TD SYNNEX

Stormshield e la protezione delle infrastrutture medicali

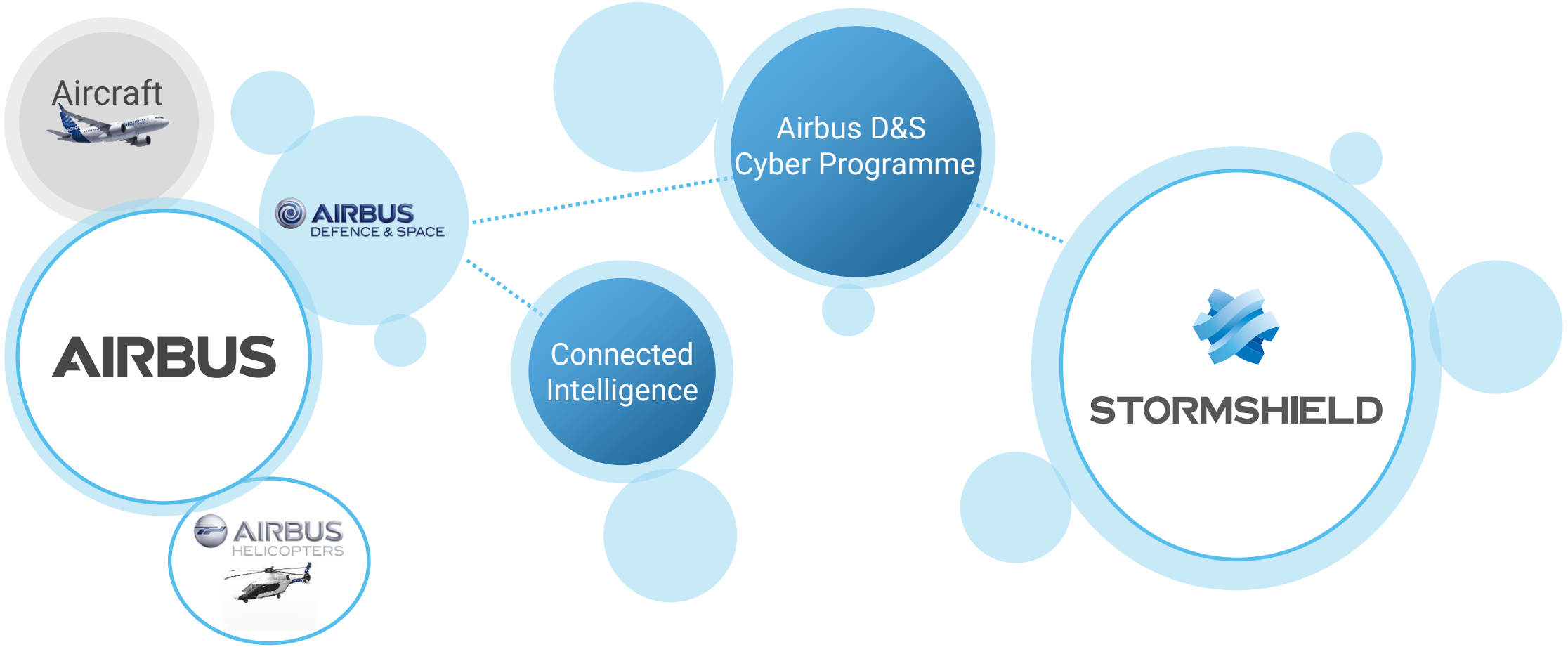
Protezione dei dati, delle reti e delle infrastrutture critiche

06 Dicembre 2024

Webinar

Andrea Scattina – Country Manager Italy - Stormshield
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

