SOPHOS
Cybersecurity evolved.

Intercept X Advanced with EDR

Una soluzione di Endpoint Detection and Response realizzata per il threat hunting e per la gestione operativa dei sistemi informatici

Sophos Intercept X Advanced with EDR offre la combinazione ottimale tra un potente sistema di rilevamento e risposta alle minacce endpoint (Endpoint Detection and Response, EDR) e una protezione endpoint di altissimo livello. Permette di individuare proattivamente gli active adversary, o di utilizzare la gestione operativa dei sistemi informatici per garantire l'integrità del sistema di IT security. Quando viene identificato un problema in remoto, aiuta a implementare un'azione di risposta precisa e accurata.

Caratteristiche principali

- EDR in combinazione con il più efficace sistema di protezione endpoint
- Un sistema progettato per gli analisti di sicurezza e gli amministratori IT
- Consente di garantire proattivamente l'integrità del sistema informatico e di individuare le minacce prima che possano generare danni
- Consente di rispondere a domande su eventi passati e attuali
- Query SQL subito pronte all'uso e completamente personalizzabili
- Accesso rapido a un massimo di 90 giorni di dati correnti o storici su disco
- Permette di rispondere con estrema precisione da remoto, tramite uno strumento a riga di comando
- Rilevamento, indagine e attribuzione di priorità agli incidenti, con tecnologie di machine learning
- Indagini più rapide, per ridurre il tempo di permanenza degli hacker nei sistemi
- Disponibile per Windows, MacOS* e Linux

L'EDR comincia dalla protezione più efficace

Per bloccare i tentativi di violazione prima ancora che vengano effettuati, la prevenzione è fondamentale. Intercept X consolida in un'unica soluzione l'EDR e la migliore protezione endpoint in assoluto. In questo modo, la maggior parte delle minacce viene bloccata prima che possa causare qualsiasi danno. Intercept X Advanced with EDR offre ulteriore garanzia di cybersecurity, in quanto offre opzioni di rilevamento, indagine e risposta alle potenziali minacce di sicurezza.

L'inclusione della nuova funzionalità di Endpoint Detection and Response (EDR) in una suite di protezione endpoint che risulta tra le migliori opzioni disponibili sul mercato, consente a Intercept X di alleggerire significativamente il carico di lavoro in termini di EDR. Una prevenzione che filtra un maggior numero di minacce aiuta a ridurre gli eventi non significativi. Questo aiuta gli analisti a non perdere tempo dietro a falsi positivi e a un volume eccessivo di notifiche.

Aggiunta di competenze, non di personale

Rilevamento, attribuzione di priorità e indagine automatica delle minacce mediante tecnologie di intelligenza artificiale: Intercept X Advanced with EDR sfrutta il machine learning per individuare e attribuire automaticamente la giusta priorità alle potenziali minacce. Se viene individuato un file potenzialmente malevolo, gli utenti possono utilizzare l'analisi antimalware basata sul deep learning per esaminare automaticamente il malware nei minimi dettagli, scomponendo il file per estrarne attributi e codice, e mettendo questi ultimi a confronto con milioni di altri file.

Query subito pronte all'uso, create da professionisti per altri professionisti: analisti di sicurezza e amministratori IT possono utilizzare Sophos EDR immediatamente, grazie alle query SQL subito pronte all'uso e classificate in base ai casi di utilizzo. Le query possono essere modificate con estrema semplicità per personalizzare le ricerche. In alternativa, è anche possibile creare query ex novo o utilizzare quelle della nostra community.

Una risposta sempre pronta, anche per le domande più difficili, grazie a un sistema che replica le capacità tecniche di analisti esperti: Intercept X Advanced with EDR consente alle organizzazioni di aggiungere alle proprie risorse competenze tecniche elevate, senza dover assumere altri dipendenti.

** In arrivo*

Realizzata per il threat hunting e per i sistemi informatici

Sophos Intercept X Advanced è la prima soluzione EDR progettata per amministratori IT e analisti di sicurezza. Consente di rispondere a domande su eventi passati e attuali riguardanti gli endpoint. Permette di individuare proattivamente gli active adversary, o di utilizzare la gestione operativa dei sistemi informatici per garantire l'integrità del sistema di IT security. Quando viene identificato un problema in remoto, aiuta a implementare un'azione di risposta precisa e accurata. Questo avviene grazie a due funzionalità: Live Discover e Live Response.

Live Discover: una risposta a qualsiasi tipo di domanda, per avere sempre tutto sotto controllo. Live Discover offre agli analisti di sicurezza e agli amministratori IT la capacità di cercare informazioni per rispondere a qualsiasi domanda che riguardi i loro endpoint e server. Permette di individuare rapidamente i problemi che incidono sulla gestione operativa dei sistemi informatici, per garantire l'integrità del sistema di IT security e individuare proattivamente le attività sospette. Live Discover utilizza potenti query SQL subito pronte all'uso e completamente personalizzabili, che consentono di effettuare ricerche su dati correnti o storici raccolti fino ad un massimo di 90 giorni prima. I casi di utilizzo includono:

Gestione operativa dei sistemi informatici

- Perché un computer è particolarmente lento? È in attesa di riavvio?
- Su quali dispositivi sono presenti vulnerabilità note, servizi sconosciuti o estensioni del browser non autorizzate?
- Ci sono programmi in esecuzione che dovrebbero essere rimossi?
- È abilitata la condivisione in remoto? Ci sono chiavi SSH non cifrate nel dispositivo? Sono abilitati account guest?
- Il dispositivo ha una copia di un file specifico?

Threat hunting

- Quali processi stanno cercando di stabilire una connessione di rete su porte non standard?
- Elenco degli indicatori di compromissione (Indicator of Compromise, IoC) mappati al framework MITRE ATT&CK
- Visualizzazione dei processi che hanno recentemente modificato file o chiavi di registro
- Ricerca di dettagli relativi alle esecuzioni di PowerShell
- Identificazione dei processi che si spacciano per file services.exe

Live Response: risposta precisa e accurata in remoto. Quando viene individuato un problema, Live Response offre agli utenti accesso mediante riga di comando a tutti gli endpoint e server dell'intera struttura informatica aziendale. Permette di accedere ai dispositivi da remoto, per svolgere ulteriori attività di indagine o correzione dei problemi. Gli amministratori possono riavviare i dispositivi, terminare processi attivi, eseguire script, modificare file di configurazione, installare/disinstallare software, eseguire strumenti di analisi approfondita e molto altro ancora.

Azioni di rilevamento e risposta gestiti (MTR)

Sophos Managed Threat Response (MTR) è un servizio completamente gestito con opzioni di threat hunting, rilevamento e risposta alle minacce, disponibile 24h su 24 e 7gg su 7 e fornito da un team di esperti Sophos. Laddove gli altri servizi di rilevamento e risposta gestiti (Managed Detection and Response, MDR) si limitano a segnalare gli attacchi e gli eventi sospetti, con Sophos MTR la vostra azienda può contare sul supporto di un team selezionato di esperti nell'individuazione e nella risposta alle minacce, in grado di intraprendere azioni mirate per conto vostro, neutralizzando anche le minacce più sofisticate. I clienti che scelgono Sophos MTR ricevono anche Intercept X Advanced with EDR.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Endpoint Protection
Tecniche fondamentali	✓	✓	✓
Deep Learning	✓	✓	
Antiexploit	✓	✓	
Antiransomware CryptoGuard	✓	✓	
Endpoint Detection and Response (EDR)	✓		

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

20-05-12 DS-IT (MP)

SOPHOS