SOPHOS

NDR Sophos Network Detection and Response

Come Migliorare L'Efficienza Delle Security Operations Con Sophos Network Detection And Response (NDR)

Whitepaper Sophos. Aprile 2023

Introduzione

Viviamo in un'epoca caratterizzata da un panorama delle minacce in continua evoluzione, in cui le organizzazioni sono costrette ad adottare un approccio proattivo per identificare i potenziali attacchi informatici e avviare una risposta adeguata. La tecnologia Network Detection and Response (NDR) svolge un ruolo fondamentale in questa strategia.

NDR sfrutta potenti funzionalità quali l'analisi con deep learning, la tradizionale corrispondenza basata sulle regole e le statistiche di flusso in base al rischio, per analizzare il traffico di rete non elaborato e identificare potenziali attività dannose all'interno della rete. Questo permette ai responsabili di sicurezza di adottare misure proattive per prevenire gli attacchi e minimizzarne l'impatto.

Tuttavia, la tecnologia NDR presenta delle sfide, tra cui l'alto tasso di falsi positivi. Sophos NDR risolve questo problema grazie a una tecnologia brevettata di clustering e assegnazione di punteggi, che sfrutta le informazioni raccolte da più motori di rilevamento delle minacce.

Anche se la tecnologia NDR è emersa negli anni '90, la sua complessità e il suo livello di precisione variano a seconda dei vendor. Per le organizzazioni è assolutamente fondamentale considerare una soluzione NDR dall'efficacia comprovata, come Sophos NDR, che offre livelli avanzati di rilevamento delle minacce, confermando i sospetti e riducendo il numero di falsi positivi. In questo whitepaper, effettueremo un'analisi approfondita delle funzionalità e dei vantaggi di Sophos NDR, indicando i motivi per cui è un componente indispensabile per le Security Operations di qualsiasi organizzazione.

Indice dei contenuti

L'Evoluzione Del Monitoraggio Della Protezione Della Rete: Cronologia Della Tecnologia NDR

Sophos NDR è un componente essenziale per le Security Operations di oggi, ma l'origine dell'NDR risale agli anni '90, con l'emergere dei primi sistemi di rilevamento delle intrusioni basati sulla rete (Network Intrusion Detection System, NIDS). I primissimi NIDS si focalizzavano sull'identificazione e sul blocco degli attacchi basati sulla rete, ma non erano in grado di mettere in correlazione più eventi o di rilevare minacce su più sistemi.

Nei primi anni di questo millennio, la tecnologia NDR ha subito un'evoluzione che ha portato al superamento di questi limiti. Invece di identificare solo gli attacchi basati sulla rete, le soluzioni NDR hanno cominciato ad analizzare il traffico di rete e a mettere in correlazione gli eventi rilevati su più sistemi; la nuova strategia ha così permesso a questi prodotti di individuare anche le minacce più avanzate. Sophos NDR è una soluzione NDR leader di mercato che sfrutta potenti funzionalità quali l'analisi con deep learning, la tradizionale corrispondenza basata sulle regole e le statistiche di flusso in base al rischio per identificare le attività sospette e potenzialmente dannose per la rete.

Con il passare del tempo, la tecnologia NDR è diventata sempre più sofisticata, offrendo una visibilità quasi immediata sulle attività di rete e una perfetta integrazione con altre soluzioni di sicurezza. La tabella che segue offre una cronologia dei momenti più importanti nell'evoluzione della tecnologia NDR:

ANNO	MOMENTO SALIENTE
Anni '80	Cominciano a emergere i primi prodotti di network security, con la rapida adozione della tecnologia firewall
Anni '90	I primi sistemi di rilevamento delle intrusioni basati sulla rete (Network Intrusion Detection System, NIDS) diventano disponibili, dando inizio al monitoraggio della protezione della rete
Anni 2000	Le tecnologie NDR (Network Detection and Response) si evolvono fino al punto di analizzare il traffico di rete e mettere in correlazione gli eventi rilevati su più sistemi
Anni 2010	Vengono integrati nelle soluzioni NDR gli algoritmi di machine learning, che permettono di identificare le minacce più complesse e di ridurre il numero di falsi positivi
2016	La botnet Mirai, che sfrutta i dispositivi IoT, sferra uno dei più estesi attacchi di Distributed Denial of Service (DDoS) in assoluto, mettendo così in evidenza l'importanza di implementare una network security avanzata
2019	Gartner introduce il termine Network Detection and Response (NDR), per sostituire il termine obsoleto Network Traffic Analysis (NTA, analisi del traffico di rete)
Anni 2020	Le soluzioni NDR offrono visibilità in tempo reale e opzioni flessibili di implementazione, per permettere alle organizzazioni di distribuire il prodotto in qualsiasi ambiente

Le soluzioni NDR come Sophos NDR permettono alle organizzazioni di rilevare e rispondere in maniera efficace alle minacce più avanzate.

Sophos NDR: Monitoraggio Avanzato Della Rete Per Identificare Le Minacce Più Recenti

Sophos NDR è una soluzione di monitoraggio avanzato della rete progettata per aiutare le organizzazioni ad affrontare il problema di un panorama delle minacce sempre più complesso e in continua evoluzione.

A differenza delle tradizionali soluzioni NDR, Sophos NDR offre la combinazione ottimale di vari motori di rilevamento realizzati internamente, che includono opzioni di analisi basata sul deep learning, per garantire la disponibilità in tempo reale di pratici dati di intelligence su un'ampia selezione di minacce di rete.

I motori di rilevamento sviluppati internamente di Sophos NDR classificano il traffico di rete in base a oltre 330 protocolli, 50 rischi relativi al flusso e migliaia di indicatori di compromissione (IoC). In questi motori sono inoltre incorporati i modelli predittivi di vari sistemi di deep learning, per garantire un livello imbattibile di precisione nel rilevamento delle minacce e per ridurre al minimo i falsi positivi.

