IBM Security

# Sei miti relativi a SIEM

IBM

# Esame dei 6 miti relativi a SIEM

**Recentemente, hai analizzato le soluzioni SIEM? Perché le cose sono cambiate.**

Si dice che le soluzioni SIEM siano complesse – e, di conseguenza, adatte solo a organizzazioni di grandi dimensioni. Vero, alcune soluzioni SIEM rientrano nel gruppo “solo per gruppi aziendali”, ma questo mito trascura le soluzioni SIEM più all’avanguardia, progettate per aziende di tutte le dimensioni.

Non è un segreto che il settore della sicurezza informatica stia affrontando un’enorme carenza di competenze. Soluzioni di sicurezza – o di altro tipo – devono essere progettate per consentire l’efficienza sul lavoro, nonostante le risorse (probabilmente) limitate. Quando si prendono in considerazione le soluzioni SIEM moderne, si devono cercare opportunità per potenziare il  team di sicurezza e ottimizzare le risorse a disposizione.

Affronteremo i sei principali miti relativi alle soluzioni SIEM e indagheremo quali dovrebbero essere oggi le aspettative riguardo a una soluzione SIEM.

# Mito n°1

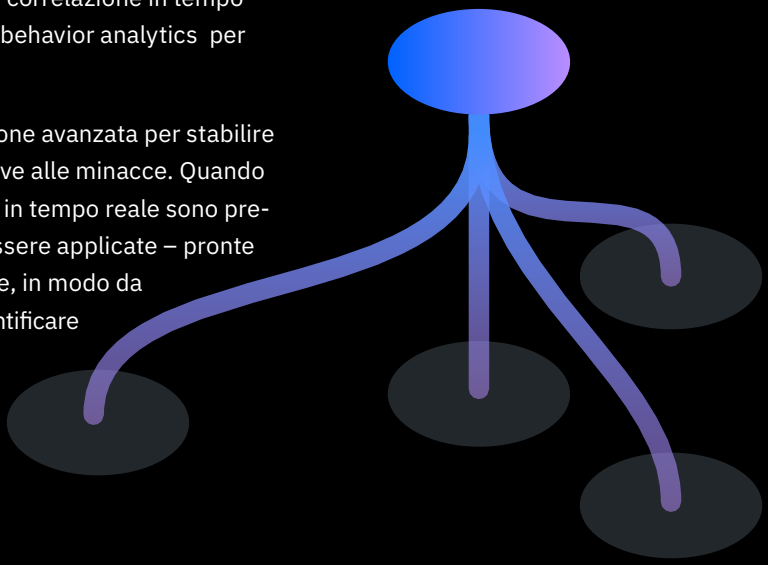
Una soluzione SIEM è in grado di rilevare solo minacce note; non è utile nel caso di minacce sconosciute.

Le soluzioni SIEM utilizzano solo la correlazione per rilevare le minacce e, per scrivere una regola di correlazione efficace, è necessario innanzitutto sapere cosa cercare

# Verità

Soluzioni SIEM efficaci utilizzano una combinazione di correlazione in tempo reale, rilevamento delle anomalie, machine learning e behavior analytics  per individuare minacce sia note – che sconosciute –.

Tali soluzioni utilizzano anche funzionalità di correlazione avanzata per stabilire collegamenti e comprendere le attività correlate relative alle minacce. Quando una combinazione di analytics avanzati e correlazione in tempo reale sono pre-integrati nella soluzione SIEM, tali funzioni possono essere applicate – pronte all'uso – all'attività di rete, asset, utente e applicazione, in modo da poter andare ben oltre le semplici minacce note, per identificare anche attività anomale, che possono indicare minacce sconosciute.



# Mito n°2

Le soluzioni SIEM sono adatte solo per gruppi aziendali di grandi dimensioni che si avvalgono di team avanzati di sicurezza.

E’ opinione comune che, dal momento che le migliori soluzioni SIEM sul mercato possono scalare per supportare le organizzazioni più grandi, esse sono destinate solo alle organizzazioni con dimensione maggiore.

