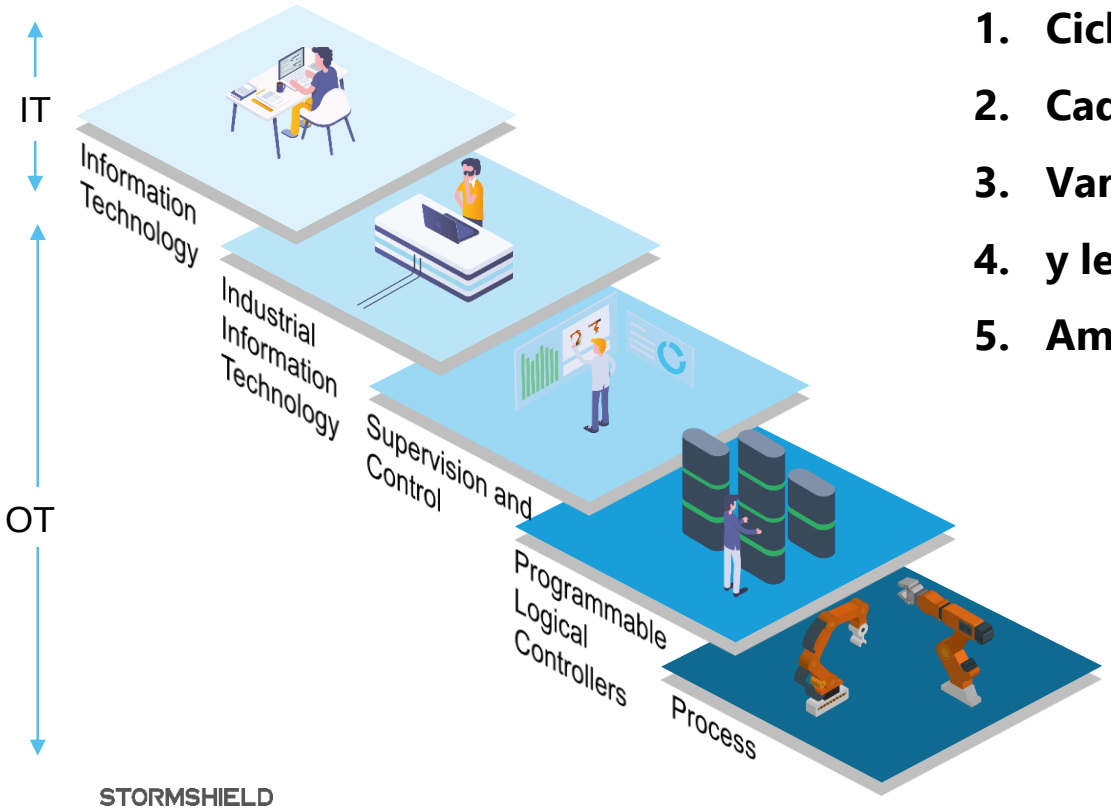
STORMSHIELD

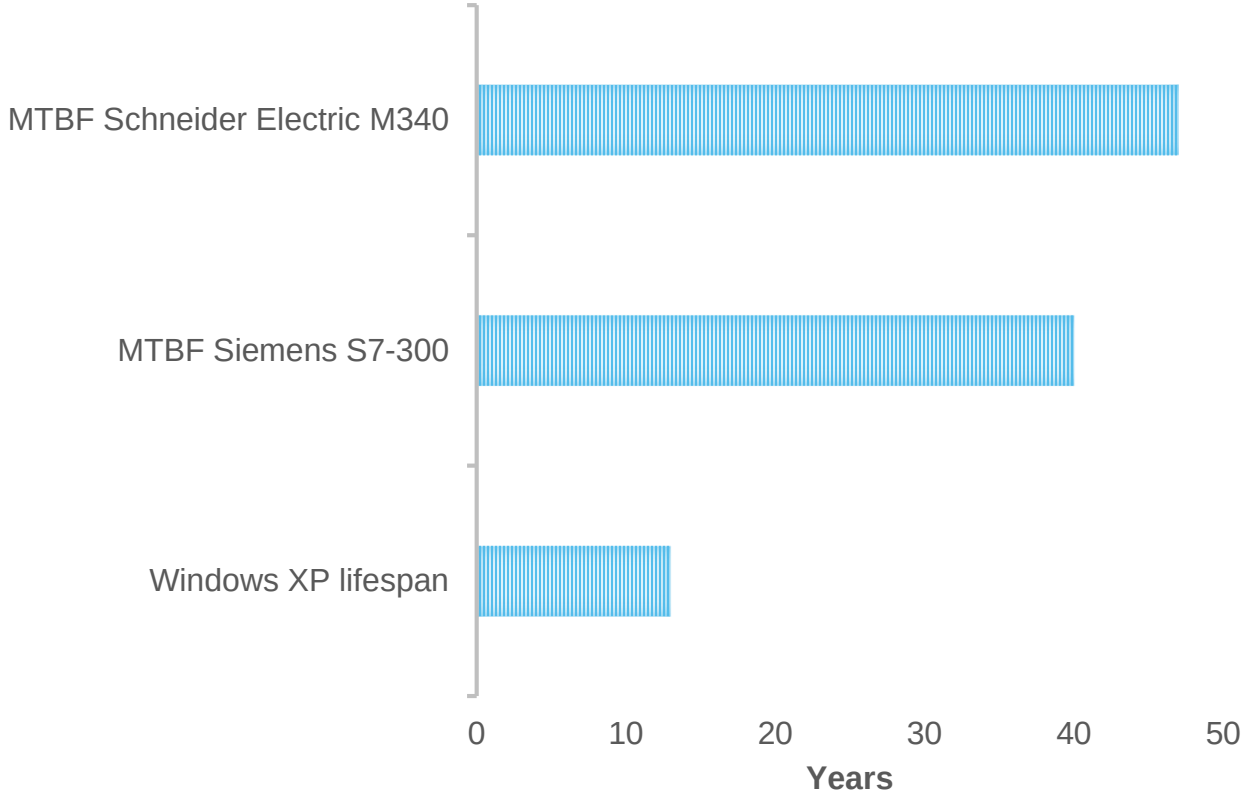
Network Endpoint Data

Retos actuales



1. **Ciclos de vida muy largos**
2. **Cada caso es particular**
3. **Variedad de normas**
4. **y legislaciones**
5. **Amenazas innegables**

1. Ciclos de vida largos



2. Particularidad de cada caso

20+
Protocolos Estandarizados

Modbus, OPC Classic, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850, EtherCAT, OPC UA, ICCP, MQTT, COSEM, ….

700+
Protocolos propietarios

UMAS, S7, TSAA, SAAT, HNZ, …….

3. Variedad de normas

ISA 95 (automatización)

EN 61373 (ferroviario)

IEC 62443 (automatización y seguridad de los sistemas de control)

EC 61850 (electromagnetismo)