Storia industriale prestigiosa



Un partner Europeo per la Cyber Security

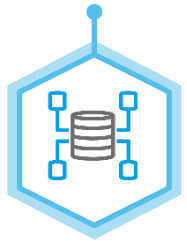
STORMSHIELD NETWORK
Security

Una gamma di Next Generation Firewall / VPN/IPS

STORMSHIELD ENDPOINT
Security

Hardenizzazione di workstation e server Windows

Stormshield XDR
CONTROLLO • PRODUTTIVITÀ • COERENZA

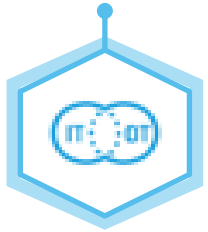


Raccolta e correlazione dati automatica tra più livelli di sicurezza (Network , Endpoint…)

STORMSHIELD DATA
Security

Criptazione end-to-end multi-device e multi-applicazione

INDUSTRIAL Cybersecurity



Messa in sicurezza delle infrastrutture industriali e operative

AIRBUS CYBERRANGE

Ambiente di test , Digital twin , piattaforma per red e blue teaming , capture the flag, Training

STORMSHIELD Log Supervisor

Normalizzazione dei dati di LOG per report, analisi e indagini efficienti

STORMSHIELD Management Center

Gestione centralizzata Firewall Stormshield e integrazione con SLS

Attacchi alla sanità

Attacco Informatico all'Ospedale di Verona rivendicato da Rhysida. 10 bitcoin al miglior offerente e dati sanitari online

Chiara Nardini : 10 Novembre 2023 10:33

Redazioni Tgr

Roma

Temi Caldi

Cronaca

BLACK FRIDAY

Accedi

nefratelli e Sacco:
llentati. «Dati dei

sky tg24 OVERVIEW MEDIORIENTE

CRONACA News Approfondimenti Numeri Pander

CRONACA

Attacco hacker a Synlab, pubblicati sul dark web i dati sanitari dei pazienti: cosa fare

