Sophos MDR Per Microsoft Defender

Un sistema di Threat Detection and Response gestito da esperti, compatibile con gli ambienti Microsoft

Sophos Managed Detection and Response (MDR) per Microsoft Defender moltiplica il potenziale del tuo team, grazie all'intervento di esperti che monitorano, indagano e rispondono agli avvisi di sicurezza Microsoft a ogni ora del giorno e della notte.

Ottieni Il Massimo Ritorno Sul Tuo Investimento In Microsoft Security

Molte organizzazioni hanno investito nella suite Microsoft Security, ma potrebbero non avere abbastanza personale interno per essere in grado di sfruttare il pieno potenziale dello stack di tecnologie multiprodotto di Microsoft, che permettono di rilevare, svolgere indagini e rispondere a centinaia di avvisi di sicurezza al giorno:

- La scarsità di professionisti della cybersecurity a livello globale ha raggiunto i 3,4 milioni[1].
- Il 71% dei team di sicurezza si trova in difficoltà quando deve stabilire quali avvisi di sicurezza meritano un'indagine, vista l'enorme quantità di dati non pertinenti generati dai loro strumenti[2].
- Il tempo mediano di risposta alle minacce per le organizzazioni dotate di un team di Security Operation interno è pari a 16 ore, il che significa che gli hacker hanno a disposizione un periodo di tempo esteso per muoversi e agire all'interno della rete[3].

Sophos MDR per Microsoft Defender offre le più potenti opzioni di rilevamento, individuazione proattiva e risposta alle minacce attualmente disponibili per gli ambienti Microsoft. I nostri analisti monitorano, svolgono indagini e rispondono agli avvisi di sicurezza Microsoft a ogni ora del giorno e della notte, svolgendo azioni di risposta immediate e coordinate da menti umane per bloccare le minacce confermate. Il nostro servizio offre il più rapido tempo medio di risposta alle minacce: 38 minuti, ovvero il 96% in meno rispetto al benchmark di settore.

Rilevamento E Blocco Delle Minacce Che Sfuggono A Microsoft Defender

Con Sophos MDR per Microsoft Defender, i nostri esperti di Microsoft Security rilevano, svolgono indagini e rispondono alle minacce utilizzando i dati di sicurezza ottenuti dai seguenti prodotti Microsoft:

- Microsoft Defender for Endpoint
- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- Centro Sicurezza e Conformità di O365
- Microsoft Sentinel
- Office 365 Management Activity

Inoltre, i nostri rilevamenti proprietari, uniti ai dati di intelligence sulle minacce e al threat hunting con supervisione umana, aggiungono ulteriori livelli di protezione, identificando e bloccando più minacce rispetto a quelle individuate dall'uso dei soli strumenti di Microsoft Security.

Le organizzazioni possono integrare anche strumenti di sicurezza e origini di telemetria non-Microsoft come le soluzioni Sophos e decine di altri vendor quali Palo Alto Networks, Fortinet, Check Point, AWS, Google, Okta, Darktrace e molti altri. Il risultato è una visibilità completa, con altissimi livelli di protezione.

