Il lato umano della sicurezza informatica

Immagina lo scenario peggiore.

L'intero data center è bloccato a causa di un sofisticato attacco ransomware. I reparti finanziario, delle vendite e dell'assistenza clienti non possono operare. Sei un leader IT senior, responsabile del ripristino dei sistemi, ma non riesci a trovare una soluzione.

Il tuo team, già sotto organico, sta lavorando senza sosta da settimane, con pochissime pause o giorni liberi. Alcuni professionisti sono arrivati a ***lavorare fino a 36 ore di fila*** senza dormire. Inizi a preoccuparti che la stanchezza possa portare a decisioni errate, che metterebbero a rischio l'intero lavoro di ripristino.

Hai urgente bisogno di risorse aggiuntive che possano intervenire immediatamente per affrontare il problema, ma dove trovarle?

Questo scenario potrebbe sembrare l'inizio di un romanzo, ma si basa sulle esperienze reali dei clienti Dell. Evidenzia un problema significativo nell'attuale contesto della sicurezza informatica: lil fattore umano.

Dati recenti indicano che il settore soffre di una carenza di quasi 5 milioni di professionisti della sicurezza. Sebbene la necessità di risorse sia percepita in maniera più acuta durante un incidente, le soluzioni devono essere implementate molto prima.

Inizia con la creazione e lo sviluppo di una pipeline di talenti

Il primo passo per garantire la disponibilità delle risorse necessarie è creare una pipeline di talenti:

Reclutamento nelle università e tirocini

La collaborazione con le università locali e le scuole tecniche può garantire un flusso costante di giovani talenti. Queste persone possono essere formate nel tempo affinché diventino membri del team ad alto impatto.

Formazione e sviluppo continui

Nonostante le continue pressioni in termini di tempo e budget, i professionisti della sicurezza informatica devono tenere il passo con le evoluzioni sia degli strumenti che delle minacce.

Focus sulla retention

I professionisti esperti sono molto richiesti, soprattutto se hanno esperienza nella gestione di un attacco. Se non riesci a trattenere i tuoi migliori talenti, lo farà qualcun altro.

Anche un team solido potrebbe non essere sufficiente per gestire lo stress di un attacco, quindi preparati in tempo trovando risorse aggiuntive prima che siano necessarie:

Valutazione delle risorse di terze parti

Le società di consulenza sulla sicurezza informatica e di aumento del personale possono supportare il tuo team sia nelle operazioni quotidiane sia durante gli incidenti. Instaurare relazioni con queste società, anche se al momento non hai bisogno dei loro servizi, ti permetterà di accedere rapidamente a queste risorse quando necessario.

Dell offre numerosi servizi per potenziare i team esistenti, tra cui CISO virtuali (vCISO), risposta agli incidenti e consulenza sulla sicurezza informatica.

Scegli AI

Sfrutta le nuove funzionalità di AI integrate negli strumenti di sicurezza informatica, come l'analisi dei registri, il rilevamento delle anomalie, la classificazione degli avvisi di basso livello o la formazione specialistica, per colmare la carenza di risorse e rispondere alle esigenze operative, aiutando i membri del team a dedicarsi ad attività di maggior valore strategico.

Le sfide legate alle risorse sono maggiori durante un attacco informatico

Come illustrato dallo scenario iniziale, un grave attacco informatico può mettere in ginocchio un'organizzazione, paralizzando i sistemi principali e le operazioni aziendali. Poiché ogni minuto comporta una perdita economica per l'azienda, il team di sicurezza informatica subirà un'enorme pressione per risolvere il problema.

Mantenere i team costantemente aggiornati influisce in modo diretto sulla capacità di risposta agli incidenti e sul livello di stress a cui sono sottoposti.

È importante ricordare che la formazione non deve riguardare solo i professionisti della sicurezza, ma tutti i dipendenti, perché rappresentano la prima linea di difesa.

Questo esempio evidenzia una sfida centrale: i responsabili della sicurezza informatica sono, in definitiva, esseri umani. Hanno dei limiti che, se superati, possono metterli in seria difficoltà. Affaticamento mentale, stress e burnout sono ormai fattori cruciali nel profilo di sicurezza informatica.

Sebbene non esista un'unica soluzione a questa sfida, le seguenti strategie possono essere estremamente utili:

Creazione di una solida pipeline di team e talenti

La soluzione più efficace a questo problema è evitare che si trasformi in un'emergenza: occorre costruire un team forte, con adeguate ridondanze.

Pianificazione della gestione delle persone in caso di attacco

I piani di risposta agli incidenti sono fondamentali e DEVONO includere strategie per la gestione del personale, la pianificazione e la gestione del downtime dei dipendenti.

Uso delle risorse di terze parti

I consulenti esterni di sicurezza informatica possono dare un contributo positivo al team. I servizi di risposta agli incidenti Dell, ad esempio, possono inviare in loco un team di esperti in poche ore, pronto a valutare, contenere e avviare immediatamente le attività di correzione. Abbiamo aiutato numerosi clienti a superare con successo attacchi informatici.