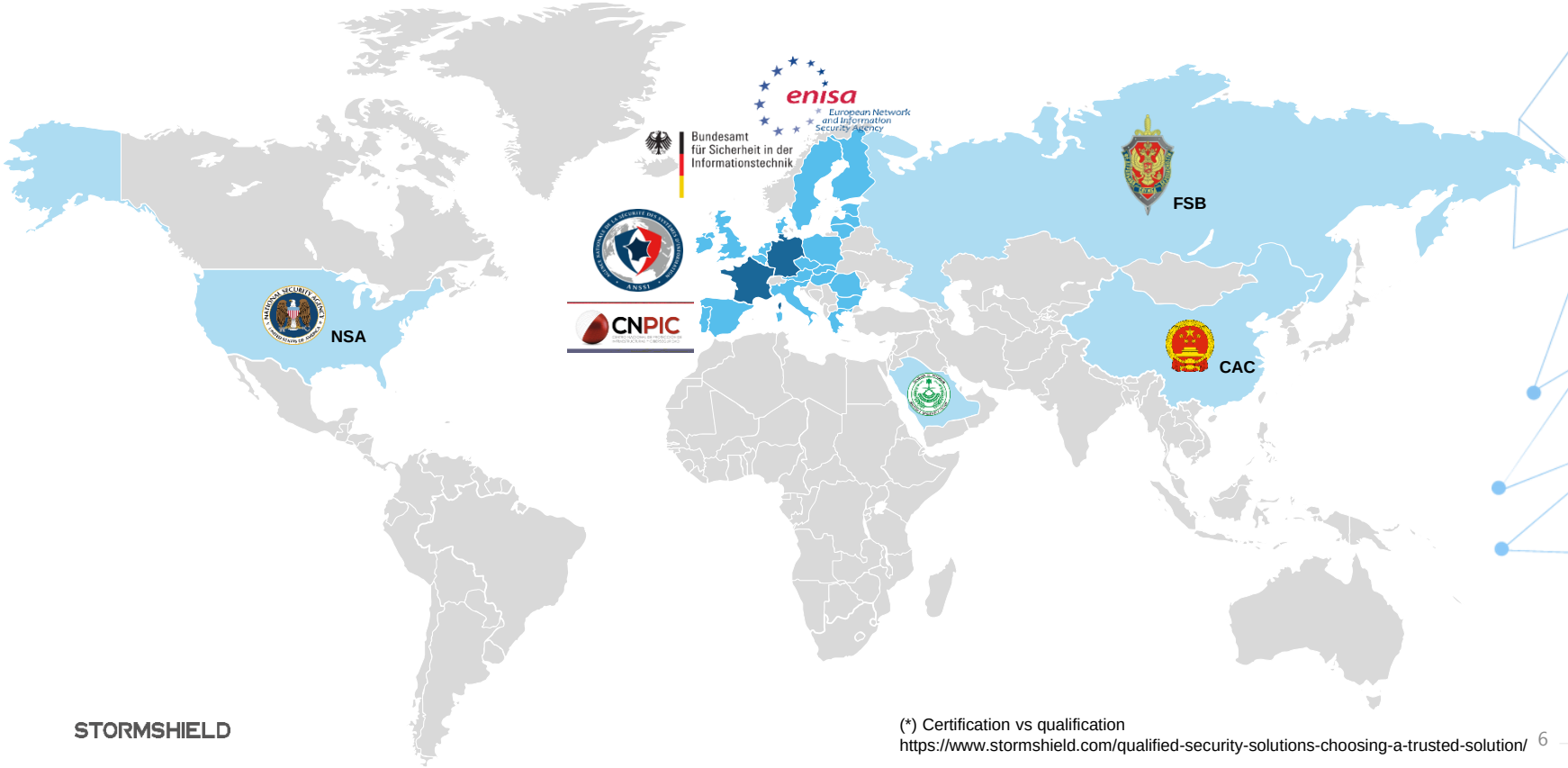
MIL STD-810G (vibración militar)

IEC 60068-2 (tests ambientales)

EN 60945 (naval)

(*) Certification vs qualification, un doute