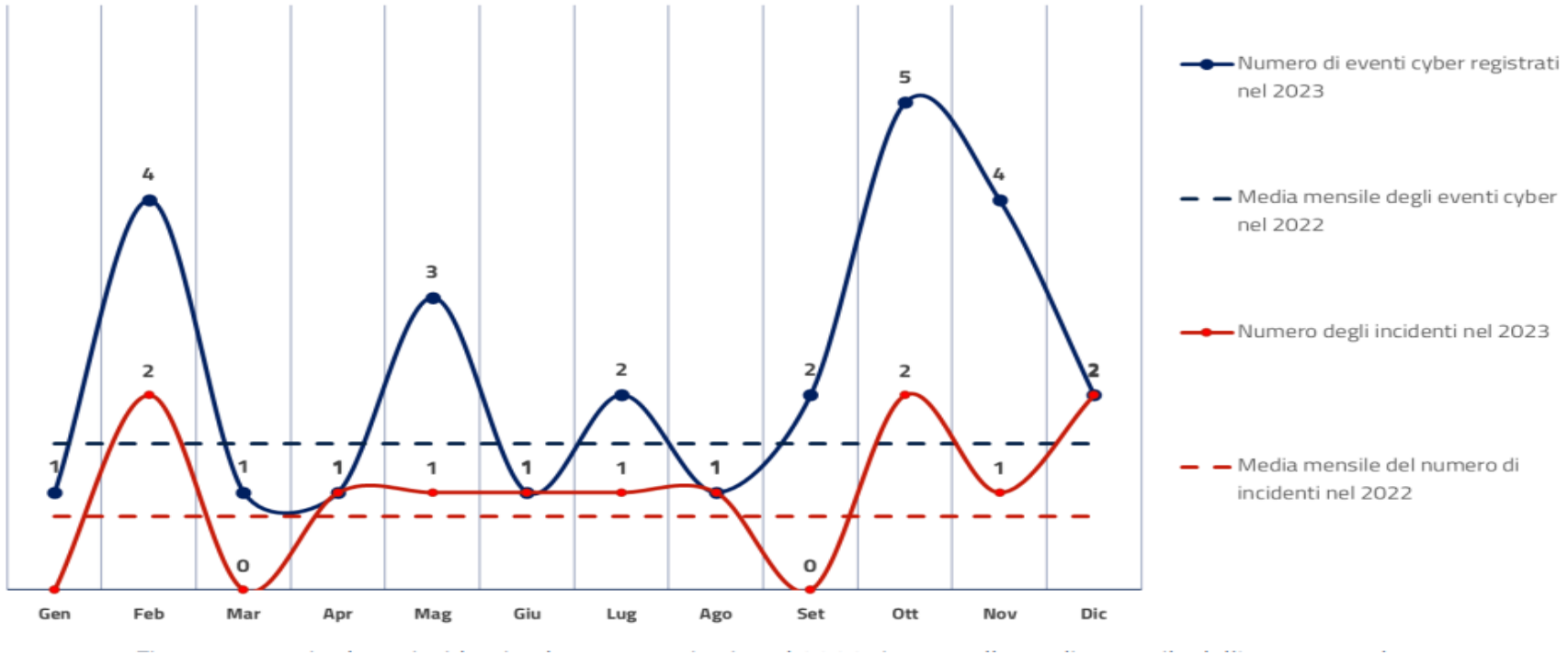
15 mag 2024 - 12:05

CORRIERE TV

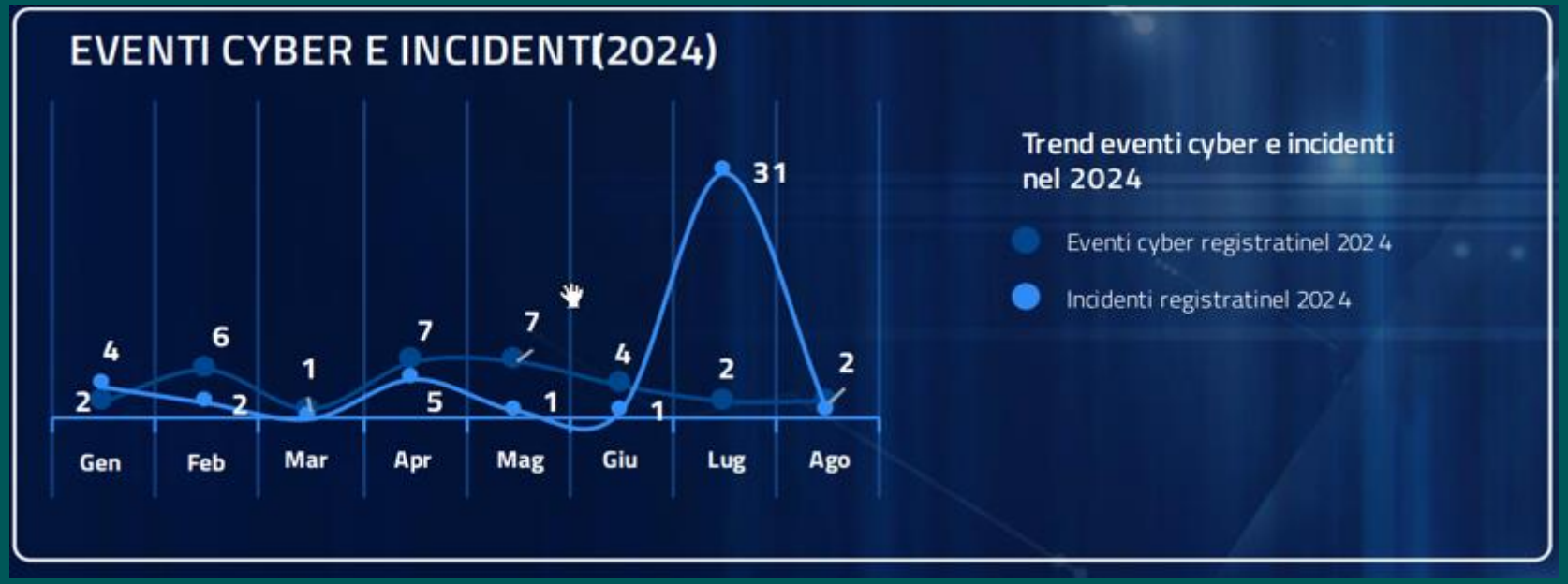
sei mesi +23%"

Tipologia di attacchi in ambito sanitario

- **evento cyber**, un avvenimento con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti;
- **incidente**, evento cyber con impatto confermato sulla disponibilità, confidenzialità o integrità delle informazioni.