I Principali Vantaggi Di NDR:

NDR TRADIZIONALE	SOPHOS NDR	MIGLIORAMENTI
Numero limitato di protocolli	Oltre 330 protocolli di rete	Sophos NDR classifica il traffico in base a oltre 330 protocolli, per fornire una visibilità più completa del traffico di rete: una capacità indispensabile per identificare le minacce nuove ed emergenti. Vedi l'Appendice B per un elenco completo dei Protocolli.
IoC di base	Migliaia di IoC	Sophos NDR utilizza migliaia di Indicatori di Compromissione (IoC) per rilevare eventuali pericoli, garantendo così un livello più elevato di precisione nel rilevamento delle minacce.
Identificazione minima dei rischi relativi al flusso	50 rischi relativi al flusso	Sophos NDR incorpora 50 rischi relativi al flusso nei motori sviluppati internamente: questo permette di rilevare anche le minacce più complesse, che potrebbero eludere il rilevamento di altre soluzioni NDR. Vedi l'Appendice A per un elenco completo dei rischi relativi al flusso.
Corrispondenza in base alle regole	Analisi basate sul deep learning	Sophos NDR utilizza le analisi basate sul deep learning per garantire un livello imbattibile di precisione nel rilevamento delle minacce. Allo stesso tempo, riduce il numero di falsi positivi.
Alti tassi di falsi positivi	Tecnologia brevettata di clustering e assegnazione di punteggi	Sophos NDR utilizza una tecnologia brevettata di clustering e assegnazione di punteggi, in grado di ridurre il numero di falsi positivi: questa tecnologia aiuta a fornire pratici dati di intelligence su un'ampia selezione di minacce della rete.

Queste evoluzioni tecnologiche sono particolarmente importanti in ambito NDR, perché permettono a Sophos NDR di identificare in maniera accurata le minacce della rete e di avviare una risposta tempestiva, senza generare una quantità eccessiva di falsi positivi. Gli elevati livelli di velocità e precisione di Sophos NDR, uniti alla capacità di gestire il traffico cifrato senza doverlo decifrare, fanno di questa soluzione un componente fondamentale per qualsiasi strategia di sicurezza a 360 gradi.

Sophos NDR offre alle organizzazioni una soluzione avanzata per il monitoraggio della rete, progettata per rilevare le minacce e avviare un'azione di risposta efficace e precisa, anche in un panorama informatico in continua evoluzione. Grazie ai vari motori di ricerca realizzati internamente e alle analisi basate sul deep learning, Sophos NDR garantisce dati di intelligence che non sono solo facili da implementare, ma anche precisi e rilevanti al contesto delle minacce più recenti.

Architettura Concettuale Di NDR Sensor

La soluzione Sophos NDR viene implementata come sistema di monitoraggio del traffico passivo, in ascolto su una porta SPAN/mirror; non aggiunge latenza al traffico di rete e non costituisce un Single Point of Failure per la rete in caso di sovraccarico o non disponibilità.

NDR Sensor raccoglie i metadati man mano che il traffico attraversa il sensore, inviando dettagli sui flussi di rete a una serie di motori di rilevamento; i flussi vengono quindi raggruppati in cluster e ricevono un punteggio. A questo punto, i risultati dei flussi di rete inseriti nei cluster vengono inviati al Sophos Data Lake e diventano visibili in Central, nella dashboard dei rilevamenti.

Elaborazione Dei Pacchetti Di Rete (NPP)

Raccogliere metadati sui flussi di rete in maniera efficiente è fondamentale per l'efficacia di una soluzione NDR. Questo processo include l'aggregazione dei pacchetti di rete in un'unica comunicazione (o flusso) e la raccolta di metadati da ciascuno dei pacchetti di rete utilizzando la Deep Packet Inspection (DPI). I metadati raccolti vengono quindi arricchiti con informazioni di geolocalizzazione e altre metriche, come destinazioni meno comuni, periodicità e dinamiche dei pacchetti. L'ultima fase prevede il rilevamento di indicatori di rischio quali informazioni TLS non valide, traffico unidirezionale, pacchetti DNS di grandi dimensioni e altro.

Le tabelle che seguono aiutano a capire meglio i dati sull'intestazione dei pacchetti e sul livello dell'applicazione che vengono raccolti in questa fase. Forniscono esempi delle deduzioni che possono essere tratte da ciascuna categoria e i motivi per cui sono importanti.

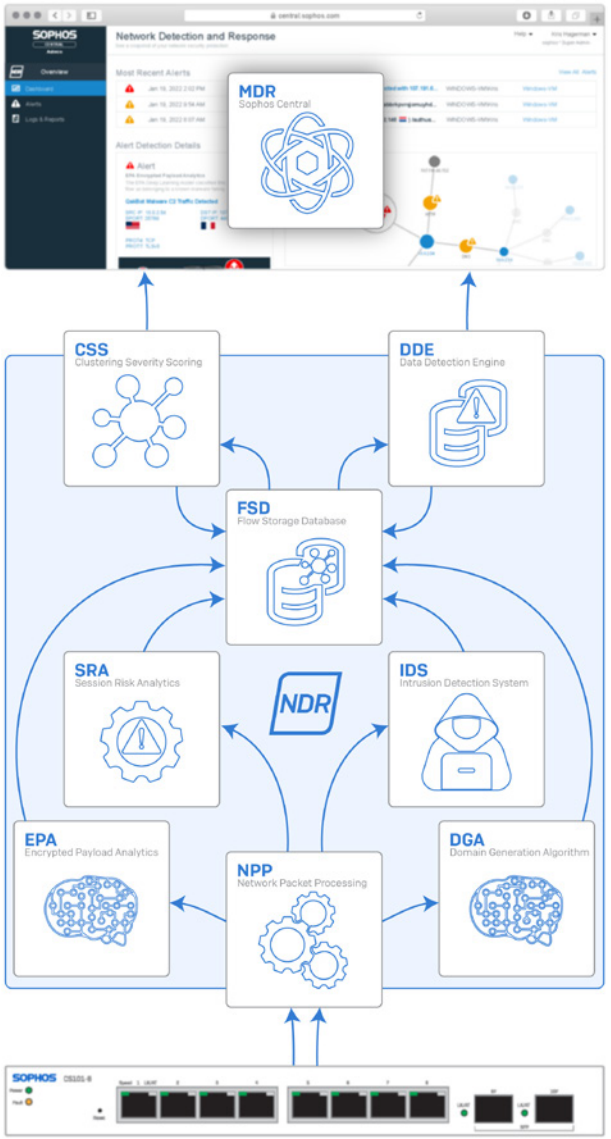

Figura 1: Diagramma dell'architettura di Sophos NDR

NPP: Dati Sull'Intestazione Dei Pacchetti

I dati sull'intestazione dei pacchetti offrono informazioni sulle comunicazioni di rete, ad esempio gli indirizzi di origine e di destinazione, il protocollo di trasporto, la durata e le dimensioni. Aiutano le soluzioni NDR a identificare l'origine delle comunicazioni e la potenziale minaccia che potrebbero costituire. Alcune delle informazioni che possono essere tratte dai dati dell'intestazione dei pacchetti includono:

