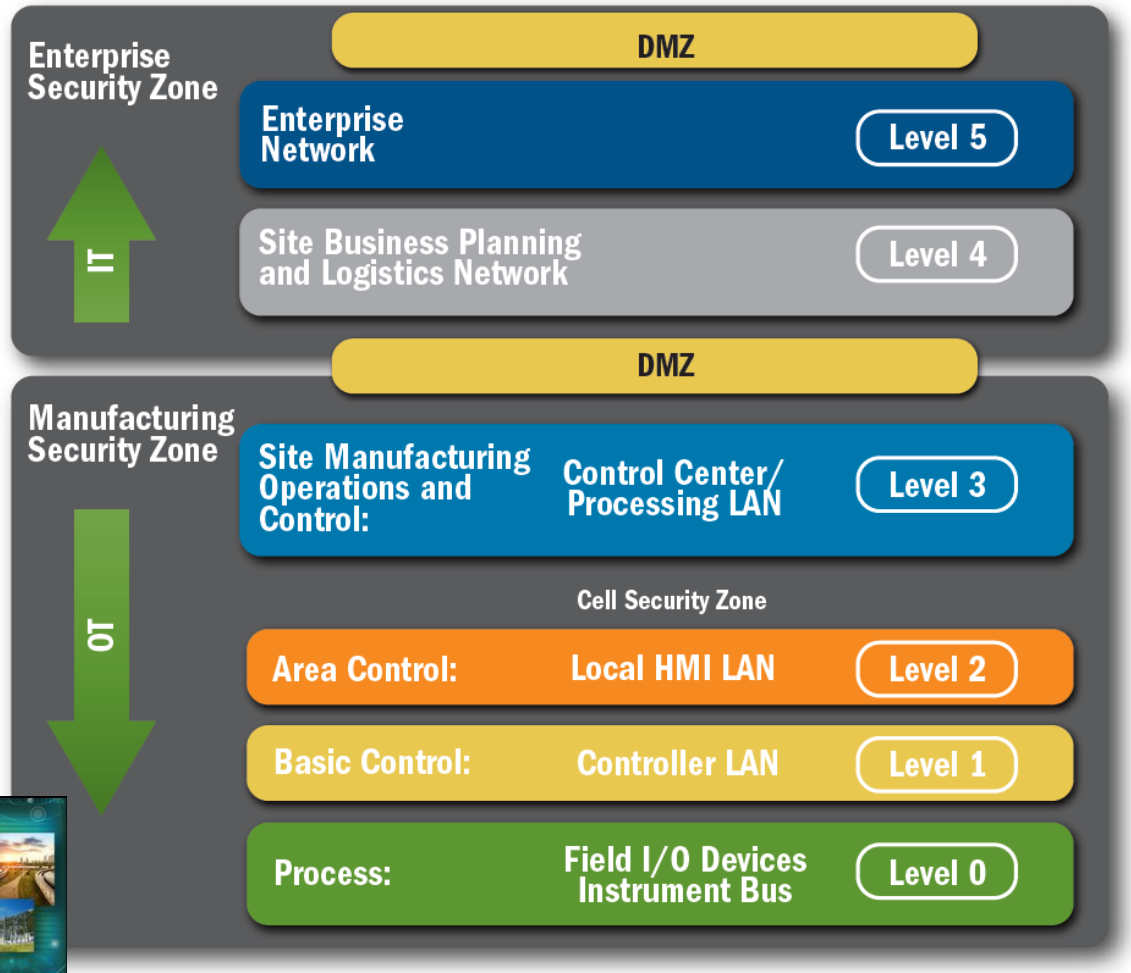

Security Awareness
People
Process
Technology
Security Controls
Security Design

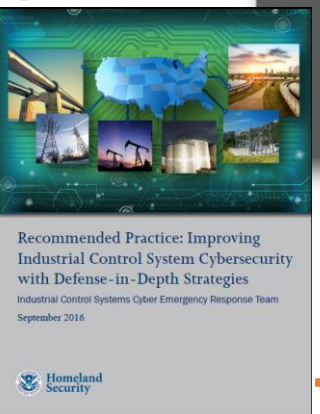

Site 2
Site 1
Site 3
VPN
Production Line 1
Production Line 2
Production Line 3
VPN
VPN
Trusted
Untrusted
Defense-in-depth and
Zero Trust Security Models

