Vantaggi principali

Prevenzione

- Identificazione delle vulnerabilità in tutto l'ambiente per assegnare priorità all'applicazione di patch
- Rilevamento di controlli di sicurezza non configurati correttamente o problematici che potrebbero essere oggetto di exploit
- Ispezione accurata e approfondita dei percorsi ad alto rischio verso dati o asset preziosi con un penetration test annuale
- Miglioramento del livello di vigilanza dei dipendenti con corsi di formazione sulla sicurezza erogati in moduli frequenti e di durata limitata

Risposta

- Rilevamento e risposta alle minacce 24 ore su 24, 7 giorni su 7 in tutto l'ambiente
- Monitoraggio dell'attività end-to-end degli attori delle minacce
- Utilizzo della telemetria e correlazione degli eventi di molti degli strumenti di sicurezza più diffusi

Dell Managed Detection and Response Pro Plus

Soluzione SecOps a 360° completamente gestita su endpoint, rete e cloud

Come affrontare le sfide critiche delle operazioni di sicurezza

Molte organizzazioni IT hanno adottato il monitoraggio e il rilevamento delle minacce per restare al passo con il volume e la varietà delle minacce in continua crescita.

Il monitoraggio e il rilevamento delle minacce forniscono una copertura vitale, ma è comunque meglio gestire anticipatamente le lacune risolvibili, prima che gli attori delle minacce abbiano la possibilità di sfruttarle. I team IT possono prevenire molte delle attività malevole affrontando in modo proattivo le vulnerabilità del software, i controlli di sicurezza non configurati correttamente e la poca attenzione dei dipendenti.

Gli esperti in materia di sicurezza sanno come applicare patch per eliminare le vulnerabilità, ma per la maggior parte delle organizzazioni IT è impossibile porre rimedio a tutte le vulnerabilità. Nel 2021, sono state segnalate più di 1.500 nuove vulnerabilità ogni mese.[1] Per mantenere gestibile il carico di applicazione delle patch, i clienti devono assegnare la priorità alle vulnerabilità che presentano il rischio maggiore.

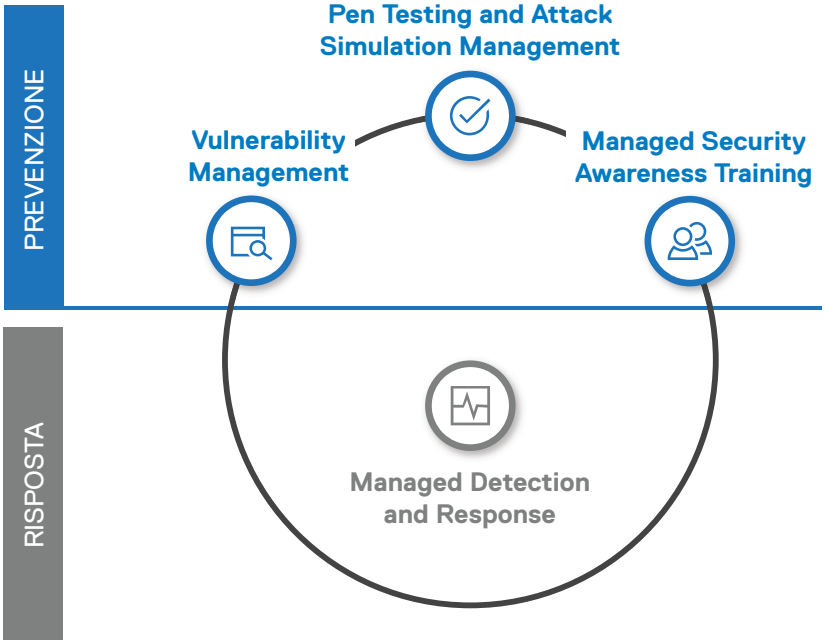
Provare a convalidare tutti i controlli di sicurezza, ad esempio gateway e-mail o firewall delle applicazioni web, è altrettanto scoraggiante. Con centinaia di controlli e configurazioni complesse, ai team addetti alla sicurezza IT viene richiesto in modo pressante di verificare che i controlli di sicurezza blocchino le attività non autorizzate.

Inoltre, per le organizzazioni è necessario che i dipendenti sappiano riconoscere quando gli attori delle minacce stanno cercando di ottenere credenziali di accesso, dati riservati o altre informazioni sensibili. Uno studio ha rilevato che l'83% delle organizzazioni intervistate ha subito un attacco di phishing tramite e-mail andato a buon fine nel 2021.[2]

Managed Detection and Response Pro Plus

Gli esperti di sicurezza di Dell Technologies hanno esaminato attentamente queste preoccupazioni chiave SecOps per progettare un nuovo servizio a 360° per le operazioni di sicurezza: Managed Detection and Response Pro Plus.

