SOPHOS

Guida all'acquisto di servizi MDR - Managed Detection and Response

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. Ne consegue una crescita del numero di organizzazioni che scelgono di affidarsi ai servizi MDR - Managed Detection and Response ovvero a servizi di rilevamento e risposta gestiti per il proprio programma di gestione operativa dei sistemi di IT security.

Secondo Gartner[1], entro il 2025, il 50% delle organizzazioni utilizzerà servizi MDR (una percentuale in aumento, rispetto a meno del 5% nel 2019).

Tuttavia, per molti il mercato dei servizi di sicurezza è un ambiente relativamente nuovo, nel quale abbondano false dichiarazioni e termini tecnici che non fanno altro che aumentare la confusione. È sempre più difficile prendere una decisione informata per la propria organizzazione. Questa guida si propone di offrire maggiore chiarezza sulla questione, analizzando le considerazioni principali che occorre tenere presente quando si sceglie un servizio MDR. Inoltre, fornisce un confronto delle prestazioni dei vari vendor di servizi MDR, per aiutare i responsabili tecnici a prendere una decisione informata.

La gestione operativa dei sistemi di IT security richiede le competenze dei professionisti

Nel settore della cybersecurity esiste un'enorme lacuna in termini di talento ed esperienza. Di conseguenza, le organizzazioni fanno fatica a implementare programmi di gestione operativa dei sistemi di IT security (SecOps) efficaci per rilevare, condurre indagini e rispondere alle minacce prima che si verifichino dei danni.

Sebbene esistano strumenti, come l'EDR, progettati per individuare proattivamente le minacce e rispondere agli incidenti, occorrono pur sempre operatori dotati di competenze tecniche specifiche per sfruttare il pieno potenziale di queste funzionalità. Da un sondaggio del 2019 che ha coinvolto 2.300 professionisti nell'ambito dell'IT e della sicurezza[2], è emerso che il 54% dei partecipanti sostiene di non essere "in grado di sfruttare il pieno potenziale della propria soluzione EDR" per via della mancanza di personale esperto.

Il problema è talmente diffuso tra le organizzazioni che, secondo le ricerche svolte dagli analisti dell'azienda ESG[3], "il 34% sostiene che la sfida principale è la mancanza di risorse umane dotate delle giuste competenze e in grado di analizzare un incidente di cybersecurity che colpisce un endpoint, per determinarne la causa originaria e identificare la catena di attacco".

Le minacce di sicurezza continuano a crescere sia in volume che in complessità. Come possono le organizzazioni tener testa a questo fenomeno senza dover ampliare il proprio team di gestione operativa dei sistemi di IT security? Questo dilemma ha dato origine a una nuova alternativa: i servizi di sicurezza gestiti. Nello specifico, i servizi di rilevamento e risposta gestiti (MDR - Managed Detection and Response).

Definizione dei servizi di rilevamento e risposta gestiti (MDR - Managed Detection and Response)

I servizi di rilevamento e risposta gestiti (MDR - Managed Detection and Response) sono servizi di gestione operativa dei sistemi di sicurezza affidati a un team esterno di specialisti. I servizi MDR svolgono per i clienti la funzione di un'estensione del loro team di sicurezza, in quanto offrono la combinazione ottimale tra servizi quali indagini supervisionate da esseri umani, threat hunting, monitoraggio in tempo reale, risposta agli incidenti e uno stack di tecnologie progettate per raccogliere e analizzare dati di intelligence.

Spesso per identificare e neutralizzare le minacce, i fornitori di servizi MDR sfruttano una combinazione tra tecnologie basate su host e livelli di rete, oltre ad analisi avanzate, intelligence sulle minacce, dati approfonditi e competenze tecniche umane. L'obiettivo dell'MDR è individuare e rispondere alle minacce che sono riuscite a eludere i controlli di sicurezza preventivi, infiltrandosi negli ambienti dei clienti. Questi controlli preventivi (ad es. firewall, antivirus e content filtering) sono metodi efficaci per bloccare le più comuni minacce note, ma potrebbero non essere in grado di difendere i sistemi in caso di cyberattacchi più recenti e sofisticati. Per colmare le lacune di questi strumenti, è sorta la figura professionale dei fornitori di servizi MDR.

