SOPHOS
Cybersecurity delivered.

Cinque Ottimi Motivi Per Utilizzare I Servizi MDR

Whitepaper Sophos. Settembre 2022

Introduzione

Le minacce informatiche continuano ad aumentare in termini di volume, complessità e impatto. In risposta a questo fenomeno, le organizzazioni scelgono sempre più frequentemente di affidarsi a servizi MDR (Managed Detection and Response) per rilevare e neutralizzare gli attacchi più sofisticati e impossibili da bloccare solo con l'uso delle tecnologie. Gartner prevede infatti che, entro il 2025, il 50% delle aziende utilizzerà servizi MDR per il monitoraggio, il rilevamento e la risposta alle minacce[1].

Tuttavia, la proliferazione delle soluzioni di protezione disponibili sul mercato può confondere, rendendo difficile una definizione specifica di cosa sia l'MDR, di dove si collochi all'interno dell'ecosistema di cybersecurity e di quali vantaggi comporti. La nostra guida ha una risposta a tutte queste domande e offre consigli pratici sugli aspetti da considerare durante la scelta di un servizio MDR.

Sophos MDR

Sophos MDR è il servizio MDR più comunemente adottato a livello globale: protegge infatti oltre 11.000[2] organizzazioni dalle minacce avanzate (incluso il ransomware). Con il punteggio più alto secondo Gartner Peer Insights™[3] e il riconoscimento "Top Vendor" della G2 Grid® del 2022 nella categoria dei servizi MDR per le medie imprese[4], Sophos MDR è un ottimo sistema di protezione e le tue difese informatiche sono in buone mani.

Definire L'MDR

Per comprendere i vantaggi dell'MDR e i fattori alla base dell'incremento della richiesta dei servizi MDR, è importante capire che cos'è e riconoscere che cosa non è l'MDR.

Managed Detection and Response (MDR) è un servizio operativo 24/7 e completamente gestito, a cura di esperti specializzati nel rilevamento e nella risposta agli attacchi informatici, che previene incidenti che sarebbero impossibili da fermare con l'uso delle sole tecnologie.

MDR non va confuso con EDR (Endpoint Detection and Response) e XDR (Extended Detection and Response). Anche se sia MDR che EDR e XDR supportano e offrono opzioni di threat hunting, EDR e XDR sono strumenti che permettono agli analisti di indagare e individuare proattivamente i potenziali tentativi di compromissione dei sistemi; con MDR, sono gli analisti di un vendor di cybersecurity di fiducia a intercettare, svolgere indagini e neutralizzare le minacce per conto tuo.

Come suggerisce il nome stesso, gli strumenti EDR recuperano informazioni da tecnologie di protezione endpoint, mentre gli strumenti XDR estendono le risorse da cui attingono i dati, in modo da includere altri ambiti dello stack informatico (inclusi firewall e soluzioni per e-mail, cloud e protezione per i dispositivi mobili). Il risultato è una visibilità e superiore, con indagini più dettagliate e approfondite. Per fornire il servizio MDR, Sophos utilizza le nostre soluzioni EDR e XDR leader di mercato.

Quello che l'MDR non offre sono le attività di gestione quotidiana della cybersecurity, come l'implementazione delle tecnologie di sicurezza, l'aggiornamento dei criteri, l'applicazione di patch e l'installazione degli aggiornamenti. Per ricevere supporto in questi ambiti, le organizzazioni si possono rivolgere a dei Managed Service Provider (MSP), che offrono servizi di gestione della sicurezza IT.

Chi Utilizza I Servizi MDR

I servizi MDR vengono utilizzati da tutti i tipi di organizzazioni, in qualsiasi settore: da aziende di piccole dimensioni con risorse IT limitate, fino a grandi imprese con un SOC interno. La vera domanda è: come vengono utilizzati i servizi MDR dalle organizzazioni? MDR prevede tre principali modelli di risposta:

- Il team MDR gestisce ogni aspetto della risposta alle minacce per conto del cliente
- Il team MDR collabora con il team interno del cliente, con una gestione collaborativa della risposta alle minacce
- Il team MDR informa il team interno del cliente, fornendo consigli per la correzione del problema

Sophos offre tutti e tre gli approcci, che vengono adattati e personalizzati a seconda delle esigenze individuali del cliente.