MDR Pro Plus è una soluzione SecOps completamente gestita in cui i principali esperti di sicurezza utilizzano strumenti all'avanguardia per prevenire le minacce, rilevare e contenere rapidamente i tentativi di attacco e avviare il ripristino in caso di violazione. MDR Pro Plus contribuisce a rafforzare continuamente il profilo di sicurezza della tua organizzazione.



Indizi di manomissione nel software e nei controlli di sicurezza

Vulnerability Management esegue la scansione mensile dell'ambiente per individuare le vulnerabilità e utilizza l'apprendimento automatico per assegnare la priorità quelle che hanno maggiori probabilità di essere oggetto di exploit e hanno un impatto significativo. L'elenco delle priorità consente al team IT di concentrarsi sulle vulnerabilità più importanti.

Gli attori delle minacce sono costantemente a caccia di vulnerabilità prive di patch, ricercando i controlli di sicurezza non configurati o obsoleti, e le organizzazioni IT devono individuare e risolvere queste vulnerabilità prima di loro. **Pen Testing and Attack Simulation Management** include simulazioni di violazioni e attacchi automatizzate (BAS) mensili e un penetration test annuale.

BAS rileva i controlli di sicurezza deficitari su dispositivi e software nell'ambiente IT. Il penetration test integra BAS tentando di raggiungere un obiettivo specifico, ad esempio un sistema a valore elevato. Penetration tester qualificati emulano le tecniche degli attori delle minacce, tra cui tecniche di pivoting e adattamento, per raggiungere l'obiettivo.

Dell esegue scansioni delle vulnerabilità e simulazioni BAS su database continuamente aggiornati per garantire che l'applicazione di patch e i controlli di sicurezza siano sempre aggiornati.

Aiuta i dipendenti a restare vigili

Un modello comune per la formazione per la consapevolezza sulla sicurezza è una sessione di formazione annuale di più ore. I dipendenti spesso tendono a dimenticare queste informazioni in quanto possono diventare un esercizio di tipo "barrare la casella giusta". Nel caso in cui siano il bersaglio di una strategia di social engineering o di un'e-mail con un link malevolo, potrebbero non reagire con sufficiente cautela.

Managed Security Awareness Training offre corsi di formazione sulla sicurezza di breve durata durante tutto l'anno, coinvolgendo i dipendenti in modo attivo e costante con percorsi di apprendimento personalizzati e facendo della sicurezza una priorità. I percorsi di formazione vengono creati in base al ruolo dei dipendenti, al livello di esposizione alle minacce e all'avanzamento.

Rilevamento e contenimento rapidi dei tentativi di attacco

Dell MDR Pro Plus offre **rilevamento e risposta gestiti** 24 ore su 24, 7 giorni su 7. Analisti qualificati monitorano il tuo ambiente e analizzano le minacce utilizzando una piattaforma di analisi della sicurezza XDR avanzata. L'analisi basata sull'apprendimento automatico e approfondito di telemetria ed eventi fornisce agli analisti informazioni dettagliate per rintracciare il percorso e le attività dell'attacker. Il team Dell fornisce quindi le istruzioni per contenere e risolvere la minaccia. In caso di incidenti di sicurezza, Dell Technologies aiuta ad avviare il processo per garantire il ripristino delle attività dell'organizzazione.

Migliora le operazioni di sicurezza con Dell

MDR Pro Plus aiuta a prevenire attività malevole segnalando regolarmente le lacune delle vulnerabilità, i controlli di sicurezza non configurati correttamente e i percorsi ad alto rischio verso asset preziosi. Inoltre, forniamo una formazione breve e facile da memorizzare sulla sicurezza per i dipendenti durante tutto l'anno. Il rilevamento e la risposta alle minacce fornisce monitoraggio e tracciatura always-on delle attività sospette.

MDR Pro Plus offre una soluzione intelligente per le operazioni di sicurezza IT a 360° con servizi basati su tecnologia avanzata, forniti da esperti. Il tutto gestito da Dell Technologies, un'azienda che organizzazioni di ogni dimensione in tutto il mondo considerano assolutamente affidabile in termini di dispositivi, infrastruttura e servizi IT innovativi.

Ulteriori informazioni su Dell Managed Detection and Response Pro Plus

Contatta un esperto Dell Technologies

[1] Fonte: With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers, ZDNet 8 dicembre 2021. https://www.zdnet.com/article/with-18376-vulnerabilities-found-in-2021-nist-reports-fifth-straight-year-of-record-numbers/

[2] Fonte: 2020 Phishing Attack Landscape Report [Greathorn]. Cybersecurity Insiders. (2020). Consultato il 15 novembre 2022 da https://www.cybersecurity-insiders.com/portfolio/2020-phishing-attack-landscape-report-greathorn/