# Verità

Le migliori soluzioni SIEM si rivolgono ad un’ampia varietà di organizzazioni, indipendentemente dal fatto che siano un business in crescita, stiano appena iniziando con il monitoraggio della sicurezza o siano gruppi aziendali globali, inclusi nell’elenco Fortune 20, che hanno bisogno di casi d’uso avanzati. La verità è che, mentre molti team di sicurezza preferiscono tutte le funzionalità opzionali per supportare casi d’uso avanzati e specializzati, una soluzione SIEM valida non necessariamente richiede tutto ciò per produrre valore. Una soluzione ideale facilita l’introduzione a casi d’uso standard, come ad esempio rilevamento di minacce, monitoraggio del cloud e produzione di report sulla conformità – immediatamente pronti all’uso. Man mano che le esigenze e il business crescono, la soluzione SIEM dovrebbe espandersi per supportare più ambienti, molteplici aree geografiche e casi di utilizzo avanzati, come ad esempio ispezione approfondita dei pacchetti, analytics del DNS e SOAR (security orchestration, automation and response) integrata.

# Mito n°3

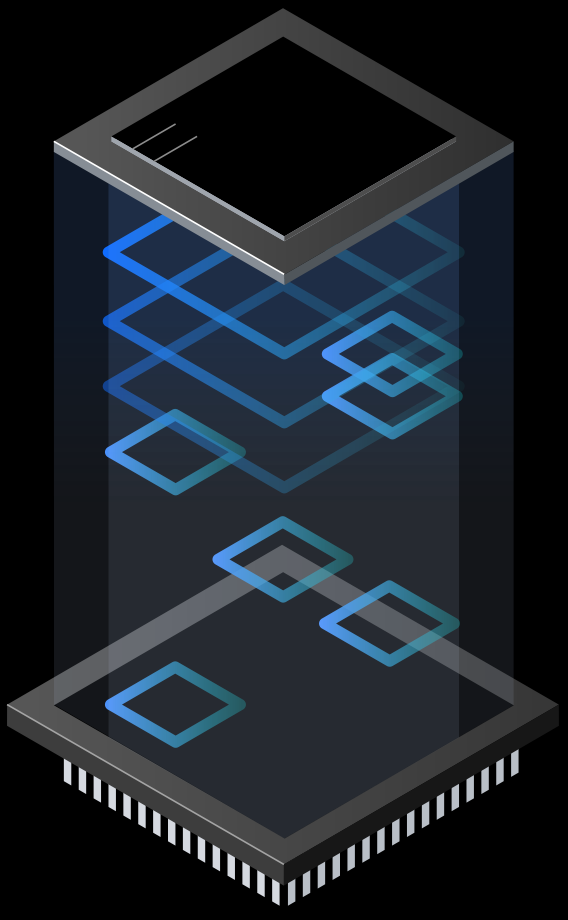
Le soluzioni SIEM richiedono una grande quantità di dati e il costo per la raccolta di tutti questi dati è estremamente elevato.

Dal momento che certi vendor sul mercato sono noti per far lievitare  molto rapidamente i prezzi a livelli proibitivi, alcuni team di sicurezza presuppongono che per tutte le soluzioni SIEM sia lo stesso.

# Verità

Se si considerano vendor che definiscono il prezzo in base alla quantità di dati archiviati, la scelta può diventare molto costosa, molto rapidamente. Ma vendor differenti presentano prezzi differenti per le loro soluzioni.

