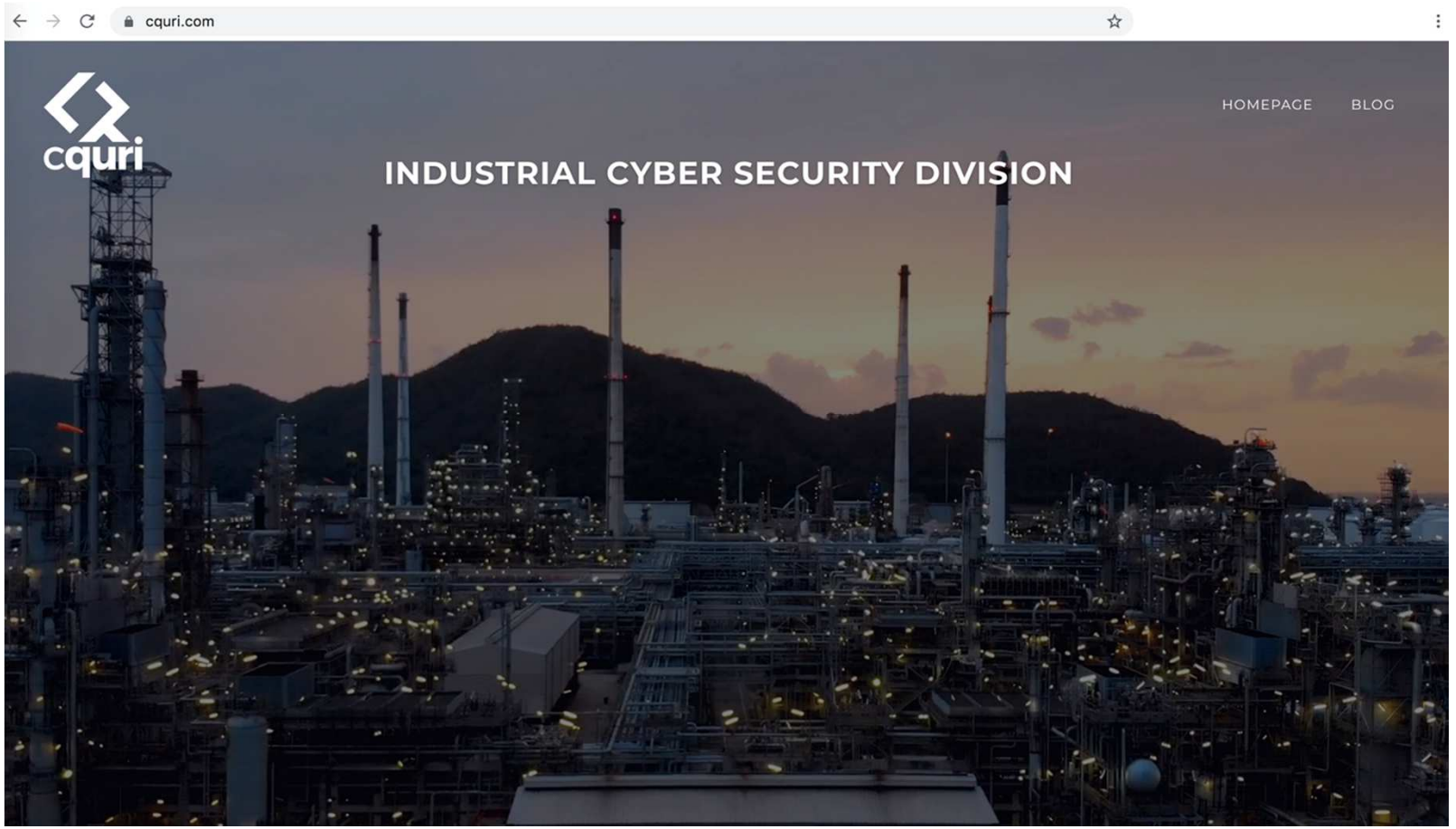
# SIF VDA
# Innovazione digitale
# automazione delle funivie

20 settembre 2019 - Quart (Aosta)

IT SECURITY

# CQURI.COM - CYBER SECURITY SPECIALIST

E’ un ramo d’azienda che segue in modo verticale la sicurezza IT ed i processi che la caratterizzano



IN LOSS

# CI SONO SOLO DUE TIPI DI CLIENTI

QUELLI CHE HANNO GIA’
PERSO
DATI E PRODUTTIVITA’

I NOSTRI FUTURI CLIENTI...

IL FOCUS

# L’ AMBITO - ICS / SCADA

# NOMENCLATURA

## ICS

Industrial Control System - Ovvero un insieme di oggetti,  sensori ed apparati industriali che vengono controllati e comandati in concerto da un sistema centrale.

## SCADA

Supervisory Control And Data Acquisition - Ovvero un sistema informatico ad interfaccia grafica per il monitoraggio e la supervisione di sistemi industriali.

## OT

Operation Technology - Applicazioni software a supporto della gestione dei processi industriali.

