SOPHOS

Managed Threat Response (MTR)

Un sistema di risposta alle minacce gestito da esperti

Sophos Managed Threat Response (MTR) offre un servizio completamente gestito con opzioni di ricerca, rilevamento e risposta alle minacce, disponibile 24h su 24 e 7gg su 7 e gestito direttamente dal nostro team di esperti.

Funzionalità principali

- Funzionalità avanzate di threat hunting, rilevamento e risposta alle minacce, disponibili come servizio completamente gestito
- Collaborazione con un team di esperti disponibile 24h su 24 e 7gg su 7, in grado di intraprendere azioni remote per contenere e neutralizzare le minacce
- Siete voi a decidere e a controllare le azioni che deve intraprendere il team MTR, e come devono essere gestiti gli incidenti
- Le più accreditate tecnologie di Machine Learning, unite all'esperienza di un team di esperti altamente qualificati
- Due livelli di servizio (Standard e Advanced), che garantiscono un set completo di opzioni per le organizzazioni di qualsiasi grado di espansione

Segnalare le minacce non è una soluzione: è solo l'inizio

Sono poche le organizzazioni che dispongono di strumenti, personale e processi interni adeguati per gestire con efficienza il proprio programma di sicurezza 24h su 24 e per proteggere attivamente i sistemi contro malware e minacce emergenti. Andando ben oltre la semplice notifica di attacchi o comportamenti sospetti, il team Sophos MTR intraprende azioni mirate per conto degli utenti, in modo da neutralizzare persino le minacce più sofisticate e complesse.

Con Sophos MTR, la vostra organizzazione può contare sul nostro team di threat hunter ed esperti che opera nell'ambito di risposta alle minacce, disponibile 24h su 24 e 7gg su 7, che:

- Intercetta e conferma proattivamente la presenza di potenziali minacce e incidenti
- Utilizza tutte le informazioni disponibili per determinare il raggio di azione e la gravità delle minacce
- Applica il giusto contesto imprenditoriale per le minacce individuate
- Avvia azioni volte a fermare, contenere e neutralizzare le minacce in remoto
- Offre consigli pratici per risolvere alla radice il problema degli incidenti ricorrenti

Risposta umana ottimizzata con sistemi automatici

Strutturata sulla base della nostra Intercept X Advanced with EDR, Sophos MTR unisce le tecnologie di Machine Learning alle analisi effettuate dagli esperti Sophos, per migliorare l'intercettazione e il rilevamento delle minacce, per indagare con maggiore profondità sugli alert e per intraprendere azioni mirate, volte a eliminare le minacce con la massima rapidità e precisione. Questa combinazione tra la pluripremiata protezione Sophos per endpoint con funzionalità intelligenti di EDR e un team di esperti di sicurezza di primissima categoria crea un sistema che ci piace definire "risposta umana ottimizzata con sistemi automatici".

Completa trasparenza e pieno controllo

Con Sophos MTR, siete voi a mantenere pieno controllo su tutte le decisioni, su come e quando effettuare l'escalation dei potenziali incidenti, nonché su quali azioni di risposta desiderate da noi (sempre che vogliate intraprenderne una) e sulle persone da includere nelle comunicazioni. Sophos MTR prevede tre modalità di risposta selezionabili, per cui potete scegliere il modo in cui desiderate che agisca il nostro Team MTR per garantire una collaborazione ottimale durante gli incidenti di sicurezza:

Notifica: invieremo notifica del rilevamento, fornendo dettagli utili a scopo di strutturazione delle priorità e della risposta.
Collabora: per rispondere al rilevamento, collaboreremo con il team interno o con il/i punto/i di contatto esterno/i.
Autorizza: saremo noi a effettuare la gestione di tutte le azioni di contenimento e neutralizzazione, fornendo informazioni su eventuali azioni intraprese.