Prima di prendere qualsiasi impegno, si pensi a quali problemi si sta cercando di risolvere: Sei un rivenditore che deve proteggere dati relativi alle carte di pagamento? La tua azienda sta migrando a Amazon Web Services e hai bisogno di visibilità in quel nuovo ambiente? I dati che si raccolgono a scopi di sicurezza dovrebbero aiutare ad affrontare i propri casi d'uso unici. Non bisogna farsi spingere ad analizzare qualsiasi dato se non si ha la necessità di analizzarli tutti. Detto questo, se si hanno anche requisiti di conservazione dei dati, grazie alle normative o alle politiche organizzative, il vendor SIEM dovrebbe essere in grado di fornire un'opzione a basso costo solo per lo storage, la ricerca e la produzione di report. Analizzando solo ciò che è importante per la propria specifica organizzazione e inviando il resto dei propri dati di log ed eventi allo storage a basso costo, è possibile farsi carico di un progetto SIEM senza che questo consumi l'intero budget.



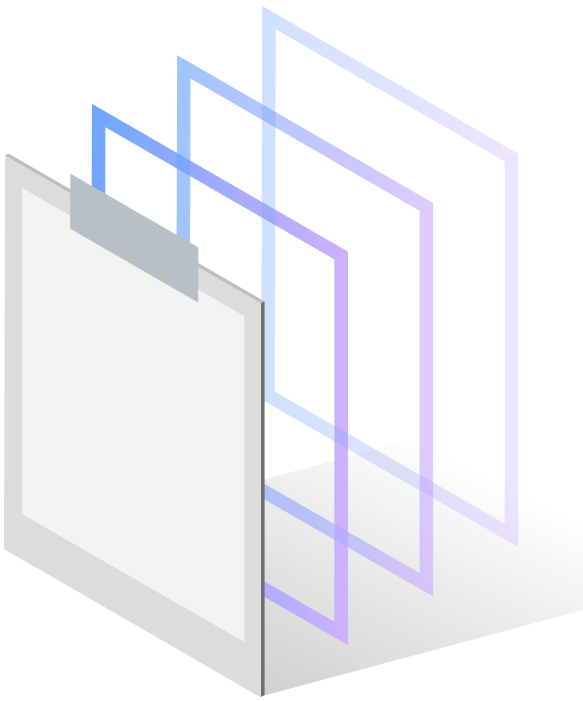
# Mito n°4

È necessario un team di data scientist a tempo pieno per rendere efficace una soluzione SIEM.

Spesso si dice che, per rendere efficace una soluzione SIEM, sarà necessario un data scientist a tempo pieno (o un team di tali professionisti), per creare da zero tutte le regole e gli strumenti di analytics.

# Verità

Se non è possibile (o non si vuole) reperire o pagare un team di data scientist, che capita abbiano anche competenze di sicurezza, è meglio cercare un vendor che fornisca contenuto pre-confezionato, immediatamente utilizzabile.



Alcuni vendor adottano il seguente approccio: dal momento che la soluzione verrà probabilmente personalizzata comunque, perché non iniziare da zero? In pratica, i team di sicurezza oggi semplicemente non hanno le risorse per farsi carico di un progetto così grande, che richiede competenze così specializzate. Con qualsiasi soluzione SIEM, sarà necessario fornire informazioni sulla propria rete, ma, dopo aver fatto questo, si dovrebbe poter usufruire di regole, strumenti di analytics e politiche di correlazione pre-compilati, per iniziare subito a rilevare minacce. Non si dovrebbe essere obbligati ad iniziare da un foglio bianco. E, se sussistono ancora preoccupazioni, molti vendor SIEM collaborano con MSSP (managed security service provider – provider di servizi di sicurezza gestiti), in modo che sia possibile ottenere tutti i vantaggi di una soluzione SIEM all'avanguardia, con il vantaggio aggiuntivo di ricevere aiuto da esperti delle operazioni di sicurezza.

# Mito n°5

Uno stack di gestione dei log è in grado di fornire la stessa visibilità di una soluzione SIEM

Il marketing creativo dei vendor di data lake e soluzioni di gestione dei log farà credere che soluzioni di gestione dei log siano superiori alle soluzioni SIEM per quanto riguarda l'individuazione e l'analisi di minacce

# Verità

Gli strumenti di gestione dei log possono realizzare casi d'uso di conformità e audit, ma non sono all'altezza quando si tratta di analisi e generazione di avvisi in tempo reale.