1 Gartner Market Guide for MDR 2021
2 Dati aggiornati al mese di agosto 2022.
3 Recensioni negli ultimi 12 mesi, dati aggiornati al 1° agosto 2022. I contenuti di Gartner Peer Insights sono una raccolta delle opinioni di utenti finali individuali, basate sulle relative esperienze con i vendor indicati nella piattaforma; non devono essere interpretate come affermazioni di fatto, né come rappresentazione delle opinioni di Gartner o dei suoi affiliati. Gartner non appoggia alcun fornitore, produttore o servizio citato nei suoi contenuti, né fornisce alcuna garanzia, espressa o implicita, in riferimento a tali contenuti, alla loro accuratezza o completezza, inclusa qualsivoglia garanzia sulla commerciabilità o sull'idoneità a un particolare scopo.
4 Sophos è stata valutata come Top Vendor della G2 Grid® del 2022, nella categoria Servizi MDR per le medie imprese.

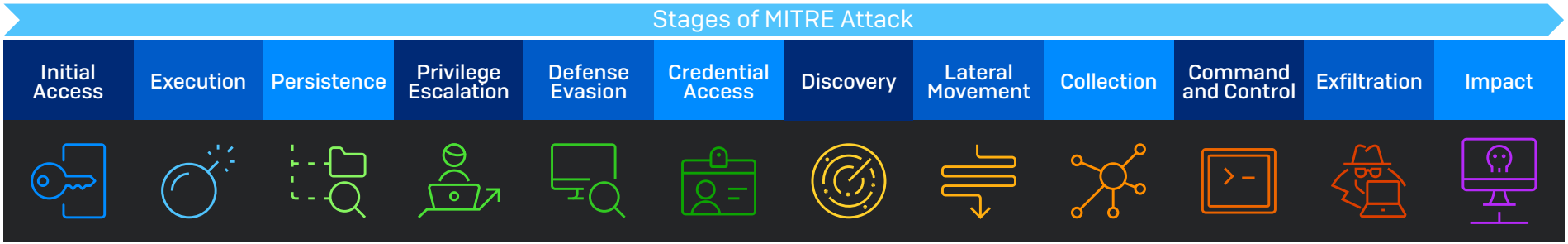
L'Esigenza Di Un Servizio Di Rilevamento E Risposta Alle Minacce Coordinato Da Menti Umane

Di fatto, da sole le tecnologie non sono in grado di prevenire tutti gli attacchi informatici. Molti cybercriminali riescono infatti a eludere le soluzioni di sicurezza e conducono attacchi sfruttando vari strumenti IT legittimi, credenziali e autorizzazioni di accesso rubate, nonché vulnerabilità per le quali non sono state applicate le giuste patch. Emulando gli utenti autorizzati e approfittando delle debolezze nei sistemi di difesa delle organizzazioni, gli hacker possono evitare di farsi notare dalle tecnologie di rilevamento automatico.

L'immagine riportata sotto descrive i principali "artefatti" (strumenti) utilizzati dai cybercriminali in tutte le fasi della catena di MITRE ATT&CK, secondo i casi osservati nel 2021 dagli esperti di threat hunting Sophos che operano in prima linea. Come si può osservare, gli strumenti adoperati più frequentemente dai team IT (come PowerShell, PsExec e RDP) sono anche quelli maggiormente sfruttati dai cybercriminali. Le tecnologie automatizzate fanno fatica a distinguere tra l'uso legittimo di queste risorse da parte di personale IT autorizzato, e quello da parte di hacker che si nascondono dietro a credenziali rubate.

Per bloccare questi attacchi avanzati di tipo "Living-Off-the-Land", serve una combinazione tra tecnologie all'avanguardia e competenze umane. Ogni volta che un hacker svolge un'azione, genera un segnale. Se alle tecnologie avanzate di protezione e ai modelli di machine learning basati sull'intelligenza artificiale vengono unite le competenze umane di personale specializzato, è possibile permettere agli analisti di sicurezza di rilevare, svolgere indagini e neutralizzare attacchi di ogni tipo, anche quelli più avanzati e coordinati in tempo reale dagli hacker, al fine di prevenire i casi di violazione dei dati.