https://www.stormshield.com/fr/solutions-de-securite-qualifiees-le-choix-dune-solution-de-confiance/

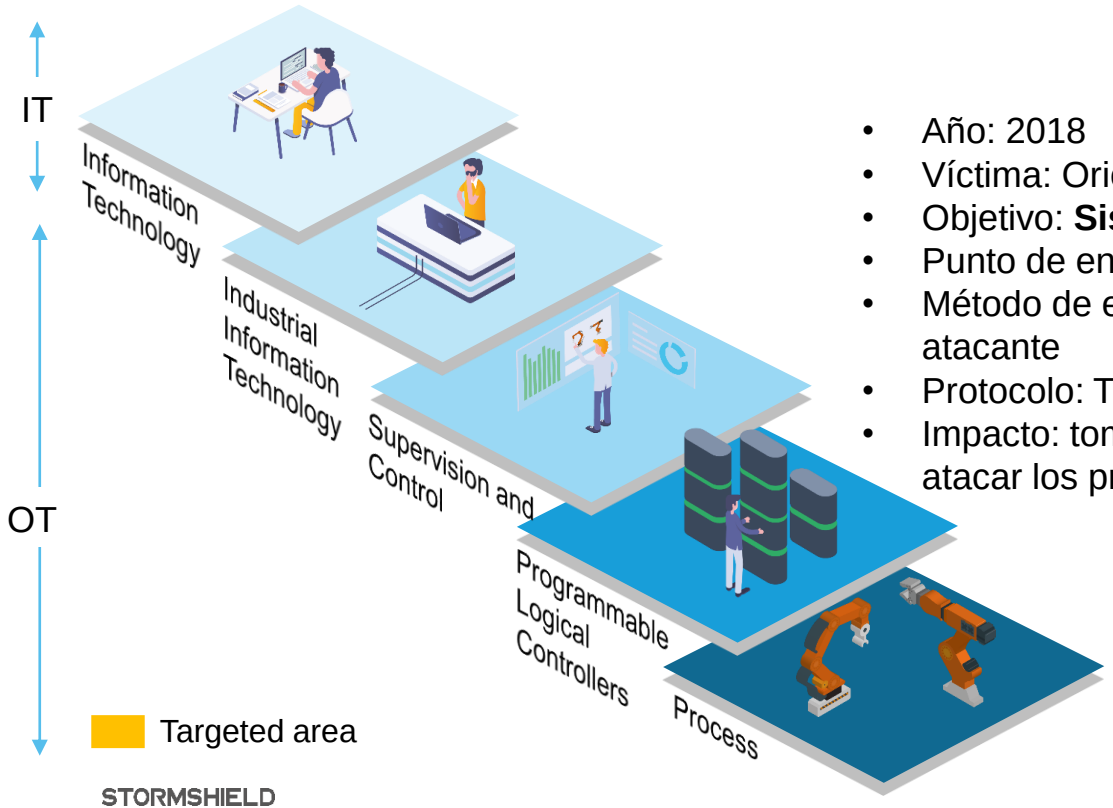
4. Variedad de legislaciones (*)



