4 modi in cui Microsoft Sentinel gestisce le principali preoccupazioni in materia di sicurezza IT

Massimizza i vantaggi e le capacità
del tuo investimento nella sicurezza.

Insight Microsoft

Esecuzione di un sondaggio sul panorama delle minacce

Per gestire con successo un SOC (Security Operations Centre), è fondamentale trovare la giusta combinazione di strumenti, tecnologie e set di competenze. Ciò è particolarmente vero in seguito al recente rapido aumento del volume degli attacchi informatici. Tieni presente che nel 2021 il costo medio di una violazione causata dal ransomware è stato di 4,62 milioni di dollari.[1] Questo comporta una grande quantità di danni potenziali. Quindi non sorprende che i team addetti alla sicurezza IT di tutto il mondo stiano facendo pressioni per migliorare i tempi di risposta e prevenire perdite future.

Per contrastare questa tendenza in evoluzione, nel 2022 le aziende dovrebbero spendere in media 24,4 milioni di dollari per il budget per la sicurezza IT.[2] Coloro che cercano di ospitare i dati on premise e nel cloud dovranno rivalutare le proprie soluzioni esistenti per garantire una copertura completa in tutte le sedi operative, gli uffici domestici, i sistemi di comunicazione e ogni altro luogo.

La crescita degli endpoint e dei volumi di dati richiede una sicurezza scalabile.

Le soluzioni puntuali offrono un ambito limitato e ulteriori difficoltà di integrazione.

Trovare e trattenere i talenti chiave nel settore della sicurezza è diventato più difficile.

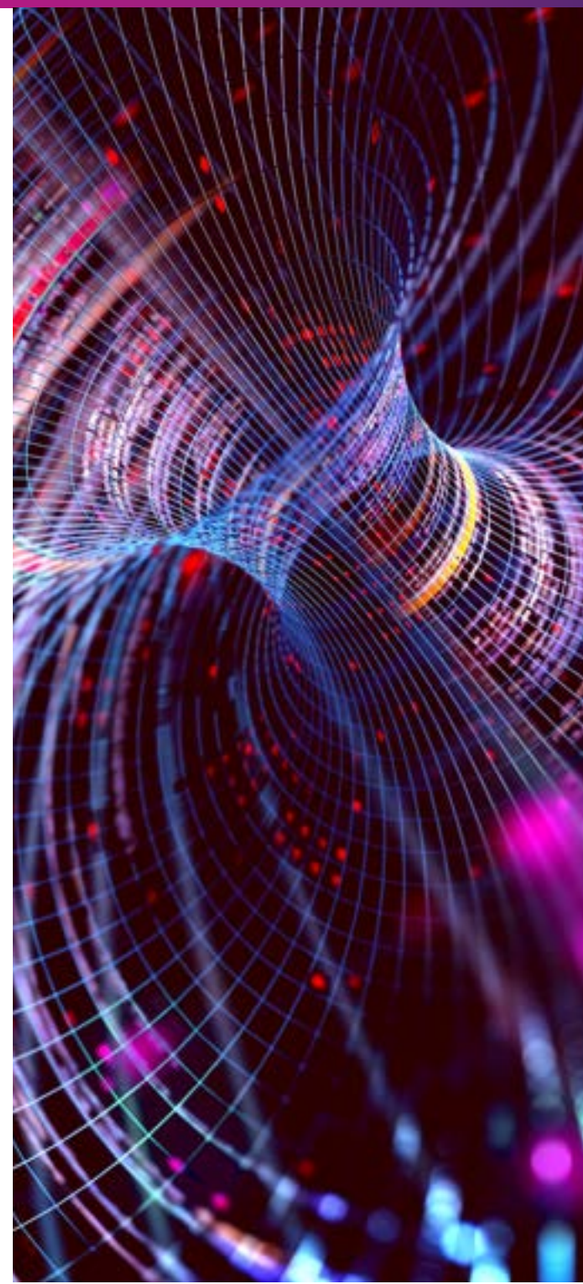
Inoltre, la complessità degli ambienti IT aumenta costantemente con un numero infinito di vettori di attacchi.

Pensa ai tuoi dati, ai tuoi utenti e ai tuoi sistemi.

Avere una visibilità completa è fondamentale per rilevare e contrastare potenziali danni, oltre che per poter sfruttare più sistemi da un unico punto di partenza e ottenere il controllo dell'intero ambiente IT. Dato che le aziende impiegano in media 280 giorni per rilevare una violazione, una quantità infinita di dati, record e sistemi può essere compromessa prima ancora di intraprendere azioni per combattere l'intrusione. Un modo per migliorare la visibilità e ridurre questo roadblock è implementare la gestione delle identità e degli accessi. Essere in grado di tenere traccia delle tendenze del comportamento degli utenti per scoprire modelli può aiutare le aziende a ridurre la finestra di esposizione al rischio ed eliminare lacune che in precedenza non erano state notate.

