Enterprise Strategy Group | Getting to the bigger truth.™

WHITE PAPER ESG

Rilevamento e risposta gestiti: un percorso verso la rapida crescita del programma di sicurezza

Di David Gruber, Principal Analyst

Agosto 2022

Il presente white paper di ESG è stato commissionato da Dell Technologies e viene distribuito su licenza concessa da TechTarget, Inc.

Sommario

Abstract

L'accelerazione della Digital Transformation, la rapida adozione del cloud, un panorama delle minacce più complesso e una continua carenza di competenze in ambito di sicurezza stanno portando al limite i team addetti alla sicurezza. Le attuali soluzioni di sicurezza non sono in grado di tenere il passo, costringendo molte aziende a dare priorità alle iniziative di modernizzazione del SOC per rinnovare le tecnologie e i processi. I megatrend di settore relativi alla strategia Zero Trust e al rilevamento e alla risposta estesi (XDR) offrono una nuova vision, tuttavia molte organizzazioni hanno difficoltà a realizzare e rendere operative implementazioni efficaci di queste strategie. I servizi di rilevamento e risposta gestiti (MDR) rappresentano una soluzione ottimale, offrendo a molte organizzazioni le persone, i processi e la tecnologia necessari per rafforzare i loro programmi di sicurezza in questo ambiente turbolento.

Introduzione

Il rischio crescente di attacchi informatici dannosi sottrae risorse e budget agli obiettivi aziendali principali e le organizzazioni devono rispondere rafforzando i programmi di sicurezza informatica. Solo alcune aziende dispongono delle risorse interne richieste per implementare e gestire l'intero programma di sicurezza, mentre per tutte le altre sono necessarie risorse di terze parti per supportare una crescita e un dimensionamento rapidi del programma.

Al centro di tutti i programmi di sicurezza informatica vi sono le operazioni di sicurezza (SecOps), responsabili del monitoraggio e della protezione di tutti i componenti della superficie di attacco digitale. Considerando che questa include estensione di rete, endpoint, cloud, identità, applicazioni e dati, l'escalation delle quantità di telemetria della sicurezza e degli avvisi coinvolti in SecOps stanno spingendo al limite le organizzazioni, causando molte richieste di assistenza ai fornitori di servizi MDR.

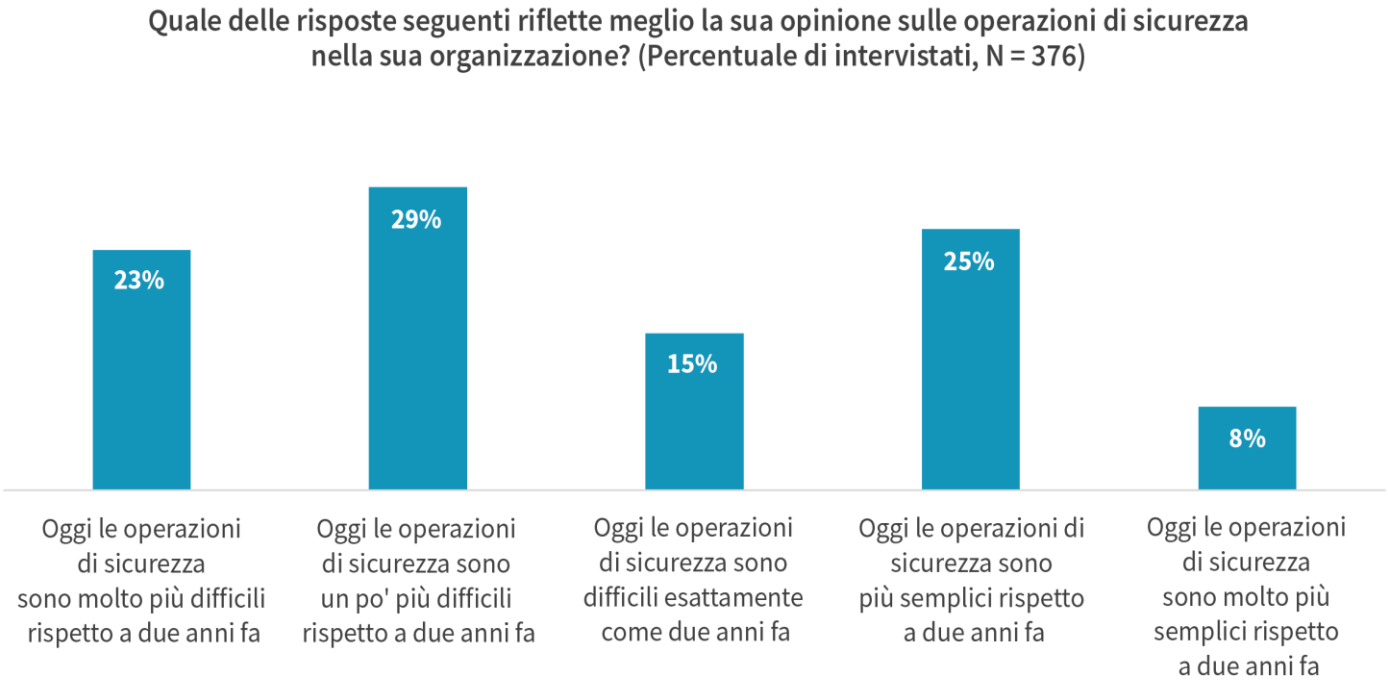
I fornitori di servizi MDR sono diventati un meccanismo critico per queste organizzazioni, fornendo una serie di offerte di servizi di sicurezza, quali risposta agli incidenti, monitoraggio 24 ore su 24, gestione dei programmi e gestione dei rischi. La ricerca Enterprise Strategy Group (ESG) indica che i servizi MDR sono diventati una componente classica delle moderne strategie di sicurezza informatica per le organizzazioni di tutte le dimensioni e la maturità della sicurezza.