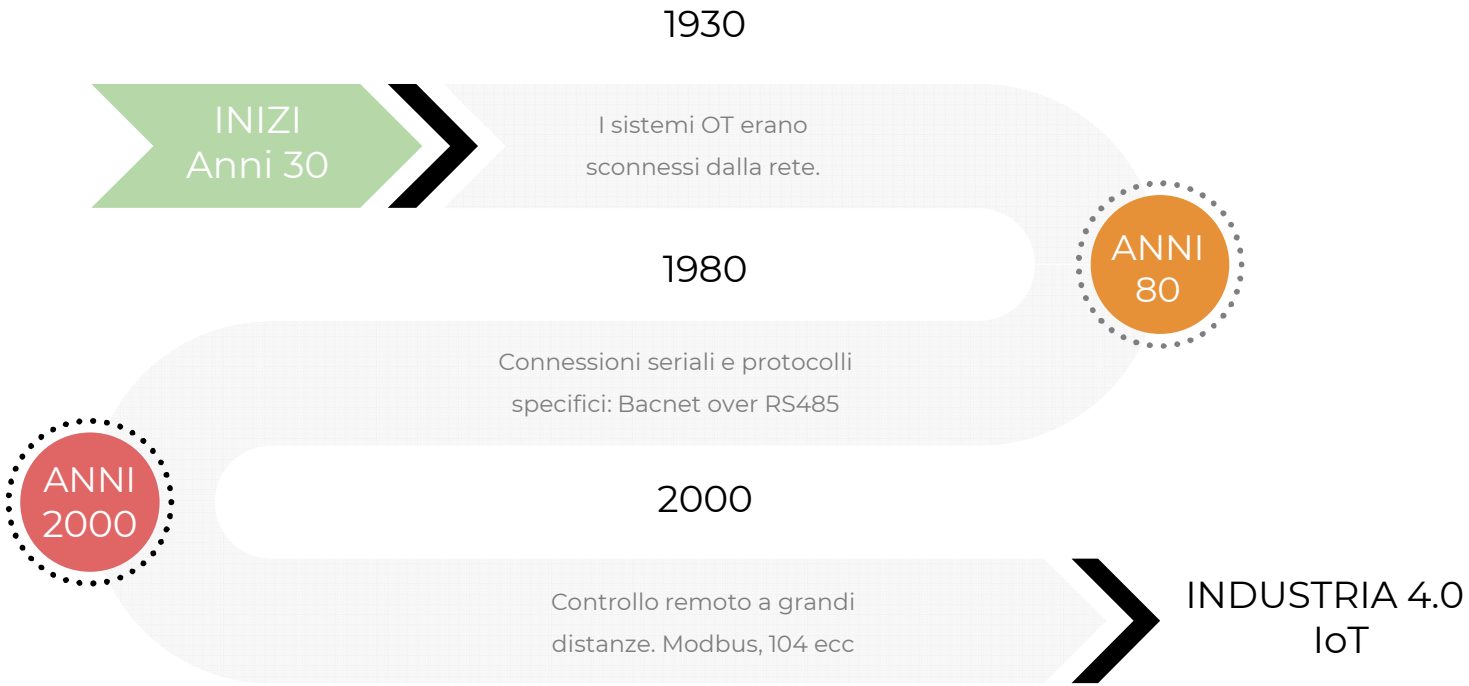
## IT

Information Technology - Termine che in generale ingloba tutte le applicazioni e sistemi informatici.

OT INCONTRA IT

# LA STORIA DEI SISTEMI ICS

Il mondo Operation incontra l'Informatica



TELECONTROLLO

# I 5 COMPONENTI

## ELEMENTI PRODUTTIVI

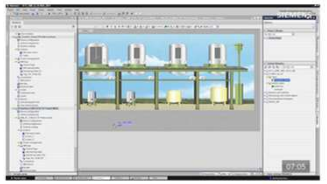
Turbina, paratia, reattore, gassificatore, cabinovia ecc.

## SENSORI ED ATTUATORI

PLC, RTU ecc.

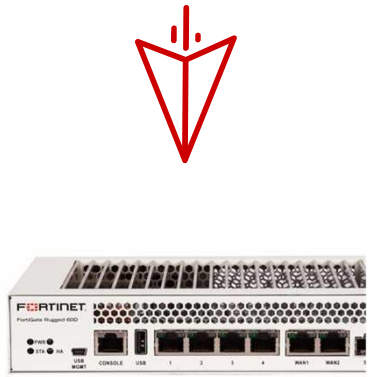
## NETWORK

Switch, Access Point, Telefoni, Webcam ecc.



## SCADA

Sistemi HMI per il controllo dei processi



## SISTEMI DI SICUREZZA

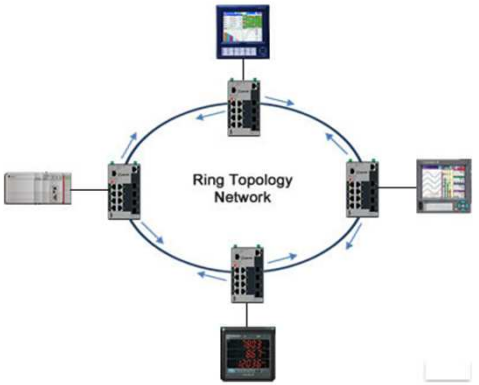
Sistemi di sicurezza IT

# CARATTERISTICHE PECULIARI

Per il mercato ICS ci sono alcune caratteristiche specifiche per quanto riguarda la creazione delle network

International Organization for Standardization

INTERNATIONAL ELECTROTECHNICAL COMMISSION




## STANDARD IEC/EMC

IEC EMC, per compatibilità elettromagnetica, vibrazioni, protocolli di comunicazione ecc.

## RUGGED

Ambienti estremi richiedono apparati ad alta resistenza ai fenomeni atmosferici

## TOPOLOGIA AD ANELLO

In alcuni casi sono richiesti protocolli di comunicazioni specifici (es. MRP)

SEMPRE PIU' CONNESSI

# MERCATO IN CRESCITA

Il mercato ICS e SCADA è in forte espansione. **Fonte - Transparency Market Research.**


**ICS nel 2014** **ICS nel 2021**

I sistemi di integrazione con gli apparati produttivi continuano con un importante tasso di incremento la propria diffusione.

**SCADA nel 2015** **SCADA nel 2022**

I sistemi SCADA sono oggetto di un incremento vertiginoso nei nuovi impianti, ma **soprattutto negli impianti già esistenti**.