I motivi per cui le organizzazioni scelgono un servizio MDR

Alcuni dei principali motivi che spingono le organizzazioni a utilizzare un servizio MDR includono:

- **Mancanza di risorse interne adeguate per la gestione operativa dei sistemi di sicurezza:** molte organizzazioni fanno fatica a implementare una strategia di sicurezza che vada oltre la prevenzione e non hanno le risorse necessarie per gestire un programma interno di security operations.
- **Difficoltà a sfruttare il pieno potenziale degli strumenti EDR:** alcune organizzazioni acquistano soluzioni EDR per utilizzarle come tecnologie reattive in caso di incidenti o con la speranza di poterle utilizzare proattivamente per le attività di threat hunting e risposta alle minacce. Tuttavia non sono in grado di implementare un adeguato programma interno di gestione operativa dei sistemi di sicurezza e devono affidarsi a esperti esterni.

- **Potenziamento delle capacità di un team di security operations già esistente:** anche le organizzazioni dotate di un team interno di analisti di sicurezza presentano lacune in termini di copertura (ovvero notti, fine settimana e periodi di ferie) e specializzazioni (ovvero analisti esperti di malware e specialisti in ambito di risposta agli incidenti). Analogamente, alcuni team di sicurezza hanno bisogno del supporto aggiuntivo di un Security Operations Center (SOC) esterno, per potersi dedicare a operazioni di IT e sicurezza più generiche che altrimenti non riuscirebbero a seguire in maniera adeguata.
- **Desiderio di garantire ai membri del proprio team tutte le risorse di cui hanno bisogno:** anche i Security Operations Center ben rodati spesso hanno bisogno di una mano in più per monitorare gli ambienti e accertarsi che non sfugga alcuna minaccia.

I vantaggi dei servizi MDR

Un team di esperti disponibile 24/7, 365 giorni l'anno

I servizi MDR devono anche poter contare su personale dotato di competenze tecniche specifiche, per rilevare e rispondere a qualsiasi tipo di attacco. Vengono gestiti da professionisti che per un'azienda sono solitamente molto difficili da trovare, che occorre formare e a cui bisogna fornire incentivi sufficienti affinché rimangano alle dipendenze dell'organizzazione; inoltre, i servizi MDR che includono un numero adeguato di esperti garantiscono una copertura ininterrotta. Tutto questo significa poter contare su servizi che monitorano costantemente gli ambienti e hanno la capacità di rispondere a ogni potenziale minaccia in qualsiasi momento, inclusi fine settimana, periodi di ferie e persino orari notturni. È come avere a disposizione un team esteso di gestione operativa dei sistemi di sicurezza che non va mai in vacanza, non si ammala e non dorme mai.

I servizi favoriscono la crescita

La maggior parte delle organizzazioni fa fatica a svolgere le proprie attività di threat hunting, risposta agli incidenti e verifica dello stato di integrità della sicurezza. Affidando le operazioni di rilevamento e risposta a personale esterno, i servizi di sicurezza permettono ai membri del team di focalizzare la propria attenzione sulle attività idonee alle proprie competenze. Per le organizzazioni più avanzate, l'aggiunta di MDR consente anche ai team di attribuire la giusta priorità agli eventi più salienti, liberandosi allo stesso tempo di gran parte del peso delle operazioni di sicurezza quotidiane.

Risparmi sui costi

Le organizzazioni che desiderano strutturare il proprio programma di gestione operativa dei sistemi di sicurezza capiscono rapidamente la difficoltà e i costi effettivi richiesti per avviare un Security Operations Center (SOC) interno. Anche le organizzazioni di medie dimensioni avrebbero bisogno di almeno quattro analisti per garantire una copertura 24/7, 365 giorni l'anno. Le organizzazioni più grandi avrebbero bisogno di stipendiare un gran numero di dipendenti specializzati, che solitamente hanno salari molto elevati. Le organizzazioni devono anche tenere presente i costi necessari per permettere ai responsabili dei team e ai tecnici di personalizzare e gestire gli strumenti del team. E questi sono solo i costi legati al processo di assunzione dei membri del team. Il budget deve anche includere tutti gli strumenti necessari, come ad es. sistemi di protezione endpoint, protezione della rete, rilevamento e risposta alle minacce endpoint (EDR - Endpoint Detection and Response), SIEM, elaborazione dei flussi di lavoro (SOAR), feed con dati di intelligence e altro.