DATI SULL'INTESTAZIONE DEI PACCHETTI	DESCRIZIONE	IMPORTANZA PER IL THREAT HUNTING DI NDR
IP di origine	L'indirizzo IP del mittente	Identifica l'origine della comunicazione, che successivamente può essere utilizzata per monitorare le attività sospette o identificare gli host infettati
Indirizzo MAC di origine	L'indirizzo MAC (Media Access Control)	L'indirizzo MAC aiuta a identificare il dispositivo fisico associato al traffico di rete e può essere utilizzato insieme ad altre informazioni ottenute dal sensore per mettere in correlazione gli avvisi generati da più sensori e individuare un dispositivo specifico.
Porta di origine	La porta utilizzata dal mittente per la comunicazione	Aiuta a identificare l'applicazione o il servizio specifico che è associato alla comunicazione; questa informazione può essere utilizzata per rilevare attività sospette o non autorizzate
IP di destinazione	L'indirizzo IP del ricevente	Aiuta a identificare il destinatario della comunicazione; questa informazione può essere utilizzata per identificare origini di minacce esterne
Indirizzo MAC di destinazione	L'indirizzo MAC del ricevente	Identifica il dispositivo fisico associato alla comunicazione; questa informazione può essere utilizzata per monitorare le attività sospette o identificare gli host infettati
Porta di destinazione	La porta utilizzata dal ricevente per la comunicazione	Aiuta a identificare l'applicazione o il servizio specifico che è associato alla comunicazione; questa informazione può essere utilizzata per rilevare attività sospette o non autorizzate
Flag TCP	I flag TCP indicano lo stato di una connessione TCP, ad es. SYN, ACK, FIN, RST ecc.	Possono essere utilizzati per rilevare attacchi o attività sospette sulla rete, come la scansione delle porte o gli attacchi Denial-of-Service
Durata della comunicazione	Il tempo di durata della comunicazione	Aiuta a identificare le attività sospette, ad es. connessioni che durano più del previsto, connessioni estremamente brevi e comunicazioni periodiche con l'uso di beacon
Byte ricevuti	La quantità di dati ricevuti durante la comunicazione	Questa informazione può essere utilizzata per rilevare attacchi o attività sospette, come l'esfiltrazione di dati o i download di malware
Protocolli livello 3 (rete) e livello 4 (trasporto)	I protocolli utilizzati per la comunicazione, ad es. IP, OSPF, ICMP, TCP, UDP	Aiutano a identificare il tipo di traffico e i servizi associati, che possono poi essere utilizzati per rilevare attività sospetta o non autorizzata
ID della VLAN (rete locale virtuale) di rete	Il tag della VLAN associato alla comunicazione	Aiuta a identificare i segmenti di rete specifici che sono associati alla comunicazione

NPP: Dati Sul Livello Dell'Applicazione

I dati del livello dell'applicazione aiutano ad approfondire sui contenuti della comunicazione di rete; questi dati permettono alle soluzioni NDR di identificare potenziali minacce nascoste. Forniscono informazioni sulle applicazioni e sui servizi utilizzati in una comunicazione di rete e aiutano a identificare i nomi utente e le password non cifrati. Alcuni esempi delle informazioni che possono essere tratte dai dati del livello dell'applicazione includono:

DATI SUL LIVELLO DELL'APPLICAZIONE	DESCRIZIONE	IMPORTANZA PER IL THREAT HUNTING DI NDR
Protocollo a livello dell'applicazione	Il protocollo utilizzato a livello dell'applicazione, ad es. HTTP, TLS, o SMB (Server Message Block)	Conoscere il protocollo a livello dell'applicazione attualmente in uso può aiutare a identificare il traffico potenzialmente pericoloso e i comportamenti che sono anomali per quel protocollo
Nomi host di origine e di destinazione	I nomi host associati agli indirizzi IP di origine e di destinazione, risolti con DNS o altri metodi	Possono aiutare a identificare traffico potenzialmente pericoloso o comportamenti anomali associati a host o domini
Tipo di contenuto HTTP	Il tipo di contenuto trasferito su HTTP, ad es. testo, immagini o video	Può aiutare a identificare traffico potenzialmente pericoloso o comportamenti anomali associati a certi tipi di contenuti
Codice di risposta	Il codice dello stato HTTP restituito dal server in risposta a una richiesta HTTP	Può aiutare a identificare traffico potenzialmente pericoloso o comportamenti anomali associati a codici di risposta specifici, come 404 Pagina non trovata o 500 Errore interno del server
URL	L'URL intero richiesto o aperto	Può aiutare a identificare traffico potenzialmente pericoloso o comportamenti anomali associati a URL o domini
Agente utente	L'agente software utilizzato dal client per inviare la richiesta, ad es. il browser web o un'app per dispositivi mobili	Può aiutare a identificare traffico potenzialmente pericoloso o comportamenti anomali associati ad agenti utenti, ad es. attività tipiche di software noti per essere dannosi
Nomi utente e password non cifrati	Qualsiasi nome utente o password trasmesso come testo in chiaro, ad es. in una richiesta HTTP non cifrata	Queste informazioni possono aiutare a identificare potenziali problemi di sicurezza o tentativi di accesso non autorizzato
Informazioni sul certificato TLS	Informazioni sul certificato TLS utilizzato in una connessione protetta, inclusi gli hash JA3	Possono aiutare a identificare certificati potenzialmente pericolosi o falsificati; in più, offrono dati approfonditi sulla natura del traffico cifrato
HASSH per client e server SSH	Un metodo per creare un'impronta digitale che serve a identificare i client e server SSH	Può aiutare a individuare traffico SSH potenzialmente pericoloso oppure a rilevare tentativi di accesso non autorizzato a SSH
Incapsulamento CAPWAP	Il protocollo CAPWAP (Control and Provisioning of Wireless Access Points), utilizzato per gestire gli access point wireless	Può aiutare a identificare tentativi di accesso wireless potenzialmente pericolosi o non autorizzati, oppure a individuare attività insolite sulla rete wireless

In conclusione, la raccolta di metadati sul flusso di rete è un'attività fondamentale per le soluzioni NDR, in quanto permette di ottenere informazioni approfondite sulle comunicazioni della rete e di rilevare potenziali minacce. I dati sull'intestazione dei pacchetti e sul livello dell'applicazione che vengono raccolti offrono informazioni preziose, che aiutano a identificare l'origine, il tipo e il potenziale livello di rischio della comunicazione. Sfruttando queste informazioni, le soluzioni NDR sono in grado di rilevare le minacce della rete e di avviare una risposta tempestiva ed efficace.

