PRESENTAZIONE ESG

Perché MDR è diventato parte integrante delle moderne strategie di sicurezza informatica

Data: agosto 2022 **Autore:** Dave Gruber, ESG Principal Analyst

ABSTRACT: nessuno mette in discussione l'importanza delle funzionalità di rilevamento e risposta in un programma di sicurezza informatica. Il problema principale è trovare il modo migliore per garantire rilevamento e risposta tempestivi, accurati, affidabili e coerenti quando le minacce si moltiplicano e diventano più complesse in tempi minori rispetto alla capacità di adattamento della maggior parte delle organizzazioni. Il servizio MDR gestito da una terza parte rappresenta un approccio che consente alle organizzazioni di restare al passo.

Introduzione: l'affermazione di MDR

Tutte le organizzazioni si trovano a dover affrontare una cruda realtà: le minacce alla sicurezza informatica sono in rapido aumento, le superfici di attacco si stanno espandendo e i processi e gli strumenti tradizionali per rilevarle e rispondervi non sono più sufficienti. Le minacce sono sempre più sofisticate e gli utenti malintenzionati sono sempre più abili, agili e persistenti e tutto questo concorre a creare un bersaglio digitale in movimento per i professionisti IT e della sicurezza incaricati di proteggere gli asset aziendali.

Una miriade di controlli di sicurezza aggiunge costi e complessità alle iniziative di rilevamento e risposta, richiedendo ai team di sicurezza di classificare manualmente un flusso costante di avvisi per separare le minacce reali dai falsi positivi. La creazione di un Security Operations Center (SOC) più grande con un numero maggiore di strumenti e di ingegneri della sicurezza è un'operazione costosa e presuppone che le organizzazioni siano in grado di identificare e assumere un numero sufficiente di professionisti della sicurezza per far fronte all'enorme e crescente divario di competenze nella sicurezza informatica.

Con la riorganizzazione dell'architettura dei programmi di sicurezza informatica, le organizzazioni si rivolgono più frequentemente a fornitori di servizi di rilevamento e risposta gestiti per ottenere aiuto.

Man mano che l'architettura dei programmi di sicurezza informatica viene riorganizzata, le organizzazioni si rivolgono con maggiore frequenza a fornitori di soluzioni di rilevamento e risposta gestiti per affinare i processi, colmare le lacune di risorse e competenze e modernizzare gli strumenti delle operazioni di sicurezza. Molte associano MDR alla sicurezza degli endpoint, in quanto la ricerca di ESG rivela che la necessità di un servizio MDR integrato è fattore chiave che spinge le organizzazioni a cambiare i propri vendor di soluzioni per la sicurezza degli endpoint (vedere la figura 1).[1]

[1] Fonte: risultati della survey completa ESG, *Endpoint Security Trends*, dicembre 2021. Tutti i grafici e i riferimenti alla ricerca ESG in questa presentazione sono stati estrapolati da questo insieme di risultati della survey.

Figura 1. Fattori che guidano il cambiamento dei vendor per la sicurezza degli endpoint

Se la sua organizzazione ha recentemente cambiato, ha un progetto attivo per il quale sta cambiando o prevede di cambiare vendor di soluzioni per la sicurezza degli endpoint, cosa ha determinato/sta determinando questo cambiamento? (Percentuale di intervistati, N = 300, più risposte accettate)

Fonte: ESG, una divisione di TechTarget, Inc.

Tuttavia, man mano che i team addetti alla sicurezza espandono i programmi di rilevamento e risposta, con l'upgrade a soluzioni di rilevamento e risposta estesi (XDR) più complete, le offerte MDR forniscono alle organizzazioni un percorso per aggiornare la tecnologia e i modelli operativi in grado di offrire una copertura della superficie di attacco e un rilevamento delle minacce avanzate più completi. Sono necessari nuovi approcci che uniscano monitoraggio 24 ore su 24, Threat Intelligence globale in tempo reale, automazione e analisi avanzata dell'apprendimento automatico che permettano di lavorare con enormi quantità di telemetria di sicurezza a supporto di rilevamento rapido e threat hunting. Sebbene le soluzioni XDR continuino a evolvere e a maturare, i servizi MDR possono consentire alle organizzazioni di tutte le dimensioni e livelli di maturità della sicurezza di rendere operativi il rilevamento e la risposta, garantendo la mitigazione delle minacce avanzate. Ciò è particolarmente importante in quanto le organizzazioni ridefiniscono l'ambito e la scala dei confini della sicurezza informatica dal data center all'edge fino al cloud. MDR riunisce le persone, i processi e le tecnologie necessari per estendere i casi d'uso di rilevamento delle minacce e risposta in tutta la Distributed Enterprise.

