Sophos XDR

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

Intercept X è l'unica soluzione XDR in grado di sincronizzare la protezione nativa di endpoint, server, firewall, e-mail, cloud e O365. Puoi così ottenere una prospettiva olistica dell'ambiente dell'organizzazione, con un set di dati più completi e analisi approfondite per offrire opzioni di rilevamento, indagine e risposta alle minacce, sia per interi team SOC dedicati che per singoli amministratori IT.

Risposta alle domande sulle IT operations e sul threat hunting

Ora è possibile trovare risposta alle domande critiche per l'organizzazione. I vantaggi nelle normali attività quotidiane di IT operations 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.

Concentrati sugli elementi importanti

Focalizzati sui problemi più importanti, grazie a un elenco in ordine di priorità di rilevamenti sospetti e configurazioni vulnerabili che include informazioni fondamentali per condurre ulteriori indagini. Puoi scegliere da una libreria di modelli precompilati da utilizzare per trovare risposta a una vasta selezione di domande sulle IT operations e sul threat hunting. Puoi anche crearne uno personalizzato.

Riduci i tempi di indagine e risposta

Le indagini guidate dall'intelligenza artificiale ti consentono di capire rapidamente l'impatto e la causa di un incidente, per ridurre al minimo i tempi di risposta. Accedi ai dispositivi per determinarne lo stato in tempo reale e per consultare 90 giorni di storico dei dati sul dispositivo, o 30 nel data lake.

Visibilità su prodotti multipli

Ottieni la massima visibilità sui sistemi della tua organizzazione, grazie all'integrazione nativa dei dati provenienti da Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix e Microsoft Office 365.

Supporto di piattaforme e sistemi operativi multipli

Ispeziona il tuo ambiente cloud, on-premise o virtuale su distribuzioni Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform e Oracle Cloud Infrastructure.

Caratteristiche principali

- Possibilità di rispondere alle domande critiche sulle IT operations e sul threat hunting
- Elenco in ordine di priorità dei rilevamenti, più indagini guidate dall'intelligenza artificiale
- Capacità di intraprendere azioni correttive da remoto sui dispositivi interessati
- Prospettiva olistica dell'ambiente IT dell'organizzazione, con approfondimenti dettagliati laddove necessario
- Integrazioni native per endpoint, server, firewall, e-mail, cloud, dispositivi mobili e O365
- Accesso a una libreria di modelli precompilati e personalizzabili per vari casi di utilizzo

SOPHOS

Casi di utilizzo

IT operations

- 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
- Identificazione dei dispositivi mobili con software obsoleti o senza le patch più recenti

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
- Identificazione degli utenti che hanno effettuato diversi tentativi di autenticazione non riusciti

Opzioni incluse

	Extended Detection and Response (XDR)
Origini dati che coinvolgono prodotti multipli	✓
Rilevamento, indagine e risposta su prodotti multipli	✓
Elenco di rilevamenti in ordine di priorità e indagini guidate dall'intelligenza artificiale	✓
Sophos Data Lake	✓
Periodo di conservazione dei dati nel data lake	30 giorni
Informazioni di stato in tempo reale	✓
Periodo di conservazione dei dati su disco	Fino a 90 giorni
Libreria di modelli per il threat hunting e le IT operations	✓
Opzioni di protezione di Intercept X	✓

Per maggiori informazioni sulle licenze, consulta le guide alle licenze di Intercept X e Intercept X for Server.

Effettua subito una prova gratuita

Registrati 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

22-01-06 DS-IT (MP)

SOPHOS