TD SYNNEX

Assessment, ETA, MDR, NIDS, IR

I servizi che rendono efficace la protezione

13 Giugno 2025

Webinar

Federico Frosini – Business Development Manager – TD SYNNEX
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX
Daniele Curto – BU Security – TD SYNNEX
Nicola Napoli – BU Security – TD SYNNEX

I Servizi sono un’opportunità

$1.7 Miliardi di opportunità

Il mercato dei Servizi crescerà in maniera significativa, con un tasso di 8% YoY fino al 2028

Crescita guidata dalla tecnologia

L’adozione di tecnologie sempre più complesse e verticali, **cloud computing, security e data and AI** alimentano la crescita.

A questi si aggiungono le normative e il tema della compliance

Verso il servizio

I servizi del ciclo di vita del prodotto, i servizi professionali forniti dai partner e la rivendita di servizi pacchettizzati crescono a un tasso del 150-200% rispetto all'hardware

Aumento del budget servizi

I Servizi sono arrivati a rappresentare il 51% del budget IT nel 2024

Sources: TD SYNNEX’s Direction of Technology Ecosystem Report 2022|2023 | Mordor’s IT Services Market Share and Size 2023 | Gartner’s Global IT Spending Forecast

Le sfide degli MSP

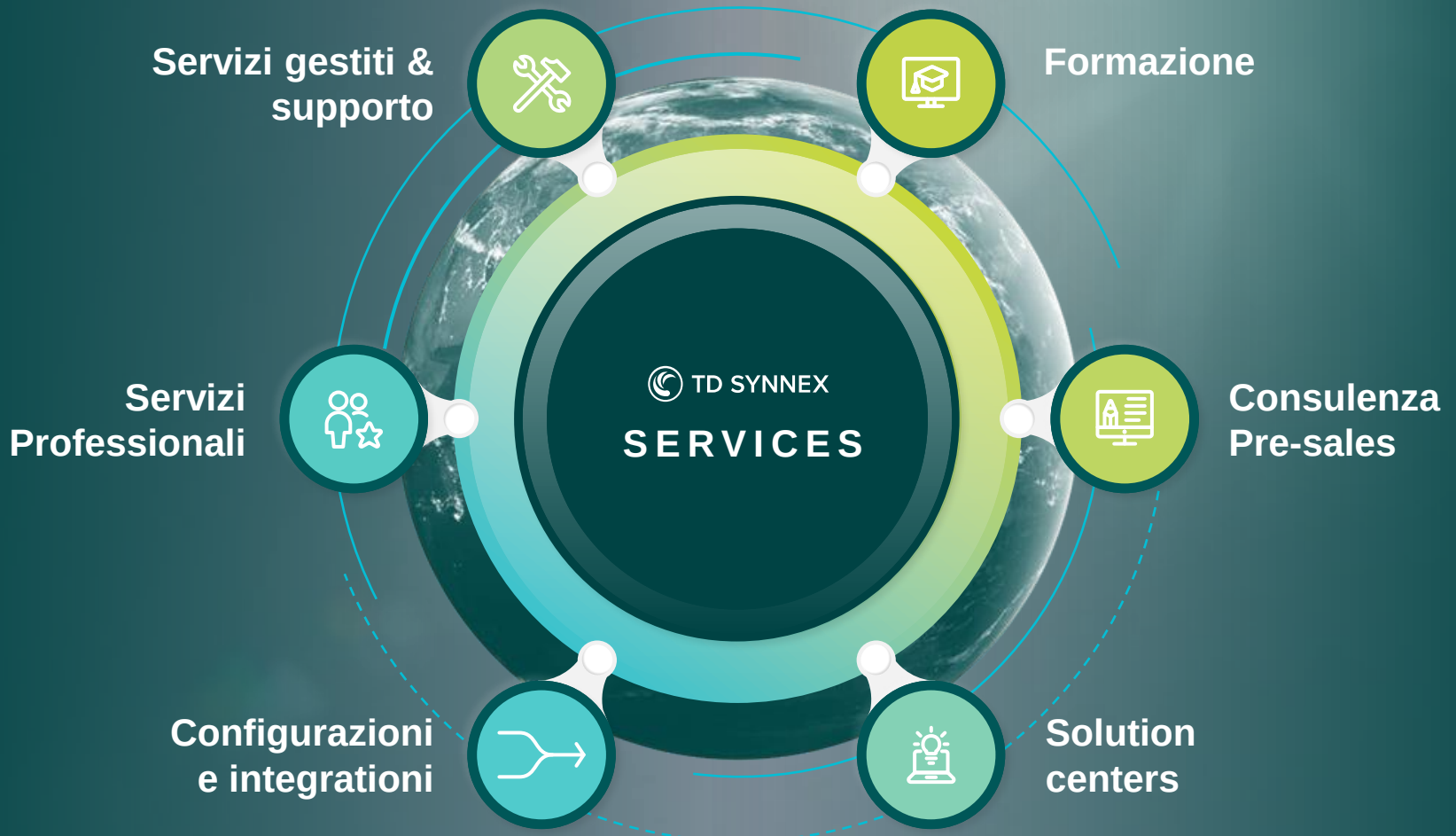
Come posso rimanere aggiornato con un mercato in evoluzione?

