NDR

Network Detection and Response

AUMENTARE IL CONTROLLO SULLA SITUAZIONE DELL'INFRASTRUTTURA DI RETE, OTTENENDO VISIBILITÀ REAL TIME: OGGI È POSSIBILE CON LA SOLUZIONE NDR DI PROFESSIONAL LINK

NDR

Network Detection and Response

Il settore energy italiano è sempre più esposto agli attacchi informatici. Sono sempre di più gli attori che prendono di mira i servizi di pubblica utilità, sfruttando le particolari interdipendenze del settore dell'energia e del gas tra infrastrutture fisiche e informatiche.

Incrementare la cyber security aziendale è quindi fondamentale.

Intelligence strategica: prevenzione, non reazione

È necessario adottare un **approccio lungimirante e preventivo alla security**, che la integri nelle decisioni critiche sull'espansione aziendale. Il primo passo per fare questo è avere **visibilità totale** sulle attività degli utenti e sui punti deboli dell'infrastruttura IT dell'azienda.

Analizzare il rischio

Nonostante l'adozione di firewall o Client EDR, gli attacchi possono comunque andare a segno dato che gli aggressori continuano a trovare nuovi vettori di attacco. Questo perché nelle reti locali potrebbero essere collegati degli a**pparati obsoleti, non aggiornati o di cui il reparto IT non ha visibilità**. Questi sono potenziali veicoli che **possono essere usati per un attacco** verso l'azienda. Tramite l'Intelligenza Artificiale, un attore malevolo riesce a eludere i controlli di sicurezza tradizionale. **Gli attacchi sono sempre più mirati** e in grado di attivarsi solo quando raggiungono un target specifico.

Le aziende energy possono essere colpite lungo l'intera value chain

Generazione

Interruzioni del servizio e attacchi ransomware contro centrali elettriche e generatori.
Causa: infrastrutture progettate senza tenere conto della sicurezza.

Trasmissione

Interruzioni su larga scala dell'alimentazione ai clienti attraverso servizi di disconnessione remota.
Causa: brecce nella sicurezza che danno accesso ai sistemi di controllo della rete.

Distribuzione

Interruzione delle substations, perdita del servizio regionale e interruzione del servizio ai clienti.
Causa: sistemi di alimentazione distribuiti e security limitata.

Network

Furto di dati dei clienti, frode e interruzione del servizio.
Causa: attacchi ai device IoT, inclusi i contatori e i veicoli elettrici.

LA SOLUZIONE:
Network Detection and Response (NDR)

La proposta di Professional Link per **incrementare il livello di consapevolezza e sicurezza** dell'infrastruttura aziendale è il servizio di Network Detection and Response, che si compone di **una Sonda e di un Server***.
La soluzione si implementa in tre fasi:

1. Network Traffic Analytics
2. Detection
3. Response

**La distanza geografica e la complessità organizzativa rendono il settore vulnerabile agli attacchi informatici.
Ecco perché è necessario agire in ottica preventiva.**

Network Traffic Analytics

La **sonda**, posizionata all'interno della rete dell'azienda (non importa quante siano le sedi), intercetta le comunicazioni che l'attraversano. Le informazioni sono inviate al **server**, che esegue **analisi sofisticate** sui dati di traffico.
Grazie a questa analisi si conosce:

- Chi ha generato traffico
- Il tipo di trasferimento
- In quale modalità e con quali protocolli
- In quale periodo di tempo

In una parola, si ha la totale VISIBILITÀ.
Questo permette di **stabilire in modo preciso il livello di rischio** in cui l'azienda si trova.

Detection

Nella fase di Detection, le informazioni ottenute dalla prima fase di analisi sono elaborate tramite Machine Learning, AI e behavioral analysis, determinando:

- Il livello di sicurezza dell'infrastruttura
- Le anomalie
- Le vulnerabilità
- Gli attacchi subiti
- La fase in cui l'attacco si trova

Con la Detection, aumenta la capacità di **individuare nel dettaglio i malware e gli attacchi** che potrebbero eludere i sistemi di sicurezza.

