Risoluzione delle sfide chiave per gli ambienti di sicurezza multi-vendor

Una guida che illustra come superare il burnout correlato alla sicurezza e rafforzare le difese con Insight e Microsoft Sentinel

Sicurezza sotto stress

degli intervistati della CISO Benchmark Survey 2020 di Cisco afferma di soffrire di affaticamento da sicurezza informatica (definito praticamente come una rinuncia alla difesa proattiva contro i malintenzionati).

Tra coloro che ne soffrono, il **93% riceve più di**

5.000 **alert al giorno,**

e ciò indica che la complessità sembra essere una delle principali cause di burnout correlato alla sicurezza.[1]

Per gestire un ambiente di minacce complesso, la maggior parte delle aziende impiega varie soluzioni di sicurezza. Tuttavia gestire e orchestrare gli alert provenienti da varie fonti non è solo impegnativo, ma espone anche le aziende a rischi maggiori.

Un eccessivo numero di alert significa che potrebbero essercene troppi da affrontare, con un impatto sulla consapevolezza e sulla visibilità del team e potenzialmente esponendo l'azienda a minacce più grandi e più dannose lungo il percorso.

Secondo Fady Younes, direttore della sicurezza informatica di Cisco, "La mancata integrazione di più soluzioni di sicurezza può anche lasciare lacune nella copertura o creare una situazione in cui il team IT non comprende correttamente quale protezione una particolare soluzione offra o come funzioni, influenzando la visibilità e la consapevolezza del vero stato di sicurezza della rete".[2]

In questi ambienti risulta meno chiaro sapere a quali rischi e alert dare la priorità.

Non tutti gli alert sono della stessa gravità e le migliori strategie di sicurezza personalizzano i controlli di sicurezza e allocano le risorse in base al livello di rischio.

In ambienti multicloud differenziati, il ripristino di emergenza diventa incredibilmente complesso, pertanto richiede l'adozione di una cultura di gestione della security proattiva e non reattiva.

"Affrontare le problematiche di integrazione e un elevato volume di alert di sicurezza può distrarre i tecnici addetti alla sicurezza dall'affrontare altre sfide che devono gestire..."

- Fady Younes, direttore della sicurezza informatica per Medio Oriente e Africa presso Cisco

SIEM e SOAR

I team addetti alla sicurezza hanno due obiettivi principali: sapere cosa succede nei loro ambienti IT e rispondere a tali informazioni. Le soluzioni SIEM (Security Information and Event Management) e SOAR (Security Orchestration, Automation, and Response) consentono di raggiungere questi obiettivi.

Gli strumenti SIEM raccolgono e aggregano i dati degli eventi provenienti da varie fonti all'interno di un ambiente IT, quindi analizzano e classificano gli eventi in ordine di priorità o criticità. I team addetti alla sicurezza sono responsabili della ricerca e della risposta alle minacce, nonché della messa a punto e della correzione della piattaforma SIEM.

Gli strumenti SOAR forniscono funzioni di analisi e automazione avanzate basate sulle capacità degli strumenti SIEM, per una risposta alle minacce più autonoma. Gli strumenti SOAR sfruttano il maggior numero possibile di dati in tempo reale e sono sensibili alla competenza dei manager: questi strumenti risultano più o meno efficaci a seconda del modo in cui vengono utilizzati.

afferma che SOAR è molto o estremamente importante per il livello di sicurezza complessiva della propria azienda.

Principali casi d'uso per SOAR:

- 65% Triage di SIEM
- 62% Attacchi di phishing
- 62% Intelligence sulle minacce

Esiti delle distribuzioni di SOAR:

- Risoluzione degli incidenti più rapida
- Maggiore efficienza del personale
- Riduzione dei costi complessivi[3]

Che cosa contraddistingue Microsoft Sentinel?

SOAR è la funzionalità di Sentinel che gli permette di distinguersi dalla concorrenza. Consente ai team addetti alla sicurezza di scrivere codice o playbook all'interno di Sentinel per rispondere automaticamente alle minacce man mano che si presentano, aiutando il team del SOC a ridurre la desensibilizzazione agli alert e a concentrarsi sulle cose che necessitano realmente di attenzione.