Livelli di servizio di Sophos MTR

Sophos MTR prevede due livelli di servizio (Standard e Advanced), che offrono un set completo di funzionalità per le organizzazioni di qualsiasi dimensione e grado di espansione. Indipendentemente dal livello di servizio selezionato, le organizzazioni possono usufruire di tutte e tre le modalità di risposta (Notifica, Collabora o Autorizza) per far fronte alle proprie esigenze individuali.

Sophos MTR: Standard

Threat hunting basata su indizi, operativa 24h su 24

Elementi o attività identificate come dannosi (indicatori importanti) vengono automaticamente bloccati o terminati, facendo risparmiare tempo prezioso ai threat hunter, che possono ora dedicarsi all'individuazione delle minacce seguendo gli indizi raccolti. Questo tipo di intercettazione delle minacce prevede l'aggregazione di eventi causali e adiacenti (indicatori minori), per rilevare nuovi indicatori di attacco (IoA) e indicatori di compromissione (IoC), che precedentemente erano impossibili da rilevare.

Controllo dello stato di integrità della sicurezza

Ottimizzazione della performance di Intercept X, a partire da Intercept X Advanced with EDR, grazie alle analisi proattive delle condizioni operative e ai consigli sull'ottimizzazione della configurazione.

Report sulle attività

I riepiloghi delle attività dei casi rilevati consentono al personale di comunicare e di attribuire la giusta priorità agli eventi, per cui il vostro team saprà esattamente quali sono le minacce individuate e quali azioni di risposta sono state intraprese in ciascun periodo del report.

Rilevamento degli active adversary

Gli attacchi che vanno a segno si basano sull'esecuzione di un processo che può assumere un aspetto legittimo per gli strumenti di monitoraggio. Grazie all'utilizzo di tecniche di indagine sviluppate internamente, il nostro team determina la differenza tra i comportamenti legittimi e le tattiche, tecniche e procedure (TTP) utilizzate dagli autori degli attacchi.

Sophos MTR: Advanced *Include tutte le funzionalità del servizio Standard, con in più:*

Threat hunting senza l'utilizzo di indizi, operativa 24h su 24

Utilizzando data science, dati di intelligence sulle minacce e il fenomenale intuito di espertissimi threat hunter, raccogliamo e confrontiamo tutte le informazioni relative al profilo della vostra azienda, alle risorse principali e agli utenti ad alto rischio, per anticipare i comportamenti degli autori degli attacchi e intercettare nuovi indicatori di attacco (Indicators of Attack, IoA).

Telemetria ottimizzata

Le indagini sulle minacce vengono arricchite dai dati di telemetria provenienti dagli altri prodotti Sophos Central, che vanno oltre la semplice analisi degli endpoint per fornire un quadro completo delle attività degli antagonisti.

Miglioramento proattivo della condizione generale del sistema

Miglioramento proattivo della condizione di sicurezza generale del sistema con potenziamento della protezione, grazie a indicazioni prescrittive volte a risolvere le vulnerabilità nelle configurazioni e nelle architetture, che possono diminuire le capacità complessive di sicurezza.

Contatto dedicato per la risposta alle minacce

All'identificazione di un incidente, viene fornito un contatto dedicato che gestirà la risposta alle minacce, che collaborerà direttamente con le vostre risorse on-premise (un team interno o un partner esterno), fino alla neutralizzazione completa della minaccia.

Supporto diretto e dedicato

Il vostro team può usufruire di accesso diretto e dedicato ai nostri Security Operations Center (SOC). Il nostro Team MTR Operations è disponibile 24h su 24 e può contare sull'assistenza di team di supporto situati in 26 località in tutto il mondo.

Individuazione delle risorse

Da informazioni sulle risorse che includono versioni del sistema operativo, applicazioni e vulnerabilità, fino all'identificazione delle risorse gestite e di quelle non gestite, offriamo importanti analisi approfondite, che sono disponibili per valutare l'impatto di un incidente, per svolgere azioni di threat hunting e per fornire consigli su come migliorare proattivamente lo stato generale del sistema.

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

17/09/2019 DSIT (GH)