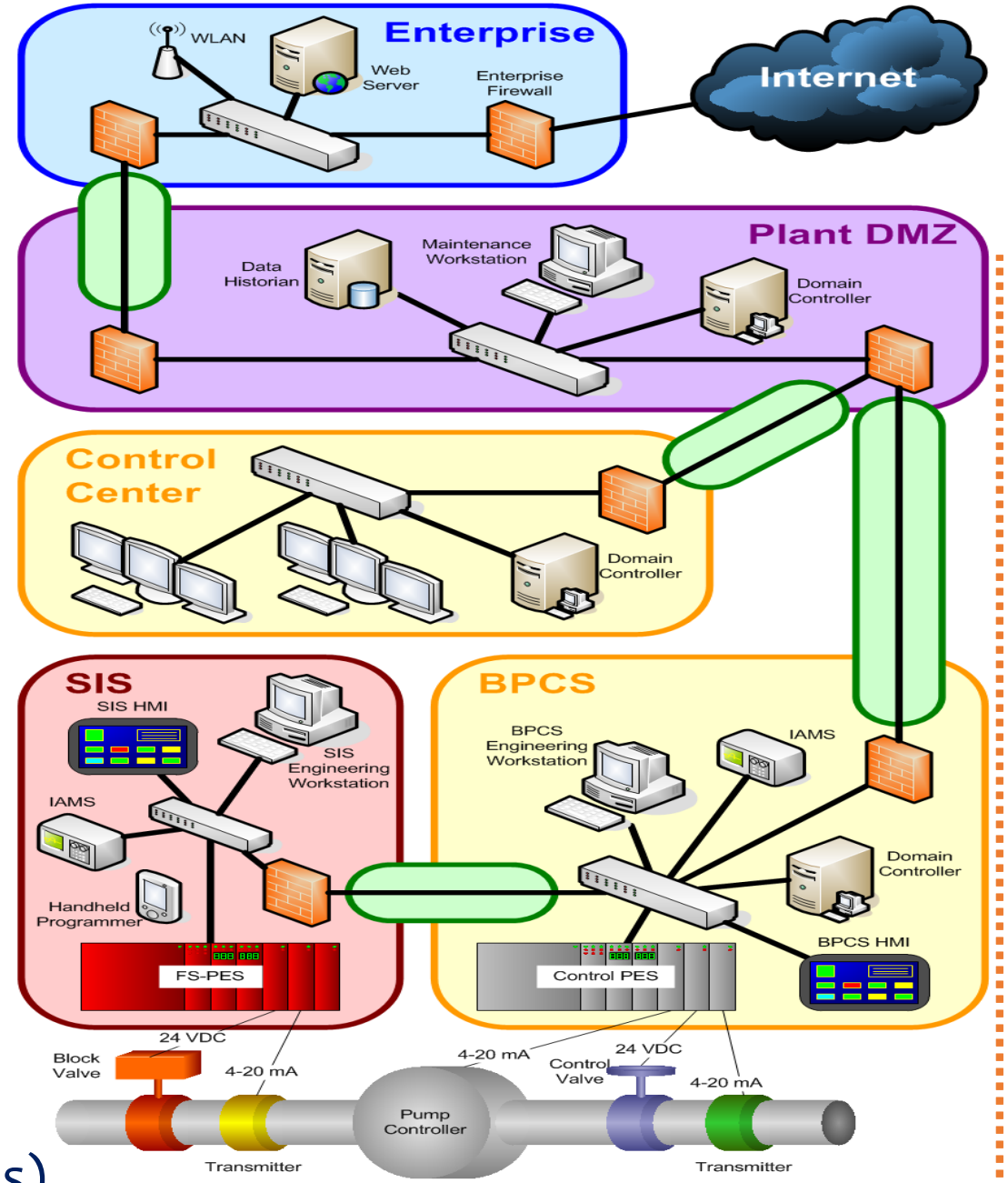
Architettura di Cyber Security per OT

- **Defense in Depth:** strategia di cybersecurity che consiste in una serie di meccanismi di difesa stratificati. Se un meccanismo fallisce, un altro prende immediatamente il suo posto per contrastare un attacco. Questo approccio a più livelli con ridondanza intenzionale aumenta la sicurezza dell'intero sistema e affronta diversi vettori di attacco;
- **Least-Privilege:** concetto di sicurezza informatica secondo il quale a un utente vengono concessi i livelli minimi - o permessi - di accesso di cui ha bisogno per svolgere le proprie mansioni;
- **Deny-by-Default:** criterio che concede il permesso solo a ciò che è esplicitamente autorizzato, mentre il resto è vietato;
- **Zero Trust:** si basa sul presupposto che nulla, sia all'interno che all'esterno del perimetro di rete di un'organizzazione, debba essere considerato attendibile per impostazione predefinita.

Segregazione







Unidirectional Security Gateways (USGs)

https://www.isa.org/isa99/

Sicurezza fisica

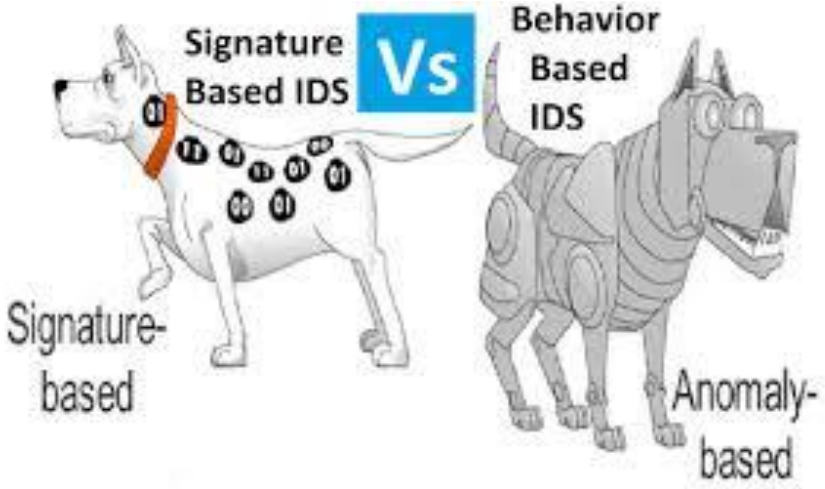
RTU sono «disperse» nel territorio in aree di difficile accesso e in assenza di sorveglianza

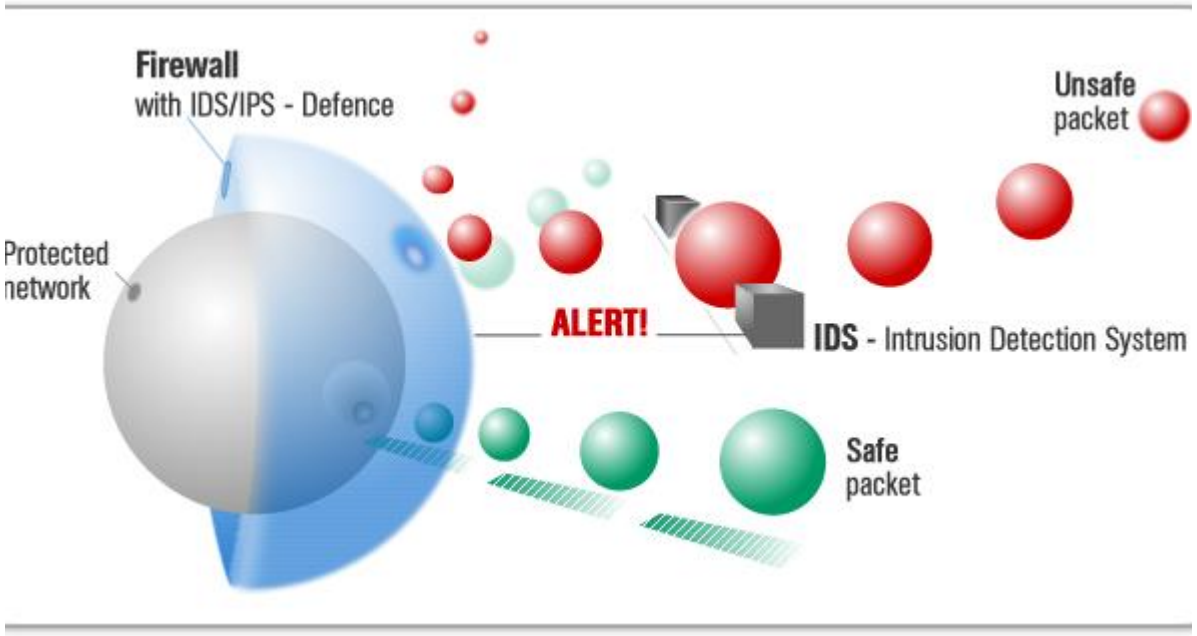
Gli involucri sono progettati per essere resistenti alle intemperie (IP) o agli urti (IK)

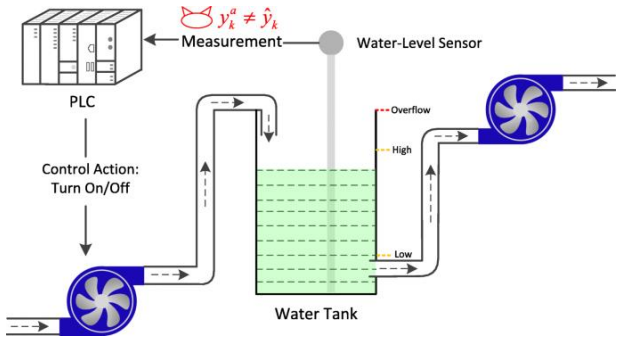
Meno considerata la problematica dell'antiscasso

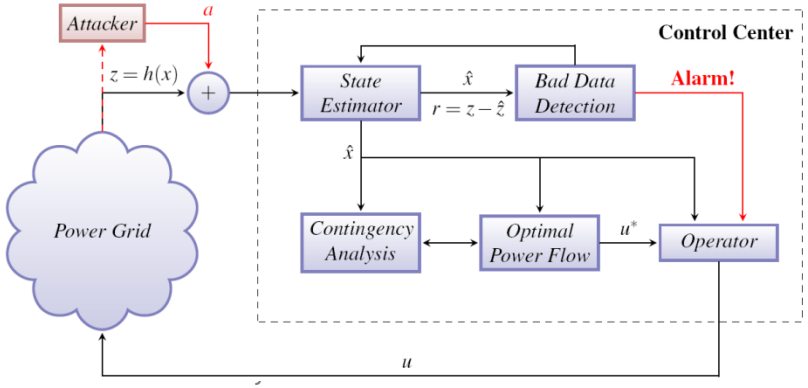
Prevedere chiusure e sistemi di (video)sorveglianza adeguati

Network Security









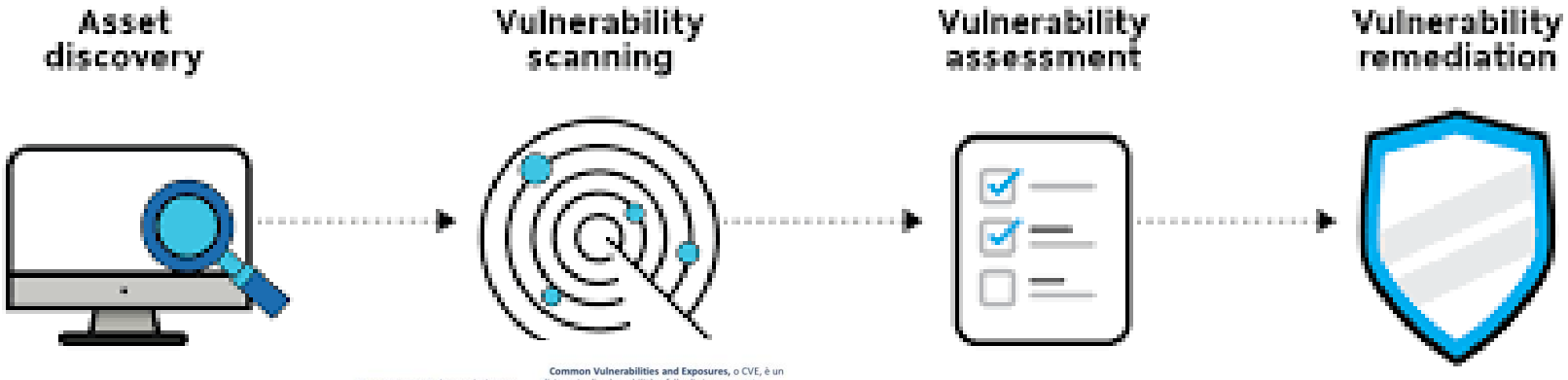
Cyber-Physical anomaly detection system

Application Security

Asset inventory

Whitelisting

Patching



Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures, o CVE, è un dizionario di vulnerabilità e falle di sicurezza note pubblicamente. È mantenuto dalla **MITRE** Corporation ed è finanziato dalla National Cybersecurity FFRDC del Dipartimento della Sicurezza interna degli Stati Uni

CVE

https://cve.mitre.org/

Currently, there are **194,863** CVE Records accessible

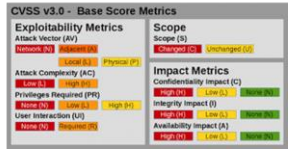
Common Vulnerabilities and Exposures

Il sistema delle **Common Vulnerabilities and Exposures** (**CVE**) cataloga in modo uniforme vulnerabilità ed esposizioni.

Vulnerabilità: una debolezza nel software e/o nel firmware che, se sfruttata, viola almeno una tra confidenzialità, integrità, disponibilità.
Esposizione: un errore nel software/nella sua configurazione che permette l'accesso a funzioni ed informazioni.

Common Vulnerability Scoring System (CVSS)

CVSS Characterizing and Scoring Vulnerabilities



Cyber Security procedure

Rule for	*Description*
System acquisition	policy regarding security check and constraints for software and hardware acquisition, development, integration, implementation and configuration. Elements that are not fully compliant with such criteria cannot be installed in the OT environment
Configuration management and system integrity	set of activities focused on creating and maintaining the integrity of IT products and information systems, through the control of processes for initialization, modification and monitoring of configurations during the life of the element
System maintenance	checks regarding system maintenance, in particular regarding the presence of documentation and the regularity of maintenance interventions
Compliance and accreditation	continuous assessment procedure of the effectiveness of security controls and the implementation of privacy controls
Physical and environmental protection	measures to be taken to protect systems, buildings and related support infrastructures from accidental and malicious threats related with physical dimension and environment
Identification and authentication	Guideline of the process that establishes the identity of an entity that interacts with the system. This element includes also the specification for access control, i.e. the process of granting or refusing specific requests for: • obtain and use information and related IT services; • o access specific physical facilities
Traceability	Set of activities to ensure the traceability of system operations and the availability of logs
System and communications protection	Implementation rules of security controls for any communication and data transfer
Contingency planning	Provisional measures to restore services following an emergency or a system outage
Risk assessment	Guideline of the process of identifying risks for operations, resources and individuals resulting from the operation of an IT system
Supply chain risk management	Prescription for managing exposure to risks, threats and vulnerabilities in the Supply Chain and for developing strategies in response to the risks presented by third parties, by the products and services provided

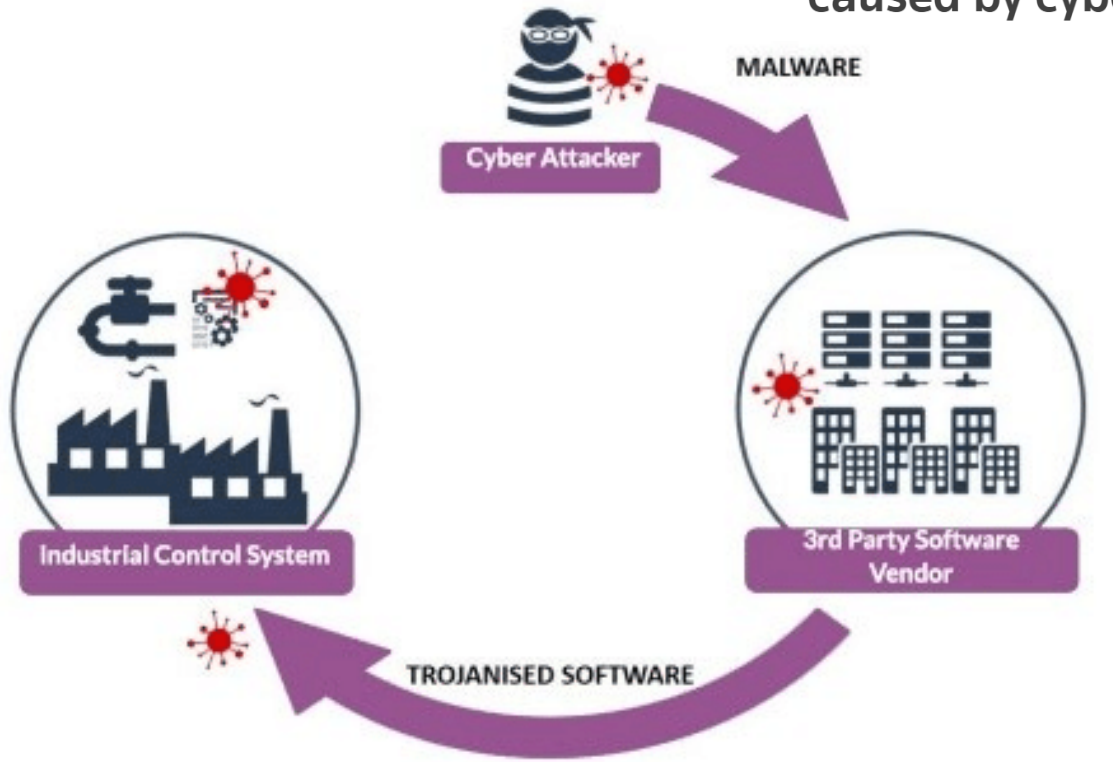
ICS supply chain

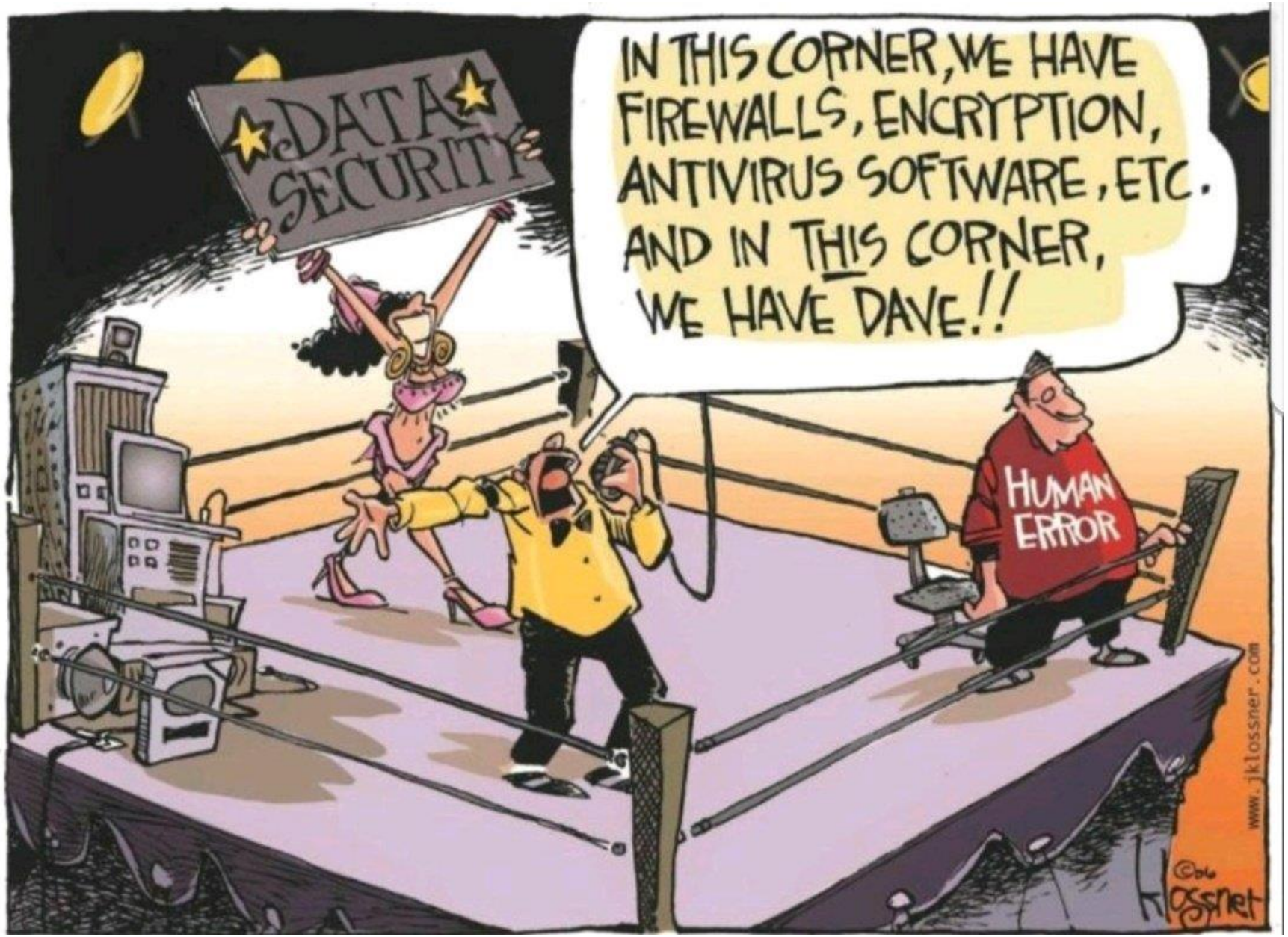
REUTERS® World Business Markets Legal Breakingviews

Technology

1 minute read · November 3, 2022 11:01 PM GMT+1 · Last Updated 5 months ago

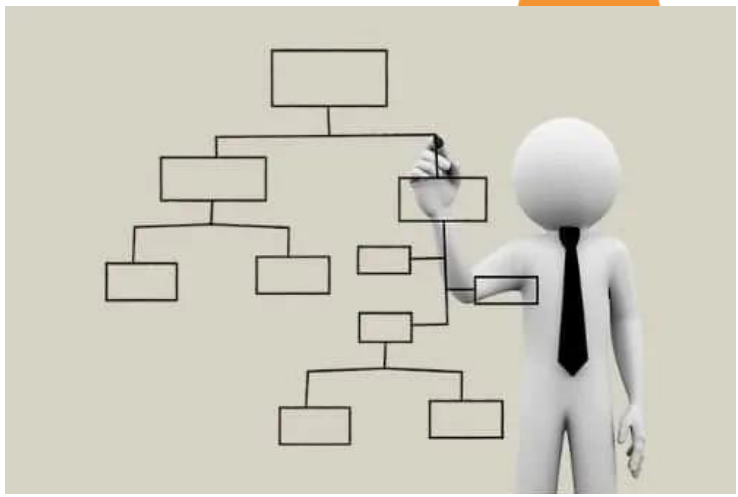
Danish train standstill on Saturday caused by cyber attack

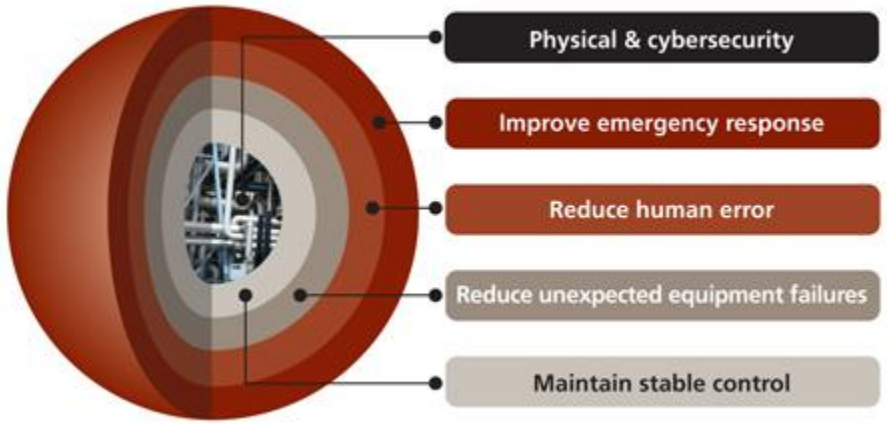



DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©JK
Klossner

Organizzazione

- **Necessità di avere un team dedicato alla cybersecurity dei sistemi OT**
- **Segregation of duties**
- **Integrazione Cyber & Physical security**





Revised Directive on Security of Network and Information Systems (NIS2)

EUROPEAN
COMMISSION

Brussels, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

(Text with EEA relevance)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

https://ec.europa.eu/digital-single-market/en/news/revised-directive-security-network-and-information-systems-nis2

New directive to enhance the resilience of critical entities CER

EUROPEAN
COMMISSION

Brussels, 16.12.2020
COM(2020) 829 final

2020/0365 (COD)