Tranquillità

Con un adeguato servizio MDR, sia voi che la vostra organizzazione potete fare sonni tranquilli, nella certezza di poter contare su un team di esperti altamente qualificati che monitora ininterrottamente la vostra azienda, individuando proattivamente le minacce, indagando sulle attività sospette e rispondendo ai potenziali incidenti. Con un panorama delle minacce di cybersecurity in costante evoluzione, tutto questo garantisce la tranquillità di un team interamente focalizzato sulla cybersecurity.

Valutazione dei fornitori di servizi MDR: le principali domande da porre

Criteri generali

Quanti sono i clienti del servizio MDR?

La caratteristica che contraddistingue i fornitori di servizi MDR è l'esperienza che hanno maturato nel rilevare e rispondere agli incidenti. Il numero attuale dei clienti permette di avere un'idea di quante siano le altre organizzazioni che considerano attendibile un fornitore e aiuta a valutarne la preparazione e la capacità di rispondere a una vasta gamma di attività sospette. Occorre inoltre assicurarsi che il fornitore abbia esperienza con organizzazioni con un profilo simile (dimensioni, mercato verticale, sfide di sicurezza) a quello della propria azienda.

Qual è l'ambito operativo del servizio? Include la risposta alle minacce?

Non tutti i servizi MDR sono progettati allo stesso modo. Uno dei principali requisiti che i clienti devono esigere dai servizi MDR (nonché una caratteristica che pochissimi vendor sono in grado di offrire) è la capacità di intraprendere azioni mirate per neutralizzare le minacce per conto dei clienti, a differenza del limitarsi semplicemente a segnalare minacce potenziali o imminenti. Nonostante la "R" di MDR, la maggior parte dei vendor si concentra principalmente o esclusivamente sull'identificazione e sulla segnalazione delle minacce, lasciando al cliente il compito di gestire l'intera strategia di risposta e correzione. Per essere efficaci, i servizi MDR hanno bisogno di analisti in grado di condurre indagini sistematiche per determinare la validità e l'ambito di azione delle potenziali minacce, nonché limitare il numero di falsi positivi, neutralizzare le minacce confermate come tali e fornire maggiore contesto e consigli pratici per migliorare lo stato complessivo di sicurezza dell'organizzazione.

Il servizio è operativo 24/7, 365 giorni l'anno? Se si dovesse verificare un problema di domenica alle 2 del mattino, chi avvierebbe la risposta?

Assicuratevi che il servizio MDR sia effettivamente in grado di monitorare l'ambiente e di implementare una risposta a qualsiasi ora del giorno o della notte.

Quali tecnologie utilizza il servizio? Sono incluse nel prezzo?

Quando si valuta un servizio MDR, è importante capire se le tecnologie utilizzate dagli operatori sono incluse nel costo del servizio. Alcuni richiedono l'acquisto a parte di altri strumenti (come ad es. soluzioni di protezione endpoint ed EDR). Altri offrono l'intero stack di tecnologie come componente dei servizi.

Il servizio fornito è proattivo o reattivo?

L'MDR è per natura una disciplina proattiva. A differenza dei servizi di indagine digitale e risposta agli incidenti con pagamento anticipato, tipicamente offerti per aiutare i clienti a risolvere una crisi già in atto (quale un incidente o una violazione di sicurezza), MDR offre un servizio proattivo e disponibile 24 h su 24, in grado di monitorare gli ambienti dei clienti per rilevare attività di potenziali antagonisti e, man mano che emergono minacce, di offrire consulenza, assistere o neutralizzare le minacce in tempo reale.

Come si interagisce con il team MDR?

È importante capire il processo utilizzato per comunicare con il fornitore del servizio. È presente un supporto telefonico diretto? È possibile comunicare tramite e-mail? È possibile parlare direttamente con gli analisti del SOC, oppure la comunicazione viene gestita da un intermediario (ad es. un Customer Success Manager)? In alcuni casi la differenza tra i fornitori di servizi MDR può essere estrema: alcuni permettono di parlare con una persona, altri utilizzano solamente un portale per le comunicazioni. Indipendentemente dalla modalità di comunicazione, i fornitori di MDR devono sempre includere un riepilogo delle attività del caso, per fare in modo che il vostro team conosca esattamente le minacce rilevate e quali sono le azioni successive da intraprendere.