Ai nostri clienti piace molto poter correlare in modo incrociato alert e incidenti, tracciando una mappa di ogni incidente associato a un'entità specifica. Quello che in genere mostro ai clienti in una demo è uno scenario in cui un utente malintenzionato ha ottenuto l'accesso all'ambiente, aumentato i propri privilegi, eseguito un download di massa di dati aziendali e quindi eliminato il proprio account. Si tratta di quattro alert separati che qualsiasi soluzione SOAR o SIEM fornirebbe. Tuttavia all'interno di Microsoft Sentinel puoi vedere un grafico di un'entità con quattro differenti linee per ogni avviso generato, nonché una cronologia di tali eventi. Microsoft Sentinel semplifica davvero la caccia alle minacce."

- Consulente associato, InfoSec, Insight

Il caso di Microsoft Sentinel

Microsoft Sentinel™ combina la potenza di un sistema SIEM e di una soluzione SOAR in un'unica soluzione. Se hai già investito in Microsoft® Sentinel, sei sulla strada giusta verso una sicurezza più solida.

La piattaforma Sentinel può aiutarti a:

Identificare le minacce prima che abbiano effetti sulla tua organizzazione.

Rispondere rapidamente e con maggiore precisione.

Semplificare la sicurezza in ambienti ibridi, multicloud, privi di server e altri ambienti moderni.

Ridurre i costi rispetto alle soluzioni SIEM legacy per l'esame di minacce, licenze, storage, infrastrutture, gestione e distribuzione.

Lo strumento sfrutta la profonda esperienza di Microsoft nella sicurezza e le più recenti capacità di intelligenza artificiale e funziona senza problemi insieme ad altri prodotti Microsoft. È veloce da configurare e facile da scalare.

Un hub, molti punti dati

Con Microsoft Sentinel, gli ambienti delle soluzioni multi-vendor diventano meno complessi da gestire. La capacità di Sentinel di estrarre le fonti di dati dall'intero ecosistema di soluzioni di sicurezza multi-vendor offre alle aziende la visibilità e il controllo necessari per semplificare la ricerca delle minacce, ridurre la desensibilizzazione agli alert e acquisire un quadro reale del tuo livello di sicurezza.

Best practice per l'implementazione

Iniziare a utilizzare Microsoft Sentinel è relativamente semplice. Prima dell'implementazione, ti consigliamo di stabilire una governance e politiche chiare. Le considerazioni da fare comprendono gli standard di conformità, i requisiti di costo, i piani di storage, il ripristino di emergenza, il personale del team addetto alla sicurezza e i piani di risposta agli incidenti.

Giorno 1:

Abilita Microsoft Sentinel.

Collega le fonti di dati.

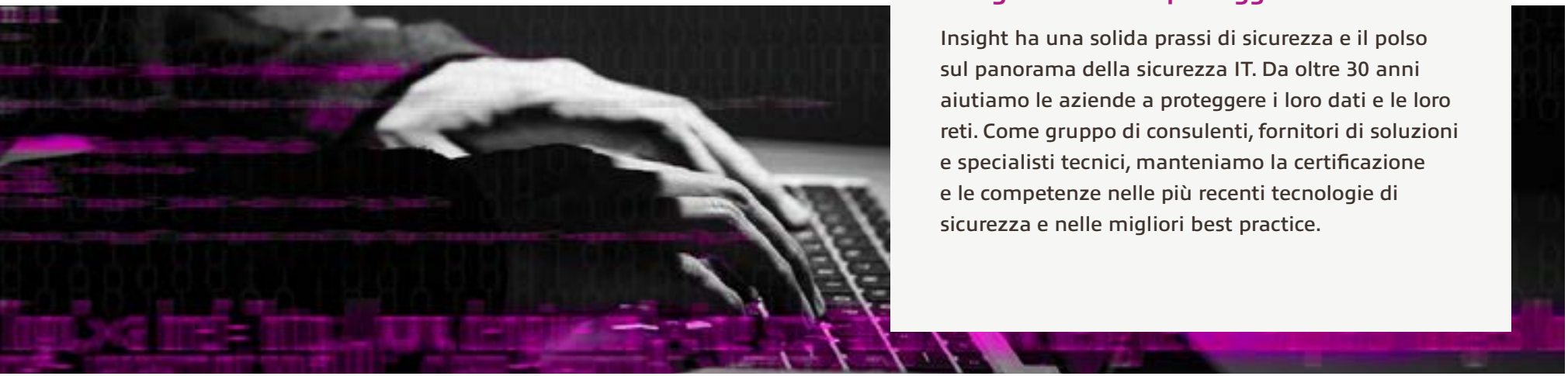
Inizia a creare query per indagare sui dati.

