TD SYNNEX

Sonicwall MDR

Il servizio Best in Class per la protezione gestita

29 Novembre 2024

Webinar

Simona Di Pinto – Security Sales Specialist – TD SYNNEX
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX
Federico Diamantini – Solution Engineer - SonicWall

TD SYNNEX

SONICWALL®

Global Footprint

500,000+ customers in 215 countries and territories

Industry Veteran

Trusted 30-year veteran of the cybersecurity industry

End-to-End Portfolio

Comprehensive cybersecurity product and service platform

Global Threat Intelligence Network

Hundreds of terabytes, artifact threat data

100% Channel

17,000+ global Channel partners

Cybersecurity Innovation

More than 300 innovative patents granted, including RTDMI™

Founded 1991

Headquarters Milpitas, California

Employees 1,600+

www.sonicwall.com

Acceleratori del tuo successo

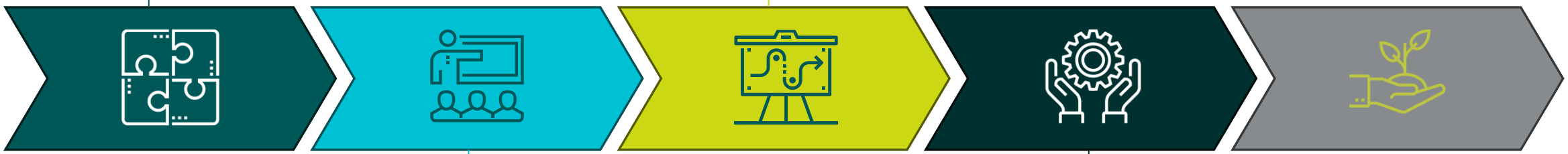
Presales
Un team dedicato per ogni tuo progetto

Academy
Corsi e training per il tuo team

Hands-on
Training dedicati per Imparare sul campo

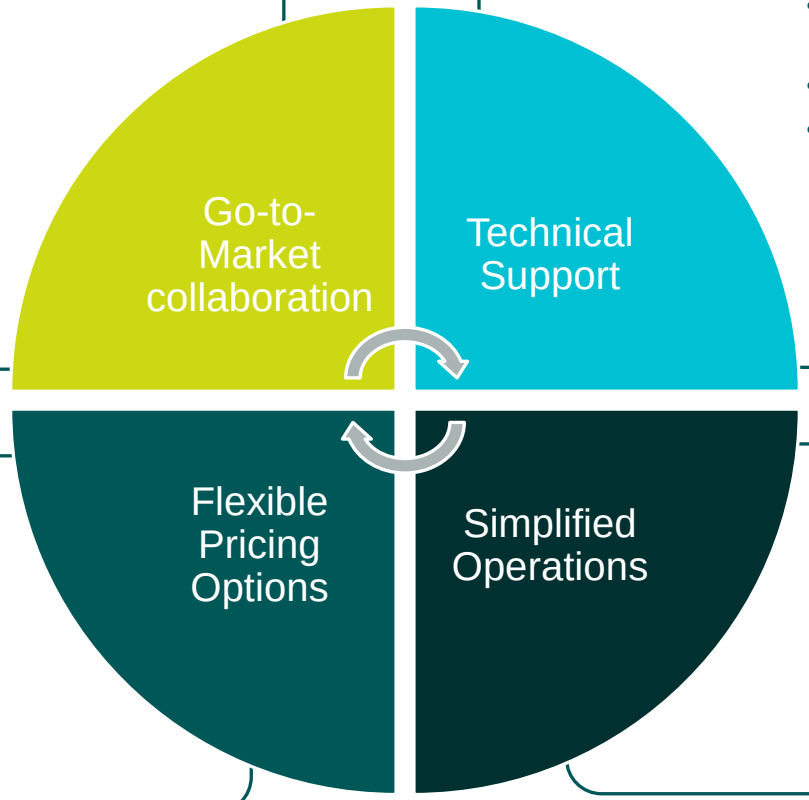
Servizi gestiti
Il nostro team tecnico, i tuoi servizi al cliente

MSSP
La piattaforma per far crescere il tuo business



Managed Security Services Partners

- 20 anni di partnership
- Un Team dedicato di Partner Manager, Sales Engineer e solution Architect per I Top Tier
- Accesso ai fondi Marketing per i Top Tier
- MSSP partner branding
- Product Previews
- Accesso al MSSP Council & agli eventi



