Enterprise Strategy Group | Getting to the bigger truth.™

Come colmare le lacune delle operazioni di sicurezza con MDR

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. Al centro di tutti i programmi di sicurezza informatica vi sono le operazioni di sicurezza (SecOps), responsabili del monitoraggio e della protezione di tutti gli aspetti della superficie di attacco digitale.

Nonostante gli investimenti, le operazioni di sicurezza sono più difficili

OLTRE LA METÀ
degli intervistati ritiene che le SecOps siano **più difficili ora** rispetto a quanto non fossero due anni fa.

» **I cinque motivi principali per cui le SecOps sono più difficili.**

1. **41%**
Il panorama delle minacce si sta evolvendo ed è in rapida evoluzione

2. **39%**
La superficie di attacco è in continuo mutamento ed evoluzione

3. **37%**
Il volume e la complessità degli avvisi di sicurezza sono aumentati

4. **34%**
Maggiore utilizzo dei servizi di public cloud da parte della mia organizzazione

5. **33%**
È difficile restare al passo con le esigenze operative delle tecnologie delle operazioni di sicurezza

Ridefinizione delle strategie del programma

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. 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.

98%
delle organizzazioni si avvale già di un provider MDR o prevede di avvalersi della sua collaborazione nei prossimi 12 mesi.

88%
di queste organizzazioni prevede di incrementare l'utilizzo di MDR nei prossimi 12 mesi.

» **Principali fattori di valore per l'impegno MDR**

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.

» **Motivi principali alla base dell'utilizzo o dei piani dell'organizzazione per i servizi gestiti.**

55%
Focus:
La mia organizzazione desidera concentrare il personale addetto alla sicurezza su iniziative di sicurezza più strategiche anziché dedicare tempo alle attività delle operazioni di sicurezza.

52%
Servizi:
La mia organizzazione ritiene che i fornitori di servizi possano svolgere un lavoro migliore con le operazioni di sicurezza.

49%
Potenziamento:
La mia organizzazione ritiene che un fornitore di servizi possa rafforzare il nostro team SOC con le operazioni di sicurezza.

42%
Competenze:
La mia organizzazione non dispone di competenze adeguate per le operazioni di sicurezza.

> **Molte soluzioni MDR di generazione 1.0 erano progettate e implementate per un'era diversa:** meno dati, meno minacce, rilevamento più semplice."
>
> *- Dave Gruber, ESG Principal Analyst*

Nuovi requisiti per la MDR

Molte soluzioni MDR di "generazione 1.0" erano progettate e implementate per un'era diversa: meno dati, meno minacce, rilevamento più semplice. La nuova generazione di soluzioni MDR deve essere in grado di fornire protezione a una superficie di attacco diversificata, rilevare minacce più complesse e sfruttare un approccio maggiormente concentrato sul rischio per la definizione delle priorità e la mitigazione.

- Monitoraggio 24/7 di eventi e registri.
- 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.
- 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 per la MDR basata su cloud.
- Funzionalità estese in ambienti multicloud 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.

Una verità più profonda

Il rischio crescente di attacchi informatici dannosi sottrae risorse e budget agli obiettivi aziendali principali e le organizzazioni devono rafforzare i programmi di sicurezza informatica. Anche se i casi d'uso variano, la maggior parte si avvale di fornitori di servizi MDR per ampliare e dimensionare i propri programmi.

L'approccio Dell Technologies al rilevamento e alla risposta gestiti combina tecnologia flessibile, intelligente e scalabile con professionisti esperti della sicurezza informatica, per aiutare le organizzazioni di tutte le dimensioni e profili di risorse ad accelerare e rafforzare i programmi di sicurezza.

FORMAZIONE APPROFONDITA

DELL Technologies

Fonte: risultati della survey completa ESG, *SOC Modernization and the Role of MDR*, agosto 2022.