Quando implementi la gestione delle identità e degli accessi, considera la possibilità di porre le seguenti domande:

- Quanto sono sensibili i tuoi dati?
- Chi ha una reale necessità di accedere a specifici file?
- Quando e per quanto tempo è necessario questo accesso?
- È necessario avviare un programma di classificazione dei dati?
- Hai definito dei tipi di utente?
- Quando hai eseguito l'ultima revisione delle autorizzazioni?
- Come verifichi le identità e i punti di accesso?
- Quali alternative di autenticazione hai preso in considerazione?
- La biometria potrebbe essere una scelta valida?
- Hai notato lacune o schemi palesi?
- Come potresti trasformare il tuo approccio attuale in uno più sicuro?



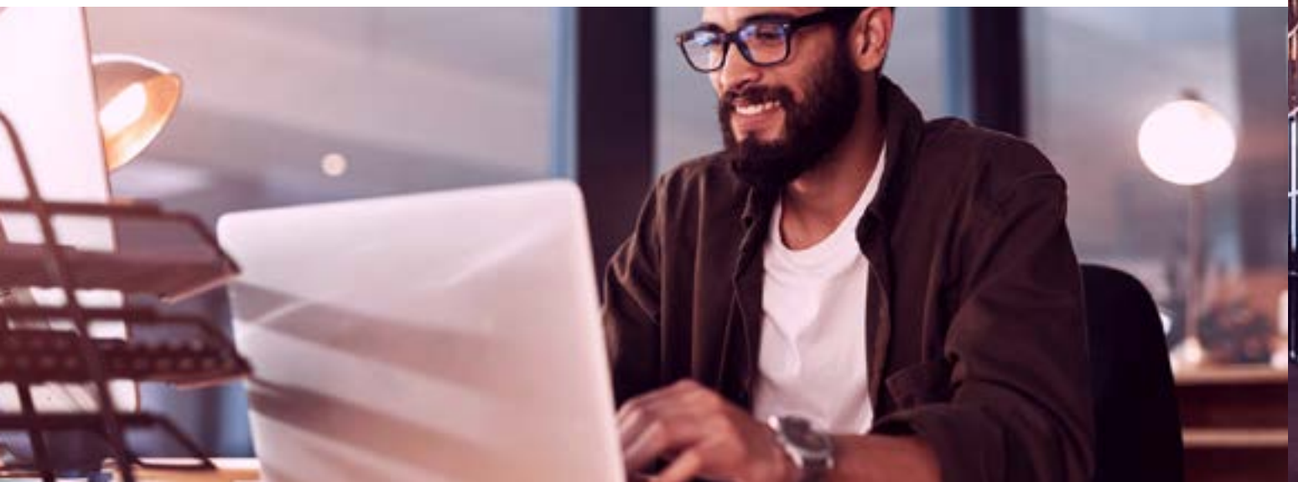
Realizzazione di un moderno programma di sicurezza

Può essere utile ricordare che l'89% delle aziende ha già adottato, o sta pianificando di adottare, un approccio multicloud.[4] Se la tua azienda fa parte di questa maggioranza, potresti avere a disposizione un ambiente IT diversificato. Essere in grado di monitorare con successo i dati, gli hacker dannosi e altro ancora, migliorerà l'efficacia del lavoro di prevenzione svolto dal tuo team addetto alla sicurezza IT. Un'altra importante caratteristica di un programma solido è una governance completa in grado di gestire proprietà e responsabilità. Definendo obiettivi, ruoli e processi di sicurezza, le aziende possono organizzare meglio linee guida e formazione, nonché convalidare utenti e processi.

Un'altra considerazione da tenere presente è che il 57% delle aziende intervistate nel report "The State of IT Modernisation 2020" ha affermato che l'aggiornamento delle infrastrutture e dei processi di sicurezza si è rivelato un forte ostacolo al lavoro di modernizzazione dei propri ambienti operativi IT.[3] Questo è quindi l'ambito in cui un partner di terze parti può essere in grado di fornire valore aggiunto tramite servizi di automazione.

L'automazione all'interno del SOC offre:

- Funzionalità di rilevamento, risposta e correzione più rapide
- Meno errori e riduzione della "desensibilizzazione agli alert"
- Risorse di sicurezza non più sottoposte ad attività ripetitive
- Miglioramento della soddisfazione e dell'esperienza utente



Investire in una soluzione SIEM nativa del cloud

Microsoft® Microsoft Sentinel® è una soluzione SIEM (Security Information and Event Management) e SOAR (Security Orchestration Automation and Response) nativa del cloud fornita come servizio cloud. Grazie alla sua capacità di fornire analisi di sicurezza intelligente per l'intero ambiente, le aziende possono bloccare le minacce prima che causino danni. Come soluzione scalabile adatta a ogni situazione, Microsoft Sentinel migliorerà o sostituirà i tuoi strumenti di sicurezza esistenti per aumentare la visibilità sul tuo panorama delle minacce.

- Acquisisci una visione generale della tua intera attività.
- Semplifica il rilevamento e la risposta con l'intelligenza artificiale (IA).
- Elimina il lavoro di configurazione e manutenzione dell'infrastruttura di sicurezza.
- Ottieni la scalabilità necessaria per soddisfare le necessità di sicurezza in evoluzione.