Tipologia di attacchi in ambito sanitario - 2024



Alcuni numeri - Eventi cyber

- gli attacchi **ransomware** risultano essere la minaccia cibernetica più diffusa per il settore, con il **35% degli eventi** nel 2023 e il **60% degli eventi** nel 2022;
- l'attività di **information disclosure** è stata rilevata nel **14% degli eventi** nel 2023;
- la **diffusione di malware tramite e-mail** è stata rilevata nell'**10% degli eventi** del 2023;
- lo **sfruttamento di vulnerabilità** ha caratterizzato il **10% degli eventi** nel 2023 e il **13% degli eventi** nel 2022.

ACN – La minaccia cibernetica al settore sanitario

Alcuni numeri - Incidenti

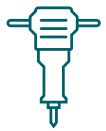
- i **ransomware** risultano essere la tipologia di incidente più diffusa, rappresentano infatti il **43% degli incidenti** nel 2023 e il **67% degli incidenti** nel 2022;
- la **diffusione di malware tramite e-mail** ha caratterizzato il **15% degli incidenti** nel 2023;
- l'**esfiltrazione** è stata rilevata nel **7% degli incidenti** nel 2023 e nel **8% degli incidenti** nel 2022;
- le **compromissioni da malware** hanno caratterizzato il **7% degli incidenti** nel 2023 e il **17% degli incidenti** nel 2022.