Metodologia e criteri di efficacia

Qual è la metodologia di rilevamento e risposta alle minacce (Threat Detection and Response, TDR) delle security operations?

È importante che i fornitori di servizi MDR si basino su una metodologia di TDR ben definita. In caso contrario, è molto probabile che faranno fatica a ridimensionare i servizi in base alla crescita del business e ci sarà una maggiore probabilità che il rilevamento non riesca a intercettare importanti indicatori di attività sospetta.

Quanto è rapido il servizio?

Nella sicurezza, ogni secondo è importante. I fornitori di servizi MDR devono essere in grado di offrire una stima delle seguenti tempistiche:

- Tempo medio di rilevamento
- Tempo medio di risposta
- Tempo medio di risoluzione

Quali tipi di azioni correttive sono in grado di intraprendere gli operatori dei servizi MDR? Possono intraprendere una risposta attiva per conto vostro?

I fornitori di servizi MDR devono essere in grado di descrivere cosa succede quando il servizio rileva attività sospette. Come specificato in precedenza, molti si limitano semplicemente a monitorare i sistemi e a segnalare che si è verificato un evento sospetto. L'operatore del servizio MDR deve essere in grado di intraprendere un'azione per conto vostro, tramite la risposta proattiva di una persona umana e non di un semplice strumento automatizzato per il blocco delle minacce.

Il threat hunting include l'utilizzo di indizi (per rispondere agli avvisi), agisce senza indizi (per cercare nuovi indicatori di attacco, senza un avviso) o prevede entrambi i casi?

Non tutti i sistemi di threat hunting sono equivalenti. Sebbene il threat hunting sia per definizione un'attività svolta da un essere umano, ci sono vendor che definiscono come threat hunting la semplice generazione automatica di avvisi (mentre si tratta di tutt'altro). È anche importante capire se gli operatori del servizio MDR interverranno in maniera proattiva per individuare gli antagonisti che si celano all'interno dell'ambiente, indipendentemente dal fatto che siano stati o meno rilevati forti indicatori di attività o di compromissione. Si consiglia di chiedere quali sono i tipi di attività che attivano un'indagine sulle minacce.

Quali fonti di dati vengono utilizzate per fornire visibilità? Il servizio è semplicemente un "EDR gestito"?

Sebbene alcuni dati provenienti dagli endpoint siano indispensabili per un programma di security operations, alcuni fornitori di servizi MDR non dispongono di una visibilità che va oltre i singoli endpoint. Questi non sono veri e propri fornitori di servizi MDR e sarebbe meglio classificarli come vendor di soluzioni "EDR gestite", con livelli limitati di visibilità sulle minacce che potrebbero infiltrarsi negli ambienti.

Il fornitore di servizi MDR può contare sulla disponibilità di dati di intelligence sulle minacce e ricercatori esperti in materia di minacce?

I fornitori di MDR devono poter contare su competenze superiori rispetto a quelle comunemente disponibili nelle organizzazioni. Queste competenze devono naturalmente includere quelle di analisti esperti di sicurezza. Tuttavia, il fornitore deve anche avere a disposizione un database interno di dati di intelligence sulle minacce e collaborare con ricercatori in tema di minacce ogni volta che ne rileva una nuova.

I vendor a confronto

I fornitori di servizi di rilevamento e risposta gestiti (Managed Detection and Response, MDR) rientrano solitamente in tre categorie:

- **Solo monitoraggio:** focalizzazione sull'assegnazione di priorità e sulla segnalazione ai clienti quando il prodotto genera un avviso automatico. Questi vendor non offrono opzioni di correzione oltre a semplici consigli sull'azione che il cliente dovrebbe intraprendere. Inoltre, utilizzano solamente un threat hunting "automatizzato", senza alcuna indagine o individuazione proattiva delle minacce per conto del cliente.
- **Una risposta limitata (con la "r" minuscola):** sono incluse azioni di risposta minori, ma sono limitate a processi automatici. Il threat hunting viene svolto, ma solamente quando un avviso attiva l'indagine.
- **Una Risposta completa (con la "R" maiuscola)**: sono incluse capacità di risposta complete. Questi vendor intraprendono le azioni necessarie per conto del cliente, grazie a una risposta manuale e implementata da un essere umano. Il threat hunting non è solamente basato sull'utilizzo di indizi, ma è anche gestito dal team MDR, che svolge controlli frequenti, alla ricerca proattiva delle minacce anche quando potrebbero non esserci indicatori di attacco visibili.

