Sophos XDR

Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X offre la combinazione ottimale tra un potente sistema di rilevamento e risposta estesi (Extended Detection and Response, XDR) e una protezione endpoint di altissimo livello. Il threat hunting rileva la presenza di hacker e permette alle IT Operations di garantire l'integrità del sistema di cybersecurity. Quando viene identificato un problema in remoto, aiuta a implementare un'azione di risposta precisa e accurata. La visibilità si estende oltre i singoli endpoint, grazie all'integrazione di varie fonti di dati, che includono endpoint, server, firewall ed e-mail.

Risposta alle domande sulle IT operation e sul threat hunting

Ora è possibile trovare risposta alle domande critiche per l'organizzazione. I vantaggi nelle normali attività quotidiane di IT operation e threat hunting saranno evidenti sia per gli amministratori IT che per i professionisti della cybersecurity.

Il modo migliore per cominciare è partire con la protezione più efficace

Intercept X blocca i tentativi di violazione prima ancora del loro inizio. Questo vuol dire poter usufruire di una protezione superiore e di conseguenza dover trascorrere meno tempo a indagare sugli incidenti che avrebbero potuto essere bloccati automaticamente. Inoltre, è anche possibile attingere dai dati di intelligence sulle minacce per ottenere informazioni approfondite e intervenire in maniera mirata.

Approfondimenti rilevanti, per una risposta rapida

Una volta identificato un elemento che richiede ulteriori indagini, è possibile svolgere, dal Sophos Data Lake, un'analisi approfondita dei dettagli in tempo reale (ottenuti direttamente dal dispositivo) e delle informazioni nello storico dei dati, conservati fino a 90 giorni. Quando viene confermata la presenza di un problema, è possibile accedere al dispositivo da remoto e intraprendere tutte le azioni necessarie per risolvere la problematica, come ad esempio la disinstallazione di un'applicazione e il riavvio del sistema.

Visibilità su prodotti multipli

Sophos XDR va oltre il livello dei singoli endpoint e server, permettendo a Sophos Firewall, Sophos Email e altre origini di dati* di inviare informazioni importanti al Sophos Data Lake, per offrire visibilità estesa sull'ambiente dell'intera organizzazione.

Informazioni reperibili anche quando i dispositivi sono off-line

Il Sophos Data Lake, un componente essenziale della funzionalità XDR, è un repository di dati nel cloud. Permette di archiviare e accedere alle informazioni critiche di endpoint, server, firewall e persino dei dispositivi off-line.

Caratteristiche principali

- Possibilità di rispondere alle domande critiche sulle IT operation e sul threat hunting
- Soluzioni progettate per gli amministratori IT e gli analisti di sicurezza
- Capacità di intraprendere azioni correttive da remoto sui dispositivi interessati
- Prospettiva olistica dell'ambiente IT dell'organizzazione, con approfondimenti dettagliati laddove necessario
- Dati provenienti da endpoint, server, firewall, e-mail e altre origini*
- Query SQL subito pronte per l'uso e completamente personalizzabili
- Disponibili per Windows, macOS e Linux

** Cloud Optix e Sophos Mobile saranno presto disponibili*

SOPHOS

Bastano pochi secondi per cominciare

È disponibile una libreria di query SQL precompilate, da utilizzare per trovare risposta a una vasta selezione di domande sui sistemi IT e sulla sicurezza. A seconda delle preferenze, è possibile personalizzare le query oppure crearne di nuove. In alternativa, si possono consultare le pagine della Sophos Community, dove vengono condivise regolarmente nuove query.

Casi di utilizzo

IT operation

- Perché un computer è particolarmente lento?
- Su quali dispositivi sono presenti vulnerabilità note, servizi sconosciuti o estensioni del browser non autorizzate?
- Ci sono programmi in esecuzione che dovrebbero essere rimossi?
- Identificazione dei dispositivi non gestiti, IoT e appartenenti a utenti guest
- Perché la connessione di rete in questo ufficio è lenta? Qual è l'applicazione responsabile?
- Possibilità di indagare sugli ultimi 30 giorni di attività di un dispositivo smarrito o reso inutilizzabile, per rilevare eventi anomali

Threat hunting

- Quali processi stanno cercando di stabilire una connessione di rete su porte non standard?
- Visualizzazione dei processi che hanno recentemente modificato file o chiavi di registro
- Elenco degli indicatori di compromissione (Indicator of Compromise, IoC) mappati al framework MITRE ATT&CK
- Estensione delle indagini a 30 giorni senza bisogno che il dispositivo sia on-line
- Utilizzo dei rilevamenti ATP e IPS del firewall per svolgere indagini sugli host sospetti
- Confronto tra dati nell'intestazione delle e-mail, SHA e altri indicatori di compromissione, per identificare il traffico diretto verso un dominio pericoloso

Opzioni incluse

	Extended Detection and Response (XDR)
Origini dati che coinvolgono prodotti multipli	✓
Query su prodotti multipli	✓
Query su endpoint e server	✓
Sophos Data Lake	✓
Periodo di conservazione dei dati nel data lake	30 giorni
Periodo di conservazione dei dati su disco	✓
Libreria di query SQL	✓
Opzioni di protezione di Intercept X	✓

Maggiori informazioni sulle licenze sono disponibili nelle guide alle licenze di Intercept X e Intercept X for Server.

Effettuate subito una prova gratuita

Registratevi per una prova gratuita di 30 giorni su: sophos.it/intercept-x

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

08/07/21 DS-IT (PS)

SOPHOS