ACN – La minaccia cibernetica al settore sanitario

TD SYNNEX

7 passi della Kill Chain

Initial Access



Exploitation

Defense Evasion

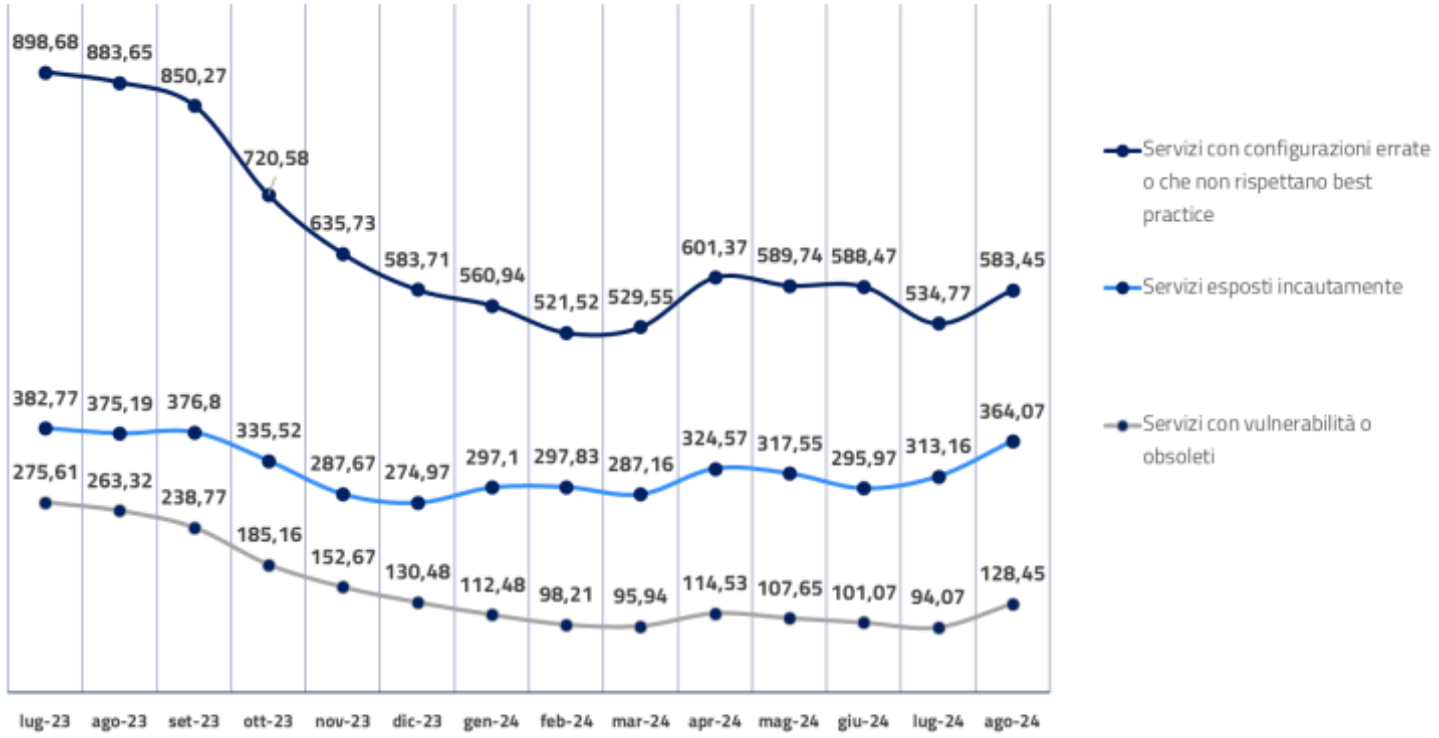
Data Exfiltration

Data Encryption

Impact

Ransom

Le Vulnerabilità



L'analisi riportata è stata svolta **analizzando passivamente** (ovvero senza interazione diretta) oltre 50.000 indirizzi IP associati al settore sanitario. Tra gli indirizzi IP analizzati dal 1° luglio 2023 al 31 agosto 2024, mediamente ogni giorno **2.178** sono risultati esporre pubblicamente dei servizi su Internet.

- Misconfiguration
- Servizi obsoleti
- Servizi esposti incautamente
- Nessuna politica di patching
- Nessun controllo su alcuni device
- Scarsa visibilità dei device
- Politica delle utenze inefficiente

Elementi critici in ambiente ospedaliero

Rete aziendale standard

Rete IT dello staff medico , farmacie, laboratori, ambulatori ecc

Apparati elettromedicali

MRI, scanner, respiratori ecc

Struttura ospedaliera

Sistemi di building automation, sistemi di gestione centralizzate di riscaldamento / raffreddamento , luci , ascensori,, gestione elettrica, controllo degli accessi ecc,