Caratteristiche principali	Solo monitoraggio	Una risposta limitata (con la "r" minuscola)	Una Risposta completa (con la "R" maiuscola)
Monitoraggio 24/7	✓	✓	✓
Segnalazione e assegnazione di priorità	✓	✓	✓
Consigli per la correzione	✓	✓	✓
Report sulle attività	✓	✓	✓
Threat hunting "automatico"	✓	✓	✓
Risposta automatica		✓	✓
Threat hunting con l'utilizzo di indizi		✓	✓
Threat hunting senza indizi			✓
Risposta gestita da un essere umano			✓

Selezione rappresentativa di vendor[4]		
Solo monitoraggio	Una risposta limitata (con la "r" minuscola)	Una Risposta completa (con la "R" maiuscola)
Carbon Black Managed Detection	Arctic Wolf	Sophos MTR Standard
CrowdStrike Falcon OverWatch	eSentire	Sophos MTR Advanced
Huntress	Expel	CrowdStrike Falcon Complete
Perch	Rapid7	
	Red Canary	
	SentinelOne Vigilance Respond	

Servizio Sophos Managed Threat Response (MTR)

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. 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.

Il team Sophos MTR, composto da esperti di threat hunting e risposta alle minacce:

- 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 confermate
- Avvia azioni volte a fermare, contenere e neutralizzare le minacce in remoto
- Offre consigli pratici per risolvere alla radice il problema degli incidenti ricorrenti

Principali funzionalità di Sophos MTR

Sophos MTR: Standard

Threat hunting con 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 gestiti 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

La maggior parte degli attacchi di successo si basano sull'esecuzione di un processo che, agli strumenti di monitoraggio, può sembrare legittimo. 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: opzioni avanzate

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 per 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 MTR Operations Team 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.

Sophos Managed Threat Response (MTR): protezione, EDR e MDR			
Caratteristiche principali	Sophos Intercept X Advanced with EDR (solo tecnologie)	Sophos MTR Standard (tecnologie + servizio gestito)	Sophos MTR Standard (tecnologie + servizio gestito)
Protezione Endpoint	✓	✓	✓
Endpoint Detection and Response (EDR) per le IT operations	✓	✓	✓
Endpoint Detection and Response (EDR) per il threat hunting	✓	✓	✓
Servizio gestito: Rilevamento e risposta 24x7		✓	✓
Servizio gestito: Risposta proattiva e manuale		✓	✓
Servizio gestito: Threat hunting con l'utilizzo di indizi		✓	✓
Servizio gestito: Threat hunting senza indizi			✓
Servizio gestito: Contatto dedicato per la risposta			✓

Principali fattori di differenziazione di Sophos MTR

Sophos intraprende l'azione giusta per conto vostro: a differenza di Sophos MTR, gli altri servizi si limitano a monitorare e segnalare la presenza di un'attività sospetta rilevata. Il team Sophos MTR entra in azione: avviamo operazioni da remoto per interrompere, contenere e neutralizzare anche le minacce più sofisticate.

Un team selezionato di esperti: con oltre 2.000 clienti, Sophos ha visto e bloccato di tutto. Il nostro team altamente qualificato di threat hunter, tecnici specializzati ed ethical hacker vi protegge 24/7, indagando sui comportamenti anomali e intraprendendo le giuste azioni contro le minacce.

Threat hunting altamente efficace: Sophos svolge attività di individuazione delle minacce sia con che senza indizi, al fine di scoprire nuovi indicatori di attacco (IoA) e indicatori di compromissione (IoC) che precedentemente erano impossibili da rilevare.

Rilevamento ad alta affidabilità: superando i limiti dei tradizionali sistemi di rilevamento, Sophos offre una combinazione tra modelli deterministici e modelli di Machine Learning, per individuare i comportamenti sospetti e le tattiche, le tecniche e le procedure utilizzate dagli antagonisti tecnologicamente più evoluti.