Come posso estendere le competenze?

Come posso aumentare l'offerta senza un piano di investimenti iniziale?

TD SYNNEX – Servizi in sintesi

Chiudere il gap tra la complessità e il risultato



Hybrid Cloud / Data & Applications / Networking / Security

Perché i servizi di TD SYNNEX?

Aumentare le skill

Ottenere di più, installare in modo più rapido ed efficace e competere in segmenti di business più ampi senza aumentare il numero di dipendenti a tempo pieno.

Aumentare l’offerta

Migliorare rapidamente le capacità e competenze ottenendo un accesso immediato a servizi, risorse e strumenti per colmare le lacune dei servizi.

Aumentare la profittabilità

Aumentate i margini di profitto al di là delle vendite tradizionali di prodotti, fornendo un ulteriore valore aggiunto ai vostri clienti.

Unica interfaccia

Creare maggiore efficienza in ogni fase del processo del ciclo di vita consolidando i servizi sotto un unico fornitore di servizi fidato, collaudato ed esperto.

I nostri Servizi sono stati studiati per essere totalmente legati al canale

Cos’è un vulnerability Assessment

Il *Vulnerability Assessment (VA)* è un’attività che analizza un sistema informatico per individuare le vulnerabilità — cioè punti deboli che un attaccante potrebbe sfruttare. Attività semplice, rapida, non invasiva: non richiede modifiche ai sistemi, può essere svolta periodicamente senza interrompere i servizi.

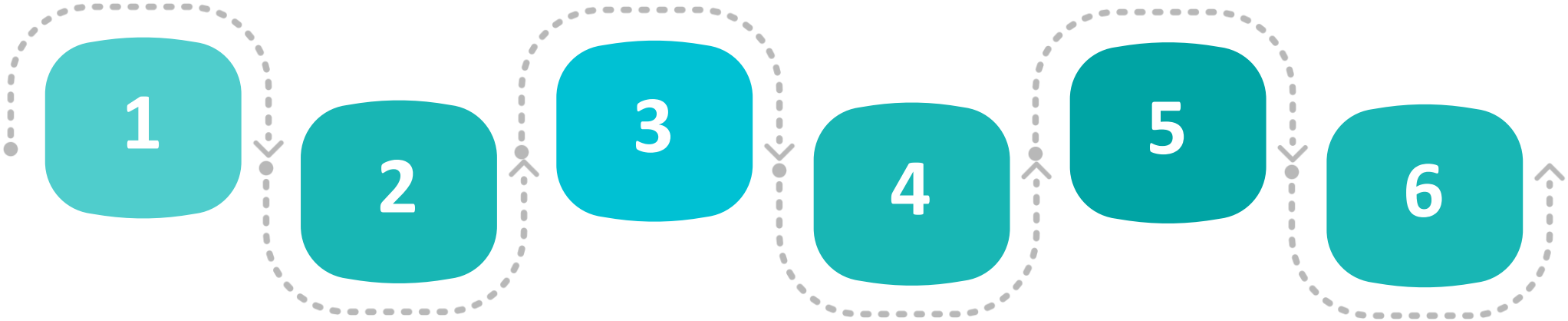
A cosa serve:

- Scoprire debolezze prima che lo faccia un attaccante;
- Creare una mappa dei rischi;
- Aumentare la resilienza dell'infrastruttura IT.

Cosa si rischia se non viene effettuato:

- Maggior esposizione a malware e furti di dati;
- Perdita di continuità operativa;
- Danni a reputazione, fiducia e conformità normativa.

Le fasi del VA



Pianificazione
Questa fase quali sistemi, applicazioni, reti o dispositivi saranno sottoposti alla valutazione.

Information gathering
In questa fase vengono acquisiti informazioni sui sistemi e sulle reti da testare attraverso un questionario inviato al partner.

Assessment
Identificare e valutare eventuali vulnerabilità che potrebbero compromettere l'organizzazione.

Report
produzione del report con i risultati del test.

Remediate
Implementare le soluzioni per ridurre i rischi legati alle vulnerabilità identificate.

Verify
Assicurarsi che le vulnerabilità siano state correttamente mitigate e pianificare eventuali test di valutazione per garantire che la sicurezza venga mantenuta nel tempo.

Focus: Information Gathering

L'***Information Gathering*** è la fase in cui un potenziale attaccante raccoglie dati sull'organizzazione per colpirla in modo preciso.

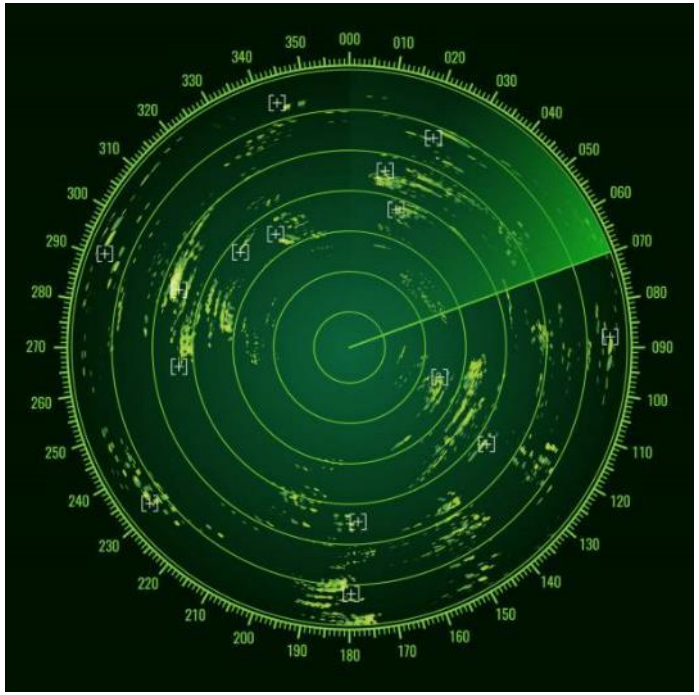
Con semplici strumenti si può limitare la quantità di informazioni esposte pubblicamente.

Cosa può raccogliere un attaccante:
Nomi di dominio, IP, portali pubblici; eventuali porte e servizi aperti
Email e nomi di dipendenti;
Tecnologie e versioni software in uso per comprendere il tipo di infrastruttura e pianificare un attacco.

Come può usarle:
Phishing personalizzati;
Sfruttamento vulnerabilità note;
Accessi non autorizzati a sistemi aziendali e molto altro..