- Servizio di supporto MSSP specializzato con un canale di accesso preferenziale
- Una knowledgebase completa
- Un servizio di support dedicato per i Top Tier (only Powered +)

- Accesso esclusivo al pricing a sottoscrizione mensile o annuale
- Accesso a scontistiche in base al volume e alle Deal Registration

- Provisioning e fatturazione automatizzati
- Piattaforma di gestione e management semplificata e sempre disponibile
- Threat analytics, reporting e workflows precompilati
- Progetti per MSSP

EDR - XDR - NDR - MDR

EDR – Endpoint Detection and Response
Tecnologia che scansiona il file o il processo, correla le informazioni tra gli endpoint e aiuta l'investigazione

XDR – Extended Detection and Response
Tecnologia che correla i dati dagli endpoint con altre fonti tipo Mail Services, Cloud e Network

NDR – Network Detection and Response
Tecnologia di sicurezza a livello di network che correla le informazioni di network alla ricerca del traffico non gestito dagli endpoint protetti

MDR – Managed Detection and Response
Servizio gestito 24/7 per monitorare, investigare e la Threat Investigation

Perché i Managed Security Services

76% Percentuale degli attacchi ransomware che avvengono fuori dall'orario di lavoro e nel weekend

Orario in cui il SOC di Sonicwall vede generarsi il maggior numero di Critical Alerts 4AM

4,88 Costo medio di una violazione dei dati in Milioni di Dollari nel 2024

Media di giorni necessari per individuazione di un data breach MTTD 258

Vantaggi di un servizio gestito

Time to respond

Gli alert che scattano di notte o durante il weekend potrebbero non essere gestiti in maniera ottimale e possono portare ad un incidente di proporzioni maggiori.

Alert Fatigue

Tanti alert sono falsi positivi, serve un controllo attento e concentrarsi sui veri avvisi, riuscendo a concentrarsi su quelli realmente importanti.

Cyber Security Expertise

Molti MSP riescono a soddisfare gran parte delle esigenze dei loro clienti, ma quanti di essi hanno reali competenze avanzate nel settore Cyber Security.

SonicWall MDR

SOC Europeo, unico punto di controllo per Endpoint, Cloud e Firewall

Verifica della rete e delle configurazioni con due audit mensili, Security Best Practice e remediation path

Il team del SOC si occuperà di notificare solo gli alerts che necessitano di follow-up

Servizi ricorsivi, vantaggi competitivi

Un servizio erogato in UE, 24/7 e completamente gestito, tramite un team di analisti qualificati, dal singolo endpoint alla azienda Enterprise