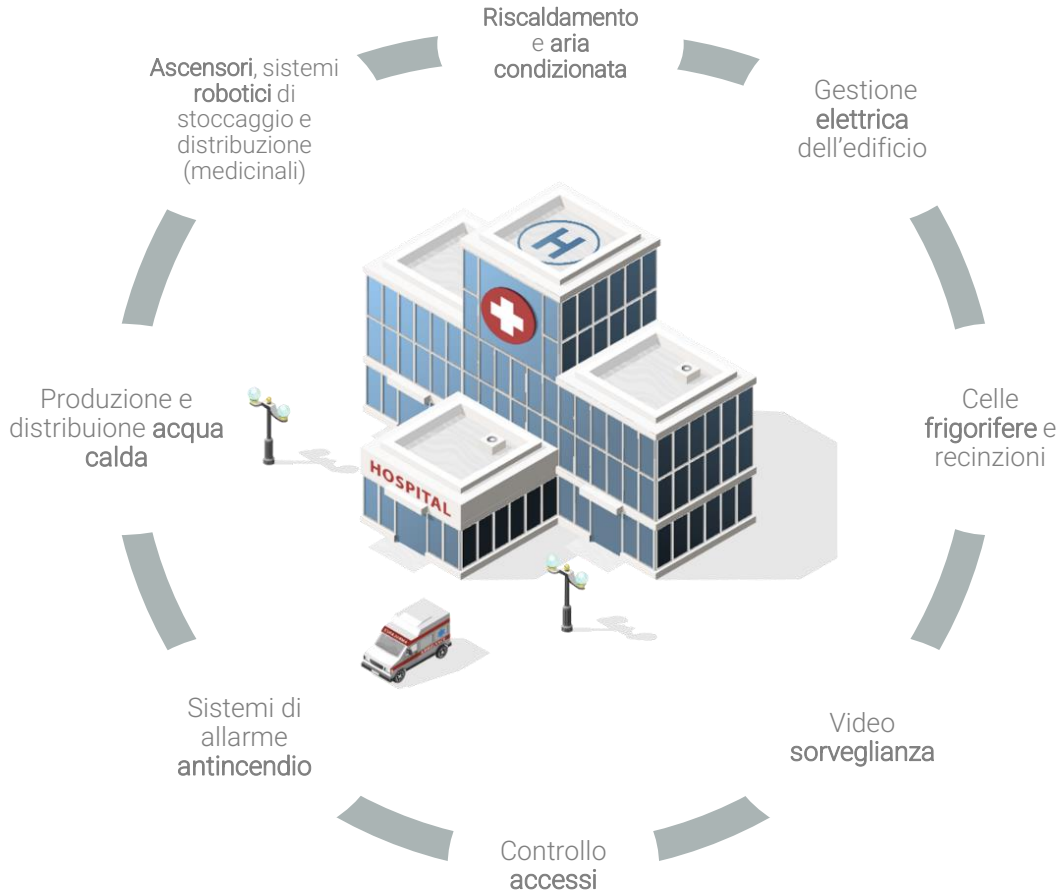
Maturita medio - alta

Parzialmente sicuri

Maturità bassa

Nessun investimento di cybersecurity pianificato

Elementi critici in ambiente ospedaliero



Protezione apparati Bio-medici

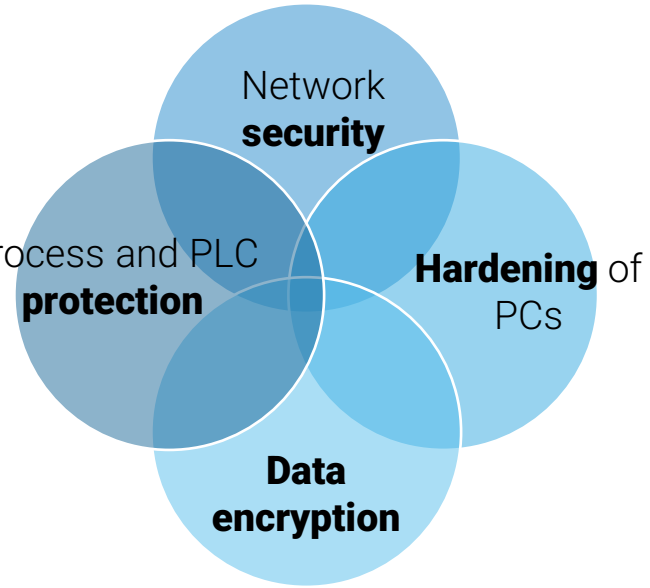
Top 10 Vulnerable devices

+ Pompe di insulina
+ Pacemakers
+ Pompe a infusione
+ Monitor paziente
+ Risonanze Magnetiche
+ Sistemi di Radioterapia
+ Dispositivi di diagnosi e immagini
+ Robot Chirurgici
+ Defibrillatori
+ Appliance di rete

La soluzione di Stormshield

NETWORK SECURITY

Segmentazione IT/OT Segmentazione e filtraggio e NAT
Manutenzione controllata da remoto tracciabilità degli eventi di sicurezza



NETWORK SECURITY

Messa in sicurezza dei flussi di processo e analisi del protocollo

ENDPOINT SECURITY

Controllare e gestire le chiavette USB
Manutenzione a distanza
Politica di sicurezza adattiva- Hardenizzazione completa degli endpoint critici

DATA SECURITY

Crittografia dei dati: progettazione dello schema, dati di manutenzione, programmi PLC, ecc.