Cos’è External Threat Analysis

L’ External Threat Analysis (E.T.A.)permette di identificare tutte le risorse esposte online o nella rete aziendale, anche quelle dimenticate o non documentate. Monitoraggio continuo e poco invasivo, che si integra facilmente con le infrastrutture esistenti.



A cosa serve:

- Scoprire tutti i punti di ingresso potenziali;
- Tenere sotto controllo asset dimenticati;
- Ridurre la possibilità di esposizione involontaria.

Cosa si rischia se non viene effettuato:

- Possibilità di attacchi invisibili su sistemi non monitorati;
- Mancanza di consapevolezza su cosa è esposto online ed esposizione della superficie ad attività malevoli

Case History: Attacco Phishing

La società “X" è stata vittima di un attacco di phishing tramite mail ufficiale.

L'attaccante ha guadagnato l’accesso ai sistemi e utilizzato la mail aziendale per promuovere una finta offerta ai vecchi clienti, invitandoli a prenotare un soggiorno e ricevere uno sconto.

Dinamiche dell'attacco:

- **Vettore d'attacco:** Mail ufficiale della società;
- **Obiettivo:** Ottenere il pagamento mediante IBAN falso;
- **Tecnica:** Phishing, con messaggio invogliante e falsa offerta.

Risultati dell'attacco:

- La società X oltre a non aver adottato misure di sicurezza sufficienti per proteggere la mail e la rete aziendale ha dovuto rimborsare i clienti truffati con il loro nome con un conseguente danno di imagine molto grave.

Come Proteggersi

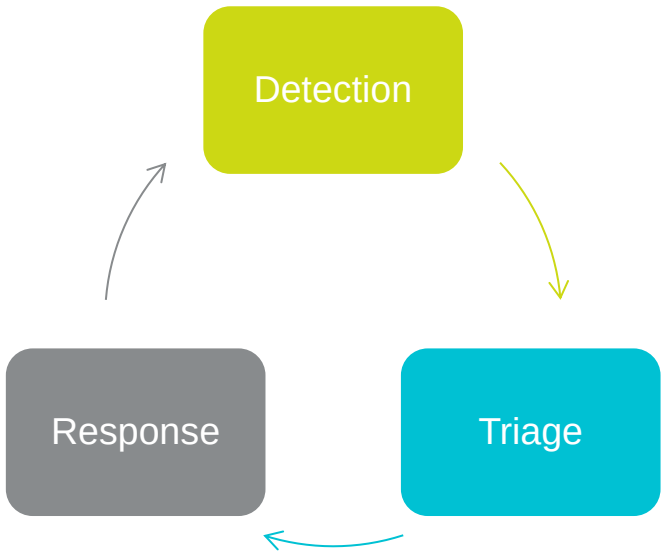
Best Practice:

- Proteggere la mail e la rete aziendale tramite misure di sicurezza adeguate, monitorazione e controlli periodici;
- La necessità di formazione e sensibilizzazione degli utenti sull'uso responsabile delle tecnologie informatiche

Conclusione:

L'attacco è un esempio lampante della rilevanza del phishing come minaccia per le aziende. È importante adottare misure di sicurezza adeguate e formare gli utenti sull'uso responsabile delle tecnologie informatiche per prevenire simili attacchi in futuro.