Aumento delle sfide per le operazioni di sicurezza

Secondo la ricerca ESG (vedere la figura 1), la maggior parte delle organizzazioni riconosce che l'intero scenario SecOps è oggi più complesso rispetto a due anni fa.[1]

[1] Fonte: risultati della survey completa ESG, *SOC Modernization and the Role of XDR*, agosto 2022. Tutti i grafici e i riferimenti di ESG inclusi in questo white paper sono stati estrapolati dai risultati della survey, se non diversamente specificato.

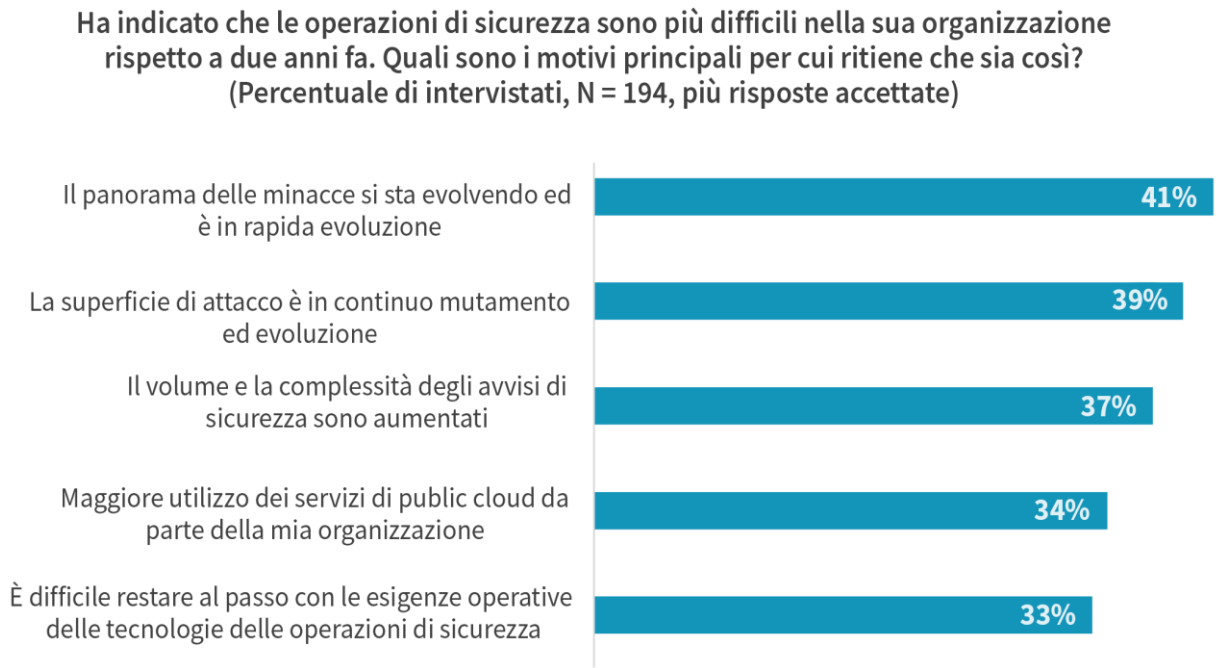
Figura 1. Più della metà ritiene che le SecOps siano più difficili