Motori Di Rilevamento Di Sophos NDR

Sophos NDR include cinque diversi motori di rilevamento incorporati, che offrono funzionalità complete di rilevamento delle minacce. I motori agiscono in perfetta sinergia per identificare vari indicatori di compromissione e metterli in correlazione. Gli indicatori ricevono quindi un punteggio e vengono visualizzati in Sophos Central come dati di intelligence pronti per l'uso, a disposizione di clienti e analisti.

Per ottimizzare la performance, i motori di machine learning EPA (Encrypted packet Analytics: analisi dei pacchetti cifrati) e DGA (Domain Generation Algorithm: algoritmo di generazione di domini) non vengono eseguiti su tutti i flussi di rete, ma si attivano in base ai risultati delle analisi degli altri motori di rilevamento. Permettere ai motori di rilevamento di interagire in maniera collaborativa nel processo di classificazione è fondamentale per mantenere elevati livelli di performance e per limitare i falsi positivi.

I risultati dei motori di rilevamento vengono quindi inviati a un algoritmo di clustering e valutazione della gravità (CSS) per generare un punteggio minacce complessivo, che l'amministratore può visualizzare come rilevamento nella dashboard dei Rilevamenti di Sophos Central. Il record del rilevamento contiene i risultati delle analisi di ogni motore.

Motore IDS - Intrusion Detection System (Sistema Di Rilevamento Delle Intrusioni)

Il motore IDS, sviluppato internamente da Sophos, è estremamente semplice ed efficiente; in più, è in grado di identificare gli Indicatori di Compromissione (IoC) nel traffico cifrato. Molti vendor di cybersecurity si ostinano a utilizzare sistemi di corrispondenza dei contenuti eccessivamente complicati, anche quando la visibilità risulta limitata per via della cifratura.

Sophos NDR sfrutta dati accuratamente selezionati di intelligence sulle minacce per creare regole IDS classificate in sei gruppi, in base al tipo di IOC. Le classificazioni delle regole e le rispettive descrizioni sono indicate di seguito:

Attività Varie

Questa classificazione delle regole ha un livello di gravità basso e viene utilizzata per rilevare il traffico di rete che non è stato associato alle altre classificazioni. Alcuni esempi includono il traffico verso server DNS pubblici, il traffico verso reti di distribuzione di contenuti, oppure il traffico verso servizi cloud attendibili. Identificare queste attività varie aiuta a stabilire una "linea di riferimento" in base alla quale è possibile classificare il traffico di rete normale, per mettere in luce eventuali deviazioni da tale linea di riferimento.

Violazione Dei Criteri

Questa classificazione delle regole ha un livello di gravità basso e viene utilizzata per rilevare il traffico che potrebbe potenzialmente violare un criterio aziendale. Alcuni esempi includono il traffico verso siti web o servizi non autorizzati oppure il traffico proveniente da dispositivi non autorizzati. Rilevare le violazioni dei criteri aiuta le organizzazioni a implementare i propri criteri di sicurezza e a prevenire incidenti quali l'accesso non autorizzato o l'esfiltrazione dei dati.

Traffico Pericoloso Sconosciuto

Questa classificazione delle regole ha un livello di gravità medio e viene utilizzata per identificare le comunicazioni di rete che hanno una destinazione potenzialmente pericolosa. Può includere le comunicazioni con un indirizzo IP o dominio noto per essere pericoloso, oppure le comunicazioni con un dominio sinkhole, che viene utilizzato per reindirizzare il traffico verso un'infrastruttura pericolosa. Il rilevamento del traffico pericoloso sconosciuto può aiutare a identificare eventuali endpoint compromessi e a prevenire l'esfiltrazione dei dati o ulteriori attività di compromissione.

Dowload Di Malware

Questa classificazione delle regole ha un livello di gravità alto e viene utilizzata per identificare le comunicazioni di rete che hanno origini note per essere fonti di distribuzione di malware. Può includere le comunicazioni con un server di comando e controllo (C2) conosciuto (adoperato per scaricare o distribuire malware) oppure con un sito noto di distribuzione di malware. Rilevare i download di malware aiuta le organizzazioni a identificare e isolare gli endpoint infetti, per prevenire un'ulteriore diffusione del malware.

Attività Dei Trojan

Questa classificazione delle regole ha un livello di gravità alto e viene utilizzata per identificare le comunicazioni di rete con server C2 noti per le loro attività di diffusione di malware. Può includere le comunicazioni con un server C2 utilizzato per controllare un endpoint compromesso da remoto, oppure le comunicazioni con un server C2 sfruttato per esfiltrare dati. Il rilevamento delle attività dei trojan aiuta le organizzazioni a identificare eventuali endpoint compromessi e a prevenire l'esfiltrazione dei dati o ulteriori attività di compromissione.

Blacklist Per TLS

Questa classificazione delle regole ha un livello di gravità critico e viene utilizzata per identificare le comunicazioni di rete con una destinazione nota per essere pericolosa, in base alla corrispondenza dei certificati TLS. Può includere le comunicazioni con un dominio noto per essere dannoso che utilizza un certificato TLS compromesso, oppure le comunicazioni con un dominio noto per essere pericoloso che non utilizza un certificato TLS valido. Il rilevamento del traffico TLS in blackilst aiuta le organizzazioni a bloccare le comunicazioni con infrastrutture note per essere pericolose, proteggendo così i sistemi dagli attacchi informatici.

Motore SRA - Session Risk Analytics (Analisi Del Rischio Della Sessione)

Il motore SRA rileva quando il traffico di rete non rispetta gli standard dei protocolli documentati, il che potrebbe indicare la presenza di attività di rete sospetta o rischiosa. Svolge un ruolo importante nel threat hunting, perché aiuta a identificare i comportamenti che deviano dagli standard e che potrebbero quindi essere associati a un attacco. Quando il motore SRA rileva questo tipo di attività, aggiunge al flusso dei metadati informazioni sul comportamento osservato. Questi rischi relativi al flusso non vengono considerati di per sé indicatori di compromissione; tuttavia, quando vengono esaminati in combinazione con i rilevamenti degli altri motori, possono aiutare a identificare le attività pericolose.