Come molti altri strumenti SIEM, Syslog e CEF fungono da punti di acquisizione. Puoi utilizzare la tua distribuzione di Linux® preferita, compresa quella di Microsoft, e installare i sistemi di inoltro di CEF e Syslog per inoltrare i registri a Microsoft Sentinel per l'acquisizione.

Microsoft ha creato Sentinel perché sia in grado di ospitare anche i registri di formattazione generici in un formato di eventi comune, in modo che anche i registri di dispositivi legacy o specializzati possano essere integrati e analizzati.

Proteggi l'intera attività.

Microsoft Sentinel risulta più efficace quando fa parte di un approccio più ampio e programmatico alla sicurezza informatica. Verifica che la tua azienda segua le best practice nell'intero ambito della sicurezza informatica: Identifica, proteggi, rileva, rispondi e ripristina.



LA SOLUZIONE DI INSIGHT

Mitiga il rischio e proteggi la tua azienda.

Insight ha una solida prassi di sicurezza e il polso sul panorama della sicurezza IT. Da oltre 30 anni aiutiamo le aziende a proteggere i loro dati e le loro reti. Come gruppo di consulenti, fornitori di soluzioni e specialisti tecnici, manteniamo la certificazione e le competenze nelle più recenti tecnologie di sicurezza e nelle migliori best practice.

Giorno 2+:

A questo punto, la flessibilità e la dinamicità della piattaforma saranno evidenti. Ecco alcuni modi in cui puoi massimizzare notevolmente i vantaggi di Microsoft Sentinel per le necessità e il profilo di rischio specifici della tua azienda.

1.

Controlla il sistema di inoltro dei registri.

Se non presti una stretta attenzione allo stato del sistema di inoltro dei registri e alla capacità della tua directory di registri VAR, il sistema può bloccarsi rapidamente con l'interruzione dell'acquisizione dei registri. Quando i consulenti di Insight eseguono la distribuzione di Microsoft Sentinel, utilizzano le distribuzioni di Linux con una partizione per il punto di montaggio dei registri VAR separato dal sistema operativo. In questo modo, se la directory si riempie, ciò non ha gravi effetti sul sistema operativo.

2.

Osserva i tuoi tassi di acquisizione.

Stimare il numero di registri che puoi acquisire all'inizio è difficile, ma dopo un mese o due disporrai di una quantità sufficiente di dati storici per supportare un migliore processo decisionale per un tasso di acquisizione dei dati appropriato. Questo ti aiuterà a ottenere un rapporto risultati/costi migliore.

3.