Risposta focalizzata fornita da personale specializzato: il servizio Sophos MTR include Intercept X Advanced with EDR, la migliore protezione endpoint disponibile in assoluto. Agisce bloccando automaticamente le minacce che sfuggono agli altri sistemi. Poiché il servizio include una prevenzione proattiva e potenziata, il team può focalizzarsi sul rilevamento, sulla risposta e sull'implementazione di azioni per gli incidenti più gravi.

Trasparenza e controllo: con Sophos 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. Le organizzazioni possono usufruire di tre modalità di risposta (Notifica, Collabora o Autorizza) per far fronte alle proprie esigenze individuali.

Outcome-Focused Security™: ogni azione di individuazione, indagine e risposta genera dati che influiscono sul processo decisionale, in quanto permettono di ottimizzare le configurazioni e le opzioni di rilevamento automatico.

Principali statistiche di Sophos MTR

Servizio Sophos Rapid Response

Sophos Rapid Response offre un'assistenza tempestiva, fornita da un team di esperti che opera nell'ambito della risposta agli incidenti, in grado di identificare e neutralizzare le minacce attive presenti nella rete di un'organizzazione. Il servizio Rapid Response è progettato per aiutare le organizzazioni che si trovano sotto attacco. I clienti Sophos MTR non hanno bisogno di implementare il servizio Rapid Response, in quanto la risposta agli incidenti è inclusa nel servizio Sophos MTR.

Il servizio Rapid Response offre azione immediata per intervenire sugli incidenti attivi. L'attivazione richiede poche ore e nella maggior parte dei casi le priorità vengono gestite entro 48 ore.

Sophos Rapid Response è composto da un team disponibile 24/7 che agisce da remoto e include esperti in materia di risposta agli incidenti, threat hunting e analisi delle minacce in grado di:

- Intervenire rapidamente per classificare, contenere e neutralizzare le minacce attive
- Espellere gli intrusi dalla vostra struttura informatica, per impedire che rechino ulteriori danni alle risorse
- Monitorare costantemente e rispondere agli incidenti 24/7 per potenziare la protezione
- Consigliare azioni preventive in tempo reale per risolvere la causa originaria del problema
- Fornire dopo la risoluzione dell'incidente un riepilogo dettagliato della minaccia, che descrive le indagini svolte

Il servizio Sophos Rapid Response è disponibile sia per i clienti Sophos che per sistemi che non includono soluzioni Sophos.

Per maggiori informazioni sul servizio Sophos Managed Threat Response (MTR), visitate il nostro sito web oppure rivolgetevi a un referente commerciale Sophos.

Se preferite svolgere attività di threat hunting in maniera indipendente, Sophos EDR offre tutti gli strumenti necessari per implementare una strategia avanzata di threat hunting e protezione dell'integrità delle IT security operations. Cominciate oggi stesso una prova gratuita di 30 giorni senza obbligo di acquisto.

Fonte:

1 Gartner, Market Guide for Managed Detection and Response Services, 26 agosto 2020, analisti: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

2 Sondaggio del 2019 condotto tra 3.100 responsabili IT https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

3 https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

4 Questo documento informativo e di confronto si basa sull'interpretazione di Sophos di dati pubblicamente disponibili al momento della compilazione del presente confronto. Questo documento è stato preparato da Sophos e non dagli altri vendor indicati nello stesso. Le funzionalità e le caratteristiche dei prodotti messi a confronto, che potrebbero influire direttamente sull'accuratezza e/o sulla validità del confronto stesso, sono soggette a cambiamenti. Le informazioni contenute in questo confronto hanno lo scopo di aiutare a capire e conoscere a grandi linee le informazioni effettive dei vari prodotti, e potrebbero non essere complete. Chiunque consulti questo documento deve assumersi la responsabilità delle proprie decisioni in base ai propri requisiti; inoltre, per la selezione di un prodotto, si consiglia di controllare anche le fonti originali delle informazioni, piuttosto che affidarsi solamente a questo confronto.

Per saperne di più su
Sophos Managed Threat Response (MTR)

visitate sophos.it/mtr

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

2021-02-25 BG-IT (PC)

SOPHOS