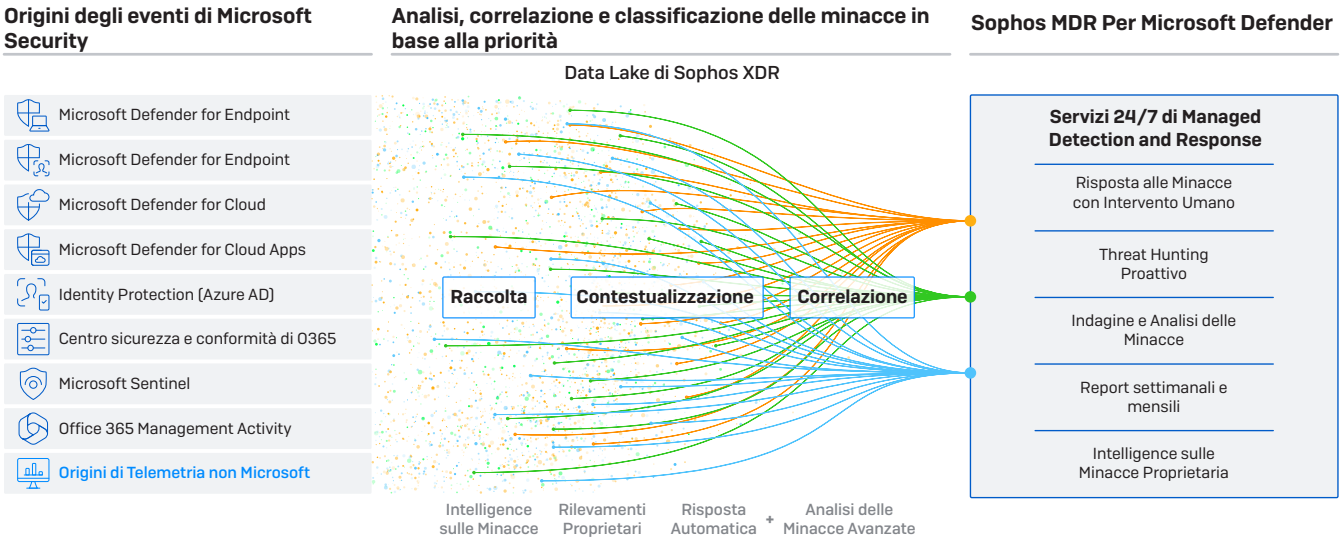
Caratteristiche Principali

- Gli analisti del team Sophos MDR monitorano, svolgono indagini e rispondono agli avvisi di Microsoft Security a ogni ora del giorno e della notte, intraprendendo azioni correttive immediate per bloccare le minacce confermate come tali
- Le capacità del servizio si estendono oltre i rilevamenti di Microsoft Defender for Endpoint e Microsoft Sentinel, garantendo protezione per l'intera piattaforma Microsoft Security
- Quando viene identificata una minaccia attiva, il team di Sophos MDR è in grado di intraprendere un'ampia selezione di azioni di risposta alle minacce per conto tuo
- Rilevamenti proprietari di Sophos, più dati di intelligence sulle minacce, threat hunting con supervisione umana e livelli aggiuntivi di protezione
- Integrazione di strumenti e origini di telemetria non Microsoft per bloccare gli attacchi che colpiscono rete, utenti e clienti

1 2022 Cybersecurity Workforce Study, (ISC)2
2 Il Panorama Della Cybersecurity 2023: L'Impatto Commerciale Degli Avversari Informatici, Sophos
3 Database Gartner Cybersecurity Business Value Benchmark, 2022

SOPHOS

Sophos MDR Per Microsoft Defender: Le Capacità Principali Del Servizio



Monitoraggio delle minacce 24/7

I nostri esperti di Microsoft Security rilevano e bloccano le minacce prima che possano compromettere i tuoi dati e causare l'interruzione dei servizi. Grazie al supporto di sei Security Operations Center (SOC) internazionali, Sophos garantisce monitoraggio e sicurezza a ogni ora del giorno e della notte.

Risposta alle minacce con intervento umano

Il team Sophos MDR può intraprendere un'ampia gamma di azioni di risposta alle minacce per conto tuo, per interrompere l'attacco, isolare il problema e rimuovere gli hacker dai tuoi sistemi. Le azioni di risposta alle minacce possono includere:

- Isolamento di host che utilizzano Sophos Central
- Applicazione di blocchi degli IP tramite firewall basato su host
- Termine dei processi
- Disconnessione forzata delle sessioni utente
- Disattivazione di account utente specifici
- Rimozione di artefatti dannosi
- Aggiunta di hash indicatori di pericolo agli elementi bloccati in Sophos Central

Per maggiori informazioni, visita:

sophos.com/microsoft-defender

Threat hunting proattivo con supervisione umana

Affidando l'individuazione proattiva delle minacce ai nostri analisti altamente qualificati, è possibile intercettare ed eliminare rapidamente le violazioni, identificando i comportamenti dei cybercriminali che sono sfuggiti agli strumenti in uso.

Compatibilità con strumenti di sicurezza non Microsoft

Sophos MDR può integrarsi agli strumenti e alle origini di telemetria non Microsoft per rilevare e bloccare gli attacchi nell'intero ambiente.

Report settimanali e mensili

Avvisi in tempo reale, con opzioni di reportistica e gestione, sono subito disponibili in Sophos Central; ci sono anche report settimanali e mensili, che offrono approfondimenti sulle indagini di sicurezza, sulle minacce informatiche e sul profilo di integrità della tua organizzazione.

Briefing mensile di intelligence sulle minacce

Tenuto dal team Sophos MDR, "Sophos MDR ThreatCast" è un webinar mensile che offre approfondimenti sulle nuove minacce e sulle più recenti best practice di sicurezza.

Rilevamenti Proprietari

I rilevamenti proprietari, le analisi delle minacce avanzate, nonché i dati di intelligence di primissima categoria che sono integrati nella piattaforma Sophos aggiungono ulteriori livelli di protezione, identificando più minacce rispetto a quelle individuate dall'uso dei soli strumenti di Microsoft Security.

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

23-07-10 DS-IT (DD)

SOPHOS