Sebbene threat hunting, indagini e risposta possano essere svolti internamente con strumenti EDR e XDR, l'uso di MDR come servizio completamente gestito o in collaborazione con il tuo team interno presenta numerosi vantaggi.



Principali artefatti utilizzati in tutte le fasi della catena di attacco secondo Mitre. Active Adversary Playbook 2022, Sophos

Le Tecnologie Di Protezione Continuano A Svolgere Un Ruolo Importante Nei Moderni Sistemi Di Difesa

Sebbene i servizi di rilevamento e risposta gestiti e coordinati da menti umane rappresentino un livello essenziale nelle difese informatiche, l'uso di tecnologie di protezione di alta qualità rimane fondamentale. Le soluzioni di sicurezza per endpoint, rete, e-mail e cloud continuano a svolgere un ruolo essenziale nei moderni sistemi di difesa. Le giuste soluzioni possono infatti amplificare l'efficacia e l'impatto di un servizio MDR:

- Le tecnologie di protezione automatizzate permettono ai responsabili di sicurezza di tenersi sempre un passo avanti rispetto a un volume di attacchi in costante crescita; questo è particolarmente importante, soprattutto visto il fatto che gli hacker stanno sempre più frequentemente ricorrendo ad automazione, intelligenza artificiale e prodotti malware-as-a-service per diffondere le proprie minacce. Sophos Endpoint Protection blocca automaticamente il 99,98% delle minacce, prima che possano avere ripercussioni negative su un'organizzazione.
- Una delle principali sfide pratiche per i threat hunter sono i dati non pertinenti: ricevono infatti un elevato volume di segnali e questo potrebbe impedire loro di distinguere tra informazioni utili e dati non essenziali. Con l'uso di tecnologie di protezione di ottima qualità, è possibile ridurre il numero di avvisi sui quali gli analisti umani devono indagare. Permettendo ai threat hunter di focalizzarsi su un numero ridotto di rilevamenti più precisi, le tecnologie di prevenzione di alta qualità velocizzano la risposta alle minacce coordinata da una mente umana.
- Gli analisti possono servirsi dei rilevamenti e dei segnali messi in evidenza dalle tecnologie di prevenzione per identificare e indagare sulle attività sospette. Incrementando la qualità dei rilevamenti e la pertinenza delle informazioni contestuali, sia le indagini che la risposta diventano così più rapide ed efficaci.

Tenendo presente tutti questi fattori, proseguiamo ora con i cinque principali vantaggi offerti dai servizi MDR, secondo le organizzazioni che li utilizzano.

1. Eleva Le Difese Informatiche

Uno dei principali vantaggi dell'affidarsi a un fornitore di servizi MDR, rispetto a programmi SecOps che contano solo su risorse interne, è l'elevato livello di protezione dal ransomware e da altre minacce informatiche avanzate.

Con MDR puoi avvalerti delle competenze vaste e approfondite degli analisti del tuo vendor. Rispetto a una singola organizzazione, i fornitori di servizi MDR hanno un'esperienza molto più estesa in termini di volume e varietà degli attacchi e per questo motivo offrono competenze molto difficili da riprodurre internamente.

Inoltre, i team MDR indagano sulle minacce e intraprendono azioni di risposta ogni giorno, per cui hanno maggiore dimestichezza con gli strumenti di threat hunting. Di conseguenza, sono anche in grado di avviare un'azione di risposta con maggiore rapidità e precisione in qualsiasi fase dell'attacco, dall'identificazione dei segnali pertinenti, alle indagini sui potenziali incidenti per neutralizzare le attività dannose.

Inoltre, lavorare a contatto con altri professionisti permette agli analisti di condividere conoscenze ed esperienze, velocizzando ulteriormente la risposta alle minacce. Il team Sophos MDR raccoglie e mette a confronto i runbook di ciascuna minaccia o hacker individuato. Questo significa che quando durante un'indagine viene identificato un cybercriminale, invece di dover svolgere ricerche approfondite ed estese al momento dell'attacco, il nostro team può consultare il runbook ed entrare subito in azione.