Quello che segue è un elenco dei rischi generali relativi al flusso (identificabili su più protocolli) e di cosa indicano:

TIPO	RISCHIO RELATIVO AL FLUSSO	DESCRIZIONE
Generale	Potenziale exploit	Indica che è stato rilevato un potenziale exploit, come Log4J/Log4Shell. È importante per il rilevamento delle attività degli exploit e per prevenire/attenuare gli attacchi.
Generale	Protocollo noto su porta non-standard	Indica che un protocollo viene utilizzato su una porta non-standard, ad es. HTTP su TCP/8000 invece della porta standard TCP/80. È importante per individuare gli hacker che utilizzano porte non standard per eludere il rilevamento.
Generale	ASN rischioso	Indica che c'è stato uno scambio di traffico di rete con un server che appartiene a un ASN (numero sistema autonomo) considerato rischioso. È importante per identificare le reti o gli host pericolosi.
Generale	Traffico unidirezionale	Indica che una sessione ha una sola direzione; questo può verificarsi in presenza di attività C2 verso un server che non opera più su quell'indirizzo. È importante per identificare host compromessi o server C2.
Generale	Sessione di condivisione di desktop o file	Indica che il flusso include dati di condivisione di desktop o file, ad es. TeamViewer o AnyDesk. È importante per identificare gli hacker che si servono di questi strumenti per controllare da remoto un host compromesso.
Generale	Protocollo non sicuro	Indica che il protocollo utilizzato non è sicuro e se ne sconsiglia l'uso; un esempio può essere Telnet invece di SSH. È importante per rilevare gli hacker in grado di intercettare e leggere il traffico inviato su protocolli non sicuri.
Generale	Credenziali non cifrate	Indica che le credenziali sono state trasmesse in chiaro su un protocollo noto, come FTP, HTTP, IMAP, POP3 o SMTP. È importante per rilevare gli hacker in grado di intercettare e leggere le credenziali non cifrate.
Generale	Pacchetto non valido	Indica che il pacchetto presenta un formato diverso dal previsto, il che potrebbe significare che c'è stato un errore del protocollo oppure che un protocollo valido è stato compromesso per trasportare un altro tipo di dati. È importante per rilevare gli attacchi basati sulla manipolazione dei pacchetti o sull'uso improprio dei protocolli.
Generale	Problemi di TCP	Indica che sono stati rilevati problemi nelle impostazioni TCP della sessione di rete. È importante per rilevare la presenza di hacker che utilizzano i problemi di TCP per interferire con il rilevamento o per eluderlo.
Generale	Flusso periodico	Indica che la sessione di rete si ripete a intervalli regolari, il che potrebbe segnalare la presenza di attività C2 di un trojan o una botnet. È importante per identificare gli hacker che si servono delle comunicazioni periodiche per mantenere da remoto il controllo sugli host compromessi.

Per un elenco completo dei Rischi relativi al flusso, vedi l'Appendice A.

Motore EPA - Encrypted Payload Analytics (Analisi Dei Payload Cifrati) e Machine Learning (ML)

Le soluzioni di Network Detection and Response (NDR) si affidano sempre più frequentemente al machine learning per rilevare il traffico sospetto sulle reti aziendali. Secondo Gartner, gli strumenti NDR analizzano continuamente il traffico non elaborato e/o i record di flusso (ad es. NetFlow) per impostare modelli che riflettono il normale comportamento della rete. Il deep learning sfrutta questo approccio, portandolo persino oltre: permette infatti di rilevare gli schemi ricorrenti che vengono riscontrati su più attributi e consente di effettuare rilevamenti anche senza i dati di intelligence sulle minacce basati sugli indicatori di compromissione.

Sophos ha sviluppato una soluzione specifica chiamata Encrypted Payload Analytics (EPA), per risolvere il problema di come rilevare le minacce nel traffico cifrato che sfruttano tecnologie meno recenti. I flussi di rete sono composti da pacchetti con intestazioni e dati sul payload. Durante l'ispezione di una comunicazione cifrata, solo i dati sul payload sono codificati, per cui è impossibile conoscerne i contenuti senza prima decifrarli. EPA è un modello predittivo di deep learning a classi multiple, addestrato per rilevare gli schemi ricorrenti nei flussi di rete, in base alla sequenza di lunghezza dei pacchetti e tempi di interarrivo (Sequence of Packet Length and Interarrival Time, SPLIT). Questi attributi SPLIT sono semplici da elaborare e vengono utilizzati per addestrare una rete neurale convoluzionale (Convolutional Neural Network, CNN) per eseguire la classificazione. Sophos NDR sfrutta un processo brevettato di normalizzazione, trasformazione e presentazione dei dati alla CNN, per permetterne la classificazione.

Figura 2: Sequenza di lunghezza dei pacchetti e tempi di interarrivo (SPLIT)

Analizzando campioni di malware attivi, il modello EPA è in grado di identificare le attività pericolose in tempo reale, incluse minacce zero-day, varianti di malware sconosciuto e server C2, grazie agli schemi dei flussi di rete rilevati negli intervalli. Inoltre, il motore EPA arricchisce i metadati del flusso con informazioni sulle famiglie di malware rilevate, fornendo anche un punteggio di attendibilità per ridurre il numero di falsi positivi. Complessivamente, EPA aiuta le organizzazioni a rilevare e a rispondere a minacce cifrate che altrimenti non verrebbero intercettate. Questo approccio è particolarmente utile quando i dispositivi endpoint non sono in grado di eseguire un prodotto di protezione endpoint tradizionale e quando le comunicazioni di rete non possono essere decifrate per ottemperare ai requisiti di protezione delle informazioni sull'identità.

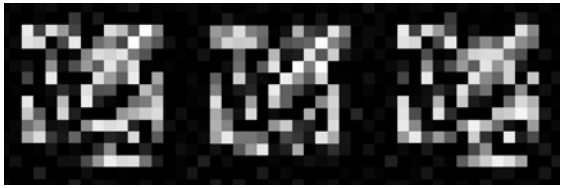

Figura 3: Variante di Cobalt Strike dopo l'elaborazione come immagine per la CNN di EPA.

Il motore EPA (Encrypted Payload Analytics) arricchisce i metadati del flusso identificando la famiglia di malware specifica (ad es. Bumblebee, Cobalt Strike, Emotet, Dridex, QakBot) e fornisce un Punteggio di attendibilità da 0 a 100. Per ridurre il numero di falsi positivi, il modello include anche una classificazione di tipo "sconosciuto".

Motore DGA – Domain Generation Algorithm (Algoritmo Di Generazione Di Domini)

I DGA (algoritmi di generazione di domini) vengono sfruttati dagli hacker per generare nomi di dominio da utilizzare per svolgere attività di comando e controllo (C2) senza finire nella blacklist. Con questi algoritmi, il malware può generare un elenco di potenziali nomi di dominio che potrebbero ospitare il server C2. Dopo diversi tentativi, l'algoritmo individua un dominio esistente e stabilisce una connessione.

husbbrkpvrqjomuyhdpd[.]com

Figura 4: Esempio di dominio DGA

In passato, i DGA sono stati utilizzati in diversi attacchi ad alto profilo. Nell'infezione del worm Conficker del 2008, ad esempio, i DGA sono stati utilizzati per generare ogni giorno un elenco di oltre 50.000 nomi di dominio da utilizzare come potenziali server C2. Questa strategia ha causato gravi problemi ai ricercatori di sicurezza, che hanno incontrato moltissime difficoltà durante i loro tentativi di fermare la rete C2 di questo worm. Il malware Gameover Zeus è un altro esempio di utilizzo di DGA, che in questo caso sono stati utilizzati per generare ogni giorno fino a 1.000 nomi di dominio da utilizzare per le comunicazioni C2. La botnet di Gameover Zeus ha mietuto vittime in tutto il mondo, con furti che ammontano a un totale di oltre 100 milioni di $.

