Sophos Managed Detection and Response

Un sistema di risposta alle minacce gestito da esperti

Sophos Managed Detection and Response (MDR) offre un servizio completamente gestito con ricerca, rilevamento e risposta alle minacce, disponibile 24/7 e gestito direttamente dal nostro team di esperti.

Segnalare le minacce non è la soluzione, è solo l'inizio

La maggior parte delle organizzazioni non ha a disposizione gli strumenti, il personale e i processi interni necessari per proteggersi dalle minacce informatiche e gestire il proprio programma di cybersecurity in maniera autonoma. Sophos MDR offre rilevamento e risposta alle minacce 24/7. Lavoriamo instancabilmente e ininterrottamente per neutralizzare anche le minacce più sofisticate.

Sophos MDR è un servizio fornito da esperti di threat hunting e risposta alle minacce che:

- Intercettano e confermano proattivamente la presenza di potenziali minacce e incidenti.
- Utilizzano tutte le informazioni disponibili per determinare il raggio di azione e la gravità delle minacce.
- Forniscono approfondimenti sul contesto e il potenziale impatto di una minaccia.
- Intraprendono azioni volte a fermare, contenere e neutralizzare le minacce da remoto.
- Offrono consulenza su come risolvere alla radice il problema degli incidenti ricorrenti.

Risposta umana ottimizzata con sistemi automatici

Strutturato sulle solide basi di Sophos XDR, Sophos MDR abbina alle tecnologie di machine learning le analisi effettuate dagli esperti Sophos, per migliorare l'intercettazione e il rilevamento delle minacce, per indagare con maggiore profondità sugli avvisi e per intraprendere azioni mirate, volte a eliminare i pericoli con la massima rapidità e precisione. Questa combinazione tra la pluripremiata protezione Sophos per endpoint con funzionalità intelligenti di XDR 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 MDR, sei tu a controllare come e quando modificare la gravità dei potenziali incidenti, quale tipo di risposta intraprendere e chi includere nelle comunicazioni. Sophos MDR prevede tre modalità di risposta, per garantirti tutta la flessibilità di cui hai bisogno per scegliere come collaborare con il team MDR durante gli incidenti, in base alle tue esigenze specifiche.

Notifica: quando viene rilevato un potenziale incidente, te lo segnaliamo, fornendoti tutti i dettagli e aiutandoti ad attribuire la giusta priorità e decidere come rispondere.

Collabora: collaboriamo con il tuo team interno o i tuoi contatti esterni per concordare le azioni di risposta.

Autorizza: isoliamo e neutralizziamo l'incidente, comunicandoti le azioni che abbiamo intrapreso.

Funzionalità principali

- Funzionalità avanzate di threat hunting, rilevamento e risposta alle minacce, disponibili come servizio completamente gestito
- Team di risposta operativo 24/7, che isola e neutralizza le minacce da remoto
- Sei tu a controllare le azioni che deve intraprendere il team MDR per conto tuo 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

SOPHOS

Livelli di servizio di Sophos MDR

Sophos MDR 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. Le organizzazioni possono scegliere una qualsiasi delle modalità di risposta (Notifica, Collabora, Autorizza), indipendentemente dal livello di servizio.

Sophos MDR: Standard

Threat hunting basata su indizi, operativa 24h su 24

Elementi o attività identificati come dannosi (segnali forti) vengono automaticamente bloccati o terminati. Questo permette ai threat hunter di risparmiare tempo prezioso e di dedicarsi all'individuazione delle minacce basata su indizi (segnali deboli), per scoprire nuovi indicatori di attacco (IoA) e indicatori di compromissione (IoC).

Controllo dello stato di integrità della sicurezza

Le nostre analisi proattive ti aiutano ad avere sempre informazioni aggiornate sulle tue condizioni operative e sulle tue configurazioni. Inoltre, offriamo raccomandazioni su come assicurarti che Sophos XDR e altri prodotti Sophos Central siano sempre ottimizzati per offrire i massimi livelli di performance.

Report sulle attività

Offriamo un riepilogo delle attività dei casi, per farti sapere quali minacce sono state individuate e quali azioni di risposta sono state intraprese nei vari periodi di reporting.

Rilevamento degli active adversary

Sfruttiamo tecniche di indagine avanzate per distinguere i comportamenti legittimi e identificare le tattiche, tecniche e procedure (TTP) utilizzate dai cybercriminali.

Sophos MDR: 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 e dati di intelligence sulle minacce, anticipiamo gli attacchi informatici e identifichiamo eventuali IoA.

Telemetria ottimizzata

Ai risultati delle nostre indagini sulle minacce aggiungiamo i dati di telemetria dei prodotti Sophos Central: in questo modo ci spingiamo oltre i singoli endpoint, per offrirti un quadro completo del tuo profilo di sicurezza.

Miglioramento proattivo della condizione generale del sistema

Forniamo una consulenza di tipo prescrittivo per aiutarti a ottimizzare il tuo profilo di sicurezza.

Contatto dedicato per la risposta alle minacce

Ti assegniamo un contatto dedicato per la risposta alle minacce, che collaborerà con il tuo team interno e partner esterni non appena viene identificato un incidente. Sarà a tua disposizione fino alla risoluzione dell'incidente.

Supporto diretto e dedicato

Il tuo team può usufruire di accesso diretto e dedicato al nostro Security Operations Center (SOC). Il nostro team MDR Operations è disponibile 24/7, grazie a team di supporto situati in 26 località in tutto il mondo.

Individuazione delle risorse

Offriamo analisi approfondite sulle tue risorse gestite e non gestite, indicando come proteggerle.

Pacchetto Onboarding Plus per i clienti MDR

Il nostro prodotto Onboarding Plus è un servizio di onboarding da remoto per i clienti che hanno acquistato Sophos MDR. Il servizio include un contatto dedicato all'interno dei Sophos Professional Services, che fornirà assistenza per onboarding, pianificazione, distribuzione e formazione. Inoltre, svolgerà una verifica dello stato di integrità per aiutarti a sfruttare il pieno potenziale delle nostre raccomandazioni sulle best practice di settore. Onboarding Plus include:

Giorno 1 - Pianificazione ed esecuzione dell'implementazione:

- Avvio del progetto.
- Configurazione di Sophos Central.
- Verifica delle funzionalità di Sophos Central.
- Strutturazione e test del processo di implementazione.
- Implementazione di Sophos Central nell'intera organizzazione.

Giorno 30 - Formazione su XDR

- Imparare a pensare e agire come un Security Operations Center (SOC).
- Individuazione proattiva di IoC.
- Compilazione di query per indagini future.

Giorno 90 - Formazione su XDR

- Verifica dei criteri di sicurezza attuali, con eventuale aggiornamento secondo necessità.
- Valutazione di quali funzionalità possono (eventualmente) incrementare il tuo livello di protezione informatica.
- Ottenimento di documentazione scritta, contenente raccomandazioni compilate in base ai risultati della verifica dello stato di integrità.

Per eventuali domande, ti invitiamo a contattare il nostro team dei Sophos Professional Services.

America: ProfessionalServices@sophos.com

Asia-Pacifico/Giappone: ProfessionalServicesAU@Sophos.com.au

Europa: ProfessionalServicesEmea@Sophos.com

Per scoprire di più, visita

sophos.it/mdr

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

22-08-01 DS-IT (DD)

SOPHOS