Rafforzamento del profilo di sicurezza con Managed Detection and Response

Rileva, analizza e rispondi alle minacce avanzate negli ambienti IT

Dell Managed Detection and Response

Le competenze in materia di sicurezza e la conoscenza approfondita degli ambienti IT di Dell Technologies unite alla tua scelta di piattaforme di analisi della sicurezza XDR leader del settore.

La tua azienda è veramente protetta?

I team IT hanno difficoltà a tenere il passo con il crescente numero di minacce alla sicurezza in continua evoluzione. Nel 2022, si sono registrati 5,5 miliardi gli attacchi malware a livello globale, con un incremento di 100 milioni rispetto al 2021.[1]

La protezione completa della tua organizzazione richiede un rilevamento rapido e una risposta efficace alle nuove minacce all'interno dell'ambiente. Questa protezione è difficile da ottenere a causa di prodotti e strumenti individuali che frammentano la visibilità, della difficoltà di reperire e mantenere professionisti della sicurezza qualificati e dei team IT che sono già completamente assorbiti da esigenze critiche e dalle operazioni quotidiane.

Managed Threat Detection and Response

Dell Managed Detection and Response è un servizio end-to-end, completamente gestito, disponibile 24/7, che monitora, rileva, analizza e risponde alle minacce in tutto l'ambiente IT, aiutando le organizzazioni con 50 o più endpoint a migliorare in modo rapido e significativo il proprio profilo di sicurezza, riducendo nel contempo la pressione sull'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.
- Piattaforme di analisi della sicurezza XDR (Extended Detection and Response) leader del settore che integrano analisi basate sull'AI di telemetria e altri eventi derivanti da diversi vettori di attacco.

Vantaggi principali:

- Rilevamento e risposta unificati nell'intero ecosistema
- Il database delle minacce continuamente aggiornato garantisce una protezione costante
- È possibile rilevare persino le tattiche dei threat actor più discreti
- Visione completa dell'attività end- to-end dei malintenzionati
- Un team di professionisti della sicurezza Dell Technologies con competenze in ambito di sicurezza, infrastrutture avanzate, cloud e molto altro
- Assistenza esperta per implementare il servizio SaaS cloud-native XDR
- Avvio rapido della risposta agli incidenti informatici in caso di violazione
- Costante allineamento al massimo livello di conformità ai criteri di sicurezza per i fornitori di servizi

Soluzione completa

Gli analisti della sicurezza Dell Technologies offrono assistenza per la configurazione iniziale, il monitoraggio, il rilevamento, la correzione e la risposta, il tutto a un prezzo prevedibile. Lavorano a stretto contatto con il tuo team IT per comprendere l'ambiente, consigliare i miglioramenti da apportare al profilo di sicurezza e contribuire a implementare l'agent software XDR negli endpoint.

Gli avvisi vengono monitorati e analizzati 24/7. Se un avviso richiede un'indagine, gli analisti determinano ed eseguono la risposta appropriata. Se una minaccia è dannosa o richiede un'azione, l'utente viene informato e, se necessario, vengono fornite istruzioni dettagliate.

In caso di incidenti di sicurezza, Dell Technologies aiuta ad avviare il processo per garantire il ripristino delle attività aziendali.

Scegli la tua piattaforma XDR

Le tue esigenze e preferenze in termini di sicurezza e tecnologia sono uniche. Ti offriamo la flessibilità di scegliere tra tre opzioni leader del settore: Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR o Microsoft Defender XDR, per consentirti di ottenere una piattaforma XDR adatta alle tue esigenze.[2]

Funzioni chiave

Supporto affidabile

- Collaborazione a stretto contatto con te per comprendere il tuo ambiente, risolvere i problemi e consigliare miglioramenti da apportare al profilo di sicurezza
- Monitoraggio 24/7 con la tua scelta di piattaforme XDR che integrano analisi basate sull'AI di telemetria e altri eventi derivanti da diversi vettori di attacco
- Consigli degli esperti per il deployment e la configurazione della piattaforma XDR

Risposta alle minacce e configurazione della sicurezza

- Grazie alle funzionalità XDR, il team Dell SOC automatizza le attività di correzione o collabora con te per affrontare le minacce rilevate durante il monitoraggio
- Fornitura di istruzioni dettagliate di facile comprensione per contenere la minaccia anche in situazioni complesse
- Fino a 40 ore di configurazione della sicurezza correlata ai servizi incluse per ogni trimestre

Rilevamento e indagine 24/7

- Processi e avvisi personalizzati in base all'ambiente di sicurezza della tua organizzazione e automatizzati per operazioni quotidiane efficienti
- Ricerca proattiva della minacce specifica per l'ambiente di ciascun cliente per individuare nuove minacce o varianti di minacce già note in grado di eludere i sistemi di sicurezza
- Il riepilogo giornaliero degli avvisi meno critici consente al team Dell SOC di concentrare l'attenzione sugli avvisi critici
- Report trimestrali su indagini, analisi delle tendenze degli avvisi e linee guida sul profilo di sicurezza

Avvio della risposta agli incidenti informatici

- 40 ore di assistenza remota annuali per la risposta agli incidenti che consentono un avvio rapido delle attività di indagine.
- Assistenza da parte dei nostri esperti di sicurezza qualificati, che hanno aiutato organizzazioni di ogni dimensione a riprendere le attività aziendali a seguito di gravi incidenti di sicurezza.

Inizia a proteggere il tuo ambiente oggi stesso con Dell

Con il costo totale medio di una violazione ransomware che raggiunge $ 5,13 milioni, il 13 percento in più rispetto al 2022, è giunto il momento di cercare di capire se Dell Managed Detection and Response è la soluzione giusta per te.[3]

Contatta il tuo responsabile vendite oggi stesso.

1. Statista, numero annuale di attacchi malware in tutto il mondo dal 2015 al 2022
2. Minimo 500 endpoint necessari per l'utilizzo di Microsoft Defender XDR
3. IBM, Cost of a Data Breach Report 2023

Febbraio 2024-NS