Il motore di rilevamento DGA di Sophos NDR è fondamentale per identificare le attività pericolose in tempo reale. Il motore di rilevamento DGA di Sophos NDR sfrutta una rete neurale di deep learning LSTM (Long Short-Term Memory, ovvero memoria lunga a breve termine), che valuta ogni nome di dominio visitato o su cui sono state eseguite query. È importante tenere presente che non tutte le attività DGA sono dannose: molti servizi legittimi utilizzano regolarmente i DGA. Di conseguenza, Sophos NDR non genera un avviso ogni volta che viene rilevato un DGA. Viene invece aggiunto ai metadati del flusso un punteggio di attendibilità (da 0 a 100), che viene poi utilizzato dal motore CSS (Clustering and Severity Scoring, ovvero Clustering e valutazione della gravità) per stabilire se le attività che utilizzano DGA sono pericolose oppure no.

DDE - Data Detection Engine (Motore Di Rilevamento Dei Dati)

Il DDE (Data Detection Engine) è un componente di Sophos NDR che si esegue su ciascun sensore. È un motore leggero di correlazione, che sfrutta l'archiviazione interna di database di flussi di rete e cluster di flussi. Il DDE svolge attività pianificate di data mining su queste informazioni, per identificare minacce di rete complesse come le attività di enumerazione. Le informazioni vengono quindi inviate a Sophos Central, dove vengono utilizzate per generare report informativi sulla rete.

Inoltre, i dati raccolti dal DDE possono essere messi in correlazione con i dati dei sensori endpoint di Sophos XDR (Extended Detection and Response), al fine di identificare le risorse non gestite all'interno della rete. Questa correlazione viene effettuata nel Sophos Data Lake e offre una visibilità a 360 gradi della rete, permettendo così agli amministratori di identificare i potenziali rischi di sicurezza e di intraprendere le azioni più appropriate. È importante tenere presente che il DDE svolge attività di data mining in maniera pianificata e non in tempo reale.

CSS - Clustering and Severity Scoring (Clustering E Valutazione Della Gravità)

La funzionalità CSS (Clustering and Severity Scoring) è un elemento fondamentale nelle attività di rilevamento delle minacce di Sophos NDR. Durante le sessioni di rete tra client e server, il sistema osserva un'ampia gamma di indicatori di minacce. Se analizzati individualmente, questi indicatori potrebbero non fornire un quadro accurato di un problema o un'attività pericolosa. Pertanto, Sophos NDR utilizza un processo brevettato che nel tempo raggruppa questi indicatori in cluster, garantendo così un livello di attendibilità più alto nell'identificazione delle minacce effettive.

Il processo di clustering raggruppa i flussi di rete in base alle informazioni di base della rete, ad es. IP/porta di origine o di destinazione e dati sul protocollo. Grazie al clustering progressivo di più flussi nel tempo, il sistema è in grado di generare una visualizzazione più completa delle attività sospette e può quindi aggregare i flussi di rete correlati in un unico evento di rilevamento. La correlazione tra i flussi aiuta così a capire le attività sospette.

Una volta creati i cluster, vengono assegnati punteggi in base alle informazioni raccolte da tutti i motori di rilevamento. L'algoritmo CSS valuta tutte le attività di un cluster, per fornire ulteriore contesto, incrementando così il livello di precisione e riducendo i falsi positivi.

Il sistema di assegnazione dei punteggi di CSS si basa su diversi fattori, inclusi i livelli di gravità e gli indicatori di minacce identificati dai vari motori di rilevamento. Grazie alla combinazione di tutte queste informazioni, Sophos NDR è in grado di assegnare a ogni cluster un punteggio, che riflette il rischio potenziale costituito dalla rispettiva attività di rete. Questo sistema di valutazione offre agli amministratori di rete informazioni estremamente importanti sulle potenziali minacce, aiutandoli ad assegnare le giuste priorità e ad avviare azioni di risposta adeguate, in base al livello di rischio.

APPENDICI

APPENDICE A: Rischi Relativi Al Flusso Identificati Dal Motore SRA

PROTOCOLLO	RISCHIO RELATIVO AL FLUSSO	DESCRIZIONE
GENERALE	Potenziale exploit	È stato rilevato un potenziale exploit (ad es. Log4J/Log4Shell)
GENERALE	Protocollo noto su porta non-standard	Un protocollo viene utilizzato su una porta non-standard (ad es. HTTP su TCP/8000, mentre lo standard è TCP/80)
GENERALE	ASN rischioso	C'è stato uno scambio di traffico di rete con un server che appartiene a un ASN (numero sistema autonomo) rischioso.
GENERALE	Traffico unidirezionale	La sessione ha un'unica direzione. Questo può succedere in presenza di attività C2 verso un server che non opera più su quell'indirizzo.
GENERALE	Sessione di condivisione di desktop o file	Il flusso contiene dati relativi alla condivisione di desktop o file (ad es. TeamViewer, AnyDesk)
GENERALE	Protocollo non sicuro	Il protocollo utilizzato non è sicuro e se ne sconsiglia l'uso (ad es. Telnet invece di SSH)
GENERALE	Credenziali non cifrate	Sono state trasmesse credenziali in chiaro su un protocollo noto (ad es. FTP, HTTP, IMAP, POP3, SMTP)
GENERALE	Pacchetto non valido	Il pacchetto di rete ha un formato diverso dal previsto. Questo potrebbe indicare che c'è stato un errore del protocollo oppure che un protocollo valido è stato compromesso per trasportare un altro tipo di dati
GENERALE	Problemi di TCP	Sono stati rilevati problemi nelle impostazioni TCP della sessione di rete
GENERALE	Sottoscrittore anonimo	L'indirizzo IP di origine è stato anonimizzato e non può essere utilizzato per identificare il sottoscrittore (ad es. nel caso di flusso generato da un nodo di uscita relay privato iCloud)
GENERALE	Flusso periodico	La sessione di rete si ripete a intervalli regolari. Potrebbe indicare la presenza di attività C2 da parte di un trojan o una botnet
TLS, HTTP, DNS	Dominio DGA sospetto	Il nome di dominio potrebbe essere un DGA, che viene utilizzato per generare nomi di dominio, spesso sfruttati dal malware
TLS, HTTP, DNS	Dominio rischioso	È stato rilevato traffico di rete con un dominio considerato rischioso
TLS, HTTP, DNS	Caratteri non validi	Il protocollo decodificato contiene caratteri che non sono consentiti in quel campo del protocollo (ad es. un nome host DNS può contenere solamente un sottoinsieme di tutti i caratteri stampabili)
TLS, HTTP, DNS	IDN in Punycode	È stato rilevato un nome di dominio in formato IDN. I domini IDN in Punycode potrebbero indicare un attacco di phishing omografo