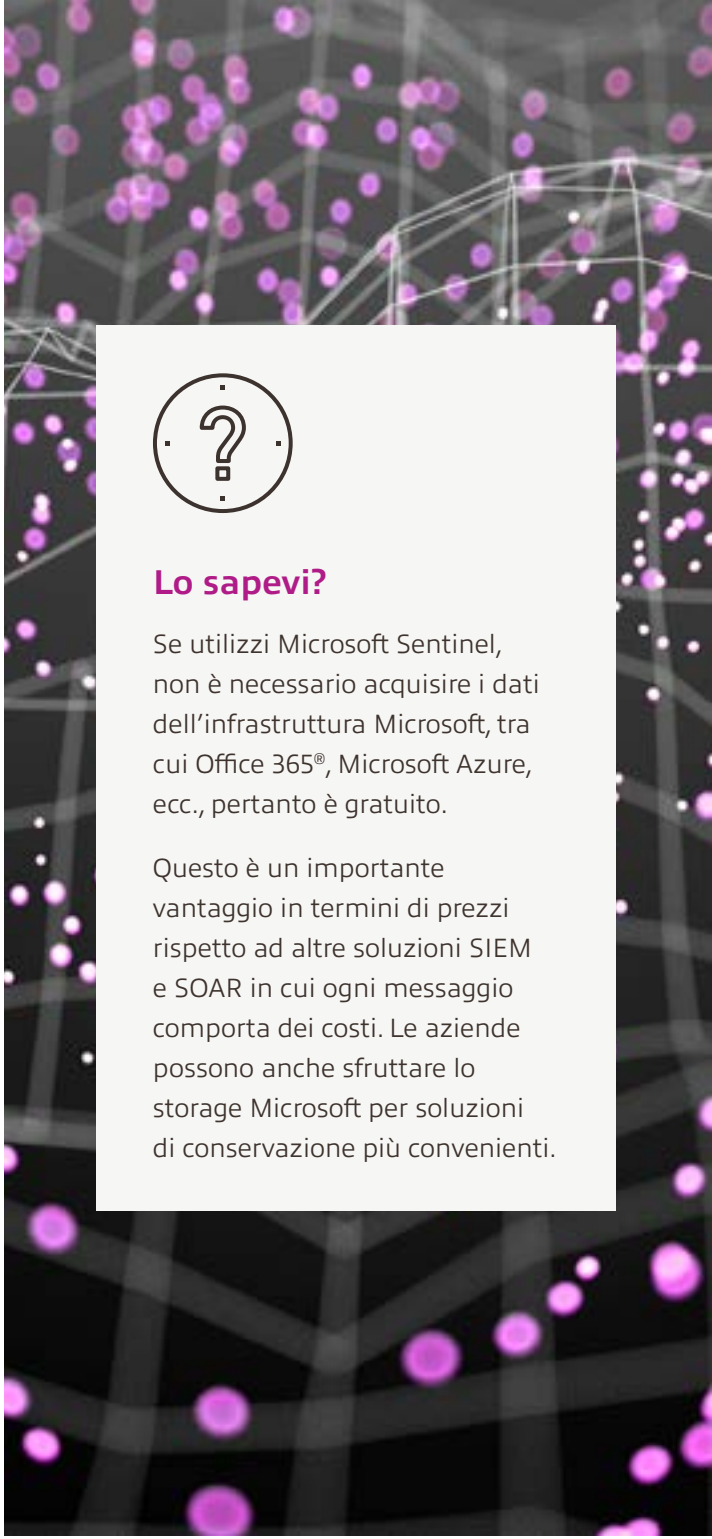
Riduci al minimo i falsi positivi.

Molte delle regole pronte all'uso che creano report sulle funzioni amministrative tramite l'analisi del comportamento possono generare falsi positivi. Microsoft ha pubblicato una funzionalità di Sentinel chiamata Watchlist che aiuta a ridurre questi falsi positivi, il rumore risultante e la desensibilizzazione agli alert. Watchlist consente di inserire query in regole di analisi che esaminano una watchlist, o una coppia di identificatori chiave, senza però inviare alert per specifiche attività.

4.

Utilizza un tenant centralizzato.