Fonte: ESG, una divisione di TechTarget, Inc.

Come illustrato nella figura 2, la ricerca ESG evidenzia anche altre sfide che rendono il rilevamento e la risposta più difficili che mai, come la superficie di attacco in espansione, la crescita e la diversità del panorama delle minacce e l'uso crescente dei servizi cloud per una gamma più ampia di applicazioni e casi d'uso.

Figura 2. I cinque motivi principali per cui le SecOps sono più difficili



Fonte: ESG, una divisione di TechTarget, Inc.

Modernizzazione dei programmi di rilevamento e risposta

Le superfici di attacco e il panorama delle minacce sono cresciuti sia in termini di dimensioni che di complessità, così come l'utilizzo di più controlli di sicurezza, generando migliaia di avvisi ed enormi quantità di dati sulla sicurezza. A supporto della classificazione e dell'analisi di avvisi e incidenti, i team addetti alla sicurezza devono aggregare, correlare e analizzare questi dati, che spesso richiedono un'elaborazione manuale intensiva. Ma l'acquisizione e l'analisi di avvisi e dati di sicurezza è solo una parte del processo.

I team addetti alla sicurezza stanno ridefinendo le operazioni complessive del programma per integrare ulteriormente i dati sugli asset e sui rischi dei team IT e delle linee di business per concentrarsi sulle minacce che rappresentano il rischio più significativo per gli obiettivi organizzativi. Ad esempio, la sottrazione delle credenziali di amministrazione del dominio può avere un'ampia gamma di potenziali effetti negativi su operazioni, finanze e reputazione del marchio dell'organizzazione sia a breve che a lungo termine.

Mentre i leader della sicurezza ripensano le strategie, sempre più organizzazioni affidano le attività operative quotidiane a terze parti, riassegnando le risorse interne ad attività di sicurezza più strategiche. Poiché le risorse di sicurezza interne si concentrano sulla riorganizzazione dell'architettura dei processi delle operazioni di sicurezza, i fornitori di servizi MDR gestiscono il rilevamento, la classificazione e la risposta degli incidenti, adottando misure rapide per prevenire i danni e limitare potenziali interruzioni operative del business.

Alcune organizzazioni si stanno rivolgendo a provider MDR per indicazioni su come sviluppare il programma complessivo, coinvolgendo esperti e processi delle operazioni di sicurezza comprovati per ottimizzare i risultati.

Inoltre, man mano che il movimento XDR crea una vision e una roadmap per ciò che è necessario per modernizzare i programmi di rilevamento e risposta, altre stanno cercando di sfruttare i provider MDR per fornire assistenza nell'implementazione di soluzioni di livello XDR.

