Managed Threat Detection

Un servizio completamente gestito di monitoraggio e rilevamento 24/7 per potenziare la vostra protezione Endpoint non-Sophos

La protezione a modo vostro

Sono poche le organizzazioni che hanno a disposizione gli strumenti, il personale ed i processi interni necessari a gestire con efficienza il proprio programma di sicurezza 24h su 24. Molte sembrano affidarsi completamente alla protezione endpoint automatica, ma cosa succede quando i cybercriminali riescono a eludere questo tipo di difesa? Ci sarà qualcuno che se ne accorgerà prima che sia troppo tardi?

Sophos Managed Threat Detection offre monitoraggio e rilevamento delle minacce 24/7 per garantire l'intercettazione di qualsiasi attività sospetta che riesca a sfuggire alla vostra protezione endpoint. Il servizio è progettato per lavorare in parallelo insieme ai prodotti di protezione endpoint non Sophos, il che significa che le organizzazioni possono continuare a utilizzare il proprio sistema di sicurezza endpoint attuale, pur usufruendo del monitoraggio a cura degli esperti di Sophos.

Rilevamento

Managed Threat Detection è disponibile in modalità di "Notifica" per la risposta alle minacce. I Clienti riceveranno avvisi se una minaccia ad alta gravità dovesse riuscire a eludere il sistema di protezione endpoint. L'intercettazione comprende una vasta gamma di attività comportamentali comunemente osservate prima di un attacco di ransomware.

Il rilevamento può ad esempio includere:

- Shellcode a fasi, come quelli solitamente osservati in Cobalt Strike Beacon o Metasploit Meterpreter
- Nuove operazioni pianificate che eseguono $PS, incluse attività su percorsi comunemente sfruttati dal malware e dagli hacker per mantenere la persistenza (ovvero chiavi di esecuzione nel registro di sistema, servizi, elementi di avvio di Windows)
- Ransomware e attività comportamentali che possono sfuggire ad altri prodotti di sicurezza

Caratteristiche principali

- Monitoraggio e rilevamento 24/7 delle attività sospette
- Soluzione progettata per eseguirsi in parallelo insieme a prodotti di protezione endpoint non Sophos
- Modalità "Notifica" per la risposta alle minacce
- Conferma di un analista per tutti i rilevamenti di gravità alta
- Notifiche che includono consigli sulle azioni di correzione
- Sophos Rapid Response è disponibile per ulteriori funzionalità di risposta in caso di incidenti

SOPHOS

Notifica e Risposta

Le comunicazioni trasparenti sono fondamentali per chi deve gestire le operazioni di sicurezza. Ed è per questo motivo che il servizio Managed Threat Detection offre un flusso di informazioni costante, con report settimanali e mensili, notifiche tramite e-mail e una dashboard in Sophos Central.

I Clienti riceveranno notifiche e-mail contenenti aggiornamenti sullo stato dei casi di minacce, che includono informazioni su quando è necessario intraprendere un'azione e quando invece i casi sono risolti. Tutti i casi saranno stati prima confermati da un analista e le notifiche includeranno un riepilogo del caso, un elenco dei dispositivi colpiti e consigli sulle azioni di correzione.

Inoltre, verranno inviati broadcast informativi per mantenere i Clienti aggiornati sulle ultime notizie di sicurezza, con i risultati delle indagini sulla minaccia rilevata, le misure intraprese da Sophos e gli accorgimenti che possono essere adottati dai Clienti per rimanere protetti.

Quando vengono rilevate minacce attive in uno degli ambienti del Cliente, gli operatori Sophos chiamano il contatto specificato al telefono per comunicare tempestivamente questa informazione critica. I Clienti possono aggiornare il proprio contatto autorizzato e le preferenze per Managed Threat Detection in qualsiasi momento dalla dashboard di Sophos Central. La dashboard offre anche un riepilogo di tutte le attività pertinenti di Managed Threat Detection, per garantire ai Clienti informazioni aggiornate in tempo reale in qualsiasi momento e ovunque si trovino.

Per i Clienti che stanno affrontando una minaccia e hanno bisogno di assistenza per l'Incident Response, il team Sophos Rapid Response è disponibile come servizio aggiuntivo. Sophos Rapid Response offre assistenza tempestiva in caso di emergenza: svolge indagini sulle minacce attive e le neutralizza. Che si tratti di un'infezione, di un tentativo di compromissione o di un accesso non autorizzato che cerca di eludere i controlli di sicurezza oppure è riuscito infiltrarsi nei sistemi, il nostro team ha già visto e bloccato di tutto. I Clienti Sophos sono avvantaggiati, in quanto possono ricevere assistenza con maggiore rapidità: il team Rapid Response ha infatti accesso immediato alla telemetria e allo strumento di registrazione dei dati degli agenti di Managed Threat Detection.

	Managed Threat Response (MTR) Standard	Managed Threat Response (MTR) Advanced	Managed Threat Detection
Compatibilità con prodotti di protezione Endpoint non-Sophos	✗	✗	✓
Monitoraggio 24/7	✓	✓	✓
Rilevamento degli active adversary	✓	✓	✓
Report, dashboard	✓	✓	✓
Notifica della presenza di minacce	✓	✓	✓
Connettore MTR di Sophos Firewall	✗	✓	✓
Connettore MTR di Sophos CloudOptix	✗	✓	✗
Supporto di sistemi operativi multipli	✓	✓	✗ (solo Win 10/2012 R2)
Threat hunting senza indizi, gestito da un analista	✗	✓	✗
Controllo Sophos dello stato di integrità degli endpoint	✓	✓	✗
Protezione in tempo reale	✓	✓	✗
Isolamento e neutralizzazione	✓	✓	✗
Comunicazione telefonica	✗ (solo per le minacce attive)	✓	✗ (solo per le minacce attive)

NPO Sistemi SRL
Sede Amministrativa e Operativa: Viale Martesana, 12 - 20055 Vimodrone (MI)
Telefono: +39 02 925961
sito: www.nposistemi.it
e.mail: info_marketing@nposistemi.it
Linkedin Npo Sistemi