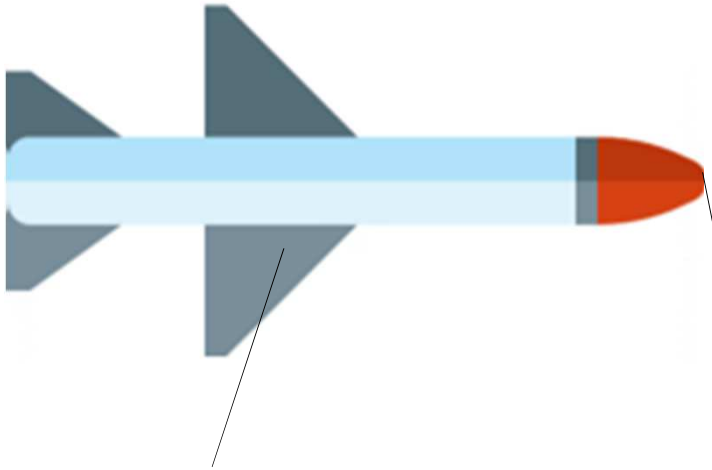
IL FOCUS

# PARTIAMO DAL PROBLEMA

*Prima di Stuxnet, nessuno ha pensato di mettere al sicuro le infrastrutture industriali.*

Tweet

# STUXNET -IL PIU' SOFISTICATO



DROPPER

PAYLOAD

Windows

SIEMENS S7 - S300

# STUXNET -IL PIU' SOFISTICATO

## COMMISSIONE

2008 il governo Usa da il via alla creazione di un virus per rallentare il programma nucleare dell' IRAN

## DIFFUSIONE

Vengono attaccate le aziende fornitrici delle centrali Iraniane, installato anche grazie a penne USB

## COME FUNZIONA

Vengono sabotati PLC specifici in base alla matricola che comandano le centrifuge delle centrali Iraniane. MITM non fa vedere le modifiche

## INFEZIONE GLOBALE

Il virus si diffonde in Internet e un suo bug compromette anche PLC non a target. Ci accorgiamo solo nel 2013

IL FOCUS

# LE CONSEGUENZE

ESEMPI

# SOLO ALCUNI ALTRI CASI

Di seguito alcuni disastri dovuti ad attacchi informatici


Erede di STUXNET, ora nelle mani degli Hacker, inganna l'operatore che crede sia tutto ok con attacchi man in the middle. Attualmente il più attivo nel mondo ICS.

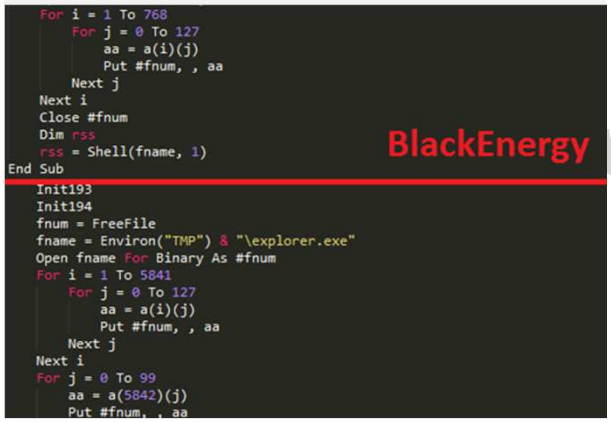
ESEMPI

# SOLO ALCUNI ALTRI CASI

Di seguito alcuni disastri dovuti ad attacchi informatici


## CRASHOVERRIDE

2016 - Shut down, spente 30 sottostazioni elettriche, 230.000 persone al buio




## BLACKENERGY

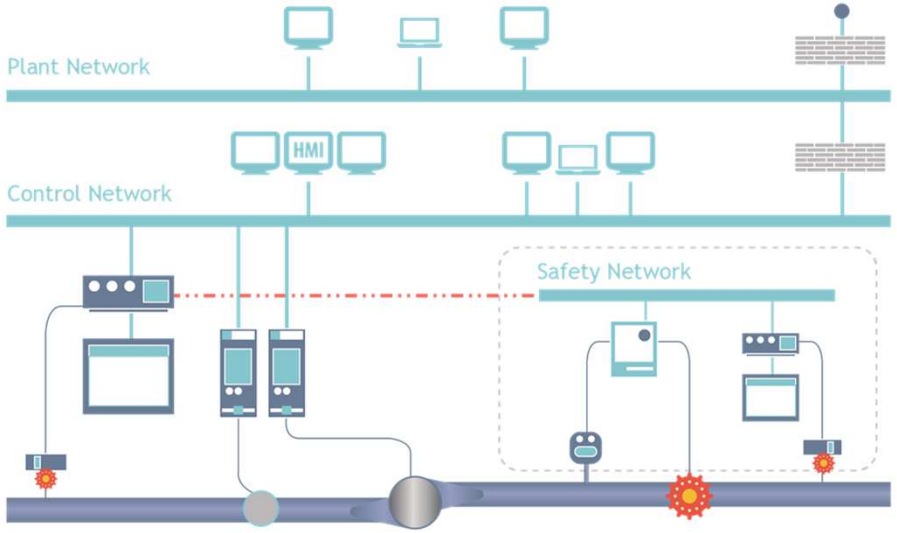
2014-2017 - Mail di phishing appositamente studiate per sistemi ICS.

ESEMPI

# SOLO ALCUNI ALTRI CASI

Di seguito alcuni disastri dovuti ad attacchi informatici

Selettore a chiave per per programmazione


## TRISIS - TRITON

2017 - Vengono presi di mira i sistemi Snyder Electric SIS (safety instrumented system).

Vengono attaccati impianti di gassificatori in Sud Arabia.

ESEMPI

# “NON A TARGET “
# IL RANSOMWARE


>2013 - Anche attacchi “NON A TARGET” creano pesanti ripercussioni nel mondo ICS.

# CATTIVE CONFIGURAZIONI

## Ski Lift in Austria Left Control Panel Open on the Internet

By Catalin Cimpanu — April 26, 2018 — 05:45 AM — 0

Officials from the city of Innsbruck in Austria have shut down a local ski lift after two security researchers found its control panel open wide on the Internet, and allowing anyone to take control of the ski lift's operational settings.

The two researchers are Tim Philipp Schäfers and Sebastian Neef, both with InternetWache.org, an IT security-focused organization.

### PATSCHERKOFEL RESORT

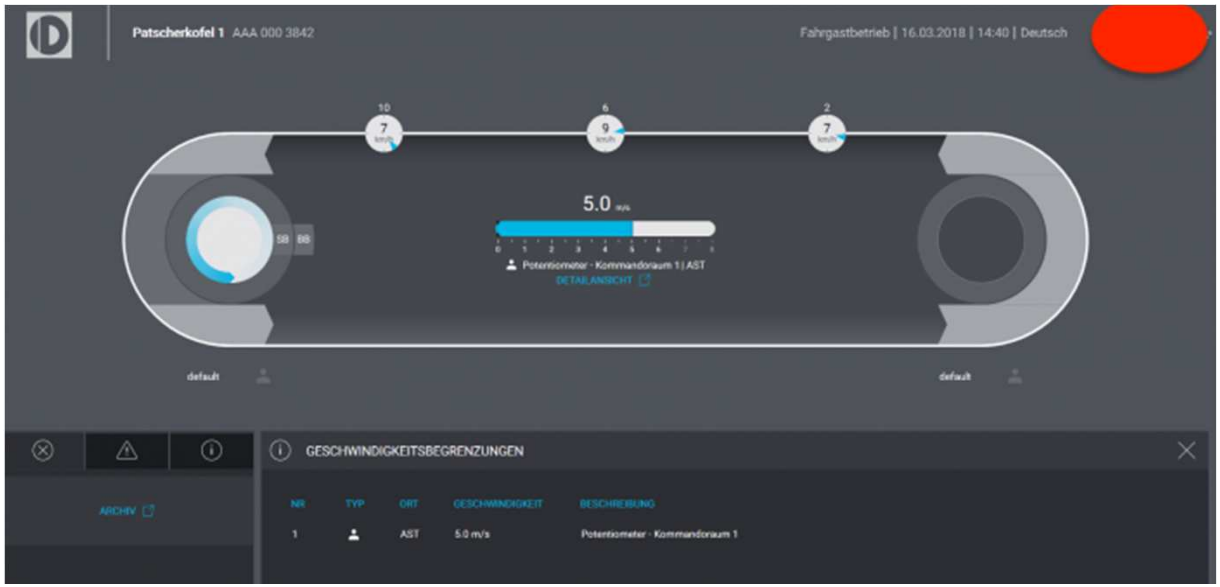
Il software di gestione HMI presentava una vulnerabilità header injection e cross-site scripting, risolta dal produttore in una versione successiva del software, ma in questo caso il software non era stato aggiornato.

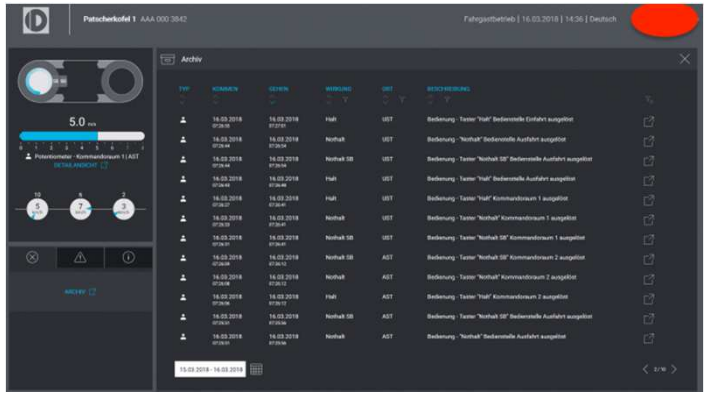
Il pannello di gestione era pubblicato direttamente in Internet e non usa il protocollo di comunicazione cifrato HTTP**S**

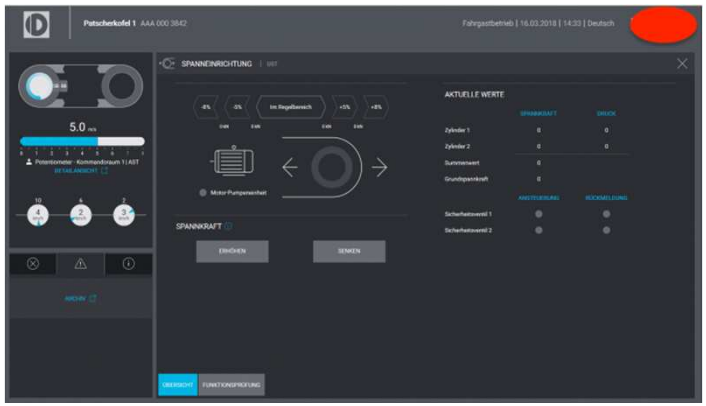
ESEMPI

# CATTIVE CONFIGURAZIONI

Di seguito alcuni disastri dovuti ad attacchi informatici



IL FOCUS

# COME FANNO

COME FANNO

# HACK SEARCH

## CVE-2019-10991 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

### Current Description

In WebAccess/SCADA, Versions 8.3.5 and prior, multiple stack-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.

**Source:** MITRE

View Analysis Description

### Impact

**CVSS v3.0 Severity and Metrics:**

**Base Score:** 9.8 CRITICAL
**Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3.0 legend)
**Impact Score:** 5.9
**Exploitability Score:** 3.9

**Attack Vector (AV):** Network
**Attack Complexity (AC):** Low
**Privileges Required (PR):** None
**User Interaction (UI):** None
**Scope (S):** Unchanged
**Confidentiality (C):** High
**Integrity (I):** High
**Availability (A):** High

**CVSS v2.0 Severity and Metrics:**

**Base Score:** 7.5 HIGH
**Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)
**Impact Subscore:** 6.4
**Exploitability Subscore:** 10.0

**Access Vector (AV):** Network
**Access Complexity (AC):** Low
**Authentication (AU):** None
**Confidentiality (C):** Partial
**Integrity (I):** Partial
**Availability (A):** Partial
**Additional Information:**
Allows unauthorized disclosure of information
Allows unauthorized modification

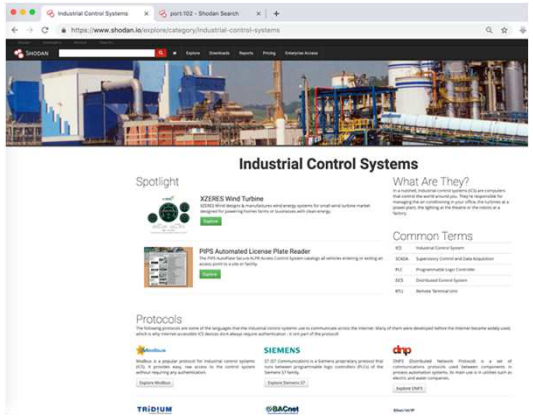
### QUICK INFO

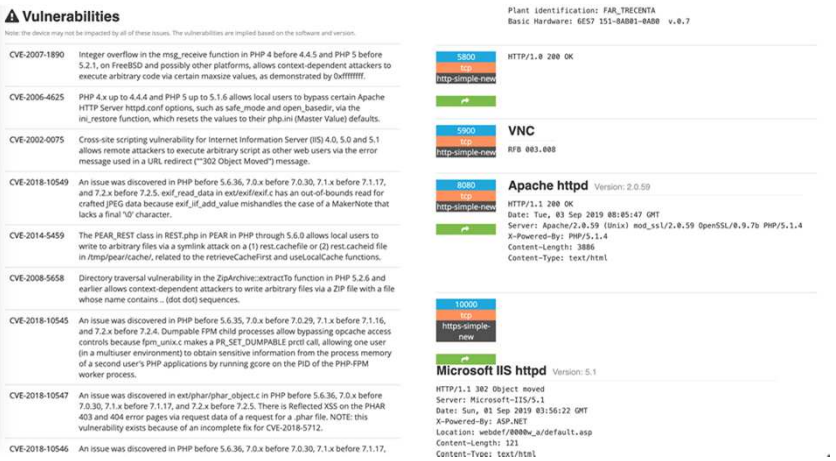
**CVE Dictionary Entry:**
CVE-2019-10991
**NVD Published Date:**
06/28/2019
**NVD Last Modified:**
07/02/2019

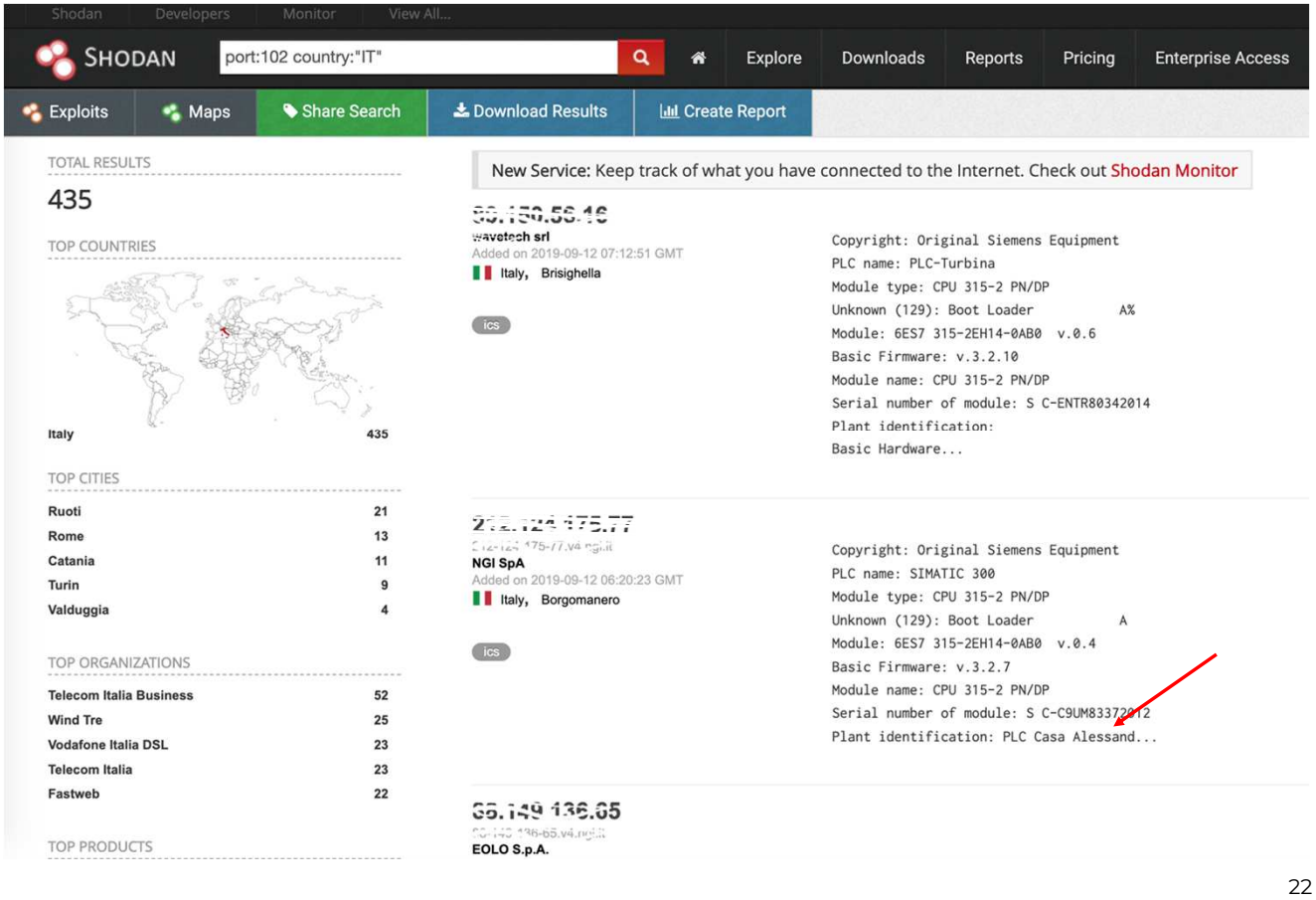
COME FANNO

# HACK SEARCH

Esiste un motore di ricerca per scoprire quali sono i sistemi industriali vulnerabili www.shodan.io



COME FANNO

# HACK SALES

Si possono comprare reti Botnet già printe

IL FOCUS

# I MOTIVI

L' INTERVISTA

# COME VALUTI L'INVESTIMENTO NELL' IT SECURITY

Alcune opinioni degli intervistati - Fonte CQURI

**Non mi è mai successo nulla, credo di essere a posto così!**

Secretato

**Gli Hacker non hanno interessi ad attaccare i miei impianti!**

Secretato

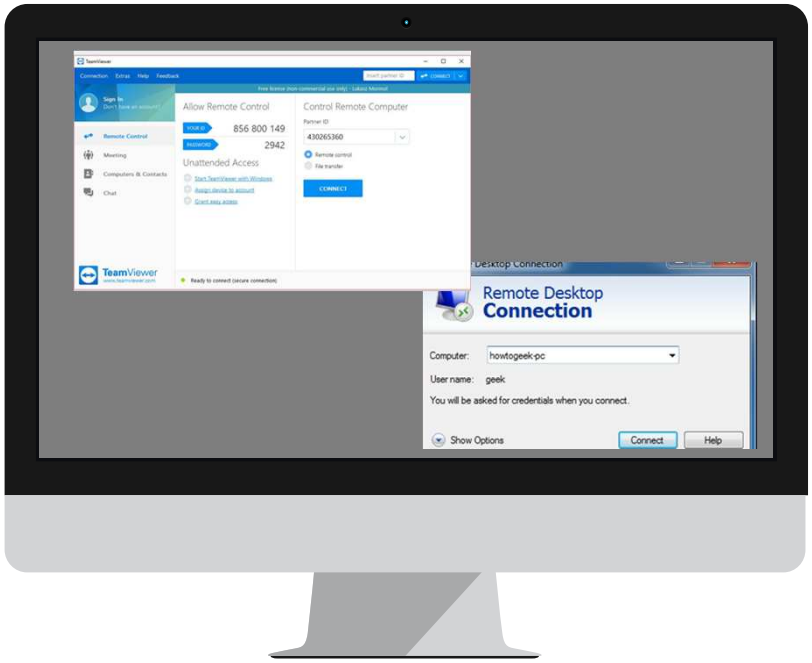
**Io sono assicurato contro la perdita dei dati e produttività, non credo investirò ulteriormente.**

Secretato

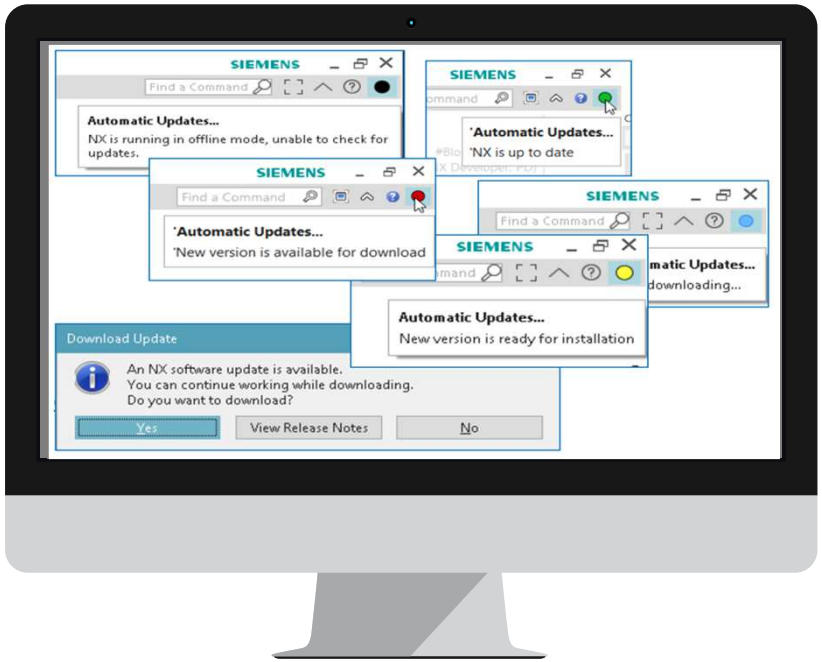
PERCHE'

# CATTIVE ABITUDINI

Esistono dei motivi tecnici che rendono gli attacchi ai sistemi ICS più “facili”




TEAM VIEWER / RDP

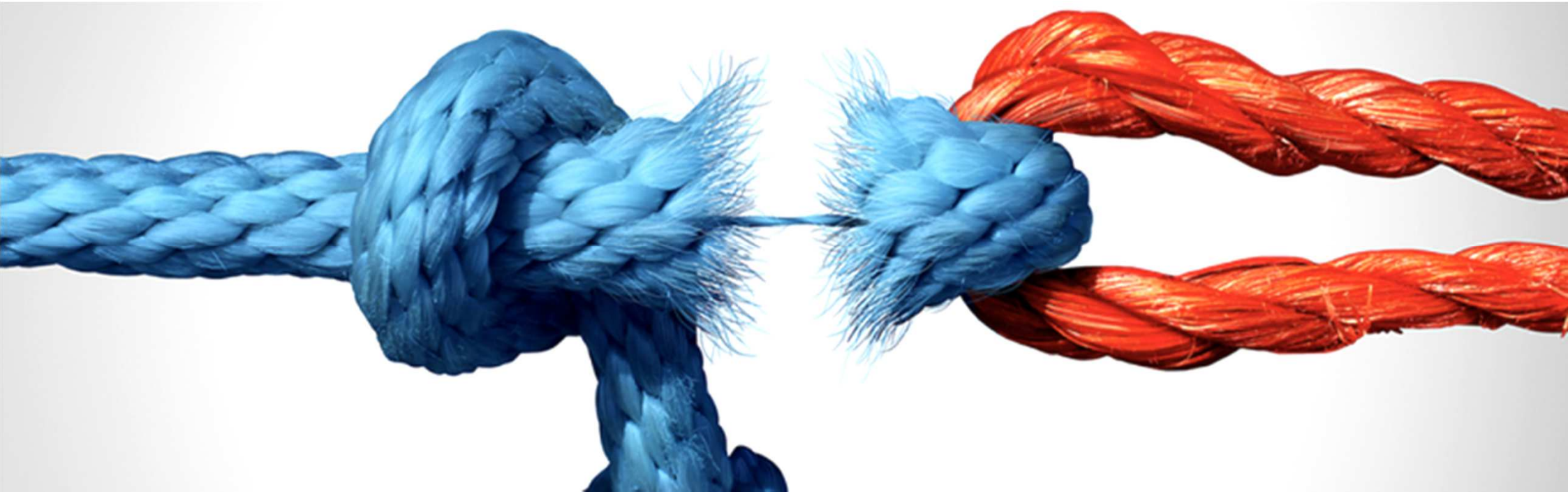



AGGIORNAMENTI

APP WEBCAM

BEST PRACTICES

# AIR GAP
# NORME & BEST PRACTICES



LA LEGGE

# GDPR – UE 2016/114

Direttiva introdotta con Decreto Legislativo n. 65 del 18/5/2018

## SECURITY BY DESIGN E BY DEFAULT

BEST PRACTICES

# NIST 800-82

National institute of standards and technology - Introduce i paradigmi per la creazione e gestione sicura di una struttura ICS