PROTOCOLLO	RISCHIO RELATIVO AL FLUSSO	DESCRIZIONE
HTTP, DNS	Rilevamento di un codice di errore	È stato rilevato un errore nel protocollo
DNS	Traffico sospetto	È stato rilevato un tipo di record DNS inatteso oppure obsoleto
DNS	Pacchetto di grandi dimensioni	Le dimensioni di un pacchetto DNS su UDP superano il limite massimo di 512 byte. Questo potrebbe indicare un tentativo di DNS Tunneling o di esfiltrazione
DNS	Frammentato	DNS su UDP frammentato. Questo potrebbe indicare un tentativo di DNS Tunneling o di esfiltrazione
SSH	Versione del client obsoleta o cifratura non sicura	Il client SSH ha utilizzato una versione obsoleta del protocollo oppure un sistema di cifratura non sicuro
SSH	Versione del server obsoleta o cifratura non sicura	Il server SSH ha utilizzato una versione obsoleta del protocollo oppure un sistema di cifratura non sicuro
SMB	Versione non sicura	È stata rilevata una versione di SMB non sicura (ad es. SMBv1)
ICMP	Entropia sospetta	È stata rilevata un'entropia sospetta nei pacchetti ICMP. Questo potrebbe indicare un'esfiltrazione dei dati su ICMP
TLS	Certificato autofirmato	È stato utilizzato un certificato autofirmato
TLS	Certificato SHA1 pericoloso	Il certificato TLS osservato è stato rilevato su un certificato pericoloso
TLS	Certificato non corrispondente	Il certificato TLS non corrisponde al nome host a cui viene effettuato l'accesso.
TLS	SNI mancante	Manca l'indicazione nome server (SNI) del server a cui è stato effettuato l'accesso.
TLS	Utilizzo sospetto di ESNI	È stato rilevato l'uso di SNI cifrato. Questo potrebbe indicare un attacco di tipo domain fronting.
TLS	Non contiene HTTPS	Il flusso TLS non è stato utilizzato per il trasporto di HTTPS.
TLS	Impronta digitale di JA3 pericolosa	L'impronta digitale di JA3 è stata rilevata in una blacklist di JA3
TLS	Estensione sospetta	Il nome di dominio nell'estensione SNI non è stampabile.
TLS	ALPN non comune	Un'estensione ALPN non comune è stata osservata nel flusso TLS (ad es. HTTP/1.1).
TLS	Certificato scaduto	Il certificato TLS utilizzato nel flusso è scaduto
TLS	Il certificato è prossimo alla scadenza	Il certificato TLS utilizzato nel flusso è prossimo alla scadenza
TLS	Validità del certificato troppo estesa	Il certificato TLS utilizzato nel flusso ha una validità che supera i 13 mesi.
TLS	Versione obsoleta	La versione di TLS è precedente alla 1.1.

PROTOCOLLO	RISCHIO RELATIVO AL FLUSSO	DESCRIZIONE
TLS	Cifratura debole	È stata utilizzata una cifratura TLS debole per la configurazione del flusso
TLS	Avviso di errore irreversibile	Il protocollo TLS ha ricevuto un avviso di errore irreversibile nel flusso.
HTTP	Host IP numerico	È stato effettuato l'accesso al server web utilizzando il rispettivo indirizzo IP invece del nome host.
HTTP	URL sospetto	L'URL di accesso è sospetto (esempio: http://127.0.0.1/ msadc/..%255c../..%255c../winnt/system32/cmd.exe.).
HTTP	Intestazione sospetta	L'intestazione HTTP contiene voci sospette, la cui presenza non è prevista nell'intestazione HTTP (ad es. UUID, versione di TLS, nome del sistema operativo).
HTTP	Agente utente sospetto	La stringa Agente utente contiene una formattazione o dei caratteri sospetti (esempio: <?qualcosa in php?>).
HTTP	Contenuti sospetti	Il flusso HTTP include contenuti in un formato diverso dal previsto (esempio: l'intestazione HTTP indica che il contesto è testo/HTML, ma il contenuto non è leggibile perché si tratta di dati binari).
HTTP	Trasferimento di un'applicazione binaria	Un'applicazione binaria viene scaricata o caricata. I file rilevati includono file binari Windows, file eseguibili Linux, script Unix e app Android.
HTTP	Potenziale XSS nell'URL	È stato identificato un potenziale attacco XSS (cross-site scripting).
HTTP	Potenziale SQL injection nell'URL	È stato identificato un potenziale attacco SQL injection.
HTTP	Potenziale RCE injection nell'URL	È stato identificato un potenziale attacco RCE (esecuzione di codice remoto).
HTTP	Bot crawler	È stato rilevato un crawler/bot/robot.
HTTP	Server obsoleto	È stata rilevata una sessione di rete con un server obsoleto Apache o Nginx.