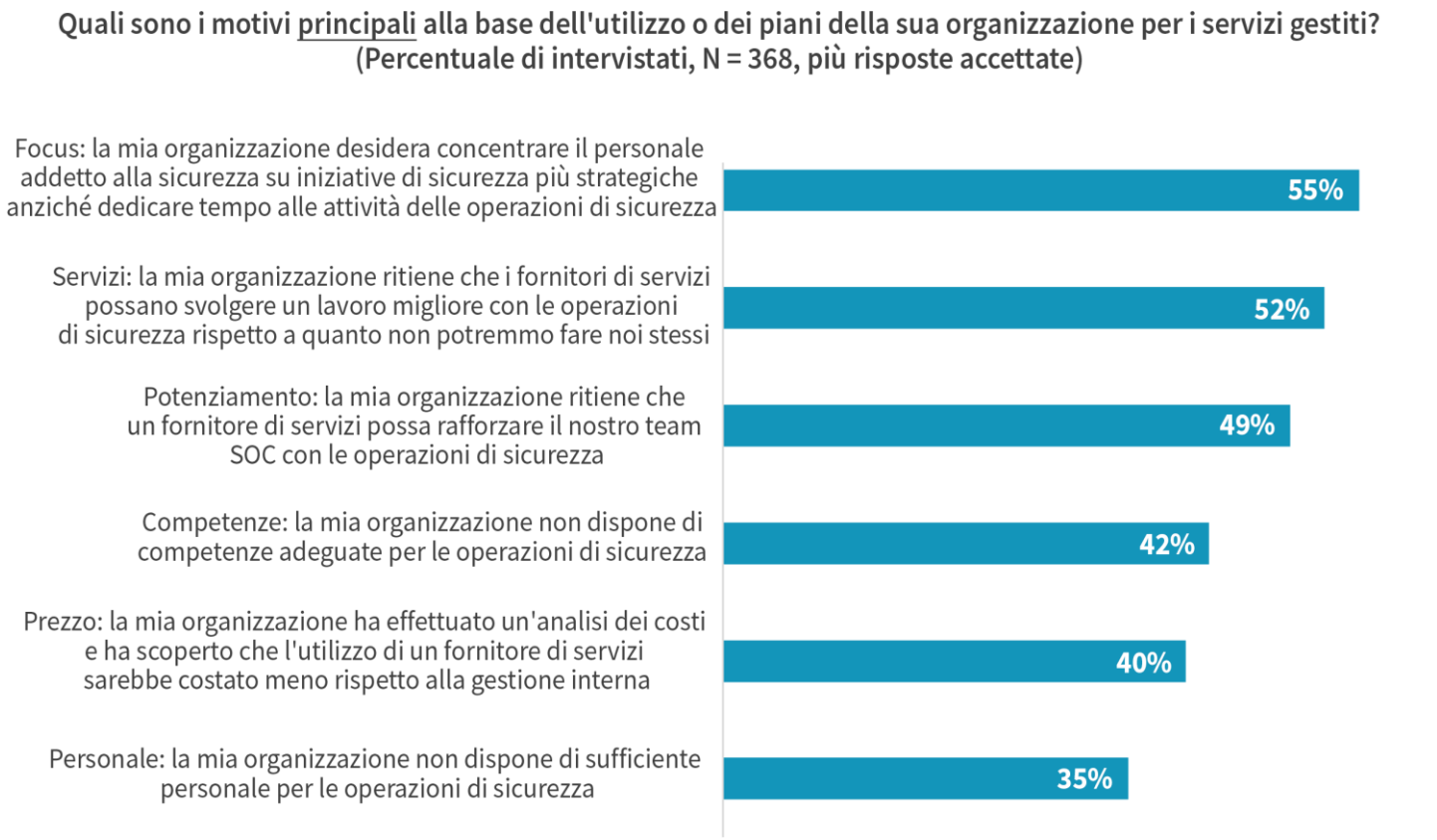
Casi d'uso MDR

Sebbene molti provider MDR offrano un'ampia gamma di servizi di sicurezza, spesso l'impegno inizia con servizi core di rilevamento e risposta che monitorano, classificano e analizzano gli avvisi. I modelli operativi variano a seconda dei provider MDR, pertanto i leader della sicurezza devono allineare attentamente i propri requisiti organizzativi con un provider MDR in grado di soddisfare i loro obiettivi specifici. Ad esempio, alcuni leader della sicurezza scelgono di esternalizzare completamente le operazioni di sicurezza, coinvolgendo un provider MDR per ottenere copertura completa della superficie di attacco, monitoraggio e correzione delle minacce. In questo modello, i provider MDR spesso forniscono lo stack tecnologico, i processi e gli esperti di sicurezza necessari per eseguire il servizio. Per altri, i servizi MDR rappresentano un'estensione della funzione delle operazioni di sicurezza interne, aggiungendo la copertura fuori dall'orario di lavoro o ulteriori esperti di sicurezza a un team interno responsabile principalmente dello stack tecnologico e del processo operativo. Questi sono solo due esempi dei numerosi casi d'uso in cui vengono utilizzati i servizi MDR.