Fattori chiave per l'adozione di MDR

L'utilizzo dei servizi MDR è in aumento, offrendo ai team addetti alla sicurezza un percorso per estendere la copertura, colmare le lacune nel personale e rafforzare gli obiettivi complessivi del programma. I casi d'uso possono variare, ma i fattori alla base includono:

- Panorama delle minacce: gli attacchi informatici sempre più numerosi e sofisticati hanno messo a dura prova la capacità delle organizzazioni di rilevare e rispondere in modo più rapido e mirato.
- Intento degli avversari: gli avversari sono diventati più intelligenti, più persistenti e ancora più strategici nel modo in cui pianificano ed eseguono gli attacchi. È emerso un potente "ecosistema criminale" in cui gli utenti malintenzionati condividono tattiche e addirittura collaborano agli attacchi.
- Economia: l'impegno CapEx per la creazione e l'espansione di un SOC è rilevante, in genere una spesa a sei zeri e talvolta ancora di più.
- Refresh della tecnologia di sicurezza informatica: lo stack di controlli di sicurezza informatica deve essere aggiornato con maggiore frequenza per le organizzazioni che svolgono internamente tutte o la maggior parte delle attività delle operazioni di sicurezza. Queste includono il passaggio dal rilevamento e la risposta degli endpoint di prima generazione a un framework XDR/MDR più completo.
- Carenza di competenze: il tanto discusso divario di competenze in ambito di sicurezza informatica è un annoso problema. L'impossibilità di trovare le figure adeguate per coprire le posizioni interne correlate alla sicurezza informatica spesso comporta problemi in termini di rilevamento e risposta che mettono a rischio gli asset.

Gli attacchi informatici sono indiscriminati. Le organizzazioni di piccole e medie dimensioni, con personale e budget limitati e un'esposizione pregressa a tutti i tipi di attacchi sono a rischio. Anche le organizzazioni di dimensioni molto grandi necessitano di personale supplementare, controlli scalabili e consulenza a livello dirigenziale sulle strategie per rilevare e rispondere al panorama delle minacce in continua evoluzione.

Cosa cercare in un servizio MDR e in un fornitore di servizi MDR

Ci sono alcuni requisiti importanti e irrinunciabili per qualsiasi organizzazione che valuta un servizio MDR, tra cui:

- Threat Intelligence contestuale: abilitare il rilevamento e la Threat Intelligence in tempo reale, inclusa la correlazione di più indicatori per identificare le minacce o ignorare i falsi positivi.
- Casi d'uso proattivi: supportare la caccia attiva alle minacce note.
- Telemetria avanzata: condurre indagini forensi approfondite e analisi sofisticate, particolarmente importanti per identificare le minacce nuove ed emergenti.
- Correzione: offrire linee guida per la correzione specifiche per il contesto e basate sull'intelligenza artificiale.
- Riduzione dei rischi: valutazione e gestione delle vulnerabilità.

Quando si tratta di scegliere un fornitore di servizi MDR, le organizzazioni devono cercare partner in grado di offrire funzionalità specifiche e dimostrate, tra cui:

- Copertura 24/7: monitoraggio continuo 24 ore su 24, 7 giorni su 7.
- Pianificazione e consulenza per gli scenari di tipo "what-if".
- Competenza ed esperienza umane da parte del fornitore di servizi.
- Linee guida per dirigenti di alto livello e membri del consiglio di amministrazione.
- Capacità di garantire governance, conformità e continuità aziendale.

Inoltre, le organizzazioni dovrebbero chiedere ai potenziali partner MDR gli obiettivi dei livelli di servizio. Queste funzioni includono il tempo medio di reazione dall'avviso all'avvio dell'indagine, il tempo medio di risposta dall'avvio dell'indagine al momento in cui viene fornita all'organizzazione un'analisi dell'incidente e il tempo medio per la risoluzione dall'avvio dell'indagine al momento in cui avviene la risoluzione completa.