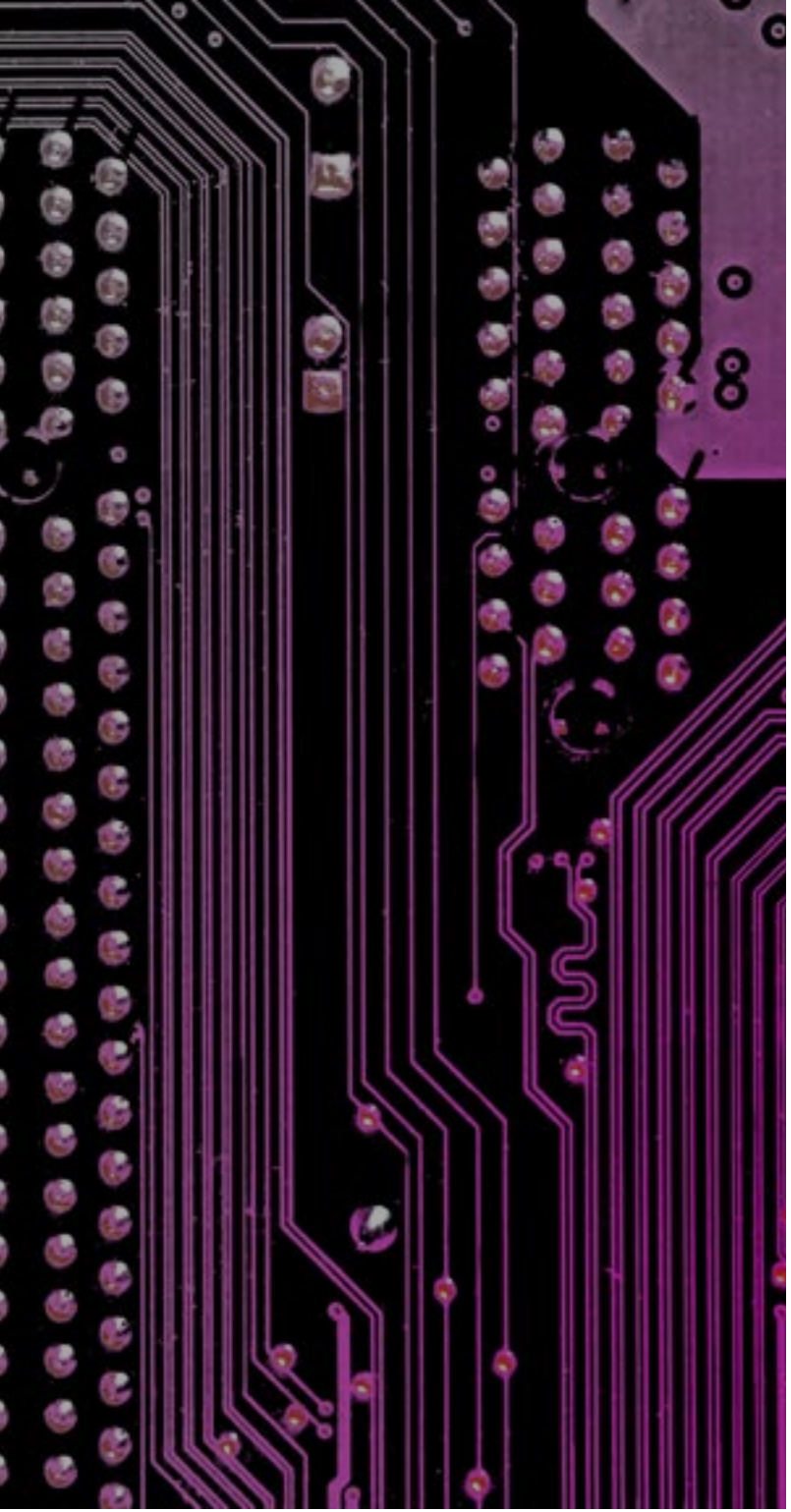
Se stai monitorando più tenant di Azure® differenti, devi creare più installazioni di Microsoft Sentinel e registrare le aree di lavoro di analisi in ognuno di tali tenant. Utilizzando Azure Lighthouse per monitorare queste aree di lavoro in un tenant centralizzato, puoi ottimizzare le regole analitiche, arrivare alla fonte della verità e distribuire le regole a tutti i tenant. Ciò ti aiuterà a stabilire una linea base coerente per le soglie, la frequenza di esecuzione e altre impostazioni.



Lo sapevi?

Se utilizzi Microsoft Sentinel, non è necessario acquisire i dati dell'infrastruttura Microsoft, tra cui Office 365®, Microsoft Azure, ecc., pertanto è gratuito.

Questo è un importante vantaggio in termini di prezzi rispetto ad altre soluzioni SIEM e SOAR in cui ogni messaggio comporta dei costi. Le aziende possono anche sfruttare lo storage Microsoft per soluzioni di conservazione più convenienti.



5.

Esegui un detuning pronto all'uso.

Microsoft Sentinel offre il grande vantaggio di integrarsi senza problemi con il tuo ecosistema Microsoft. I nostri consulenti consigliano regolarmente ai clienti di utilizzare Microsoft Defender for Identity (MDI) per Active Directory® (AD) on premise, ad esempio. Tuttavia, quando colleghi MDI a Sentinel, l'impostazione predefinita inoltra automaticamente tutti gli alert provenienti da MDI. Probabilmente preferirai accedere al connettore plug-in ed eseguire il detuning in modo da non ricevere alert non urgenti e ricevere solo quelli che rientrano in un intervallo di gravità specificato.

Esamina anche le gravità delle regole analitiche esistenti e inoltrale, ridimensionale o rimuovile a seconda delle tue necessità. Molte regole analitiche pronte all'uso vengono eseguite con una frequenza preimpostata che potrebbe risultare eccessiva da gestire. Ti consigliamo di utilizzare regole analitiche eseguite ogni 15 o 30 minuti per gli alert a elevata gravità oppure solo una volta al giorno per gli alert a bassa gravità o informativi che non hanno grandi effetti sull'azienda. Infine, il detuning ti aiuterà a ridurre al minimo la desensibilizzazione e il rumore causati dagli alert.

6.

Valuta l'equivalente.

Che cosa hai utilizzato per proteggere il tuo ambiente IT prima di Microsoft Sentinel? Quali sono le somiglianze e le differenze? I nostri consulenti consigliano di osservare fianco a fianco il tuo vecchio sistema e l'ambiente Microsoft Sentinel e di confrontare output visivi, dashboard, alert, fonti di registri e altri attributi chiave per assicurarti di ottenere l'equivalente. Nessuna fonte di dati deve essere trascurata. Questo ti aiuta anche a comprendere appieno il nuovo ambito delle attività quotidiane, la cura e la fornitura e i requisiti relativi al personale per supportare la nuova piattaforma.

7.

Considera le indicazioni di Microsoft.

Microsoft ha pubblicato raccomandazioni per le normali attività da svolgere al fine di garantire che Sentinel possa offrirti la migliore sicurezza possibile. Consultale per ottenere suggerimenti su attività quotidiane, settimanali e mensili, integrazioni da configurare e processi per la gestione e la risposta agli incidenti.

Opportunità di automazione

Uno dei punti di forza della piattaforma Microsoft Sentinel è rappresentato dalle sue capacità di automazione. Sfrutta l'automazione per ottenere efficienza e sicurezza ottimali.

Ecco un paio di modi per automatizzare con Microsoft Sentinel:

Fidelizzazione

Ogni organizzazione ha necessità in materia di conservazione dei dati che differiscono a seconda dei requisiti di settore, legali e di compliance. Microsoft Sentinel offre la possibilità di automatizzare lo storage per periodi di tempo prestabiliti, rendendo incredibilmente facile per il tuo team spuntare questa casella senza dover impostare promemoria o preoccuparsi della capienza.