Nessun contratto annuale

Nessun numero minimo

Accelera le tue revenue

Servizio 24/7

Vendor agnostic

Compliance

TD SYNNEX

Difesa di tutta la superficie di attacco

SonicWall Managed XDR

Alert Management · Threat Hunting · Threat Mitigation
Log Retention · Reporting

MDR

Protection and response for endpoints

Capture Client

SentinelOne

CYLANCE

Microsoft Defender

SOPHOS

CDR

Protection and response for cloud apps and email

Cloud Email Security

Microsoft 365

Google Workspace

Cloud Threat Analytics

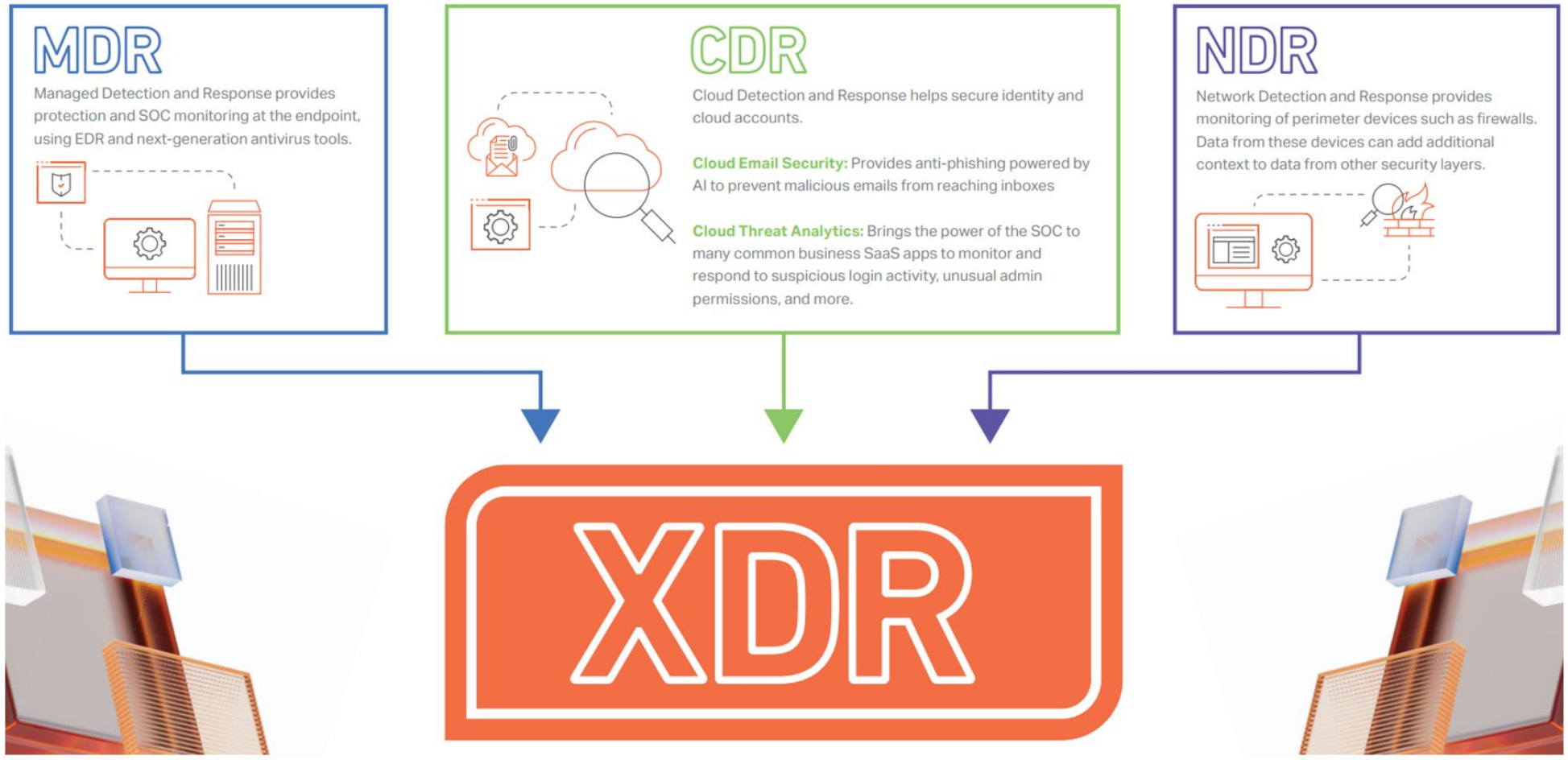
datto · SITGlue · VSA · ninjaOne · syncro · Customer Apps · Dropbox · slack · salesforce · okta · DUO