APPENDICE B: Protocolli NPP

1KXUN	GIT	MICROSOFT_365	SPOTIFY
ACCUWEATHER	GITHUB	MICROSOFT_AZURE	SSDP
ACTIVISION	GITLAB	MINING	SSH
ADS_ANALYTICS_TRACK	GMAIL	MODBUS	STARCRAFT
ADULT_CONTENT	GNUTELLA	MONGODB	STEAM
AFP	GOOGLE	MPEGDASH	STUN
AJP	GOOGLE_CLASSROOM	MPEGTS	SYNCTHING
ALIBABA	GOOGLE_CLOUD	MQTT	SYSLOG
ALICLOUD	GOOGLE_DOCS	MS_ONE_DRIVE	TAILSCALE
AMAZON	GOOGLE_DRIVE	MS_OUTLOOK	TARGUS_GETDATA
AMAZON_ALEXA	GOOGLE_MAPS	MSSQL_TDS	TEAMSPEAK
AMAZON_AWS	GOOGLE_PLUS	MSTEAMS	TEAMVIEWER
AMAZON_VIDEO	GOOGLE_SERVICES	MUNIN	TELEGRAM
AMONG_US	GOTO	MYSQL	TELNET
AMQP	GTP	NATPMP	TENCENT
ANYDESK	GTP_C	NATS	TENCENTVIDEO
APPLE	GTP_PRIME	NEST_LOG_SINK	TEREDO
APPLE_ICLOUD	GTP_U	NETBIOS	TFTP
APPLE_ITUNES	GUILDWARS	NETFLIX	THREEMA
APPLE_PUSH	H323	NETFLOW	TIDAL
APPLE_SIRI	HALFLIFE2	NFS	TIKTOK
APPLESTORE	HANGOUT_DUO	NINTENDO	TINC
APPLETVPLUS	HBO	NOE	TIVOCONNECT
ARMAGETRON	HOTSPOT_SHIELD	NTOP	TLS
AVAST	HPVIRTGRP	NTP	TOCA_BOCA
AVAST_SECUREDNS	HSRP	OCS	TOR
BADOO	HTTP	OCSP	TPLINK_SHP

BGP	HTTP_CONNECT	OOKLA	TRUPHONE
BITTORRENT	HTTP_PROXY	OPENDNS	TUENTI
BJNP	HULU	OPENVPN	TUMBLR
BLOOMBERG	I3D	ORACLE	TUNEIN
CACHEFLY	IAX	PANDORA	TUNNELBEAR
CAPWAP	ICECAST	PASTEBIN	TUYA_LP
CASSANDRA	ICLOUD_PRIVATE_RELAY	PINTEREST	TVUPLAYER
CHECKMK	IEC60870	PLAYSTATION	TWITCH
CISCOVPN	IFLIX	PLAYSTORE	TWITTER
CITRIX	IHEARTRADIO	PLURALSIGHT	UBNTAC2
CLOUDFLARE	IMO	POSTGRES	UBUNTUONE
CLOUDFLARE_WARP	INSTAGRAM	PPSTREAM	ULTRASURF
CNN	IP_EGP	PPTP	USENET
COAP	IP_GRE	PSIPHON	VEVO
COLLECTD	IP_ICMP	QQ	VHUA
CORBA	IP_ICMPV6	QUIC	VIBER
CPHA	IP_IGMP	RADIUS	VIMEO
CRASHLYSTICS	IP_IP_IN_IP	RAKNET	VK
CROSSFIRE	IP_OSPF	RDP	VMWARE
CRYNET	IP_PGM	REDDIT	VNC
CSGO	IP_PIM	REDIS	VUDU
CYBERSECURITY	IP_SCTP	RIOTGAMES	VXLAN
DAILYMOTION	IP_VRRP	RPC	WARCRAFT3
DATASAVER	IPP	RSH	WAZE
DAZN	IPSEC	RSYNC	WEBEX
DEEZER	IRC	RTCP	WEBSOCKET
DHCP	JABBER	RTMP	WECHAT
DHCPV6	KAKAOTALK	RTP	WHATSAPP

DIAMETER	KAKAOTALK_VOICE	RTSP	WHATSAPP_CALL
DIRECTV	KERBEROS	RX	WHATSAPP_FILES
DISCORD	KISMET	S7COMM	WHOIS_DAS
DISNEYPLUS	KONTIKI	SALESFORCE	WIKIPEDIA
DNP3	LASTFM	SAP	WINDOWS_UPDATE
DNS	LDAP	SD_RTN	WIREGUARD
DNSCRYPT	LIKEE	SFLOW	WORLD_OF_KUNG_FU
DOFUS	LINE	SHOWTIME	WORLDOFWARCRAFT
DOH_DOT	LINE_CALL	SIGNAL	WSD
DRDA	LINKEDIN	SIGNAL_VOIP	XBOX
DROPBOX	LISP	SINA	XDMCP
DTLS	LIVESTREAM	SIP	XIAOMI
EAQ	LLMNR	SIRIUSXMRADIO	YAHOO
EBAY	LOTUS_NOTES	SKINNY	YANDEX
EDGECAST	MAIL_IMAP	SKYPE_TEAMS	YANDEX_CLOUD
EDONKEY	MAIL_IMAPS	SKYPE_TEAMS_CALL	YANDEX_DIRECT
ELASTICSEARCH	MAIL_POP	SLACK	YANDEX_DISK
ETHERNET_IP	MAIL_POPS	SMBV1	YANDEX_MAIL
FACEBOOK	MAIL_SMTP	SMBV23	YANDEX_MARKET
FACEBOOK_VOIP	MAIL_SMTPS	SMPP	YANDEX_METRIKA
FASTCGI	MAPLESTORY	SNAPCHAT	YANDEX_MUSIC
FIX	MDNS	SNAPCHAT_CALL	YOUTUBE
FORTICLIENT	MEGACO	SNMP	YOUTUBE_UPLOAD
FTP_CONTROL	MEMCACHED	SOAP	Z3950
FTP_DATA	MERAKI_CLOUD	SOCKS	ZABBIX
FTPS	MESSENGER	SOFTETHER	ZATTOO
FUZE	MGCP	SOMEIP	ZMQ
GENSHIN_IMPACT	MICROSOFT	SOUNDCLOUD	ZOOM

Per Sapere Di Più Su Sophos NDR, visita: sophos.com/ndr

Le dichiarazioni contenute in questo documento si basano su informazioni disponibili pubblicamente, consultate in data 30 marzo 2023. Questo documento è stato preparato da Sophos e non dagli altri vendor elencati. Le funzionalità e le caratteristiche dei prodotti posti a confronto, che possono influire direttamente sull'accuratezza o sulla validità di questo confronto, sono soggette a cambiamenti. Le informazioni contenute in questo confronto hanno lo scopo di aiutare a capire e conoscere a grandi linee le informazioni effettive su vari prodotti, e potrebbero non essere complete. Chiunque consulti questo documento deve assumersi la responsabilità delle proprie decisioni di acquisto in base ai propri requisiti; inoltre, quando si seleziona un prodotto, si consiglia di consultare le fonti originali di informazioni, piuttosto che affidarsi solamente a questo confronto. Sophos non rilascia alcuna garanzia relativamente all'affidabilità, all'accuratezza, all'utilità o alla completezza di questo documento. Le informazioni di questo documento vengono fornite "così come sono" e senza garanzia, esplicita o implicita, di alcun tipo. Sophos si riserva il diritto di modificare o ritirare questo documento in qualsiasi momento.

29/03/2023 (WP-NP)

SOPHOS