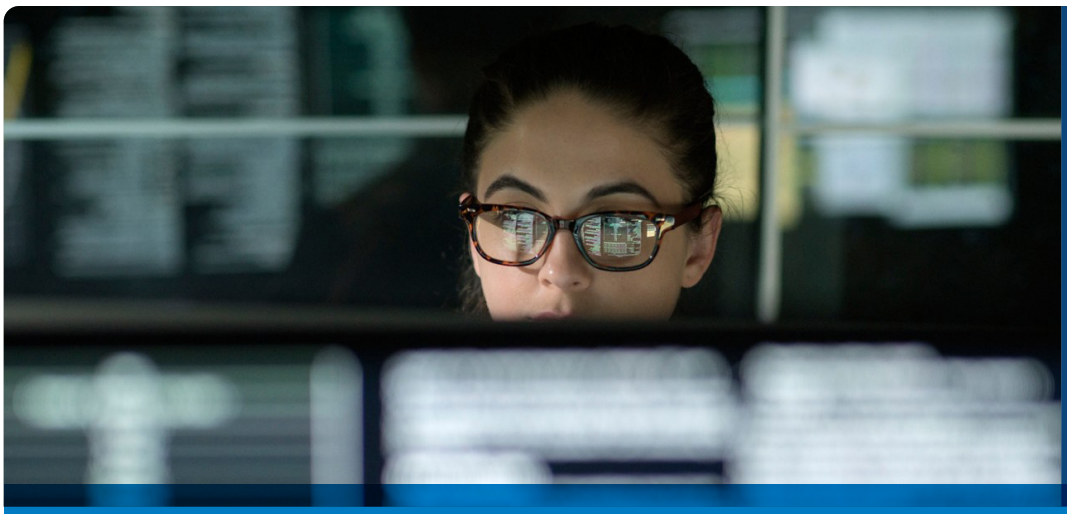
Prevenire e rispondere alle minacce avanzate in tutto l'ambiente IT



Identificazione delle vulnerabilità e definizione delle priorità per un'attenzione immediata

Managed Detection and Response Pro

Combinazione di gestione delle vulnerabilità e rilevamento e risposta gestiti in un'unica soluzione per proteggere l'ambiente IT

Nel 2022, il costo medio di una violazione dei dati è stato pari a $ 4,35 milioni.[1] Nel 2021, sono state pubblicate quasi 22.000 nuove vulnerabilità e questo numero continua ad aumentare.[2] Le organizzazioni devono trovare un modo per proteggere il proprio ambiente dal volume crescente di minacce alla sicurezza e dalle implicazioni delle violazioni.

La protezione dell'ambiente IT richiede la risoluzione delle vulnerabilità, l'analisi delle minacce e una risposta efficace. Inoltre, le organizzazioni IT devono affrontare la sfida di trovare e trattenere professionisti della sicurezza qualificati, mentre le loro energie vengono assorbite da esigenze critiche e dalle operazioni aziendali quotidiane.

Queste sono le ragioni che ci hanno spinto a progettare Managed Detection and Response Pro. MDR Pro è una soluzione completamente gestita, che offre l'identificazione delle vulnerabilità e la definizione della loro priorità, oltre a rilevamento delle minacce e risposta ad esse 24 ore su 24, 7 giorni su 7. I nostri esperti collaborano con il tuo team di sicurezza interno per migliorare costantemente il profilo di sicurezza ed essere sempre vigili.

Identificazione delle vulnerabilità e della loro priorità sull'intera superficie di attacco

Gli esperti Dell utilizzano la tecnologia leader del settore per eseguire periodicamente la scansione dell'ambiente IT ed offrire una panoramica completa delle vulnerabilità negli endpoint, nell'infrastruttura di rete e negli asset cloud. Gli esperti Dell applicano l'apprendimento automatico per individuare le vulnerabilità in circolazione e che hanno maggiori probabilità di essere prese di mira nel futuro immediato. In questo modo potrai dare maggiore priorità alle attività di applicazione delle patch per le vulnerabilità e gli asset critici che presentano un rischio elevato.