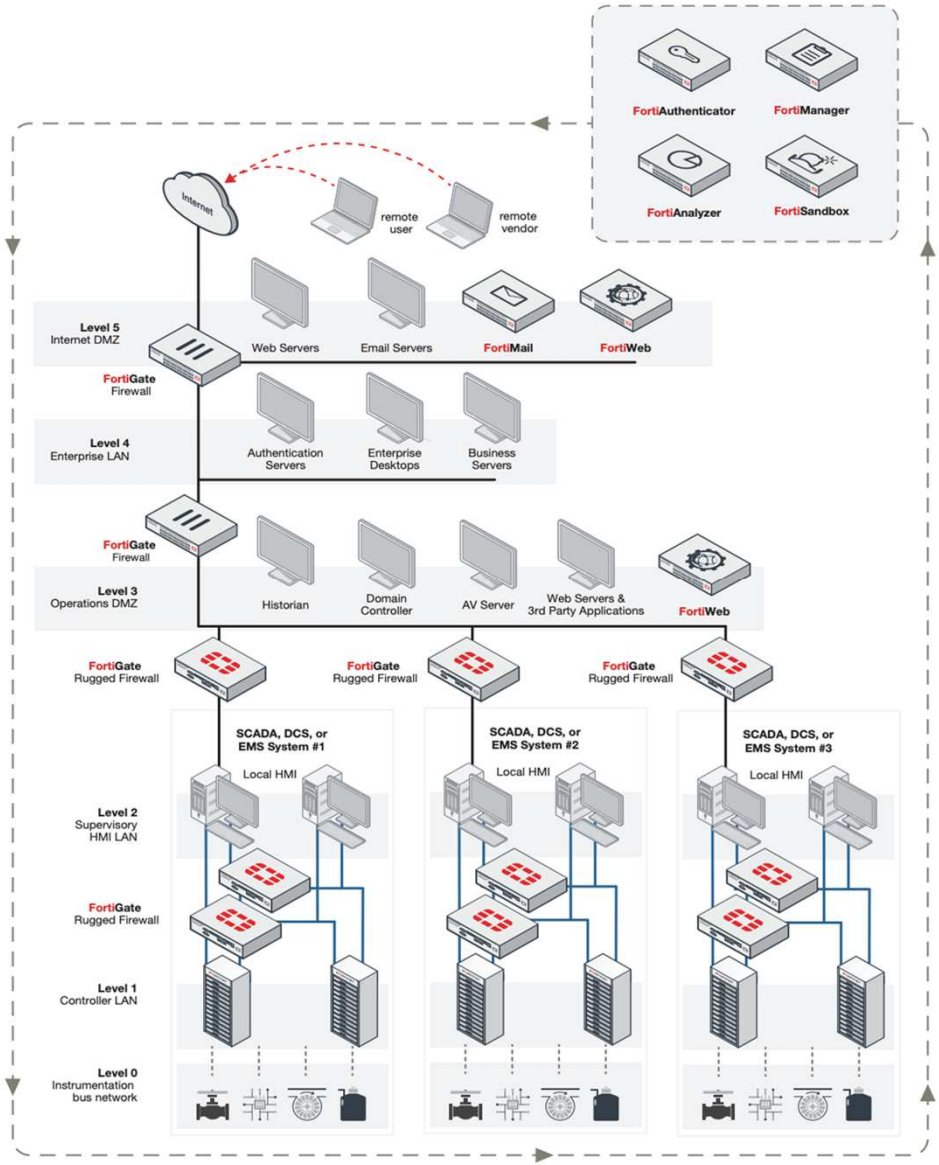
## Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

BEST PRACTICES

# IEC-62443 / ISA 99

International Society for Automation - introdurre una segmentazione logica a 6 live

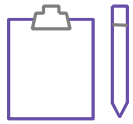


COME RISOLVERE

# LE SOLUZIONI

SECURITY SOLUTIONS

# SOLUZIONE



## PROGETTO

Il design di rete e la progettualità è la base fondante dove si sviluppa un processo di sicurezza

## MESSA IN OPERA

L'installazione e la configurazione degli apparati/software secondo criteri e standard riconosciuti