(*) Certification vs qualification
https://www.stormshield.com/qualified-security-solutions-choosing-a-trusted-solution/

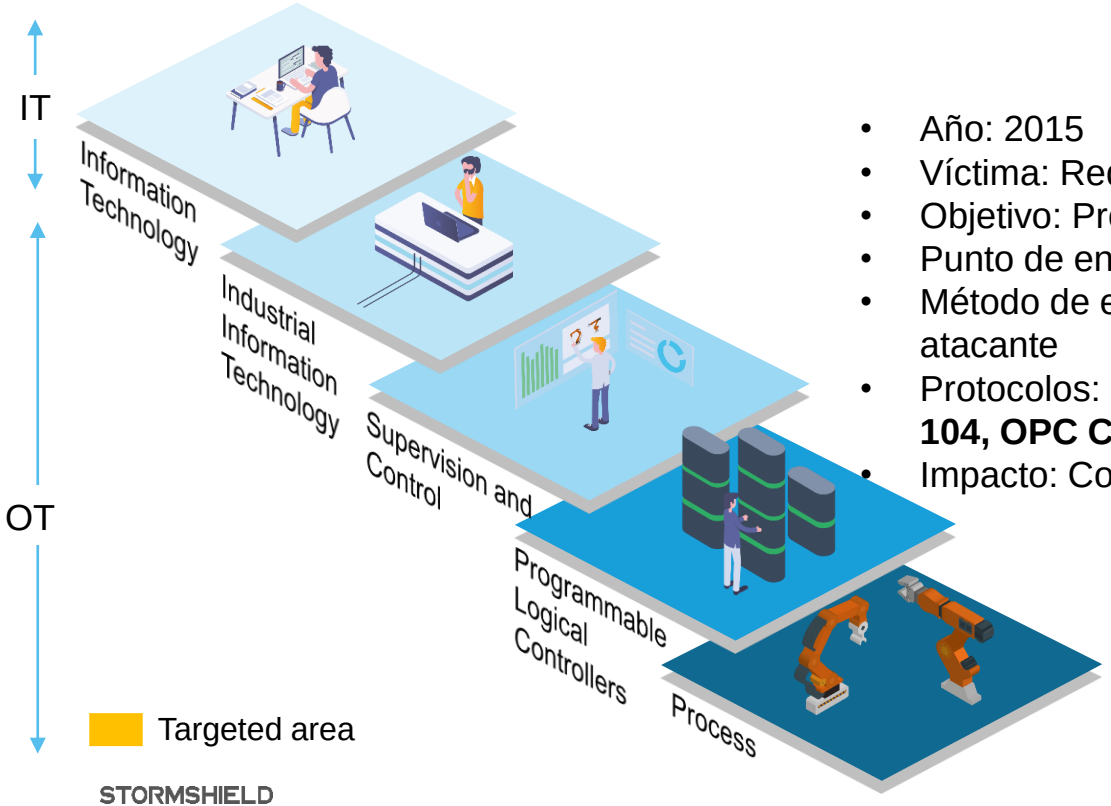
5. Y sin embargo, las amenazas son innegables

