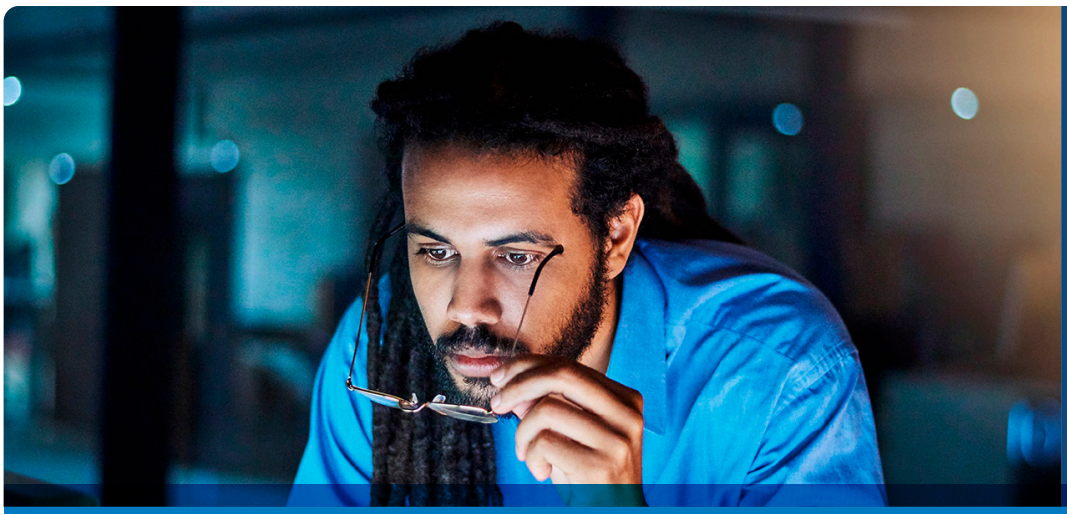
Convalida dei controlli e delle policy di sicurezza per chiudere i vettori di attacco



Simulazione delle tecniche degli attacker per l'accesso iniziale, l'esecuzione malevola dei file, il furto di dati e altro ancora

Penetration test e gestione delle simulazioni di attacchi

Dell convalida i controlli e le policy di sicurezza la cyber kill chain

Le organizzazioni dispongono di centinaia di controlli di sicurezza, dagli endpoint ai gateway web ed e-mail. I controlli sono spesso complessi e difficili da gestire e una configurazione errata può causare un'esposizione rischiosa. Gli attori delle minacce cercano di sfruttare controlli interrotti o obsoleti.

Per mettere alla prova e convalidare l'efficacia dei controlli di sicurezza, Dell Pen Testing and Attack Simulation Management riproduce accuratamente le azioni delle minacce reali.

Il servizio combina:

- simulazioni mensili automatizzate di violazioni e attacchi (BAS) per confermare il corretto funzionamento dei controlli
- un test annuale di penetrazione, in cui esperti qualificati tentano di violare le difese per acquisire asset e dati critici

Le simulazioni di attacco testano i controlli di sicurezza

I professionisti della sicurezza Dell utilizzano la tecnologia BAS avanzata per testare diversi vettori di attacco, ad esempio per tentare di inserire malware in un endpoint o per ottenere informazioni non autorizzate da un web server. I tester Dell applicano BAS per simulare gli attacchi nell'intera cyber kill chain[1] e individuare le minacce, incluse le più recenti TTP[2] degli attacker.

La tecnologia BAS è sicura per gli ambienti di produzione e viene continuamente aggiornata con le informazioni, gli attacchi e i comportamenti più recenti delle minacce.

Il penetration test valuta i percorsi verso gli obiettivi di valore elevato

Anche con la simulazione degli attacchi, alcuni attacker possiedono le competenze per navigare nell'ambiente, eludendo gli ostacoli per raggiungere dati preziosi. È qui che entra in gioco il penetration test:

Vantaggi principali:

- Rilevamento dei controlli di sicurezza non configurati correttamente che potrebbero essere sfruttati, utilizzando simulazioni complete di violazioni e attacchi
- Esame dei problemi e delle lacune emersi di recente con simulazioni mensili
- Ispezione accurata dei percorsi ad alto rischio verso asset o dati di valore elevato con un penetration test annuale
- Report dei risultati dei test, delle tendenze trimestrali e delle attività rilevanti per migliorare il profilo di sicurezza
- Acquisizione rapida di informazioni approfondite sulle nuove minacce ad alto rischio con test ad hoc

Il penetration test integra BAS: anziché testare singoli controlli o set di controlli, il test della penna si concentra su percorsi vulnerabili o ad alto rischio in un ambiente. I penetration tester Dell possono emulare varie tecniche di attori di minacce e perfino payload diversi nel loro sforzo di raggiungere un obiettivo specifico, come l'acquisizione di un sistema di valore elevato oppure la sottrazione o la disabilitazione di un particolare set di file. Come un vero attacker, un penetration tester esperto può variare, adeguare e affinare le tecniche per raggiungere l'obiettivo.

Applicazione delle informazioni di test per migliorare il profilo di sicurezza

Dell Technologies Services fornirà un reporting mensile sui problemi di controllo della sicurezza da correggere in base ai risultati dell'esecuzione delle sequenze BAS. Con cadenza trimestrale, Dell esaminerà le tendenze delle varie simulazioni di attacco, indicherà le attività più rilevanti osservate all'interno dell'ambiente IT e presenterà suggerimenti per migliorare il profilo di sicurezza.

Funzionalità chiave

Simulazione di violazioni e attacchi (BAS)

- Esecuzione mensile di simulazioni automatizzate di violazioni e attacchi in funzione dell'ambiente del cliente
- Convalida dei controlli di sicurezza sul perimetro e dei componenti dell'infrastruttura interna, tra cui gateway web, gateway e-mail ed endpoint
- Aggiornamento continuo dello strumento BAS con le informazioni, gli attacchi e i comportamenti più recenti delle minacce
- Applicazione di modifiche al flusso di lavoro della simulazione in base alle simulazioni precedenti e ai fattori dell'ambiente di sicurezza
- Esecuzione di simulazioni ad hoc per i problemi di sicurezza appena rilevati, in base alla Threat Intelligence e alla valutazione di Dell

Penetration test della sicurezza della rete

- Esecuzione di un penetration test annuale su sottoinsiemi definiti di gateway web, API, dispositivi mobili, indirizzi IP esterni ed interni e configurazioni cloud
- Nuova esecuzione del penetration test dopo aver corretto i problemi emersi dai risultati del primo test (opzionale)

Reporting e revisione

- Reporting mensile sulle simulazioni di violazioni e attacchi condotte
- Presentazione di un report trimestrale e revisione delle tendenze e delle attività rilevanti osservate nell'ambiente IT del cliente
- Formulazione di suggerimenti per migliorare il profilo di sicurezza complessivo

Onboarding

- Conduzione della riunione per l'avvio del servizio
- Revisione dell'elenco di controllo preliminare completato dal cliente
- Esame dell'ambiente IT del cliente
- Attivazione dell'applicazione BAS per il cliente
- Assistenza per il roll-out dell'agente

Contatta il tuo responsabile vendite oggi stesso.

[1] "Intera cyber kill chain": include minacce esterne, tra cui phishing, gateway web e altre minacce in grado di compromettere gli endpoint, spostamenti laterali per sottrarre credenziali o diffondere l'attacco, esfiltrazione di dati ecc.
[2] "TTP": tattiche, tecniche e procedure