Elementi critici

Protocolli

Modbus

BACnet

HL7

Dicom

Vulnerabilità

SO obsoleti

Impossibilità di aggiornamento

Nessuna segmentazione

Protezione

Segmentazione trasparente

Profilazione degli accessi

Gestione remota sicura con accessi autorizzati

Action	Source	Destination	Dest. port	Protocol	Security inspectio
pass	HIS RIS PACS	Any	Any	hl7	IPS
pass	Any	HIS RIS PACS	Any	hl7	IPS
pass	PACS	XRayNetwork	Any	dicom	IPS
pass	XRayNetwork	PACS	Any	dicom	IPS

Prodotti per IOT

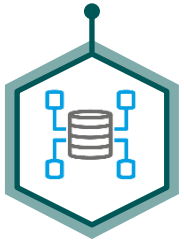
STORMSHIELD NETWORK
Security

Una gamma di Next Generation Firewall / VPN/IPS

STORMSHIELD ENDPOINT
Security

Hardenizzazione di workstation e server Windows

Stormshield XDR
CONTROLLO • PRODUTTIVITÀ • COERENZA



Raccolta e correlazione dati automatica tra più livelli di sicurezza (Network , Endpoint…)

STORMSHIELD DATA
Security

Criptazione end-to-end multi-device e multi-applicazione

Prodotti per IOT

2.4 Gbps
Firewall throughput

1.6 Gbps
IPS throughput

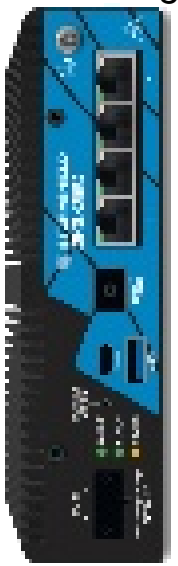
600 Mbps
VPN throughput

SNi20

3 Gbps
Firewall throughput

1.0 Gbps
IPS throughput

1.6 Gbps
VPN throughput



SNi10

SNi40

4.8 Gbps
Firewall throughput

3.3 Gbps
IPS throughput

1.2 Gbps
VPN throughput

TD SYNNEX

“At the end of the day, the goals are simple: safety and security.”

Jodi Rell

https://www.stormshield.com/it/
https://www.stormshield.com/it/prodotti-e-soluzioni/per-settore-di-attivita/salute/
https://www.stormshield.com/it/il-nostro-supporto/servizi/stormshield-academy/
https://www.acn.gov.it/portale/documents/20119/551838/acn_la+minaccia+cyber+al+settore+sanitario_clear.pdf/
https://www.ansa.it/attacchi-cyber-110-in-cinque-anni-sanita-nel-mirino
https://tg24.sky.it/cronaca/2024/05/15/attacco-hacker-synlab-dark-web
https://www.fortuneita.com/2024/09/20/cybersecurity-ospedali-italiani-sotto-attacco/
https://www.rainews.it/tgr/attacco-hacker-allasst-rhodense
https://milano.corriere.it/notizie/cronaca/milano-blocco-informatico-all-ospedale-fatebenefratelli.shtml
https://www.redhotcyber.com/post/crisi-sanitaria-in-kuwait-un-cyber-attacco-blocca-gli-ospedali-salvati-dai-backup/
https://www.redhotcyber.com/post/attacco-informatico-allospedale-di-verona-rivendicato-da-rhysida
https://bluegoatcyber.com/blog/a-critical-alert-the-top-10-most-vulnerable-medical-devices-to-cyber-attacks/

TD SYNNEX

Q&A

Your Opinion Counts!

PROSSIMI APPUNTAMENTI

13 DICEMBRE: SonicWall TZ80 e MSSP Program

20 DICEMBRE: RSA e protezione delle identità

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

https://forms.office.com/r/B8pN50j9f3

TEAM SECURITY: security.it@tdsynnex.com
SPEAKERS: andrea.scattina@stormshield.eu
andrea.pezzoni@tdsynnex.com