

NDR

by Professional Link

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

by Professional Link

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

Nella cybersecurity, è essenziale partire dalla comprensione dettagliata dell'ambito da proteggere e delle aree in cui è necessario intervenire.

Evoluzione delle Reti Dati

Il nostro Paese è sempre più esposto agli attacchi informatici, la principale fonte di questi problemi sono solitamente i sistemi aziendali non aggiornati (e quindi vulnerabili).

Incrementare la cyber security aziendale è quindi fondamentale.

Il primo passo per fare questo è avere visibilità totale sulle attività degli utenti collegati e sui punti deboli dell'infrastruttura IT dell'azienda

Analizzare il rischio

Internet è un'infrastruttura di accesso «pubblica» ove non è possibile esercitare un controllo puntuale né su chi si collega alla rete, né sul percorso che faranno i dati. Questi potrebbero essere intercettati da degli attori malevoli, oppure del traffico malevolo (virus e malware) potrebbe compromettere i dispositivi di altri utenti.

Il controllo e la gestione di un'architettura Internet Based, dal punto di vista della sicurezza, è complesso e richiede competenze puntuali, risorse specializzate ed investimenti.

Nonostante l'adozione di firewall o Client EDR, gli attacchi possono comunque andare a segno. Questo perché nelle reti locali potrebbero essere collegati degli apparati **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 nascondere il contenuto dei pacchetti, eludendo i controlli di sicurezza tradizionale. Gli attacchi sono sempre più mirati e in grado di attivarsi solo quando raggiungono un target specifico.

Non tutte le aziende hanno la possibilità di organizzarsi con un Security Operations Center o con delle risorse dedicate alla sicurezza e, ad ogni modo, strutturare un SOC risulta oneroso, complesso, con benefici visibili solo sul medio - lungo periodo.

LA SOLUZIONE: Network Detection and Response (NDR)

La proposta di Professional Link per incrementare il livello di consapevolezza e sicurezza dell'infrastruttura è il servizio di Network Detection and Response.

L'infrastruttura di Network Detection and Response si compone di una Sonda ed un Server*, che implementano la soluzione attraverso tre fasi:

1. Network Traffic Analytics
2. Detection
3. Response

La mancanza di visibilità è un elemento di rischio a cui le aziende dovrebbero porre attenzione; la soluzione NDR di PLINK è la risposta a questa esigenza.

Network Traffic Analytics

La **sonda**, posizionata all'interno della rete dell'azienda, intercetta la maggior parte delle comunicazioni che la 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 e completa VISIBILITÀ.

Questo aspetto è fondamentale, poiché 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, Artificial Intelligence 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, la soluzione NDR 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, in maniera automatizzata, 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, quindi, operano sinergicamente in modo da 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 investigazione e reazione alle minacce, **riducendo il perimetro di rischio** ed il carico di lavoro per i reparti IT e Security.

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.

La piattaforma NDR garantisce visibilità totale sulle attività effettuate dagli utenti collegati, la loro «security posture» e fornisce risposte automatizzate per mitigare gli attacchi.

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 estremamente sofisticati 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.

Non sono necessarie modifiche all'infrastruttura esistente per l'attivazione del servizio.

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



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 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:

- 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

Poiché 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

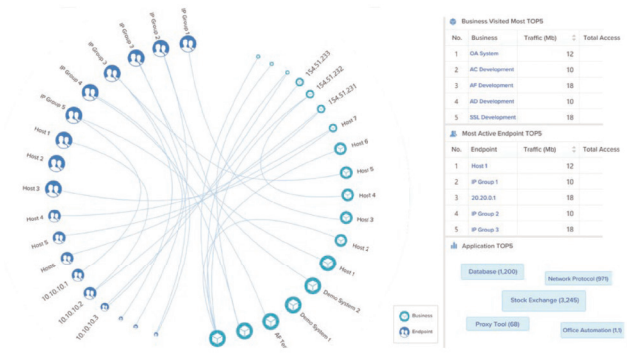
Cyber Command fornisce un **report di analisi dell'impatto**, nonché una **visuale per i punti di ingresso** e per il ripristino delle patch di attacco, che consente al team IT di condurre una **verifica delle minacce** facile e veloce.

Approfondimenti precisi

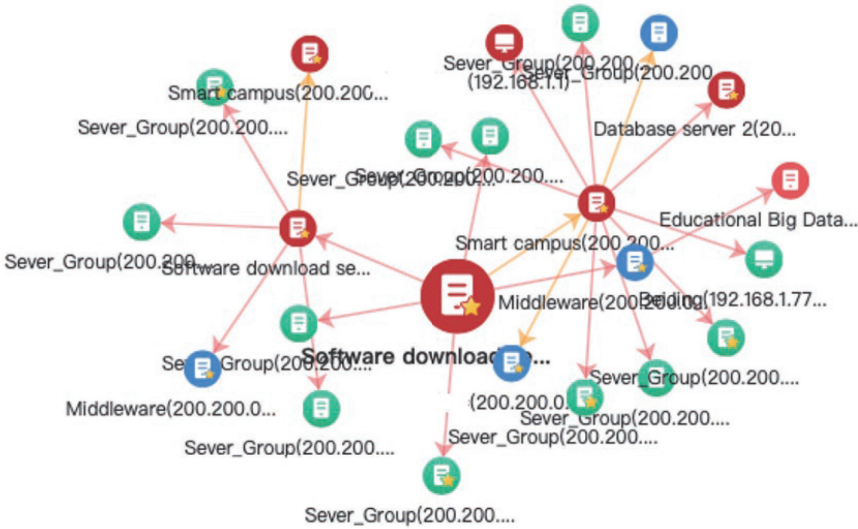
Cyber Command aiuta il team IT a eseguire un'**analisi completa dell'impatto delle violazioni** e a rintracciare il "paziente zero", valutando tutti i possibili punti di ingresso.

Cyber Command studia il comportamento delle risorse compromesse, come le connessioni in entrata e in uscita e l'utilizzo di porte e protocolli. Tali informazioni possono essere usate poi per rafforzare le difese del sistema aziendale.

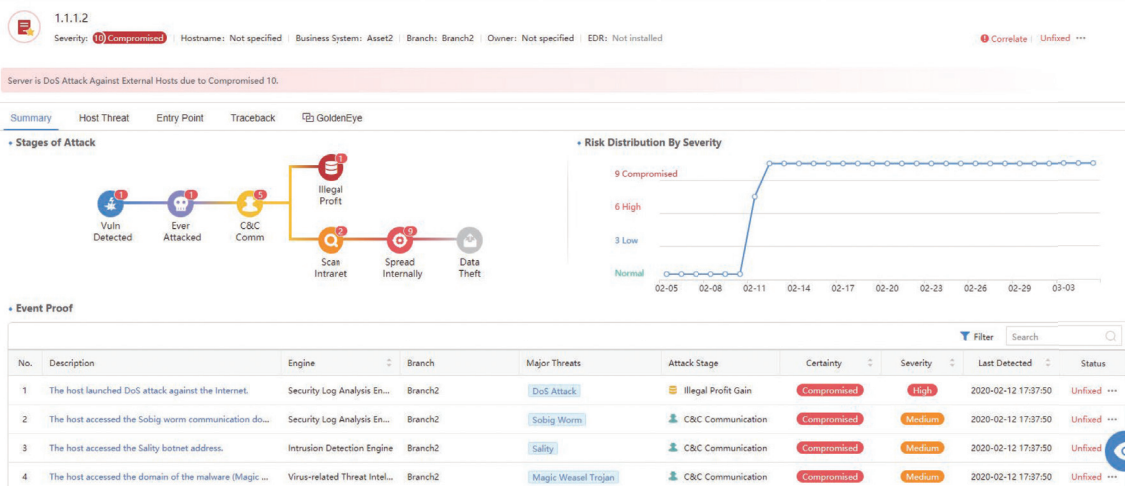
Attraverso l'identificazione automatica, Cyber Command consente un controllo di tutte le risorse aziendali mostrando chiaramente le relazioni di accesso tra utenti, aziende e Internet, nonché i potenziali rischi.



Cyber Command valuta l'influenza delle minacce in più dimensioni, rilevando il "chi", "cosa", "quando", "dove", e "perché" di un attacco, presentandolo in un formato leggibile.



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.



Scheda tecnica

Piattaforma Cyber Command

		CC-1000	CC-2000	CC-3000
Prestazioni basate sulla modalità STA		5 STA-100	8 STA-100	12 STA-100
Prestazioni basate su registri	Numero di registro di accesso giornaliero (milioni/giorno)	200	250	350
	EPS medio (per log/SEC)	2500	3150	4350
	Picco EPS (per log/SEC)	10000	12000	15000
	Consumo del disco (GB/ giorno)	110	140	200
	Stima dei giorni di conservazione in base al parametro di cui sopra (giorni)	1350	1440	1290
Memoria	96G	128G	256G	
CPU	16 Cores	16 Cores	20 Cores	
Disco di sistema	SSD 128G	SSD 128G	SSD 128G	
Capacità del disco rigido dei dati	SATA 4T*8	SATA 4T*10	SATA 4T*12	
LSI Raid	Raid50	Raid50	Raid50	
Dimensioni (cm)	800*448*90	800*448*90	800*448*90	
Altezza rack	2U	2U	2U	
Peso lordo	42KG	45KG	45KG	
Alimentazione	Redundant	Redundant	Redundant	
Potenza nominale	383W	385W	473W	
Potenza massima	800W	800W	800W	
Bypass	N/A	N/A	N/A	
Porte di analisi del rame	4 x 10/100/1000 BASE-T	4 x 10/100/1000 BASE-T	6 x 10/100/1000 BASE-T	
SFP + Porte di analisi	N/A	2x 10Gbe SFP+	2x 10Gbe SFP+	
Porte seriali	N/A	DB9*1	DB9*1	
USB	USB3.0*4	USB3.0*4	USB3.0*3	
Relazione di conversione per STA	STA-200 = 2* STA-100 STA-300 = 3* STA-100 STA-400 = 6* STA-100 STA-500= 10* STA-100			

STA: analisi minacce invisibili

	STA-100	STA-200	STA-300	STA-400	STA-500
Rendimento massimo sostenuto	Up to 1.0Gbps	Up to 2.0Gbps	Up to 3.0Gbps	Up to 6.0Gbps	Up to 10.0Gbps
Memoria	8G	8G	8G	16G	32G
CPU	4 Cores	8 Cores	8 Cores	16 Cores	16 Cores
Disco rigido	SSD 64G	SATA 1T	SATA 1T	SATA 1T	SATA 1T
Dimensioni (cm)	400*430*44.5	600*440*89	600*440*89	600*440*89	600*440*89
Altezza rack	1U	2U	2U	2U	2U
Peso lordo	7.5KG	18.65KG	18.65KG	18.65KG	24KG
Alimentazione	Single	Dual	Dual	Dual	Dual
Potenza nominale	30W	55W	55W	55W	350W
Potenza massima	60W	150W	150W	150W	760W
Bypass	N/A	N/A	N/A	N/A	N/A
Porte di analisi del rame	6x10/100/1000 BASE-T	6x10/100/1000 BASE-T	6x10/100/1000 BASE-T	6x10/100/1000 BASE-T	8x10/100/1000 BASE-T
SFP + Porte di analisi	2 x 1Gbe SFP	2 x 10Gbe SFP+	2 x 10Gbe SFP+	2 x 10Gbe SFP+	8 x 1Gbe SFP 4 x 10Gbe SFP+
Porte seriali	RJ45*1	RJ45*1	RJ45*1	RJ45*1	RJ45*1
USB	USB2.0*2	USB2.0*2	USB2.0*2	USB2.0*2	USB2.0*2

Cyber Command + apparecchio virtuale

	vCC-100	vCC-500	vCC-1000	vCC-2000	vCC-3000
Capacità di gestione del traffico	2G	3G	4G	5G	7G
Capacità di gestione blog (EPS/s, Peak)	5000	5000	10000	12000	15000
CPU (frequenza principale, numero di core)	3.60GHz * 8	3.60GHz * 8	2.10GHz * 16	2.60GHz * 32	2.60GHz * 40
Memoria	64G	64G	128G	128G	256G
Disco di sistema	128G SSD	128G SSD	128G SSD	128G SSD	128G SSD
Disco rigido	2T	2T	4T	8T	8T





STA Virtuale

	vSTA-100	vSTA-200
Capacità di gestione del traffico	1G	2G
CPU (frequenza principale, numero di core)	2.4G * 8	2.4G * 16
Memoria	8G	16G
Disco di sistema	>64G	>64G
Disco dati consigliato (minimo)	>128G	>128G



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