SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

Un sistema intelligente di rilevamento e risposta alle minacce endpoint

Sophos Intercept X Advanced with EDR integra un sistema intelligente di rilevamento e risposta alle minacce endpoint (Endpoint Detection and Response, EDR) alla più accreditata soluzione di rilevamento antimalware disponibile sul mercato, nonché alla migliore soluzione di difesa contro gli exploit.

Caratteristiche principali

- EDR in combinazione con il più efficace sistema di protezione endpoint
- Analisi antimalware con Deep Learning
- Collegamento in tempo reale con i dati di intelligence gestiti dai SophosLabs
- Utilizzo delle tecniche di Machine Learning e assegnazione di priorità agli eventi sospetti*
- Indagini guidate, per rendere l'EDR accessibile e facilmente utilizzabile
- Risposta agli incidenti attraverso pochi passaggi

L'Endpoint Detection and Response per una 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 livelli di protezione mai raggiunti prima e straordinarie opzioni di rilevamento e risposta alle minacce endpoint. Questo sistema permette di bloccare la maggior parte delle minacce, prima che possano provocare danni irreversibili; in più, Intercept X Advanced with EDR contribuisce a incrementare i livelli di difesa grazie alle sue capacità 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. Aumentando l'efficacia della prevenzione delle minacce, diminuiscono gli eventi non significativi generati e di conseguenza anche quelli su cui i team di sicurezza devono investigare. Ciò permette al personale tecnico di ottimizzare le risorse e dedicarsi maggiormente alle attività più relevanti, invece di perdere tempo dietro a falsi positivi e a un volume eccessivo di notifiche.

L'importanza di aggiungere competenze, non personale

Intercept X Advanced with EDR consente alle organizzazioni di aggiungere alle proprie risorse competenze tecniche elevate, senza dover assumere altri dipendenti. A differenza delle altre soluzioni di EDR, che si affidano all'esperienza di analisti per cercare le informazioni giuste e interpretare i dati, Intercept X Advanced with EDR si basa sul Machine Learning e sui dati di intelligence gestiti direttamente dai SophosLabs.

Esperienza nell'ambito della sicurezza*: Intercept X Advanced with EDR affida la sicurezza ai sistemi informatici, grazie al rilevamento e all'assegnazione automatica di priorità alle minacce potenziali. Il Machine Learning consente di identificare gli eventi sospetti e di segnalare quelli più importanti che richiedono attenzione immediata. In questo modo, è possibile identificare in modo immediato quali sono le situazioni critiche più urgenti da gestire e quali sono i computer che potrebbero essere stati colpiti.

Malware expertise: nella maggior parte dei casi, le organizzazioni affidano l'analisi dei file sospetti ad attività manuali gestite da esperti di sicurezza. Questo approccio implica un inutile dispendio di tempo, è considerato di dubbia efficacia e si basa sul presupposto che ci sia una conoscenza profonda delle varie tecniche di cybersecurity che in realtà non sono presenti nella maggior parte delle organizzazioni. Intercept X Advanced with EDR offre una strategia più efficace, in quanto sfrutta la capacità di analisi antimalware del Deep Learning, che analizza automaticamente il malware nei minimi dettagli e lo mette a confronto con milioni di dati di intelligence gestiti direttamente dai SophosLabs. Attraverso questa analisi, è possibile vedere immediatamente quali attributi e segmenti di codice del file analizzato sono simili a file "noti per essere innocui" o "noti per essere malevoli" e stabilire se bloccare o autorizzare un file specifico.

Competenze elevate in termini di intelligence sulle minacce: quando Intercept X Advanced with EDR segnala un file potenzialmente sospetto, gli amministratori IT possono ottenere maggiori informazioni attraverso l'accesso diretto ai dati di intelligence sulle minacce messi a disposizione dai SophosLabs. Ogni giorno, i SophosLabs ricevono ed elaborano circa 400.000 campioni di malware inedito. Successivamente, tutti i dati di intelligence disponibili vengono raccolti, aggregati e riepilogati, per semplificarne l'analisi. Questo processo permette ai team che non dispongono di personale specializzato e dedicato esclusivamente a questa tipologia di analisi, di potersi affidare ad uno dei migliori team di ricercatori di cybersecurity ed esperti di data science al mondo.

Risposta guidata agli incidenti

Intercept X Advanced with EDR permette agli amministratori di trovare risposta a qualsiasi domanda relativa agli incidenti di sicurezza, anche quelli più problematici, in quanto viene visualizzata graficamente l'estensione di un attacco, come ha avuto origine, quali sono gli elementi colpiti e qual è la strategia di risposta più adeguata. Indipendentemente dal livello di preparazione, i team di sicurezza dell'organizzazione possono facilmente capire quale è il livello di sicurezza generale dei sistemi e quali sono le migliori azioni da intraprendere, considerando i dati di intelligence analizzati.

Ottenuti i risultati dopo l'analisi effettuata, gli amministratori IT possono compiere la scelta migliore attraverso semplici passaggi. Tra le opzioni disponibili, è possibile isolare gli endpoint per azioni di correzione immediate, a scopo di disinfezione e blocco dei file e per acquisire dati di analisi approfonditi.

Casi di utilizzo del sistema EDR

Il sistema EDR (endpoint detection and response) fornisce ai responsabili della sicurezza la visibilità e le competenze necessarie per rispondere a qualsiasi domanda che riguardi il processo di risposta a un incidente.

Consente di analizzare tutti gli aspetti di un incidente, anche quelli più difficili da smascherare:

- Comprensione dell'estensione e dell'impatto degli incidenti di sicurezza
- Rilevamento degli attacchi che potrebbero essere passati inosservati
- Ricerca di indicatori di compromissione all'interno della rete
- Assegnazione di priorità agli eventi, per approfondire le indagini
- Analisi dei file per stabilire se costituiscano una minaccia o se siano elementi potenzialmente indesiderati
- Analisi dello stato di sicurezza dell'organizzazione in qualsiasi momento

Oltre l'EDR

Per bloccare un ampio spettro di minacce, Intercept X Advanced with EDR adotta un approccio di difesa in profondità alla protezione endpoint. Si contraddistingue dai sistemi tradizionali, che adottano un'unica tecnica principale. È la una combinazione tra tecniche tradizionali e tecniche moderne messe a disposizione da un vendor leader di mercato. Intercept X Advanced with EDR consolida in un'unica soluzione il rilevamento antimalware leader del settore, la migliore struttura di difesa contro gli exploit e un sistema intelligente di rilevamento e risposta alle minacce endpoint (EDR).

Le tecniche moderne includono il rilevamento antimalware con Deep Learning, la prevenzione degli exploit e funzionalità dedicate all'individuazione del ransomware. Le tecniche tradizionali includono antivirus, analisi del comportamento, rilevamento del traffico malevolo, prevenzione della perdita di dati e altro ancora.

Intercept X Advanced with EDR offre la combinazione ideale tra le tecnologie moderne di rilevamento e risposta alle minacce endpoint, grazie alle funzionalità di Intercept X, e le tecniche di protezione tradizionali di Sophos Central Endpoint Protection. L'intero sistema viene distribuito come un'unica soluzione e con un singolo agente.

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

* Disponibile a inizio del 2019

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

Effettuate subito una prova gratuita

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

18-10-02 DS-IT (3098-DD)

SOPHOS