La soluzione MDR, come abbiamo visto, non è universale. Al contrario, spesso rappresenta un set personalizzabile di funzionalità che possono essere applicate alle esigenze di una singola organizzazione.

Organizzazioni diverse sceglieranno un partner MDR per aspetti specifici del rilevamento e della risposta, a seconda delle risorse e delle competenze interne. La ricerca ESG prende in esame i motivi principali per cui sono presenti nella figura 3.

Figura 3. Perché le organizzazioni scelgono i partner MDR



Fonte: ESG, una divisione di TechTarget, Inc.

Principali fattori di valore per l'impegno MDR

Lo sviluppo del programma di sicurezza richiede un focus sia sull'efficienza che sull'efficacia, e i servizi MDR possono avere un impatto positivo su entrambi.

- Miglioramento operativo ed efficienza. Una soluzione MDR può aiutare le organizzazioni a ridurre il costo complessivo delle operazioni di sicurezza in vari ambiti, tra cui l'infrastruttura, il personale e la gestione. Permette inoltre di risolvere il problema di "sovraccarico degli avvisi", nonché migliorare la probabilità che i falsi positivi vengano ridotti in modo significativo.

- Miglioramento dell'efficacia della sicurezza informatica e riduzione dei rischi. La soluzione MDR può aiutare le organizzazioni a bloccare le minacce già in corso, migliorare il rilevamento di potenziali minacce e attacchi persistenti avanzati, attivare la threat hunting proattiva e istituzionalizzare controlli più solidi per identificare e prevenire gli attacchi futuri.

Cosa ricercare in un moderno fornitore di soluzioni MDR

Una cosa da tenere presente è che le soluzioni MDR, in generale, non sono una novità. Infatti, sono presenti da tempo e hanno già dimostrato la loro efficacia. Tuttavia, molte soluzioni MDR di "generazione 1.0" erano progettate e implementate per un'epoca diversa: meno dati, meno minacce, rilevamento più semplice. La nuova generazione di soluzioni MDR, e le terze parti che le implementano e le gestiscono, devono tenere conto di una serie più ampia, approfondita e complessa di sfide che rendono il rilevamento e la risposta più importanti e più difficili che mai.

Quando valutano soluzioni MDR, le organizzazioni dovrebbero ricercare funzionalità quali:

- Monitoraggio 24/7 di eventi e log, che produce informazioni rapide e ad alta visibilità su attività sospette e avvisi per volume, posizione e tipo.
- Monitoraggio continuo e scalabile della rete e analisi delle minacce.
- Suggerimenti basati sull'intelligenza artificiale per opzioni di risposta contestuale.
- Reporting sulla conformità alle normative.
- Consulenti per la sicurezza "umani" in contatto diretto con i team interni.
- Analisi dettagliata in tempo reale basata su rilevamento delle minacce, classificazione, analisi e indagine forense.
- Valutazioni delle vulnerabilità, definizione delle priorità e linee guida per la riduzione dei rischi.

Quando si considera l'elevato numero di fornitori di servizi potenziali in grado di fornire alcune, la maggior parte o addirittura tutte le funzionalità MDR in outsourcing, le organizzazioni dovrebbero ricercare partner in grado di offrire:

- Threat Intelligence contestuale.
- Telemetria avanzata.
- Comprovata esperienza nell'area di copertura geografica, nel mercato verticale e nel profilo normativo dell'organizzazione.
- Funzionalità di threat hunting dimostrate.
- Un impegno a lungo termine rispetto a MDR basato su cloud, con ampie funzionalità in ambienti multi-cloud e hybrid cloud, Zero Trust e il modello di responsabilità condivisa della sicurezza del cloud.
- Una capacità comprovata di dimensionare il servizio nel tempo, basata su tecnologia innovativa, processi comprovati e competenze dimostrate dai suoi dipendenti.