Proposal for a

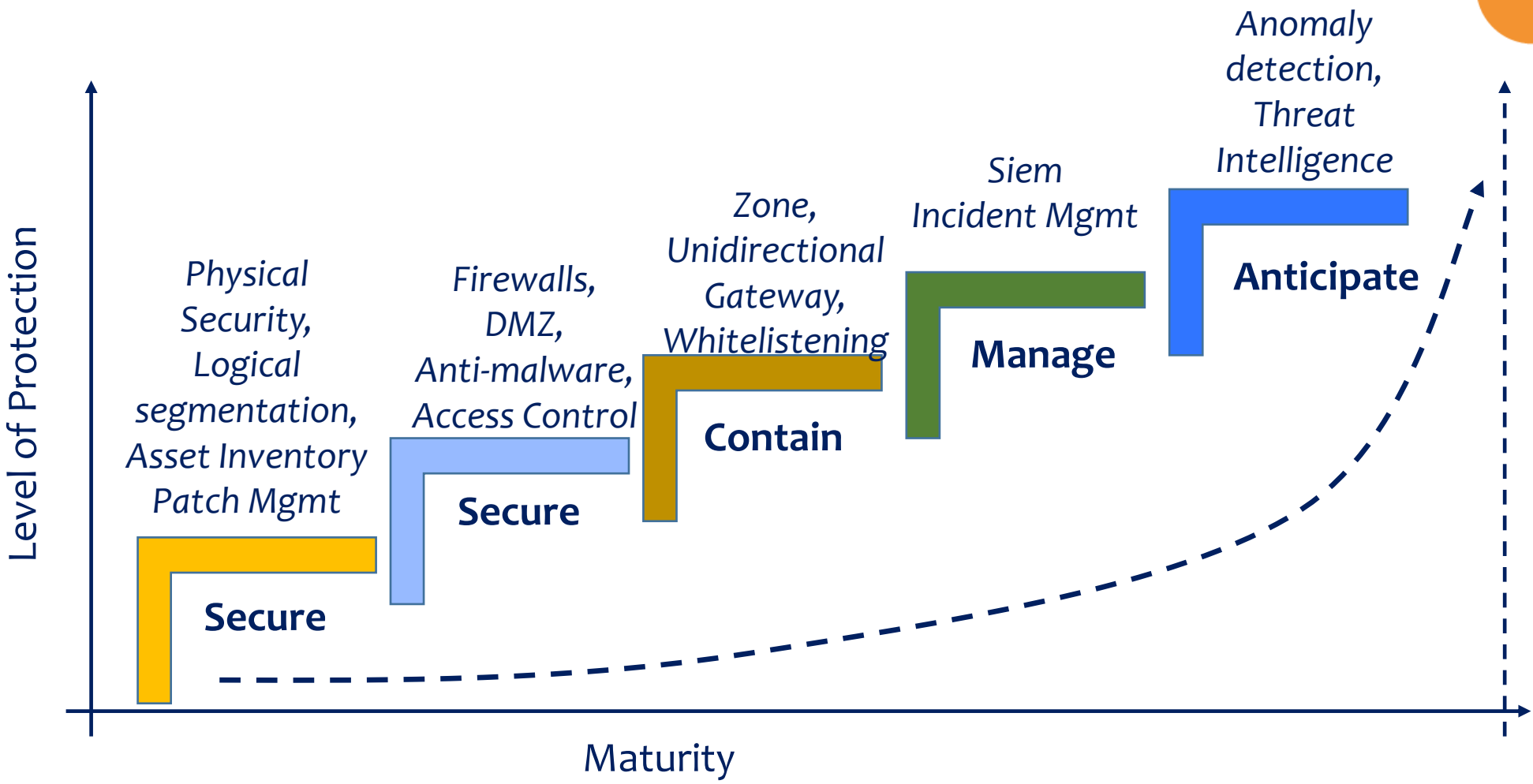
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the resilience of critical entities

{SEC(2020) 433 final} - {SWD(2020) 358 final} - {SWD(2020) 359 final}

https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential_en

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA


Level of Protection
Physical Security, Logical segmentation, Asset Inventory Patch Mgmt
Secure
Firewalls, DMZ, Anti-malware, Access Control
Secure
Zone, Unidirectional Gateway, Whitelistening
Contain
Siem Incident Mgmt
Manage
Anomaly detection, Threat Intelligence
Anticipate
Cost
Maturity

Il principio fondamentale

La sicurezza di un sistema informatico dipende

- **molto dal processo con cui un sistema viene gestito**
  - pianificazione, analisi dei rischi, gestione dei sistemi, formazione del personale, ecc.
- **poco dagli specifici prodotti adottati**
  - specifici firewall, antivirus, ecc.

r.setola@unicampus.it