L'AI può essere d'aiuto, ma non risolve tutto

L'AI offre un enorme potenziale di miglioramento degli strumenti e dei programmi di sicurezza informatica. Le sue capacità spaziano dall'analisi predittiva allo sviluppo di programmi di formazione personalizzati fino alla gestione proattiva delle minacce prima che si diffondano.

Ancora più importante, l'AI può fornire ai responsabili della sicurezza un sistema di supporto in tempo reale durante un incidente. I modelli di apprendimento automatico, addestrati su dati relativi ad attacchi precedenti, possono infatti suggerire azioni basate su eventi simili già affrontati in passato.

Con l'integrazione dell'elaborazione del linguaggio naturale negli strumenti di sicurezza informatica, gli analisti possono interagire direttamente con i sistemi, individuare le minacce e distribuire soluzioni.

L'AI può inoltre monitorare i modelli comportamentali per segnalare quando un analista umano commette errori ripetuti, magari dovuti alla stanchezza, e suggerire un cambio di turno o l'intervento di un collega con una mente più fresca.

Sebbene gli strumenti di sicurezza informatica stiano integrando rapidamente funzionalità di AI sempre più avanzate, molte delle capacità più potenti sono ancora in fase di sviluppo. È importante ricordare che, al momento, l'AI non può sostituire le competenze di un professionista esperto, ***soprattutto di qualcuno che ha già affrontato in prima persona un attacco***.

Suggerimenti per sfruttare l'AI:

Comprendi in che modo gli strumenti possono aiutare le operazioni di sicurezza

Analizza in dettaglio gli strumenti di AI e implementali dove possono essere più utili. Alcuni risultati immediati possono riguardare il rilevamento delle minacce avanzate, l'automazione delle attività ripetitive e l'uso dell'AI nella gestione delle identità.

> Avere un partner che si occupi di risposta agli incidenti, correzione e ripristino su base continuativa è una best practice."
>
> ***Jason Rosselot***
> *VP, Cybersecurity and Business Unit Security Officer, Dell Technologies*

Pianifica il futuro dell'AI

Scopri quando saranno rese disponibili nuove funzionalità, valuta i benefici per il tuo team e sviluppa un piano per adottarle in modo strategico.

Integra l'AI nella pianificazione della forza lavoro

Con l'automazione e la relativa riduzione delle attività manuali, la composizione del team di sicurezza potrebbe richiedere modifiche. Ti serviranno risorse di livello più alto, capaci di analizzare e agire sulle informazioni di sicurezza, non solo di raccoglierle. Adatta di conseguenza le tue strategie di assunzione e sviluppo delle competenze.

L'AI diventerà presto una parte essenziale delle tue operazioni di sicurezza informatica, se non lo è già. Ricorda però che l'esperienza e le competenze di un professionista qualificato sono insostituibili. L'obiettivo deve essere usare l'AI per automatizzare le operazioni e rendere le risorse umane più efficaci, grazie alla prevenzione degli attacchi e alla riduzione del loro impatto quando si verificano.

Miglioramento della maturità della sicurezza informatica: un passo alla volta

Come in ogni ambito della sicurezza informatica, gestire il fattore umano è un viaggio, non una destinazione. Anche i progressi graduali e i piccoli passi fanno la differenza e si accumulano nel tempo. È importante ricordare che anche la tecnologia e gli strumenti di sicurezza più avanzati sono efficaci solo nella misura in cui lo sono le persone che li utilizzano.

DELL Technologies

Prodotti e soluzioni Dell utili

Soluzione consigliata Dell	Descrizione
Servizi di risposta agli incidenti	Un team di esperti di sicurezza informatica con certificazioni del settore a disposizione per fornire una risposta rapida in caso di attacco informatico. Lavoriamo fianco a fianco con te per eliminare le minacce fino al completo ripristino delle normali operazioni.
Servizi di consulenza per la sicurezza informatica	Esperti che ti aiutano a individuare e risolvere i punti deboli nella strategia di sicurezza, proteggere asset e dati e abilitare la vigilanza e la governance continue.
vCISO	Chief Information Security Officer virtuale ed esperto di sicurezza informatica in grado di aiutarti a identificare e gestire i rischi, oltre a guidarti nelle decisioni strategiche.
Managed Detection and Response	Riduce gli sforzi manuali e semplifica le operazioni quotidiane di sicurezza fornendo monitoraggio, rilevamento delle minacce, indagini e risposte rapide in tutti gli endpoint, la rete e il cloud. I clienti scelgono la loro piattaforma XDR preferita (Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR o Microsoft Defender XDR) e ricevono indicazioni da parte di esperti, report trimestrali e fino a 40 ore di risposta agli incidenti annuali.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi su **dell.com/cybersecuritymonth**