TRITON: Ataque por un Estado



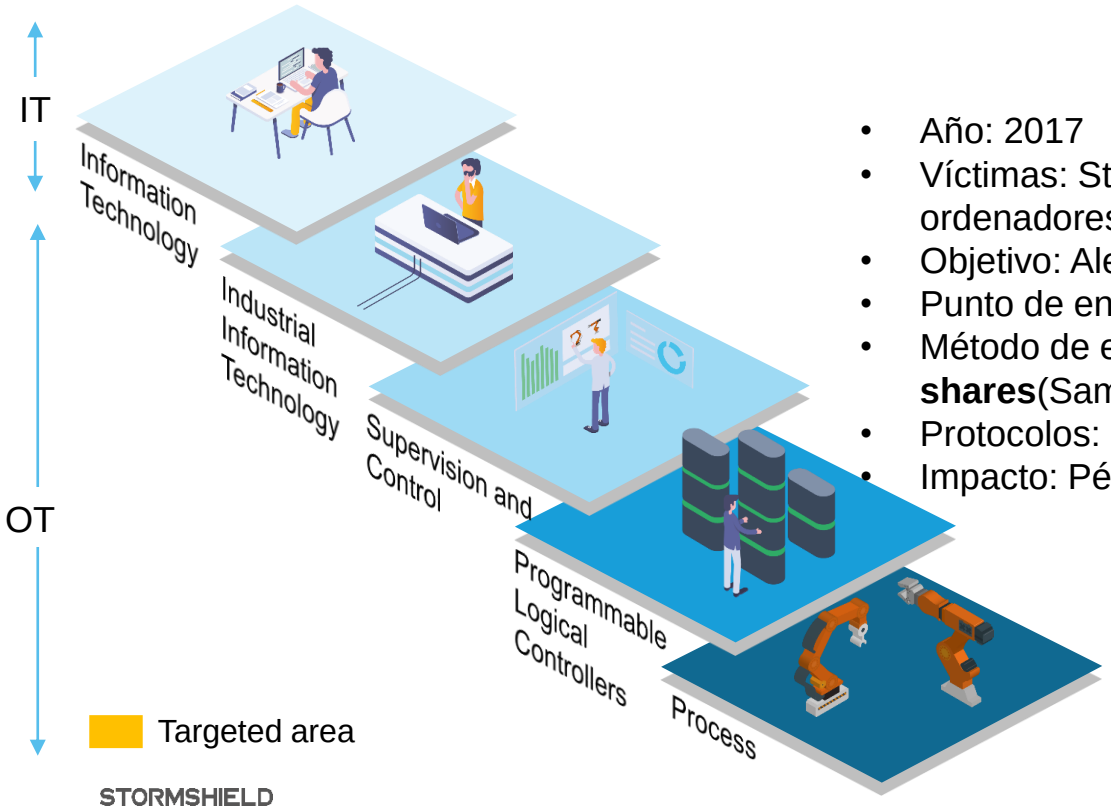
- Año: 2018
- Víctima: Oriente Medio – Desconocido
- Objetivo: **Sistema Triconex**
- Punto de entrada: IT DMZ
- Método de expansión: Controlado por el atacante
- Protocolo: TSAA (Triconex propietario)
- Impacto: toma de control de Triconex para atacar los procesos sin ser detectado