I runbook vengono aggiornati continuamente e a ogni incarico gli analisti registrano qualsiasi informazione pertinente, come:

- TTP (tattiche, tecniche e procedure) comuni o caratteristiche di un attacco o hacker specifico.
- Indicatori di compromissione (IoC) pertinenti.
- Esempi dimostrativi noti per exploit connessi a vulnerabilità aperte.
- Query di threat hunting utili per contrastare un attacco o un cybercriminale specifico.

Un ulteriore vantaggio dei servizi MDR è il fatto che possono raccogliere dati di intelligence su un caso e applicarli a potenziali vittime che presentano lo stesso profilo. Questo permette loro di prevenire proattivamente attacchi simili nella stessa comunità. Alcuni esempi di scenari in cui il team Sophos MDR indaga proattivamente sugli ambienti dei clienti includono:

- Quando i clienti in un mercato verticale specifico subiscono un particolare tipo di attacco.
- Quando i team Sophos X-Ops forniscono dati di intelligence su un certo tipo di attacco che prende di mira settori oppure organizzazioni con un profilo ben definito.
- Quando si verifica un evento significativo nel panorama della sicurezza informatica e occorre stabilire se abbia avuto ripercussioni sui clienti.

Se i nostri analisti rilevano segnali sospetti, sono in grado di svolgere rapidamente indagini e correggere i problemi, creando immunità nella comunità del gruppo preso di mira.

L'esperienza estesa e approfondita maturata dai nostri esperti, unita alla loro capacità di applicare le proprie conoscenze agli ambienti dei clienti, permette al team Sophos MDR di elevare le difese delle organizzazioni, portandole ben oltre i limiti di ciò che avrebbero potuto fare da sole.

"I vantaggi di Sophos MDR sono tangibili e includono una diminuzione del 90% del tempo necessario per individuare minacce ad alto rischio su cui occorre svolgere indagini; abbiamo anche osservato una riduzione del 95% del tempo richiesto per identificare l'origine dell'attacco e i tipi di minacce, nonché una maggiore precisione nei rilevamenti."
Chitale Dairy, India

"I penetration tester sono rimasti sorpresi di non trovare una via di accesso: è questo che ci ha convinti che potevamo riporre completa fiducia nel servizio Sophos."
University of South Queensland, Australia

"Con Sophos MDR, abbiamo abbreviato drasticamente i nostri tempi di risposta."
Tata BlueScope Steel, India

"Riceviamo notifiche in tempo reale per qualsiasi tipo di minaccia."
Bardiani Valvole, Italy

2. Libera Più Risorse IT

Il threat hunting richiede diverso tempo ed è imprevedibile. Per i professionisti dell'IT che devono gestire attività e priorità diverse, può essere difficile tenere il passo con questa sfida: il 79% dei team informatici ammette infatti di essere indietro nella verifica dei log per l'identificazione di segnali o attività sospetti[5].

Considerando il potenziale impatto di un attacco sulle organizzazioni, non appena viene rilevato un elemento sospetto il personale tecnico deve interrompere qualsiasi altra attività e dedicarsi completamente all'indagine e all'intervento sulla minaccia. La natura urgente del lavoro stesso può impedire a questi team di focalizzarsi su sfide più strategiche e spesso più interessanti.

Collaborando con un servizio MDR, puoi liberare più risorse per il tuo team IT, in modo che possa concentrarsi su iniziative dal maggiore impatto commerciale. Le organizzazioni che utilizzano Sophos MDR affermano regolarmente che il nostro servizio implica per loro notevoli vantaggi in termini di efficienza del reparto informatico, e questo a sua volta comporta una maggiore capacità di raggiungere gli obiettivi aziendali.

"Da quando abbiamo implementato Sophos, siamo riusciti a liberare ore di lavoro preziose per i nostri team, che a loro volta si sono così potuti focalizzare su iniziative volte a incrementare il tasso di soddisfazione dei nostri studenti."
London South Bank University, Regno Unito

"Sophos MDR è in grado di correggere i problemi o rimuovere le minacce rapidamente, segnalandoci la loro presenza. Questa capacità ci permette di dedicare un maggior numero di risorse ad attività più critiche."
Tomago Aluminium, Australia

"Potendo contare su Sophos MDR, siamo riusciti a valorizzare e sviluppare altri ambiti della nostra organizzazione, come la gestione delle vulnerabilità, l'applicazione delle patch e la sensibilizzazione in materia di sicurezza."
The Fresh Market, U.S.A.

"Sophos anticipa le strategie dei più recenti tipi di attività e minacce, per permetterci di focalizzarci sul garantire un servizio sicuro e di primissima classe sia per i clienti che per gli artisti."
CD Baby, U.S.A.

5 Sondaggio indipendente condotto tra 5.600 professionisti IT a gennaio-febbraio 2022. Condotto per conto di Sophos da Vanson Bourne.

3. Completa Tranquillità, 24/7

I cybercriminali si trovano in ogni parte del mondo, e il rischio di attacco è sempre imminente. Gli hacker sono più attivi nei momenti in cui c'è maggiore probabilità che il personale tecnico non sia operativo, ad esempio di sera, nel fine settimana e nei giorni festivi. Il rilevamento e la risposta alle minacce sono pertanto attività per cui non è possibile prendere pause: se vengono svolti solo in orario ufficio, l'organizzazione rimane esposta ai rischi.

Grazie alla continuità che offrono 24/7, i servizi MDR garantiscono massima tranquillità e sicurezza. Questo per i membri del personale IT significa, letteralmente, poter fare sonni tranquilli; possono infatti riconquistarsi il proprio tempo libero, nella consapevolezza che la responsabilità viene assunta dal fornitore del servizio MDR.

Per i dirigenti senior e i clienti, la protezione 24/7 a cura di esperti e l'elevato livello di preparazione informatica in qualsiasi momento è garanzia di sicurezza per i propri dati e per l'intera organizzazione.

"Poter contare sul team Sophos MDR mi aiuta a dormire sonni tranquilli, perché so che siamo protetti 24/7."
Vancouver Canucks, Canada

"Il team Sophos svolge un ruolo simile al portiere di una squadra di calcio: le elevate competenze tecniche sempre a nostra disposizione ci garantiscono piena tranquillità, intercettando qualsiasi cosa ci sfugga."
Inspire Education Group, Regno Unito

"Ora sappiamo di poter contare su una configurazione di sicurezza molto più affidabile, efficace e completa."
Aligned Automation, India

"Con Sophos MDR abbiamo aumentato la resilienza della nostra organizzazione."
McKenzie Aged Care Group, Australia

4. L'importanza di aggiungere competenze, non personale

Il threat hunting è un'operazione estremamente complessa. Chi lavora in questo ambito deve avere una serie di competenze tecniche estremamente specializzate; tipicamente, le caratteristiche di un threat hunter includono:

- **Creatività e curiosità**: l'individuazione proattiva delle minacce può essere un po' come cercare un ago in un pagliaio e i threat hunter spesso passano giorni e giorni a cercare le minacce, utilizzando vari metodi per scovarle.
- **Esperienza nell'ambito della cybersecurity**: il threat hunting è una delle operazioni di cybersecurity più avanzate, per cui un'esperienza approfondita sul campo è fondamentale.
- **Conoscenza del panorama delle minacce**: avere una buona comprensione delle nuove tendenze in tema di minacce è un must quando si devono cercare e neutralizzare elementi sconosciuti.
- **Buona intuizione delle intenzioni dei cybercriminali**: la capacità di pensare come un hacker è fondamentale quando si contrastano attacchi coordinati da menti umane.
- **Ottime abilità di scrittura tecnica**: come parte del processo di indagine, i threat hunter devono registrare i risultati delle loro ricerche. Pertanto, la capacità di comunicare informazioni complesse è indispensabile per il successo delle attività di threat hunting.
- **Conoscenza dei sistemi operativi e della rete**: è fondamentale avere conoscenze pratiche avanzate per entrambi.
- **Esperienza di programmazione/scripting**: è richiesta per aiutare i threat hunter a compilare programmi, automatizzare le operazioni, esaminare i log e analizzare i dati necessari per svolgere le indagini.

Questo elenco rappresenta una combinazione più unica che rara di competenze, e il problema viene accentuato da un'evidente carenza di personale specializzato nel settore dell'IT: questi fattori rendono la ricerca di esperti di threat hunting un'operazione difficilissima, se non del tutto impossibile, per molte organizzazioni.

I servizi MDR mettono a tua disposizione queste competenze. Sophos vanta centinaia di analisti esperti, che forniscono ininterrottamente servizi MDR ai nostri clienti in tutto il mondo. Sophos MDR permette ai clienti di ampliare le proprie capacità SecOps, senza dover assumere altro personale.

"Ora possiamo contare su una vera e propria estensione del nostro reparto di sicurezza, senza dover incrementare le risorse umane interne."
Hammondcare, Australia

"Sophos MDR ci ha aiutato a contrastare minacce informatiche sempre più prolifiche e sofisticate, senza dover ampliare il nostro team SecOps."
Tourism Finance Corporation of India Limited, India

"Sophos ci ha risparmiato il costo di cinque nuovi membri del personale per svolgere queste mansioni."
AG Barr, Regno Unito

5. Ottimizza Il Tuo Ritorno Sull'Investimento Nella Cybersecurity

Un team di threat hunting operativo 24/7 può essere costoso da gestire. Per garantire una protezione ininterrotta, occorrono come minimo cinque o sei dipendenti dedicati alla cybersecurity che lavorano a turni alterni.Sfruttando le economie di scala, i servizi MDR offrono un modo pratico ed economico per difendere la tua organizzazione e ottimizzare l'uso del tuo budget di sicurezza.

Inoltre, i servizi MDR elevano il livello di protezione, riducendo così il rischio delle conseguenze finanziarie di un caso di violazione ed evitandoti i costi implicati da un eventuale incidente grave. Considerando che il costo medio di riparazione dei danni di un attacco di ransomware per le organizzazioni di medie dimensioni è stato 1,4 milioni di $ nel 2021[6], investire nella prevenzione è una decisione molto saggia dal punto di vista finanziario.

Se il tuo vendor di servizi MDR offre anche soluzioni di cybersecurity per endpoint (e magari anche altro), affidandoti a un unico fornitore potrai anche usufruire di notevoli vantaggi in termini di costo totale di proprietà, semplificando allo stesso tempo anche le operazioni di gestione.

Infine, scegliendo un vendor con prodotti e servizi in grado di integrarsi con le tecnologie di sicurezza che già usi, puoi incrementare il ritorno sull'investimento delle soluzioni esistenti. Sophos adotta un approccio all'MDR agnostico rispetto ai vendor, che ti permette di sfruttare i prodotti già implementati nei tuoi sistemi per svolgere attività di rilevamento, indagine e risposta: potrai così sfruttare al massimo i tuoi investimenti attuali. Con Sophos MDR puoi utilizzare sia i nostri strumenti di fama internazionale che strumenti non Sophos. In alternativa, puoi anche optare per una combinazione delle due opzioni.

"Per un costo inferiore a quello di un singolo membro del personale, Sophos offre una copertura equivalente a sei dipendenti che lavorano a tempo pieno."
Detmold Group, Australia

"Riunire tutti i nostri prodotti di sicurezza in un unico ecosistema ci ha permesso di risparmiare e di incrementare la nostra efficienza."
Independent Parliamentary Standards Authority, Regno Unito

"Il valore di Sophos MDR supera nettamente il suo prezzo. Anche se dovesse bloccare un solo incidente all'anno, varrebbe già 10 volte tanto, se non di più."
Hammondcare, Australia

"Abbiamo risparmiato 15 ore alla settimana, con una produttività 2,6 volte superiore."
Tourism Finance Corporation of India Limited, India

6 La Vera Storia Del Ransomware 2022, Sophos. Un sondaggio indipendente condotto tra 5.600 professionisti dell'IT in 31 paesi

I Fattori Da Considerare Per La Scelta Di Un Servizio MDR

I servizi MDR variano a seconda del fornitore. Per sceglierne uno valido, occorre valutare diversi fattori; ti consigliamo quindi di tenere in considerazione i quattro ambiti riportati di seguito.

1. **Livelli di supporto e interazione offerti**

   Per la risposta alle minacce, cerchi un vendor di MDR che la gestisca completamente per conto tuo, che la co-gestisca insieme al tuo team, oppure che si limiti a segnalare la presenza del pericolo ai tuoi responsabili interni, in modo che possano coordinare una risposta autonoma? Identifica il livello di supporto e interazione che preferisci e metti a confronto i vari vendor.