NDR

Protection and response at the perimeter

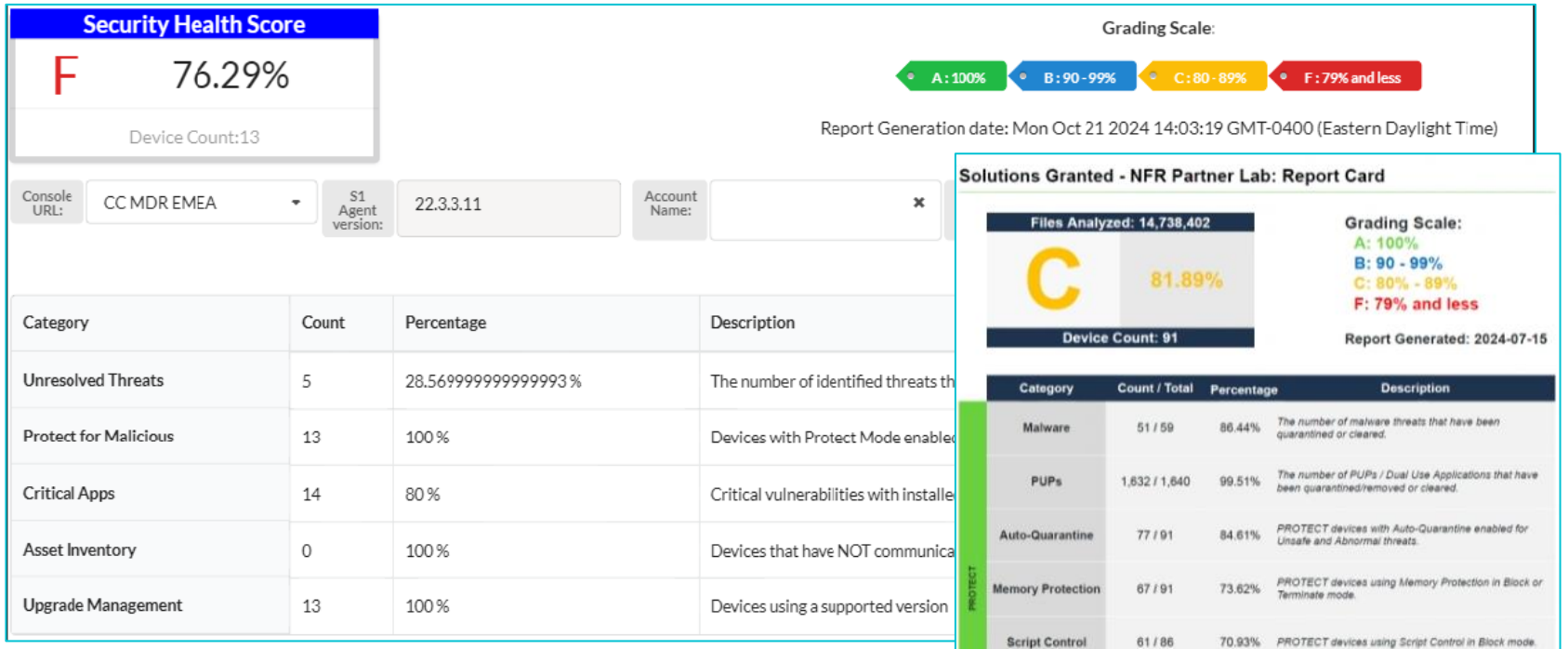
Any network device from any maker like Firewalls, Switches, Servers, VPN appliance, Access points...

Visibilità a 360°



Incident Response Cycle

Audit di sicurezza



Due volte al mese, gli analisti del SOC valutano le configurazioni degli endpoint, dando un voto e fornendo indicazioni di remediation per tornare ad uno stato di sicurezza ottimale.

Cloud Detection and response

Due prodotti per una efficacia ottimale

Cloud Email Security

- Usa le tecniche di Machine Learning per bloccare le mail di phishing prima della delivery alla mailbox.
- Il modello AI può essere costantemente allenato per migliorare l'efficacia nel rilevamento, usando il Natural Language Processing (NLP) per imparare specifici pattern specifici delle comunicazioni dell'azienda.
- Scansiona i link e gli allegati in cerca di malware
- Compliant con HIPAA, FERPA e GDP
- Il monitoraggio da parte del SOC è incluso quando venduto in accoppiata con **Cloud Threat Analytics**, o come servizio stand alone

powered by AVANAN

Cloud Threat Analytics

- Porta la potenza del SOC nel monitoraggio delle applicazioni SaaS come SalesForce, Slack, Google Workspace, e altre.
- Gli MSP possono includere il monitoraggio dei tool RMM
- Controllo efficiente dei login su base temporale, geografico o multi IP. Ispezione delle policy MFA.
- Il SOC è reattivo nel contrastare le minaccie che scatenano degli alert nell'infrastruttura del cliente e notificano il partner.

powered by SaaS Alerts™

Cloud Email Security

Advanced

Protection from advanced phishing, malicious links and files

- [x] Secure all email - incoming, outgoing and internal
- [x] Advanced AI-based anti-phishing
- [x] Anti-spam filtering
- [x] Known malware prevention (Antivirus)
- [ ] Protection from zero-day malware (File Sandboxing)
- [ ] File sanitization (CDR)
- [x] Malicious URL protection (URL Reputation)
- [x] URL click-time protection (URL Rewriting)
- [ ] Protection from zero-day malicious URLs (URL Sandboxing)
- [x] Account takeover prevention (Anomalies)
- [x] Unauthorized applications detections (Shadow IT)
- [ ] Data loss prevention (DLP)
- [ ] Encryption for M365

SonicWall Cloud App Security Basic

Complete

Protection from advanced phishing, malicious links and files

- [x] Secure all email - incoming, outgoing and internal
- [x] Advanced AI-based anti-phishing
- [x] Anti-spam filtering
- [x] Known malware prevention (Antivirus)
- [x] Protection from zero-day malware (File Sandboxing)
- [x] File sanitization (CDR)
- [x] Malicious URL protection (URL Reputation)
- [x] URL click-time protection (URL Rewriting)
- [x] Protection from zero-day malicious URLs (URL Sandboxing)
- [x] Account takeover prevention (Anomalies)
- [x] Unauthorized applications detections (Shadow IT)
- [ ] Data loss prevention (DLP)
- [ ] Encryption for M365