## DISASTER RECOVERY PLAN

La scrittura di piano di ripristino nel caso di incidenti IT

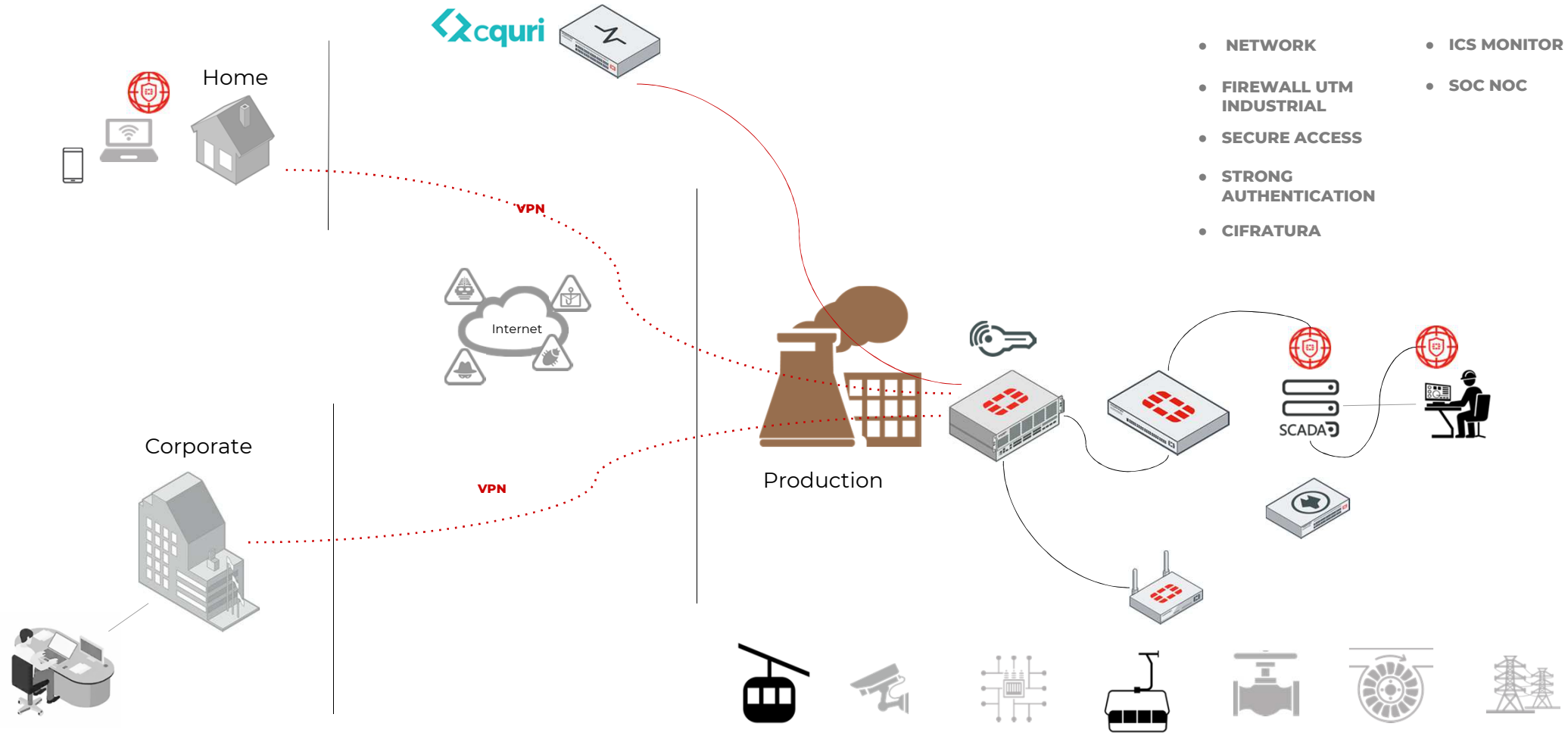
## MANTENIMENTO

Il mantenimento costante della sicurezza e dei componenti ad essa legata

LA SICUREZZA E' UN PROCESSO, NON UN SOFTWARE E/O UN "PEZZO DI FERRO"

SECURITY SOLUTIONS

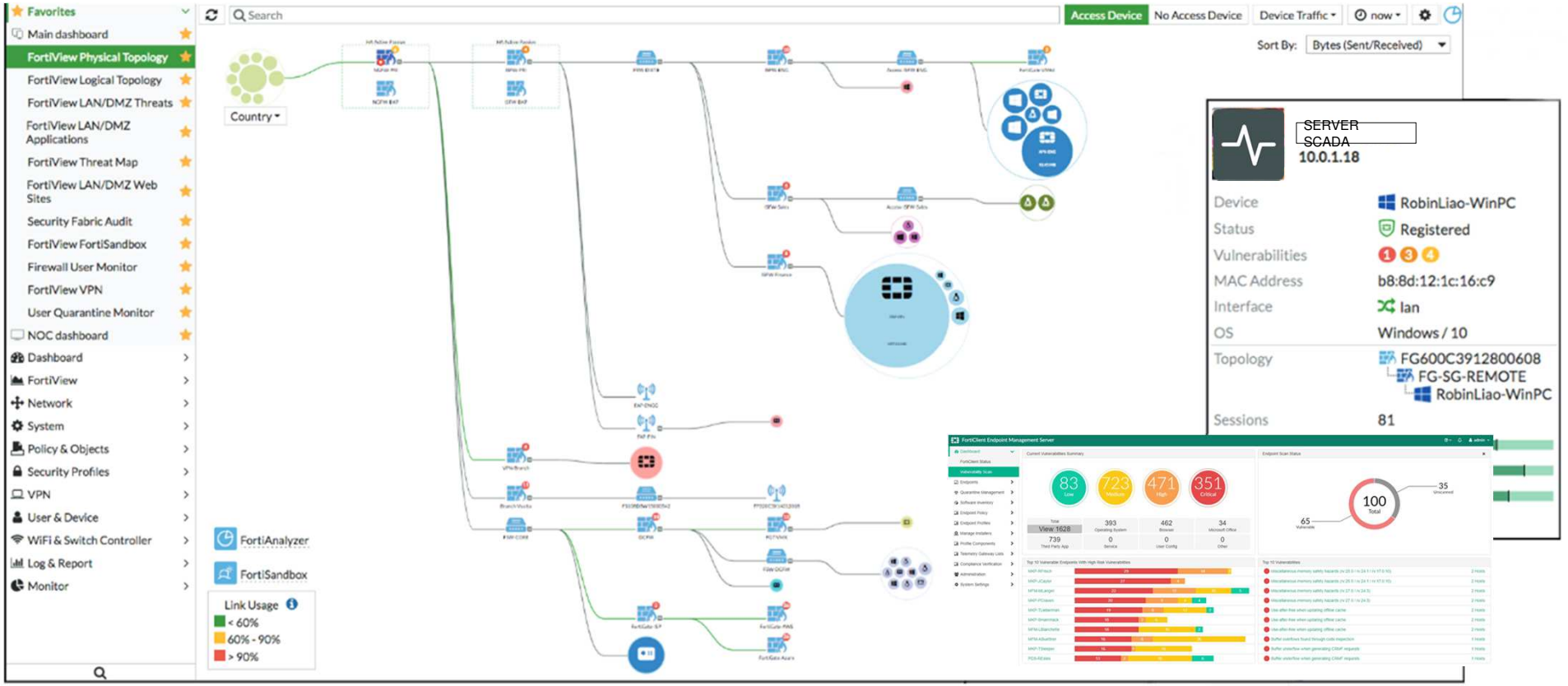
# SOLUZIONE




- NETWORK
- FIREWALL UTM INDUSTRIAL
- SECURE ACCESS
- STRONG AUTHENTICATION
- CIFRATURA
- ICS MONITOR
- SOC NOC

SECURITY SOLUTIONS

# SECURITY FABRIC



COME TROVARCI

# CONTATTI

**800.978.302**

sales@cquri.com

www.cquri.com