   Sophos agisce come un'estensione del team IT, nel modo specificato dal cliente. Che tu cerchi supporto completamente gestito e operativo 24/7, oppure solo assistenza marginale per i tuoi team interni, ti veniamo incontro per soddisfare i tuoi requisiti specifici.

2. **Profondità Ed Estensione Dell'Esperienza Sulle Minacce**

   A un'esperienza più estesa e approfondita nella risposta alle minacce informatiche corrisponde una maggiore efficacia per la strategia di difesa. Occorre capire i livelli di competenza degli analisti del servizio MDR di un vendor, e quale strategia viene adottata per applicare negli ambienti dei clienti i dati raccolti collettivamente.

   Ti consigliamo inoltre di scoprire quanta esperienza in materia di sicurezza abbia maturato il team di un vendor di MDR, nonché di appurare la qualità delle informazioni contestuali fornite per aiutare gli analisti ad attribuire la giusta priorità alle minacce e svolgere indagini.

   Sophos MDR protegge oltre 11.000 organizzazioni in tutto il mondo, che operano in settori quali sanità, istruzione, industria manifatturiera, retail, tecnologie, finanza, pubblica amministrazione, servizi e molto di più. La nostra esperienza estesa e approfondita ci permette di garantire ai nostri clienti una protezione imbattibile.

   Sophos MDR può inoltre contare sul sostegno del team Sophos X-Ops. Con oltre 30 anni di esperienza sul malware e con capacità di intelligenza artificiale leader a livello mondiale, Sophos X-Ops offre analisi dettagliate e approfondimenti utili per aiutare i tecnici di MDR a identificare e neutralizzare rapidamente gli attacchi.

3. **Esperienza quotidiana di assistenza clienti**

   Un vendor di MDR degno di questo nome diventa una vera e propria estensione del tuo team: assicurati che sia un vendor con cui sia facile collaborare una volta firmato il contratto. Consulta i clienti che si avvalgono dei suoi servizi per capirne l'esperienza e leggi recensioni indipendenti per scoprire il loro feedback.

   Sophos MDR è il vendor di MDR con il maggior numero di recensioni e con le valutazioni più alte su Gartner Peer Insights (dati aggiornati al 1º agosto 2022), con un punteggio medio di 4,8/5*. Leggi qui le testimonianze indipendenti dei clienti.

4. **Estensione e profondità della telemetria**

   I cybercriminali non si limitano a seguire un unico modello tecnologico, per cui la strategia di threat hunting del tuo vendor non deve essere da meno. Con maggiore visibilità sull'intero ambiente, gli analisti avranno più probabilità di rilevare e rispondere tempestivamente alle attività pericolose. Chiedi ai vendor quali integrazioni di sicurezza offrono e qual è il loro livello di integrazione dei vari segnali raccolti nel tuo ambiente IT.

   Sophos MDR include moltissime integrazioni con terze parti a tutti i livelli dello stack informatico, comprese integrazioni native e di terze parti con tecnologie per endpoint, rete, cloud, e-mail e Microsoft 365. Il nostro approccio agnostico rispetto ai vendor consente agli analisti di avere massima visibilità sull'intero ambiente dei clienti, e questo potenzia le capacità di rilevamento, indagine e risposta.

Riepilogo

Con la costante evoluzione delle minacce informatiche, MDR sta diventando sempre di più un must nell'arsenale di protezione delle organizzazioni di tutte le dimensioni. Collaborare con un vendor di MDR dall'attendibilità e dall'efficacia comprovate offre diversi vantaggi, sia che tu desideri affidare l'intera gestione delle tue attività di threat hunting a un servizio esterno, o che preferisca semplicemente potenziare le tue risorse interne:

1. Eleva le difese informatiche.
2. Libera più risorse IT.
3. Offre completa tranquillità, 24/7.
4. Aggiunge competenze, non personale.
5. Ottimizza il tuo ritorno sull'investimento nella cybersecurity.

Per scoprire di più su Sophos MDR, parla con un Partner Sophos o visita www.sophos.it/mdr

www.sophos.it/mdr

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di Intelligenza Artificiale e Machine Learning.

2022-09-16 IT-WP (DD)

SOPHOS