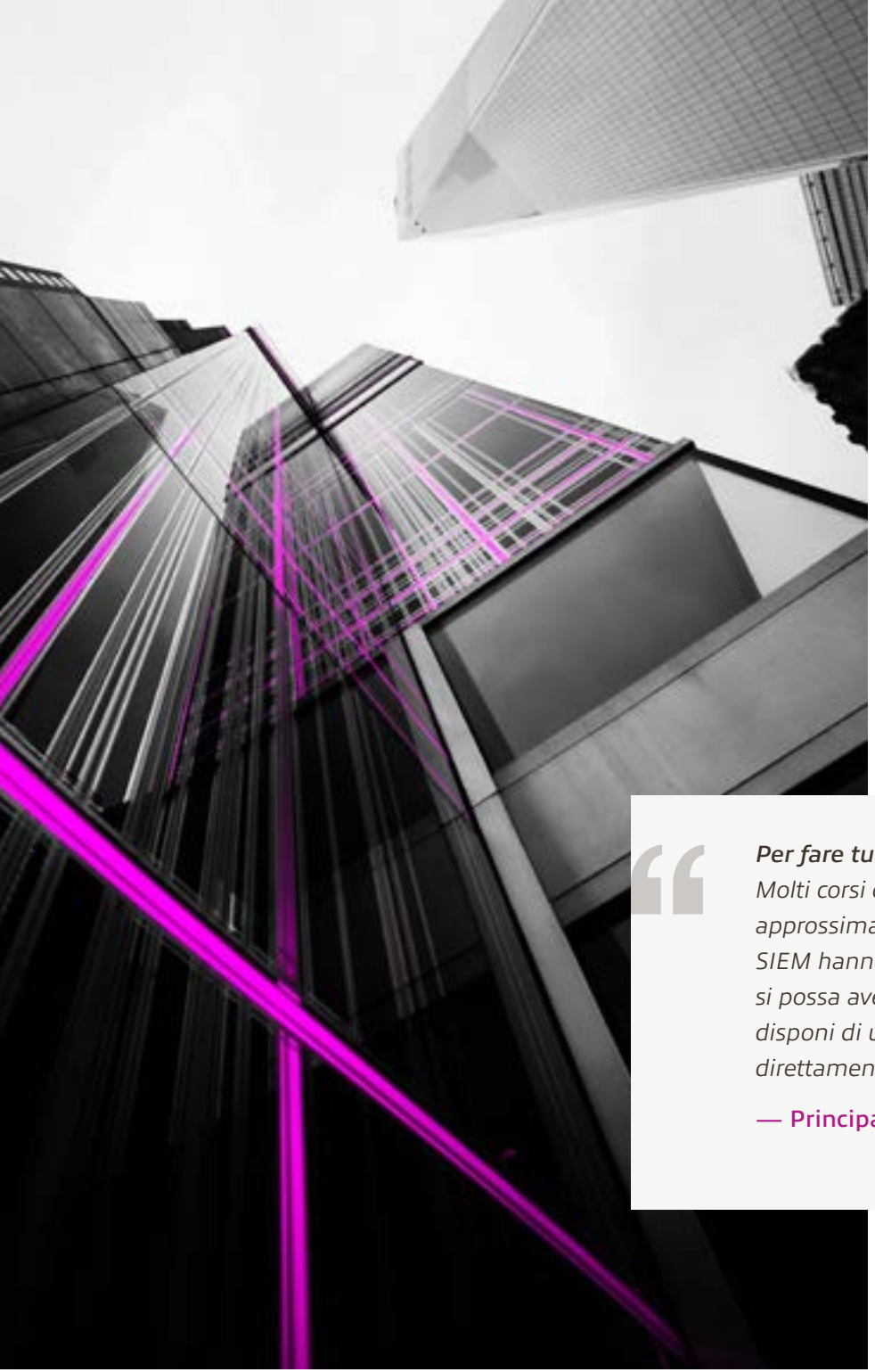
Playbook

I playbook sono un'opzione eccellente per le automazioni più complesse. I playbook di Microsoft Sentinel possono essere configurati per una serie di attività tra cui:

- Blocco di un utente dopo un alert di accesso non riuscito
- Creazione di un incidente ServiceNow® che viene acquisito nel sistema di emissione dei ticket
- Modifica del CMDB in ServiceNow in caso di modifiche ai dispositivi bloccati sulla rete

Su GitHub di Microsoft sono disponibili molti playbook e molte idee di personalizzazione, oltre ad automazioni specifiche per i fornitori da poter esplorare in Microsoft Sentinel.

> ***Abbiamo clienti che desiderano conservare i dati per sette anni per HIPAA oppure per un anno per motivi di conformità normativa governativa o NIST. Capire quale schema di conservazione funzioni meglio per un'azienda è una sfida.*** *Blob Storage di Microsoft è una buona opzione, poiché consente di conservare i registri in modo conveniente fino a sette o otto anni. Per semplificare questo processo, creiamo app logiche di Azure che spostano automaticamente i registri acquisiti da Microsoft Sentinel a Blob Storage perché siano conservati per sette anni. Le azienda mantengono l'accesso ai registri nell'eventualità che sia necessario consultarli per un'indagine o una ricerca sulla sicurezza."*
>
> **— Consulente associato, InfoSec, Insight**



Guardiamo al futuro

Esistono molti modi per espandere e migliorare Microsoft Sentinel e queste opportunità continuano ad aumentare man mano che la piattaforma e la comunità di utenti maturano.

BYO ML

Bring Your Own Machine Learning (BYO ML) è un ambito che sta attirando molta attenzione. Questa pagina di GitHub di Microsoft funge da archivio per le informazioni più recenti e da libreria di notebook di formazione di esempio in fase di crescita. Le aziende utilizzano BYO ML per avviare Databricks e distribuire formazione e analisi mediante un ambiente Spark che estrae tutti i dati da Sentinel, per creare modelli per accessi remoti o comportamenti anomali e molto altro ancora.

> ***Per fare tutto questo, non è necessario aver conseguito un dottorato di ricerca.*** *Molti corsi di formazione e molti modelli basati sulla comunità sono una buona approssimazione che deve solo essere personalizzata per il tuo ambiente. Altre soluzioni SIEM hanno qualcosa di simile a questo, ma per me è piuttosto interessante l'idea che si possa avere un'esperienza davvero nativa di Data Science, in cui sostanzialmente disponi di un notebook Jupiter, di un mucchio di librerie di dati Python ed estrai dati direttamente dall'ambiente in cui è in esecuzione il notebook."*
>
> **— Principal Architect (Cybersecurity, Networking, Data Science), Insight**

Visualizzazione avanzata

I workbook di Azure Monitor all'interno di Microsoft Sentinel offrono una visualizzazione avanzata dei dati. Naturalmente questo è estremamente utile per i team addetti alla sicurezza. La visualizzazione dei dati può facilitare l'identificazione dei punti deboli e delle vulnerabilità, aiutando i team addetti alla sicurezza ad assegnare le priorità. La visualizzazione può anche aiutare i team addetti alla sicurezza a giustificare i budget per la C-suite con un effetto rapido. Riteniamo che in futuro la visualizzazione dei dati sarà un obiettivo chiave, con comunità di utenti che sviluppano workbook personalizzati per soddisfare ogni necessità di sicurezza o aziendale.

LA SOLUZIONE DI INSIGHT

I consulenti dei nostri servizi di sicurezza possono aiutarti a valutare le implicazioni delle tue attività aziendali per la sicurezza e ad adottare soluzioni in linea con le tue necessità e i tuoi obiettivi. Iniziamo valutando il tuo ambiente attuale, le sfide e i requisiti.

Soluzioni di Managed service

A causa della mancanza di tempo e risorse, le aziende odierne sono solamente in grado di porre rimedio **50%** alle minacce alla legittima sicurezza.[1]

Molte aziende incontrano difficoltà nell'attrarre e nel trattenere professionisti esperti in materia di security che siano aggiornati sugli ultimi gruppi di strumenti SIEM, SOAR e SOC (Security Operations Center). Attualmente stiamo assistendo a un generale consolidamento dei questi talenti all'interno delle aziende fornitrici di servizi in grado di gestire con competenza gli ambienti di sicurezza, oltre a fornire supporto critico su gestione del ransomware, architettura di sicurezza e infine risposta e risoluzione degli incidenti.

In molti casi, la sfida principale è la gestione del tempo. Il compito di imparare come accrescere l'automazione o sfruttare il machine learning per migliorare la ricerca delle minacce può essere messo in secondo piano a causa delle innumerevoli richieste quotidiane di gestione di problematiche di security.

La chiave per amplificare la tua sicurezza? I managed services.

Insight offre servizi di sicurezza gestiti (Managed Security Services, MSS) che si basano sulle funzionalità di Microsoft Sentinel e assicurano il monitoraggio del tuo ambiente 24 ore su 24, 7 giorni su 7. Combinando le best practice consolidate nel settore con tecniche all'avanguardia per la minimizzazione dei rischi, aiutiamo i clienti a ridurre il pesante carico di lavoro di assistenza e a migliorare un ambiente di sicurezza dinamico.

Un approccio avanzato.

I consulenti dei nostri servizi di sicurezza possono aiutarti a valutare le implicazioni delle tue attività aziendali per la sicurezza e ad adottare soluzioni in linea con le tue necessità e i tuoi obiettivi. Iniziamo valutando il tuo ambiente attuale, le sfide e i requisiti.

16 anni
di esperienza nella gestione di incidenti e minacce

Oltre 1.500
architetti, ingegneri ed esperti in materia di sicurezza e distribuzione di servizi

Risultati di sicurezza gestiti:

- Tempi di risposta più rapidi
- Governance e compliance più solide
- Contesto e visibilità completi
- Rilevamento migliorato delle minacce
- Riduzione del carico di lavoro del team addetto alla sicurezza

Non ci sono limiti

Microsoft Sentinel è facile da implementare, ma la sua corretta ottimizzazione richiede competenze aggiuntive.

Fortunatamente, ci sono pochi limiti a dove può portarti la piattaforma nel percorso verso la sicurezza completa e, con un team di fiducia come Insight, è più facile che mai scoprire il valore del tuo investimento. I nostri consulenti, tecnici e architetti hanno un'esperienza comprovata di Microsoft Sentinel in un'ampia varietà di ambienti client.

Indipendentemente dal tuo grado di maturità con Microsoft Sentinel, puoi sfruttare Insight per:

- Valutazione dell'ambiente di sicurezza attuale
- Valutazione della prontezza di Microsoft Sentinel
- Distribuzione, integrazione e personalizzazione di Microsoft Sentinel
- Servizi di sicurezza gestiti per gestire Microsoft Sentinel
- Ottimizzazione di Microsoft Sentinel e automazioni e messa a punto avanzata delle funzionalità

Contatta oggi stesso il nostro team per discutere delle tue necessità

Informazioni su Insight

Insight Enterprises, Inc. è un Solutions 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.

Per saperne di più, visita **it.insight.com**

Insight®

Fonti:
[1] Cisco. (2020). Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020. CISO Benchmark Survey.
[2] Younes, F. (21 gennaio 2021). Complexity Still Remains Cybersecurity Worst Enemy. Techeconomy.ng.
[3] Rockett, J. (25 giugno 2020). 2020 SOAR Report Highlights Key Drivers and Impacts. Swimlane.