INDUSTROYER: Malware disponible en la Darkweb



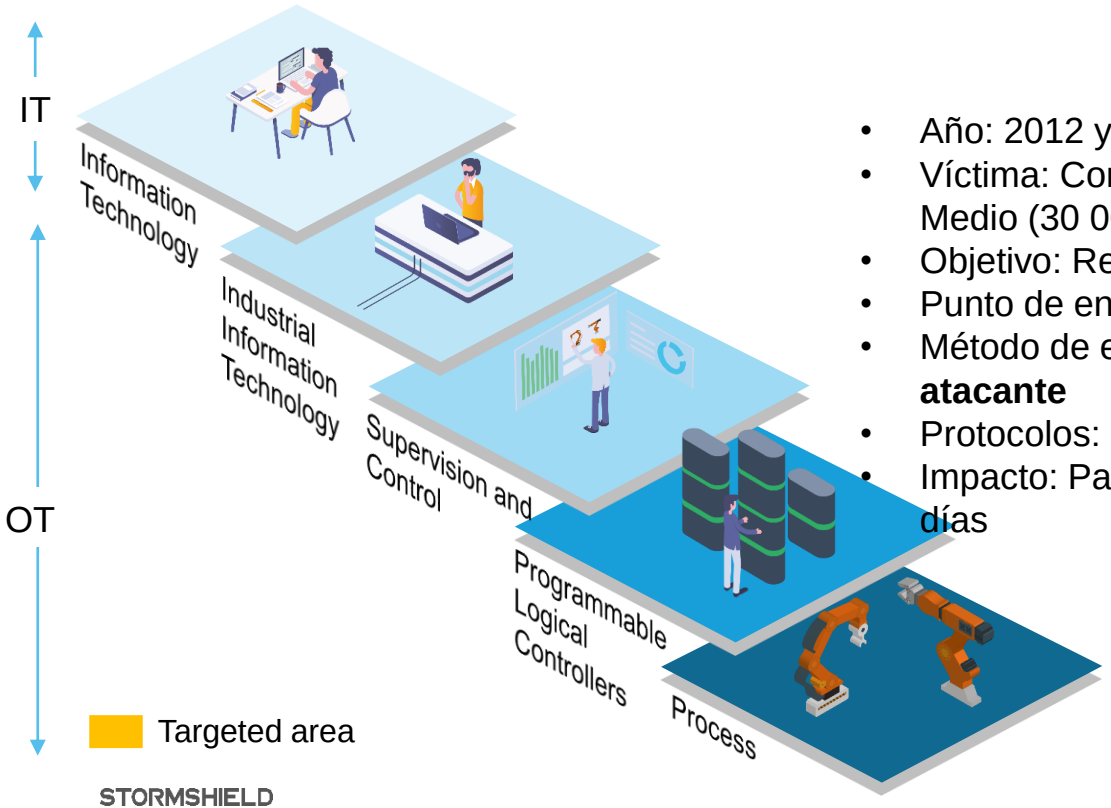
- Año: 2015
- Víctima: Red eléctrica de Ucrania
- Objetivo: Procesos
- Punto de entrada: IT spearphishing
- Método de expansión : Controlado por el atacante
- Protocolos: **IEC 60780-5-101, IEC 60780-5-104, OPC Classic, IEC 61850**
- Impacto: Control de subestaciones eléctricas

WANNACRY: Ataque masivo



- Año: 2017
- Víctimas: St Gobain, Renault,…. 150 000 ordenadores en todo el mundo
- Objetivo: Aleatorio
- Punto de entrada: email
- Método de expansión : **Windows shares**(Samba)
- Protocolos: SMB v1 (IT)
- Impacto: Pérdida de producción

SHAMOON: Ataque dirigido desde IT



- Año: 2012 y 2016 (V2)
- Víctima: Compañía de Oil & Gas en Oriente Medio (30 000 PCs en 2012)
- Objetivo: Red industrial
- Punto de entrada: Email
- Método de expansión: **Controlado por el atacante**
- Protocolos: Cualquiera disponible
- Impacto: Parada de la producción durante 15 días

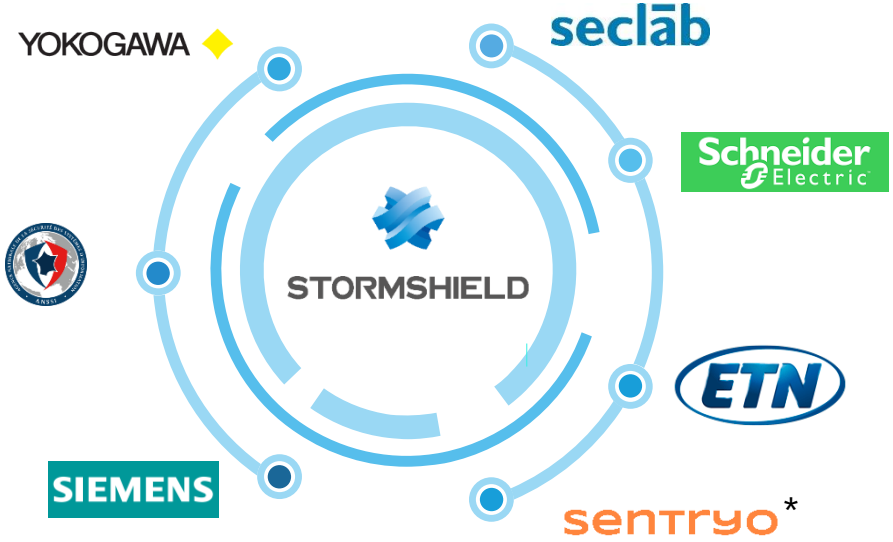
Oferta Industrial

IT/OT end to end protection

STORMSHIELD

Nuestra historia en industria

Desde hace más de 10 años, Stormshield y su ecosistema proporcionan protección para los sitemas OT y la convergencia IT/OT.



Stormshield: Una propuesta industrial diferenciadora

NETWORK SECURITY

SNS - NETWORK SECURITY

12 Next Gen firewall range

ENDPOINT SECURITY

SES - ENDPOINT SECURITY

Workstations and servers protection

SMC - MANAGEMENT CENTER

Network monitoring and handling

Stormshield Network Security

IT/OT end to end protection

STORMSHIELD

SNS – Protección para redes industriales

Ruggedized

SNi40

SN160W SN210W

SN160 SN210 SN310 SN510 SN710 SN910 SN2100 SN3100 SN6100

Small remote sites

Main sites and VPN concentrators

Backbones and datacenters

Un único firmware

CITRIX ready · openstack · KVM · Hyper-V · vmware READY · Microsoft Azure · amazon web services

Virtualized range

Stormshield Endpoint Security

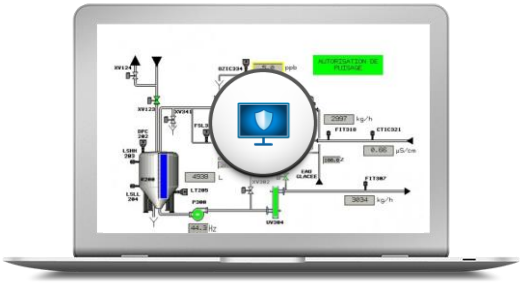
IT/OT end to end protection

STORMSHIELD

SES – Agente protector de ordenadores industriales (EPP/EDR)

Supervisión

Consola de Ingeniería



Mantenimiento remoto

Protección incluso en entornos no conectados

Protección no basada en firmas

Análisis determinístico de comportamiento ✓

Sólo aplicaciones certificadas

Whitelisting ✓

Blacklisting ✓

Prevención de la difusión del ataque

Aislamiento de la estación de trabajo

- Conformidad ✓
- Cuarentena ✓
- IPS/IDS firewall ✓

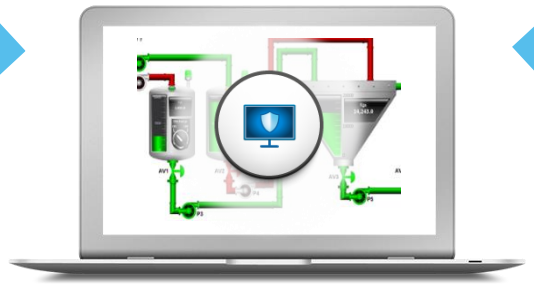
Mantenimiento remoto

- Control de VPNs ✓
- Conformidad ✓
- Restricción de uso de redes ✓

Gestión de dispositivos externos

Gestión de USBs

- Permisos a USBs de confianza listados ✓
- Prohibición a USBs no listados o no de confianza ✓
- Cifrado del contenido de USB ✓



Control de uso de dispositivos externos

- Permiso/Prohibición de USBs por tipo ✓
- Modo de solo lectura en dispositivos externos ✓

Extensión de la vida de las estaciones de trabajo

Sistemas actuales

Windows 7 SP1 – 32/64bits	✓
Windows 8.1 Update 1 – 32/64bits	✓
Windows 10 2015 LTSB - 32/64 bits	✓
Server 2008 R2 - 64 bits	✓
Server 2012 R2 - 64 bits	✓

Sistemas en fin de vida

	Fin de vida	SES
Windows Vista SP2 – 32 bis	Abril 2017	2021
Windows 2003 Server 32 bits	Julio 2015	2021
Windows 2003 Server R2 32 bits	Julio 2015	2021
Windows XP SP3	Abril 2014	2021

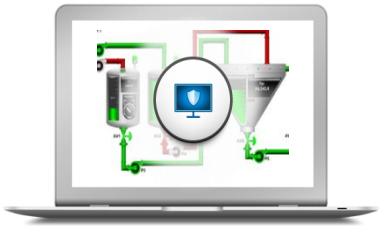
¿Por qué Stormshield?

Stormshield Industrial Offer

Solución Europea que cumple **sus necesidades**

Cualificación estándar y las certificaciones europeas **más altas**

Equipo **dedicado** que realiza **deep packet inspection**



Agente diseñado para **sistemas con altas restricciones**

Gracias

We look forward to seeing you again

https://www.stormshield.com/solutions/by-industry/industries/