Briefing del prodotto

Sophos NDR

Rileva i comportamenti sospetti che vanno oltre i tuoi Endpoint e Firewall

Sophos Network Detection and Response è un'opzione disponibile sia per Sophos MDR che per Sophos XDR, che consente di rilevare le attività di rete pericolose nelle parti più nascoste della rete, dove il firewall e le soluzioni endpoint non hanno visibilità. Sophos NDR analizza continuamente il traffico per identificare comportamenti sospetti, incluse attività insolite generate da dispositivi sconosciuti o non gestiti; individua le risorse non autorizzate, i nuovi server C2 zero-day e qualsiasi trasferimento di dati inatteso.

Casi di utilizzo

1 | LIVELLI CRITICI DI VISIBILITÀ

Esito desiderato: ottenere una maggiore visibilità sulle attività della rete che gli altri prodotti non sono in grado di analizzare

Soluzione: Sophos NDR agisce in perfetta sinergia con i tuoi firewall ed endpoint gestiti per monitorare l'attività della rete alla ricerca di comportamenti sospetti e dannosi, che altrimenti passerebbero inosservati. Analizza le parti più nascoste della rete per rilevare i flussi di traffico anomali che vengono generati da sistemi e dispositivi IoT non gestiti, da risorse non autorizzate, da minacce interne, da attacchi zero-day mai visti prima e da comportamenti sospetti.

2 | RILEVAMENTO TEMPESTIVO

Esito desiderato: cinque motori di rilevamento indipendenti, che agiscono in tempo reale per identificare prima le minacce

Soluzione: Sophos NDR include cinque motori di rilevamento indipendenti che interagiscono in maniera fluida e in tempo reale per rilevare rapidamente il traffico sospetto o dannoso. Sfruttano tecnologie quali Deep Learning, Deep Packet Inspection, analisi dei payload cifrati, analisi dei nomi di dominio e potenti capacità di analisi. Le nostre esclusive funzionalità di analisi generano solo avvisi estremamente accurati, per non costringerti a sprecare tempo prezioso valutando segnalazioni non pertinenti.

3 | RISPOSTA AUTOMATICA

Esito desiderato: blocco automatico degli active adversary e delle minacce, per stroncare gli attacchi sul nascere

Soluzione: le straordinarie capacità di automazione multiprodotto di Sophos permettono a Sophos NDR, Sophos XDR, Sophos MDR e Sophos Firewall di coordinare una risposta immediata, in grado di bloccare le minacce attive sul nascere. Non appena Sophos NDR identifica un indicatore di compromissione, una minaccia attiva o un active adversary, lo segnala immediatamente agli analisti, che possono quindi inviare un feed sulle minacce a Sophos Firewall per attivare la risposta automatica e isolare l'host compromesso.

4 | GESTIONE DA UN'UNICA CONSOLE

Esito desiderato: meno tempo da dedicare alla gestione della protezione della rete

Soluzione: Sophos Central offre un'unica piattaforma di gestione per tutti i tuoi prodotti Sophos, inclusi NDR, XDR, Endpoint, Firewall e molti altri. Potrai così sfruttare il pieno potenziale di strumenti ricchi di funzionalità, che ricevono dati dal nostro Data Lake e permettono di svolgere attività di threat hunting, risposta tempestiva, reportistica e controllo su più prodotti contemporaneamente. La maggiore rapidità di azione ti permette, in ultima analisi, di guadagnare tempo prezioso, che altrimenti avresti dovuto dedicare alla gestione della protezione della tua rete.

Identificazione di risorse non protette e non autorizzate

Individuazione di trasferimenti di dati insoliti e di minacce interne

Rilevamento di attacchi zero-day mai visti prima

Scopri di più e prova gratuitamente
Sophos NDR
sophos.com/ndr

2023-11-06 DS-IT (MP)

SOPHOS