SonicWall Cloud App Security Advanced

Full-Suite

Protection from advanced phishing, malicious links and files

- [x] Secure all email - incoming, outgoing and internal
- [x] Advanced AI-based anti-phishing
- [x] Anti-spam filtering
- [x] Known malware prevention (Antivirus)
- [x] Protection from zero-day malware (File Sandboxing)
- [x] File sanitization (CDR)
- [x] Malicious URL protection (URL Reputation)
- [x] URL click-time protection (URL Rewriting)
- [x] Protection from zero-day malicious URLs (URL Sandboxing)
- [x] Account takeover prevention (Anomalies)
- [x] Unauthorized applications detections (Shadow IT)
- [x] Data loss prevention (DLP)
- [x] Encryption for M365

Cloud Threat Analytics

Cloud Threat Analytics (per singolo account utente gestito)

Monitoraggio delle attività sospette
SaaS Alerts monitora costantemente le applicazioni SaaS critiche dei tuoi clienti cercando attività sospette e allertandoti in caso di:

- Login avvenuto lontano dalle location approvate
- Multi-factor authentication disabilitata
- Eccessivo download di dati
- Accesso con autorizzazioni Admin
- Creazione di regole di inoltro sulle mail
- Modifica di Permissions/Ruoli security
- Modifica di Security policy
- Creazione di user account
- Fortifica e unifica i tool di supporto
- E altro

Agisci proattivamente per bloccare gli attacchi
Riduci i falsi positive e i log risparmiando tempo
Risolvi automaticamente gli avvisi di sicurezza attivi

I log vengono mantenuti 360 giorni come da normative di compliance

Network Detection and Response

- Network Detection and Response (NDR) mette a disposizione un SOC 24/7 all'interno del perimetro aziendale monitorando tools come firewalls, switches, servers, VPN appliance, Access points...
- Servizio completamente vendor agnostic; **monitoring per dispositivi perimetrali di qualsiasi vendor.**
- Retention Log: 1 anno

Proof of Concept

Endpoint MDR
30 days PoC

1. **Provide basic company info**
    1. - Company name, any DBA, etc
2. **Kickoff call**
    1. - Tenant navigation walkthrough
    2. - Review deployment process
3. **Week 1**
    1. - Endpoint installation
4. **Week 2**
    1. - Review alerts that have been identified as potential threats
    2. - Quarantine files and make appropriate exclusions
5. **Week 3 and 4**
    1. - Review implementation
    2. - Additional training as needed

Cloud MDR
14 days PoC

1. **Provide basic company info**
    1. - Company name, any DBA, etc
2. **Kickoff call**
    1. - Tenant navigation walkthrough
    2. - Review deployment process
3. **Week 1**
    1. - Review alerts that have been identified as potential threats
    2. - Quarantine files and make appropriate exclusions
4. **Week 2**
    1. - Review implementation
    2. - Additional training as needed

NDR
14 days PoC

1. **Provide basic company info**
    1. - Company name, any DBA, etc
2. **Kickoff call**
    1. - Tenant navigation walkthrough
    2. - Review deployment process
3. **Week 1**
    1. - Review alerts that have been identified as potential threats
    2. - Quarantine files and make appropriate exclusions
4. **Week 2**
    1. - Review implementation
    2. - Additional training as needed

TD SYNNEX

“Technology trust is a good thing, but control is a better one”

Stephane Nappo

https://www.sonicwall.com/products/managed-security-services
https://www.sonicwall.com/products/managed-detection-and-response
https://www.sonicwall.com/knowledgebase
https://www.techtarget.com/searchsecurity/definition/extended-detection-and-response-XDR
https://www.verizon.com/business/resources/reports/dbir/
https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf
https://media.bitpipe.com/io_15x/io_152272/item_2184126/ponemon-state-of-vulnerability-response-.pdf

TD SYNNEX

Q&A

Your Opinion Counts!

PROSSIMI APPUNTAMENTI

6 DICEMBRE: Stormshield e Medical Devices Protection

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: simona.dipinto@tdsynnex.com
andrea.pezzoni@tdsynnex.com fdiamantini@sonicwall.com