La gestione dei log era una soluzione per un problema vecchio di decenni – le aziende avevano bisogno di soluzioni per rispettare la conformità alle verifiche per Sarbanes Oxley (SOX), Payment Card Industry (PCI) e altre normative di settore. Gli stack di gestione dei log sono tornati in auge in anni recenti a causa di elevate necessità di ricerca e indicizzazione di petabyte, tuttavia una mancanza di analytics in tempo reale implica una quantità sproporzionata di responsabilità di rilevamento manuale – sia che si tratti di esecuzione di query, creazione di pivot o threat hunting – sullo staff già limitato.

La maggior parte dei provider SIEM fornisce un livello di gestione dei log o data lake, come parte della soluzione, per aggregazione, analisi e storage. Spesso, il livello di gestione dei log può essere concesso in licenza separatamente dalla soluzione SIEM, consentendo ai team di stabilire un data lake di sicurezza con un modello di prezzo basato sull'host, conveniente e prevedibile. Il valore incrementale del SIEM risiede nell'analytics pronta all'uso (correlazione in tempo reale, machine learning, ecc) che esegue il lavoro pesante di monitoraggio e rilevamento. In altre parole – la gestione dei log non rappresenta una soluzione SIEM di per sé stessa, ma una funzione di una soluzione SIEM.

# Mito n°6

Le soluzioni SIEM sono difficili da integrare con altre soluzioni nel proprio ambiente.

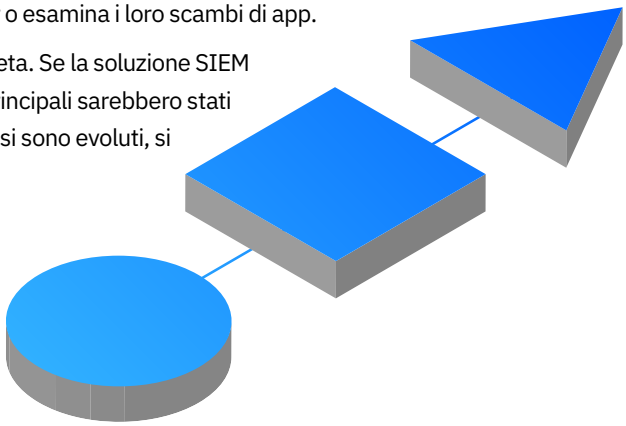
Le soluzioni SIEM hanno la reputazione di essere difficilmente integrabili con altre soluzioni, anche se dipendono da dati di altre soluzioni per fornire valore

# Verità

Le soluzioni SIEM leader devono essere facilmente integrabili – e, fortunatamente, molte lo sono.

Le prime soluzioni SIEM presentate sul mercato un decennio fa e che non sono riuscite ad evolversi in base alle esigenze mutevoli e alla tecnologia in evoluzione, sono difficili da integrare. Tuttavia, questi player sono completamente scomparsi o sono in notevole difficoltà al momento. Le soluzioni leader oggi offrono centinaia di integrazioni pronte all'uso con tecnologie IT e OT commerciali e mettono a disposizione connettori semplici per l'integrazione con log di applicazioni personalizzate e la relativa analisi. Se vuoi approfondire le integrazioni esistenti – e che sono completamente supportate dai vendor – dai uno sguardo ai siti Web del supporto clienti dei vari vendor o esamina i loro scambi di app.

Gli stereotipi diffusi oggi tendono ad essere basati su una tecnologia obsoleta. Se la soluzione SIEM fosse stata valutata dieci anni fa – o anche cinque anni fa – molti dei miti principali sarebbero stati veri. Ma, nella stessa misura in cui la tecnologia e gli scenari delle minacce si sono evoluti, si sono evolute anche le soluzioni SIEM.



Se si incontrano difficoltà nel rilevamento delle minacce o nell'interpretazione dei log nel log manager, può essere arrivato il momento di dare un altro sguardo alle soluzioni SIEM e scoprire autonomamente quanto siano cambiate.