Managed Detection and Response



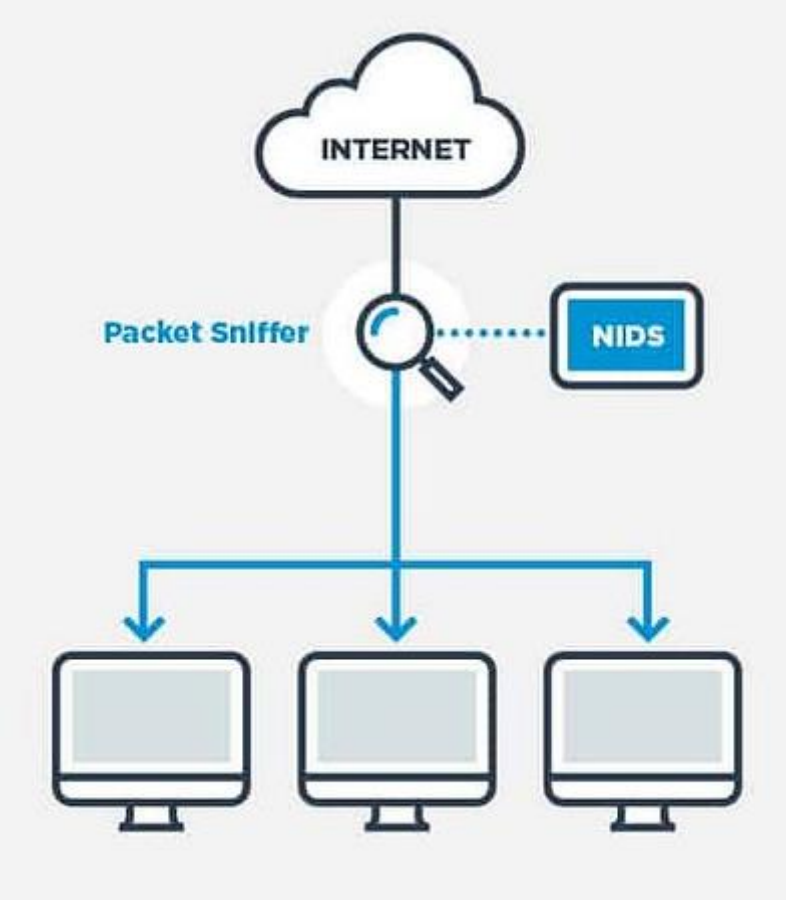
MDR: servizio di cybersecurity che combina la tecnologia con l'esperienza umana per identificare rapidamente e limitare l'impatto delle minacce eseguendo attività di threat hunting, monitoraggio e risposta. (Crowdstrike)

Perché è utile:

Un servizio di monitoraggio e risposta gestito è fondamentale per avere un ulteriore livello di sicurezza e capacità di risposta rapida in caso di attacco.

Il servizio estende il periodo di copertura della protezione presidiata oltre orario di lavoro classico.

Network Intrusion Detection System



Monitorare il traffico di rete in ascolto di flussi non autorizzati

- Protezione ambienti di produzione IoT e OT
- Basato su network e agentless
- Riconoscimento di protocolli non visibili a molte appliance di sicurezza
- Riconoscimento dei movimenti laterali

Perché è utile:

E’ in grado di avere il monitoraggio costante dei flussi di rete. Un ulteriore layer di sicurezza che prescinde dai client e i sensori presenti a livello software sui device.

Incident Response

E dopo un incidente cosa succede?

- Compliance legale
- Segnalazione del breach
- Ripristino sicuro dei Sistemi
- Ricerca dei vettori di attacco
- Bonifica del Sistema
- Ripartenza delle attività

Il servizio di Incident Response è il miglior salvagente per un'azienda che ha subito un attacco.

Perché i Servizi

Le attività di Vulnerability Assessment, ETA (attack surface management), che simula l'attività di information gathering, MDR e NIDS sono:

- Semplici da avviare;
- A basso impatto sull'infrastruttura;
- Efficaci nel prevenire attacchi;
- Migliorano i margini;
- Migliorano i flussi di lavoro sia del consulente che dell'azienda.

TD SYNNEX

“Security is not a product, but a process with human awareness.”

Q&A

20 GIUGNO: Sonicwall CSE – ZTNA fatto semplice

27 GIUGNO: Nella mente di un hacker – Un attacco Bruteforce

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

TEAM SECURITY: security.it@tdsynnex.com
TEAM SERVIZI: serviziprofessionali-ita@tdsynnex.com