Response

Nella fase di Response, il server coordina in real-time la risposta all'attacco, istruendo le componenti di sicurezza a protezione dell'infrastruttura.
Next Generation Firewalls, Client EDR e NDR server, operano sinergicamente per bloccare la minaccia e mitigare gli effetti di incidenti che hanno già compromesso la rete.
L'automatizzazione del processo di Response comprime i tempi di reazione alle minacce, **riducendo il perimetro di rischio** e il carico di lavoro per i reparti IT.

VISIBILITÀ TOTALE

La soluzione di Network Detection and Response è fondamentale per incrementare la sicurezza della rete, a partire dalla **visibilità totale sui punti deboli del sistema** e sugli utenti collegati.

La soluzione NDR, mettendo in evidenza le vulnerabilità dell'azienda, segnala chiaramente il suo livello di adeguatezza in merito alla cyber security.

Aumentare il controllo sulla situazione dell'infrastruttura di rete, ottenendo visibilità real time: oggi è possibile con la soluzione NDR di Professional Link.

Semplicità di installazione e di analisi

L'attivazione del servizio non richiede cambi sull'infrastruttura LAN, basta collegare una sonda per iniziare ad analizzare il traffico.
La piattaforma utilizza algoritmi di Intelligenza Artificiale per individuare attacchi e minacce che a loro volta utilizzano l'IA per eludere i sistemi di protezione già in essere.
Questo consente un'analisi semplificata degli attacchi e dello stato di propagazione degli stessi con risposte automatizzate che riducono drasticamente i tempi di reazione e, quindi, i rischi.

La dashboard, completa e intuitiva, consente un'analisi immediata e semplice degli attacchi e del loro stato di propagazione fin nel minimo dettaglio.

*Soluzione Cyber Command, powered by Sangfor Technologies

Professional Link seleziona e implementa soluzioni tecnologiche che consentono di ridurre la complessità.

Professional Link è un operatore B2B in grado di fornire tecnologie di cyber security, telecomunicazione dati e fonia, fisse e mobili, in Italia e all'estero.
Le nostre soluzioni **ad alta affidabilità** sono personalizzate sui bisogni specifici dei singoli business, con una pronta risposta al guasto e una grande attenzione al lato umano del rapporto col cliente e con il partner: trasparenza e comunicazione chiara sono alla base del nostro operare.
Negli anni abbiamo acquisito risorse e competenze nell'ambito dei servizi internazionali e abbiamo consolidato numerose partnership con operatori domestici e regionali a livello globale, per garantire la miglior **implementazione e gestione di soluzioni geograficamente distribuite**.

Servizio gestito da PLINK, unico interlocutore

Tutte le attività di delivery sono coordinate da un Project Manager di PLINK, così come gli apparati sono gestiti e monitorati dal nostro assurance team italiano, che mette a vostra disposizione un portale di monitoring per visualizzare le statistiche del servizio.

Grazie al nostro team di supporto e al nostro ecosistema di servizi integrati, PMI, grandi corporate e multinazionali possono contare sulle migliori soluzioni di fonia e trasmissione dati. Forniamo, infatti:

- Soluzioni NDR (Network Detection and Response)
- Telefonia VoIP e servizi UCM
- Telefonia mobile come MVNO
- Connettività dati
- Servizi cloud, backup e disaster recovery
- Managed services con monitoraggio e gestione sulla nostra infrastruttura dati
- Servizi ISP/ASP su struttura totalmente proprietaria

Cyber Command

PIATTAFORMA INTELLIGENTE DI RILEVAMENTO DELLE MINACCE

by Sangfor Technologies

Cyber Command scopre le violazioni dei controlli di sicurezza esistenti, mentre l'impact analysis identifica le minacce nascoste all'interno della rete.

Cyber Command dà visibilità dei potenziali punti di ingresso e di attacco. Questo consente al team IT di condurre una caccia alle minacce rapida e precisa.

La piattaforma Cyber Command, di Sangfor Technologies, migliora significativamente le capacità complessive di rilevamento e risposta.