# Informazioni su IBM Security QRadar

Gestisci le difese contro le crescenti minacce con IBM Security QRadar, la soluzione SIEM (security information and event management) leader sul mercato. Fai evolvere ed espandi le operazioni di sicurezza attraverso visibilità integrata, rilevamento, indagine e risposta. Ottieni completa visibilità del tuo ambiente e applica analytics avanzati per determinare la priorità delle tue minacce più critiche. Con QRadar, è possibile una rapida scalabilità, con supporto pronto all'uso per migliaia di casi di utilizzo di sicurezza e integrazioni. Rileva le minacce in tempo reale con analytics avanzati e threat intelligence incorporati con competenze approfondite, derivanti da anni di protezione di aziende incluse nell'elenco Fortune 100. QRadar può aiutare ad accelerare la conformità e gestire il rischio normativo con supporto per GDPR, ISO 27001, HIPAA e altro ancora. Utilizza efficacemente IBM Watson per potenziare team di sicurezza con indagini basate su AI, che stabiliscono la priorità e automatizzano il triage – con il risultato di un miglioramento fino a 60 volte della velocità di indagine. Infine, rispondi alle minacce, più rapidamente e con maggiore efficienza, con orchestrazione e automazione, gestione dei casi e playbook dinamici forniti dalla stretta integrazione con IBM Security SOAR.

Per ulteriori informazioni, visita il sito ibm.com/qradar.

IBM Security

**IBM Italia S.p.A.**
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

La home page di IBM Italia si trova all'indirizzo:
**ibm.com**



Questo documento è aggiornato alla data iniziale della pubblicazione e può essere modificato da IBM senza darne preavviso. Non tutte le offerte sono disponibili in ogni paese in cui opera IBM.

I dati relativi alle prestazioni e gli esempi relativi ai clienti, citati nel presente documento, vengono presentati a scopo meramente esplicativo. Le prestazioni reali possono variare a seconda delle specifiche configurazioni e condizioni operative.

LE INFORMAZIONI CONTENUTE IN QUESTO DOCUMENTO SONO FORNITE NELLO STATO IN CUI SI TROVANO, SENZA ALCUNA GARANZIA, ESPRESSA O IMPLICITA, INCLUSE, A TITOLO DI ESEMPIO, GARANZIE DI COMMERCIABILITÀ E DI IDONEITÀ PER UNO SCOPO SPECIFICO E DI NON VIOLAZIONE. I prodotti IBM sono garantiti secondo i termini e le condizioni dei contratti che ne regolano la fornitura.

Il cliente è responsabile per la garanzia di conformità con i requisiti legali. IBM non fornisce consulenza legale, né dichiara o garantisce che i propri servizi o prodotti assicurino che il cliente sia conforme alle normative vigenti.

Dichiarazione di conformità alle procedure di sicurezza IBM: la sicurezza dei sistemi IT richiede la protezione di sistemi e informazioni tramite prevenzione, identificazione e risposta agli accessi impropri di origine interna o esterna alle aziende. L'accesso improprio può causare l'alterazione, la distruzione, l'appropriazione indebita o l'uso improprio delle informazioni; può inoltre provocare danni e uso improprio dei sistemi, che possono essere utilizzati per attaccare altri sistemi. Nessun prodotto o sistema IT può essere considerato completamente sicuro e nessun prodotto, servizio o misura di sicurezza è del tutto efficace nel prevenire l'uso o l'accesso improprio. Sistemi, prodotti e servizi IBM sono progettati come elementi di un approccio di sicurezza completo, nel rispetto delle normative, che richiederà necessariamente procedure operative aggiuntive e il probabile impiego di altri sistemi, prodotti o servizi per raggiungere la massima efficienza. IBM NON GARANTISCE IN ALCUN MODO CHE SISTEMI, PRODOTTI O SERVIZI SIANO IMMUNI O RENDANO IMMUNI LE AZIENDE DA ATTIVITÀ ILLEGALI O DANNOSE DI TERZE PARTI.