L'approccio Dell Technologies a MDR

Per identificare e valutare un fornitore di servizi MDR, nonché per avviare una partnership con esso, le organizzazioni devono concentrarsi non solo sulle loro attuali esigenze di rilevamento e risposta alle minacce, ma anche sul modo in cui tali esigenze potrebbero evolvere e aumentare in futuro. Sebbene possa essere difficile prevedere le esigenze future in tema di minacce alla sicurezza informatica, le organizzazioni devono cercare un partner MDR con una comprovata capacità di adattare il servizio nel tempo sulla base di tecnologie innovative, processi collaudati e competenze comprovate dei dipendenti.

L'approccio Dell Technologies al rilevamento e alla risposta gestiti combina tecnologia flessibile, intelligente e scalabile con professionisti esperti della sicurezza informatica. Il servizio basato su abbonamento è progettato per garantire alle organizzazioni prevedibilità dei costi e un passaggio senza problemi a un livello più elevato di servizio, se e quando necessario.

La piattaforma tecnologica per Dell Managed Detection and Response è Taegis XDR, un servizio completamente gestito nativo per il cloud sviluppato da Secureworks, una business unit Dell. Taegis XDR rileva, analizza e agisce su minacce completamente esaminate su una superficie di attacco distribuita e diversificata per contribuire a proteggere le organizzazioni, dalle multinazionali fino alle aziende relativamente piccole.

Taegis XDR è ulteriormente rafforzato dalle competenze dell'ampio gruppo di analisti della sicurezza e ingegneri Dell, la cui conoscenza collettiva si basa su decenni di competenza, contribuendo a proteggere le organizzazioni sia dalle minacce note che da altre minacce sconosciute. Questa combinazione offre un modo efficiente per unificare il rilevamento e la risposta nell'intera architettura IT, in gran parte attraverso il database di Threat Intelligence costantemente aggiornato. Dell Managed Detection and Response monitora, analizza e identifica inoltre il comportamento delle minacce per ridurre i tempi medi di rilevamento e risposta.

Dell Managed Detection and Response monitora, analizza e identifica inoltre il comportamento delle minacce per ridurre i tempi medi di rilevamento e risposta.

Infine, poiché si tratta di un servizio gestito, Dell Managed Detection and Response riduce drasticamente la necessità per le organizzazioni di ricercare e assumere professionisti della sicurezza per team IT e delle operazioni di sicurezza interni già oberati di lavoro. Dell Managed Detection and Response è progettato per integrare ed estendere le funzionalità delle organizzazioni in modo strategico, ma a costi contenuti.

Una verità più profonda

La superficie di attacco in rapida espansione, i ripetuti attacchi ransomware e un panorama di minacce generalmente più complesse sono alla base della crescita degli investimenti e dell'affermazione di XDR e MDR, ora che le organizzazioni modernizzano i programmi di rilevamento e risposta alle minacce. Anche se le singole strategie di sicurezza variano, la necessità di una visione più ampia della superficie di attacco e la capacità di aggregare, correlare e analizzare enormi quantità di dati sulla sicurezza dai singoli controlli di sicurezza che la proteggono sono un passo importante per ottenere il controllo.

I servizi di rilevamento e risposta gestiti sono efficaci e immediatamente disponibili, in quanto i team addetti alla sicurezza sfruttano i provider MDR per rafforzare le competenze, i processi e le tecnologie di sicurezza. La ricerca ESG mostra che le organizzazioni che investono in XDR desiderano servizi MDR complementari per implementare e utilizzare queste soluzioni. Ciò significa coinvolgere i fornitori di soluzioni che hanno una comprovata esperienza nella fornitura di soluzioni e servizi di sicurezza. Se applicato nel tempo, ciò può aiutare i team IT e di sicurezza a sviluppare e dimensionare i propri programmi di sicurezza.

ESG consiglia di esplorare le soluzioni MDR di aziende come Dell Technologies che vengono fornite con le persone, i processi e le tecnologie idonei per aiutare le organizzazioni a raggiungere questi obiettivi.

Enterprise Strategy Group è una società integrata di analisi della tecnologia, ricerca e strategia che offre intelligence di mercato, informazioni pratiche e servizi per i contenuti go-to-market alla community IT globale.

www.esg-global.com contact@esg-global.com 508.482.0188