L'approccio Dell Technologies a MDR

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, un'azienda Dell Technologies. 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 dall'esperienza e 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.

Configurato e implementato come servizio gestito basato su abbonamento, Dell Managed Detection and Response riduce drasticamente la necessità per le organizzazioni di ricercare e assumere professionisti della sicurezza per gestire più minacce, più attacchi e più avvisi. Dell Managed Detection and Response integra ed estende le funzionalità interne di un'organizzazione in modo efficiente ed efficace. Di conseguenza, il personale SecOps interno può dedicare più tempo ed energia ad altre attività correlate alla sicurezza.

Storie di successo: come funziona MDR nel mondo reale

ESG ha parlato con i leader IT e della sicurezza dei clienti Dell MDR per ottenere informazioni dettagliate su casi d'uso specifici, modelli operativi e risultati.

Esempio 1: pubblica amministrazione locale di medie dimensioni

Le risorse IT e di sicurezza informatica delle pubbliche amministrazioni raramente corrispondono a quelle delle controparti del settore privato, ma ciò non significa che non si trovino ad affrontare gli stessi tipi di problemi. In questo esempio, una contea di medie dimensioni in uno stato del sud-ovest degli Stati Uniti faticava ad affrontare e superare un numero crescente di minacce alla sicurezza, ma anche a mantenere la spesa entro rigidi vincoli.

Quando è stato assunto un nuovo IT Director, ha riconosciuto immediatamente il panorama delle minacce in continua crescita che il suo team ristretto doveva affrontare e ha individuato potenziali vulnerabilità nelle funzionalità di rilevamento e risposta. "Il profilo di sicurezza non era all'altezza, ma dovevamo espandere le nostre funzionalità senza che ciò incidesse sulle buste paga, un argomento cui i dirigenti responsabili delle decisioni erano altamente sensibili", ha affermato. "Ma sapevo di poter fare breccia nel loro desiderio di frugalità fiscale evidenziando la necessità di affrontare le nostre vulnerabilità".

Ha in primo luogo stabilito di valutare l'attuale vendor di sicurezza degli endpoint della contea richiedendo una "prova gratuita" di 90 giorni di aggiornamenti software per testare il miglioramento del rilevamento e della risposta. Tuttavia, resosi conto che le funzionalità del software non erano adatte alle esigenze e le comunicazioni del vendor non erano all'altezza delle aspettative, ha deciso di scegliere una soluzione MDR più completa.

"Fortunatamente, avevamo un accordo con Dell per fornire un CSO (Chief Security Officer) virtuale, quindi i leader della contea erano consapevoli dei vantaggi derivanti dall'utilizzo di un approccio basato sui servizi gestiti, in questo caso per il rilevamento e la risposta". Ha aggiunto che il team Dell ha integrato, e non sostituito, il team interno ristretto di professionisti di sicurezza e IT della contea. "Erano un'estensione del nostro team e hanno lavorato insieme ai nostri dipendenti in maniera trasparente".

Il vero vantaggio dell'accordo è diventato presto evidente quando una campagna di hacking globale ha preso di mira la web mail di Microsoft Exchange, una popolare piattaforma utilizzata da un'ampia gamma di organizzazioni, tra cui la contea stessa. "Microsoft ha sviluppato e inviato una patch non appena ha scoperto l'attacco, ma il giorno zero dell'attacco era stato probabilmente un mese prima", ha affermato l'IT Director della contea. "Siamo stati contattati dal nostro CSO virtuale Dell dopo l'orario lavorativo e il team Dell MDR è intervenuto immediatamente. Ci hanno inviato degli script per controllare il server e abbiamo scoperto rapidamente che uno dei server era compromesso".

"Dell (e i suoi partner Secureworks) sapevano esattamente quello che facevano. Abbiamo ricevuto due, tre chiamate al giorno, ogni giorno, per tutto il tempo in cui abbiamo avuto a che fare con il tentativo di violazione". Ha aggiunto che il team di risposta agli incidenti ha analizzato i risultati con il personale della contea, mostrando loro frammenti di codice e altre indicazioni del tentativo di violazione e la prova della compromissione.