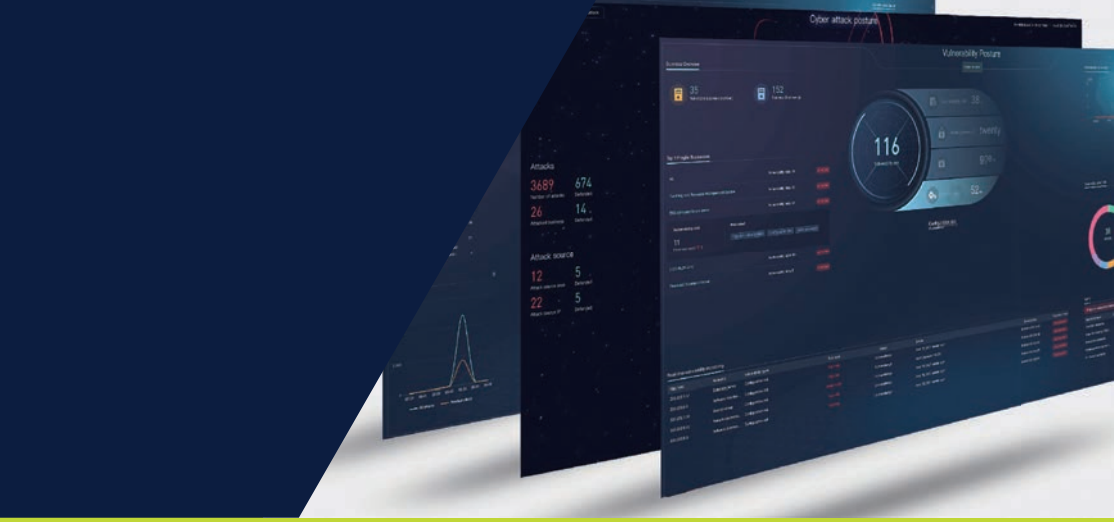
Come?

- **monitorando il traffico di rete interno**
- **correlando gli eventi di sicurezza**
- **applicando l'intelligenza artificiale e l'analisi del comportamento**

Cyber Command **scopre le violazioni dei controlli di sicurezza** esistenti, mentre l'impact analysis **identifica le minacce nascoste** all'interno della rete.

Cyber Command integra le soluzioni di sicurezza sia della rete sia degli endpoint, la capacità degli amministratori IT di **analizzare e comprendere il panorama globale** delle minacce migliora notevolmente.

Cyber Command è facilmente installabile all'interno di data center e filiali senza necessità di modificare la rete o le impostazioni di sicurezza.



Perché proprio Cyber Command?

Rapidità

Cyber Command è in grado di **rilevare le potenziali minacce** utilizzando motori di rilevamento basati su firma e Threat Intelligence, inoltre **rileva le anomalie** utilizzando motori AI. In questo modo, Cyber Command fornisce risultati estremamente precisi.
Poiché il Cyber Command è abbinato all'intelligence sulle minacce, esso **rileva gli attacchi a tutti i livelli della catena**, il che significa avvisi rapidi in caso di pericolo.

Semplicità

Cyber Command fornisce un **report di analisi dell'impatto**, nonché una **visuale per i punti di ingresso** e per il ripristino delle patch di attacco, che consente al team IT di condurre una **verifica delle minacce** facile e veloce.

Approfondimenti precisi

Cyber Command esegue **un'analisi completa dell'impatto delle violazioni** e rintraccia il "paziente zero", valutando tutti i possibili punti di ingresso.
Con l'identificazione automatica, Cyber Command consente un **controllo di tutte le risorse aziendali** mostrando chiaramente le relazioni di accesso tra utenti, aziende e Internet, nonché i **potenziali rischi**.

Attraverso il **monitoraggio in tempo reale**, Cyber Command controlla lo **stato della sicurezza**, consentendo un processo decisionale intelligente. Visualizza, inoltre, il dettaglio delle risorse perse, piuttosto che elencare semplicemente il numero di incidenti di sicurezza.
La **visibilità della catena di attacco** fornisce la misura della gravità dell'attacco stesso.

PLINK®
TELECOMMUNICATIONS

Connections beyond Connectivity

Professional Link S.r.l.
Via Alcide De Gasperi, 4/A
22072 Cermenate (CO)
Tel. +39 031 778912
comunicazioni@plink.it
www.plink.it

comunicazioni.plink.it/blog
PLINK: Professional Link
Professional Link
plink_professional_link