Come ulteriore vantaggio, questa soluzione riduce fino al 48% i costi e può essere distribuita il 67% più velocemente rispetto ai sistemi SIEM tradizionali.[5] Di conseguenza, le aziende possono dedicare più tempo alla rapida ricerca di minacce reali eseguendo operazioni di sicurezza più strategiche. Quindi come funziona esattamente? In che modo utilizza l'IA e il machine learning per rilevare, analizzare e studiare le minacce? Approfondiremo il processo in quattro passaggi nella pagina successiva.

4 passaggi per le operazioni di sicurezza di prossima generazione

1. Raccogliere

Oggi le aziende ospitano documenti, dati, record e molto altro su una moltitudine di dispositivi, applicazioni e infrastrutture, sia on premise che su più cloud. Inoltre, tutti questi file sensibili sono accessibili agli utenti pressoché in qualsiasi momento e ovunque. Microsoft Sentinel® raccoglie dati su scala cloud, aggregando infrastrutture
e dispositivi di sicurezza come i firewall.

2. Rilevare

Trovare eventi regolari e modelli di attacchi informatici può aiutare le aziende a bloccare le minacce. L'analisi e l'ineguagliabile intelligence sulle minacce aiutano le aziende a scoprire anche le minacce precedentemente non rilevabili e a ridurre al minimo le possibilità di falsi positivi. Immagina di essere in grado di monitorare e correlare contemporaneamente milioni di anomalie e quindi di ricavare rapidamente valore dal report. Questo è ciò che offre questa soluzione.

3. Indagare

Grazie ai decenni di lavoro nella sicurezza informatica svolto da Microsoft, Sentinel ricerca attività sospette su larga scala con la guida dell'IA, eliminando la necessità di hardware o macchine virtuali. Impara dai registri giornalieri come eliminare il rumore, in modo che i team addetti alla sicurezza possano concentrarsi sui segnali essenziali.

4. Rispondere

Con l'orchestrazione integrata e l'automazione delle attività comuni, le aziende possono rispondere rapidamente agli incidenti. Sfruttando la tecnologia intelligente, il tuo team addetto alla sicurezza IT non farà solamente risparmiare tempo, ma migliorerà anche la precisione. Ad esempio, all'interno di Microsoft Sentinel possono essere eseguiti playbook attivati da regole di analisi o automazione, per semplificare i tempi di risposta e bloccare i malintenzionati.

Perché Insight per Microsoft Sentinel?

Noi di Insight crediamo che non ci sia mai stato un momento più adatto per migliorare il tuo livello di sicurezza, soprattutto con l'aumento del lavoro da remoto e ibrido. Affidati ai nostri anni di esperienza per proteggere la tua azienda dalle minacce informatiche in evoluzione. Insieme, aiuteremo la tua azienda a realizzare una soluzione flessibile e scalabile che sfrutti funzionalità di IA e machine learning all'avanguardia. Obiettivo: migliorare la sicurezza, la visibilità e il controllo dell'intero ambiente IT.

Siamo uno dei principali partner Microsoft e uno dei soli 12 partner pubblicamente indicati da Microsoft per la consulenza e la fornitura di servizi Microsoft Sentinel®:

- 18 competenze Microsoft Gold e Silver
- Partner Microsoft da oltre 25 anni
- Oltre 1.000 tecnici e professionisti dell'assistenza dedicati ad Azure
- Un provider di managed services (MSP) di Azure Expert e il più grande partner di Azure
- Vincitore del premio Microsoft Security 20/20 per la categoria Azure Security Deployment Partner of the Year
- Supporto ovunque e distribuzione di servizi di consulenza

Informazioni su Insight

Insight Enterprises, Inc. è un solution integrator nella lista Fortune 500 con 11.500 colleghi sparsi in tutto il mondo che aiutano le aziende ad accelerare il loro percorso digitale per modernizzare le proprie attività e massimizzare il valore della tecnologia. Aiutiamo a effettuare una trasformazione end-to-end sicura e soddisfiamo le necessità dei nostri clienti con un portafoglio completo di soluzioni, partnership di vasta portata e oltre 33 anni di ampia esperienza nel settore IT. Premiati come miglior datore di lavoro al mondo secondo Forbes e certificati come Great Place to Work, amplificheremo le nostre soluzioni e i nostri servizi su scala globale, competenza locale ed esperienza di e-commerce di livello mondiale, realizzando le ambizioni digitali dei nostri clienti in ogni occasione.

Insight®

it.insight.com

Fonti:

[1] IBM Security. (2021). Cost of a Data Breach Report.

[2] Channel Futures. (Febbraio 2022). The High Cost of Ransomware.

[3] Insight. The State of IT Modernisation 2020.

[4] Flexera. (Marzo 2022). 2022 State of the Cloud Report.

[5] Forrester. (Novembre 2020). The Total Economic Impact™ of Microsoft Microsoft Sentinel. Cost Savings and Business Benefits Enabled By Microsoft Sentinel.

MKT6231