Infine, il team ha fornito una serie di raccomandazioni tecniche e non tecniche che non solo hanno disinnescato il potenziale impatto del tentativo di violazione, ma hanno anche rafforzato il profilo di sicurezza informatica della contea in una prospettiva e un periodo di tempo più ampi.

"La nostra esperienza ci ha dimostrato che la strada da percorrere nella ricerca di una soluzione di rilevamento e risposta avanzati consiste nel trovare uno specialista MDR affidabile, comprovato e serio che abbia esperienza in materia, anziché cercare di trovare un modo economico per aggiornare il software EDR", ha affermato. "Non solo durante il tentativo di violazione, ma anche nel corso della nostra regolare collaborazione, ricordo solo la sensazione rassicurante di sapere che avevamo un team valido che lavorava per la nostra sicurezza".

Esempio 2: distretto scolastico di medie dimensioni

I distretti scolastici hanno da sempre investito in modo insufficiente nell'IT in generale e nella sicurezza informatica in particolare. Ma con il ransomware e altri attacchi informatici contro i distretti scolastici in aumento, i funzionari locali dell'istruzione pubblica si stanno ingegnando per trovare modi migliori, più affidabili e convenienti per proteggersi dalle vulnerabilità.

Ad esempio, un distretto scolastico statunitense di medie dimensioni si è trovato sotto attacco da ransomware che ha causato l'arresto di tutte le operazioni basate sulla tecnologia. Con 8.500 tra studenti e personale distribuiti in 21 strutture, il distretto aveva un profilo IT di dimensioni ragionevoli con 100 server fisici e altri 63 server virtuali, collegati a più di 11.000 dispositivi per studenti e personale. Chiaramente, questo distretto aveva molti potenziali punti di ingresso per gli utenti malintenzionati e necessitava di un partner in grado di agire rapidamente.

Dopo aver determinato che l'attacco ransomware era reale e doveva essere affrontato immediatamente, il team IT del distretto scolastico ha contattato Dell Managed Detection and Response. "Entro il secondo giorno dell'attacco, c'erano 10 persone di Dell", ha ricordato il direttore IT del distretto. "Abbiamo avuto una relazione molto affidabile con il team di Dell, che ha subito preso il controllo".

Fortunatamente, il risultato finale è stato positivo per il distretto. "Degli oltre 6 milioni di file nei nostri sistemi, ne abbiamo persi solo sei", ha osservato l'IT Director. "E non abbiamo mai pagato l'autore della minaccia. Siamo un esempio reale di sopravvissuti al ransomware e continuiamo a svolgere il nostro lavoro in modo sicuro.

"Lavorare con Dell è stata un'esperienza positiva. Il nostro analista della sicurezza on-site è sempre soddisfatto dopo aver parlato con il personale Dell e oggi abbiamo un approccio migliore del 95% rispetto a prima che iniziassimo a collaborare con Dell per il rilevamento e la risposta gestiti".

Una verità più profonda

Il rischio crescente di attacchi informatici dannosi sottrae energie e budget ai principali obiettivi aziendali, e per questo le organizzazioni devono rafforzare i programmi di sicurezza informatica. I casi d'uso possono variare, ma molte organizzazioni ricorrono ai fornitori di servizi MDR per rafforzare e dimensionare i propri programmi.

I fornitori di servizi MDR offrono un percorso per superare molte delle sfide riconosciute nella creazione di un programma di sicurezza di successo, tra cui esperti di sicurezza, processi comprovati e tecnologie di sicurezza scalabili e facili da implementare.

Dell Technologies ha messo assieme un set di tecnologie strettamente integrate, esperti di sicurezza e best practice per aiutare le organizzazioni a rilevare e affrontare le minacce in tempo quasi reale. Come osservato dai casi di studio in questo white paper, Dell Technologies ha aiutato un'ampia gamma di organizzazioni in diversi settori e profili di risorse a contrastare l'impatto delle minacce emergenti in tutta l'azienda.

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