Vantaggi principali:

- Aggiornamento costante dei tuoi sistemi di difesa con gestione e scansioni delle vulnerabilità ricorrenti.
- Quadro completo delle tue vulnerabilità in endpoint, infrastruttura di rete e cloud.
- Maggiore priorità alle vulnerabilità critiche da correggere prima che vengano sfruttate.
- Rilevamento e risposta unificati nell'intero ecosistema.
- Rilevamento di nuovi tipi di attacco con un database delle minacce in costante aggiornamento.
- Correlazione degli eventi e monitoraggio dell'attività end-to-end degli autori degli attacchi.
- Utilizzo ottimale delle conoscenze e delle competenze del team di sicurezza Dell.

Rilevamento e risposta agli autori degli attacchi prima che si verifichino danni

Managed Detection and Response è un servizio end-to-end 24x7 completamente gestito che monitora, rileva, analizza e risponde alle minacce nell'intero ambiente IT. Le organizzazioni con almeno 50 endpoint possono migliorare rapidamente e in modo significativo il profilo di sicurezza, riducendo, al contempo, il carico di lavoro per i dipartimenti IT.

Il servizio sfrutta due elementi principali:

- Le competenze degli analisti di sicurezza Dell Technologies, acquisite grazie a un'esperienza pluriennale nell'assistenza fornita a organizzazioni di tutto il mondo per proteggere meglio la loro attività.
- Il software avanzato di analisi della sicurezza XDR, frutto di oltre 20 anni di esperienza di SecOps, threat intelligence e ricerca di minacce reali e di rilevamento e risposta alle minacce avanzate.

Funzioni chiave

Rilevamento delle minacce e relative indagini

- I partner Dell collaborano con te per comprendere l'ambiente e assistere nell'implementazione dell'agente software negli endpoint applicabili senza costi aggiuntivi.
- Utilizzo ottimale dei dati degli autori degli attacchi raccolti in oltre 1400 attività di risposta agli incidenti nell'ultimo anno.
- Istruzioni dettagliate per contenere la minaccia anche in situazioni complesse.
- Fino a 40 ore di correzione guidata da remoto incluse per trimestre.
- Fino a 40 ore di assistenza remota annuale per la risposta agli incidenti che consentono un avvio rapido delle attività di indagine.

Identificazione e definizione delle priorità delle vulnerabilità

- Scansioni mensili delle vulnerabilità, con scansioni aggiuntive in base a quanto stabilito dal confronto tra il team Dell e il cliente.
- Inventario degli asset da confrontare con gli attuali database delle vulnerabilità già note, per individuare i punti deboli e gli aggiornamenti necessari.
- Feedback al cliente sulla priorità delle vulnerabilità a rischio più alto da affrontare e indicazioni per l'applicazione delle patch.
- Scansioni eseguite utilizzando una piattaforma avanzata basata sull'apprendimento automatico.
- Revisioni trimestrali per informare il cliente sulle tendenze delle vulnerabilità nel proprio ambiente e nel settore.

Proteggi il tuo ambiente oggi stesso con Dell

A fronte del costante aumento della frequenza e del costo delle violazioni, Managed Detection and Response Pro contribuirà a proteggere l'ambiente IT e gli asset più critici dagli autori di minacce dannose, migliorando, al contempo, il profilo di sicurezza dell'organizzazione.

Contatta il tuo responsabile vendite oggi stesso.

[1] IBM. (2022). Cost of a Data Breach Report 2022. Consultato il 20 settembre 2022, dalla pagina https://www.ibm.com/downloads/cas/3R8N1DZJ

[2] Tenable (2021) Tenable's 2021 Threat Landscape Attack. Consultato ad agosto 2022, dalla pagina https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective