Il SIEM: cinque requisiti per risolvere i problemi delle grandi imprese

Dopo oltre un decennio di utilizzo negli ambienti di produzione, le soluzioni per la gestione delle informazioni e degli eventi di sicurezza (SIEM) sono ormai considerate mature. Le funzioni di raccolta eventi, correlazione, allarme e dimostrazione della conformità alle normative sono fondamentali e la maggior parte delle soluzioni SIEM soddisfa queste esigenze. Tuttavia il panorama sta cambiando. Le aziende affrontano nuove minacce quali gli attacchi mirati e persistenti, nuove tendenze come i dispositivi mobili, il cloud e la virtualizzazione. Le priorità delle aziende ruotano attorno all'acquisizione della clientela, alle efficienze operative e al risparmio sui costi. Il risultato è che i casi di utilizzo del SIEM richiedono delle funzioni più avanzate per risolvere i problemi delle grandi imprese.

McAfee ha parlato con gli utenti delle soluzioni SIEM, chiedendo loro di spiegare le difficoltà principali incontrate nel suo utilizzo. Ecco le cinque problematiche principali:

- I Big Data della sicurezza
- La consapevolezza della situazione
- Il contesto in tempo reale
- La facilità d'implementazione
- La sicurezza integrata

Affinché il SIEM possa accompagnare verso strategie più efficienti di sicurezza e di gestione dei rischi (soprattutto perché sono pertinenti alla mitigazione delle minacce, al seguire le tendenze e ad allinearsi con le priorità delle aziende) queste cinque problematiche vanno affrontate. Ogni problema viene descritto qui con i corrispondenti casi utente e casi di utilizzo.

Caso di utilizzo: i Big Data della sicurezza.

- Espandi l'acquisizione dei dati con più feed da più fonti.
- Esegui analisi forensi su insiemi enormi di dati.
- Ottimizza la velocità e i volumi dei Big Data della sicurezza.
- Aumenta l'efficienza di dipendenti e processi.

1. I Big Data della sicurezza

I Big Data della sicurezza sono estremamente preziosi, se si è capaci di utilizzarli. Le soluzioni SIEM legacy non erano progettate per integrarsi con un così gran numero di endpoint, reti e sorgenti di dati, né si pensava che dovessero elaborare tassi di eventi così elevati o mantenere delle policy di conservazione così lunghe. Il risultato è che i database relazionali e soluzioni simili SIEM legacy, concepiti in primo luogo per gli eventi incentrati sulla rete, semplicemente non sono in grado di soddisfare le esigenze di sicurezza delle infrastrutture IT dinamiche di oggi. Mancano di velocità, estensibilità e scalabilità per essere efficaci e utilizzabili.

Caso di studio: governo federale

Una grande agenzia governativa era interessata nell'applicazione di analitiche avanzate ai Big Data della sicurezza conservati nel database relazione multipetabyte della sua soluzione SIEM. Ma erano necessarie ore anche per generare i report più semplici, a volte anche più di un giorno, così che il SIEM dell'agenzia era inutilizzabile per le analisi forensi.

Passando a McAfee® Enterprise Security Manager come soluzione SIEM, l'agenzia è riuscita ad espandere il numero e i tipi di servizi integrati, aggiungendo alle analisi più dati e contesto sugli utenti. L'agenzia ha anche aumentato il numero degli eventi e dei dati conservati. Ora i report vengono generati in pochi minuti, migliorando l'intero approccio alle analisi forensi.

Caso di utilizzo: la consapevolezza della situazione

- Arricchisci la consapevolezza sulle situazioni con più soluzioni sulle identità.
- Rispondi alle domande chi, quando, come, dove e cosa.
- Comprendi durata, partecipanti e altri fattori.
- Includi le risorse BYOD come portatili e smartphone.

2. La consapevolezza della situazione

Un tempo il SIEM serviva solo a correlare gli eventi di più firewall e sistemi di rilevamento delle intrusioni, eventualmente applicando alcuni dati di valutazione delle vulnerabilità. Anche oggi alcune soluzioni SIEM si affidano in primo luogo ai dati dei flussi nella rete. Anche se queste fonti sono importanti, devono essere arricchite con informazioni su applicazioni, contesti dei dati e identità. Senza di esse sono necessari più tempo e risorse per comprendere e dare priorità agli eventi, con una quantità di informazioni sulle situazioni che sia fruibile e tempestiva.

Caso di studio: fornitore di servizi sanitari

Un fornitore di servizi sanitari locale aveva abbracciato il BYOD ("Bring your own device"), supportando i tablet personali per aumentare l'agilità dei dipendenti. Però, a causa di circostanze passate, il fornitore aveva preoccupazioni in merito agli abusi dei dipendenti. La precedente soluzione SIEM dell'azienda mancava della capacità di comprendere quali erano gli utenti che interagivano con i dati sensibili, indipendentemente dal dispositivo (laptop, desktop, tablet o computer virtuale).

Con McAfee Enterprise Security Manager, il fornitore di servizi sanitari ha potuto connettersi con i prodotti per la gestione dell'identità e dei dispositivi mobili, Active Directory e LDAP, per guadagnare in consapevolezza su utenti e dispositivi. Grazie all'integrazione con i dati strutturati e non strutturati, come il supporto nativo per i database, oltre che l'integrazione con la prevenzione delle fughe di dati (DLP) e il monitoraggio delle attività del database (DAM), ora è presente una consapevolezza più completa sulle situazioni e una maggiore mitigazione delle minacce interne.

Caso di utilizzo: il contesto in tempo reale

- Comprendi le minacce all'interno e all'esterno dell'ambiente.
- Migliora l'intelligenza del SIEM con il contesto in tempo reale.
- Riduci l'incidenza degli eventi e i tempi di risposta.
- Identifica e ordina per priorità le minacce grazie alle informazioni aggiuntive sulla sicurezza.

3. Il contesto in tempo reale

Uno dei primi utilizzi tipici del SIEM era la gestione del log: raccolta, conservazione e interrogazione con alcune funzioni aggiuntive. I log sono tuttora un componente fondamentale del SIEM, ma i SIEM odierni necessitano anche del contesto in tempo reale.

Esempi di tale contesto sono McAfee Global Threat Intelligence (McAfee GTI) e McAfee Vulnerability Manager. McAfee GTI offre un servizio di reputazione in tempo reale e basato sul cloud, mentre McAfee Vulnerability Manager raccoglie le informazioni sulle vulnerabilità delle risorse a livello aziendale.

Caso di studio: retailer

Un retailer Fortune 100 con una soluzione SIEM in produzione e nessuna soluzione McAfee aveva condotto un PoC (proof-of-concept). Nella prima settimana, l'impresa aveva scoperto che più del 30% del traffico in ingresso nella rete proveniva da fonti pericolose e/o conteneva dei payload pericolosi.

Usando McAfee Enterprise Security Manager per correlare le informazioni sugli eventi con McAfee GTI, l'esercente identificò rapidamente le risorse prese di mira in tutte le sedi dei negozi e dei centri dati, ottenendo una migliore comprensione dei tipi di attacco che l'organizzazione stava subendo. La soluzione McAfee SIEM determinò qual era il livello di gravità più elevato e quindi diede la priorità alla relativa risposta. Il SIEM abbinato al contesto in tempo reale consentì il rilevamento, l'assegnazione della priorità e la remediation della minaccia in un tempo più breve.

Caso di utilizzo: la facilità d'implementazione

- Implementa il SIEM con il whitelisting dinamico e la sicurezza assistita da hardware per proteggere i dispositivi a funzioni fisse.
- Semplifica le analisi forensi con gli approfondimenti personalizzabili.
- Integra il SIEM con il firewall e io sistemi di prevenzione delle intrusioni (IPS) per una rapida risposta agli eventi.
- Allunga la vita delle risorse legacy grazie alla maggiore sicurezza.

4. La facilità d'implementazione

Le soluzioni SIEM legacy hanno un'architettura molto rigida e mancano di alcune funzioni essenziali. Per esempio, non si integrano facilmente con i dispositivi non supportati in precedenza, al fine di rendere utilizzabili le informazioni. Invece un SIEM di nuova generazione è facile da personalizzare e abbastanza flessibile per adattarsi a qualsiasi ambiente. Questo è proprio ciò che rende un SIEM di nuova generazione strategico per qualsiasi azienda.

Caso di studio: società di servizi pubblici

Una grande società di servizi pubblici doveva utilizzare dei controlli di sicurezza per prevenire gli attacchi simili a Stuxnet che avrebbero compromesso l'infrastruttura causando un blackout a milioni di clienti. Con McAfee Enterprise Security Manager, la società ha ottenuto la consapevolezza della situazione in ambito IT aziendale, SCADA e sistema di controllo industriale (ICS) con il supporto nativo per dispositivi, applicazioni e protocolli.

McAfee SIEM ha fornito al cliente gli strumenti necessari per realizzare la propria integrazione con i dispositivi SCADA e ICS. Questo a sua volta ha consentito la correlazione, il rilevamento delle anomalie e l'analisi delle tendenze in tutte e tre le aree. Oltre alla raccolta personalizzate degli eventi, il cliente ha creato in modo rapido e semplice dashboard, report, regole di correlazione e allarmi specifici. Ciò ha reso il SIEM uno strumento prezioso per la sicurezza, la dimostrazione della conformità alle normative e la disponibilità delle risorse. In altre parole, ha tenuto accese le luci delle città.

Caso di utilizzo: la sicurezza integrata

- Semplifica il flusso di lavoro di sicurezza e operazioni.
- Riduci la complessità con l'automazione e la facile personalizzazione.
- Migliora la visibilità e la consapevolezza sulle situazioni grazie a soluzioni di sicurezza che lavorano insieme.
- Offri maggiore protezione con informazioni e integrazione.

5. La sicurezza integrata

Il SIEM è un componente importante di qualsiasi iniziativa di sicurezza strategica, ma è solo uno dei tanti. L'integrazione delle soluzioni di sicurezza e conformità offre molto di più delle singole soluzioni, mentre un'architettura non integrata crea complessità. La complessità è il motivo per cui la sicurezza rimane spesso ampiamente tattica anziché divenire più strategica e allineata con le priorità aziendali.

Caso di studio: servizi finanziari

Una banca multinazionale possedeva svariati prodotti di diversi fornitori. Alcuni di essi si trovavano in produzione, ma molti di essi non erano usati regolarmente a causa della limitatezza delle risorse. La banca decise che sfruttando il SIEM insieme ai controlli integrati di endpoint, rete e dati avrebbe potuto mitigare più efficacemente i rischi e ridurre i costi, rendendo al contempo la sicurezza più importante per gli affari.

La banca ha ridotto il numero di fornitore ottenendo economie di scala. Ha potuto diminuire i costi di formazione e il numero di agent, console, server e altro. Ha inoltre ridotto il costo dei contratti e la moltitudine di spese associate. Ma oltre ai risparmi, la banca ha fatto in modo che tutte le soluzioni esistenti e future fossero pienamente integrate con McAfee Enterprise Security Manager per assicurare migliori controlli e visibilità sullo stato della sicurezza.

Conclusioni

- Quanto è importante la capacità di gestire facilmente i problemi di raccolta, conservazione, accesso, elaborazione e analisi posti dai Big Data della sicurezza?
- Gli addetti alla sicurezza ottengono le informazioni necessarie, quando sono necessarie per prendere decisioni informate e intraprendere azioni tempestive?
- Il tuo team di sicurezza dispone del contesto in tempo reale di cui ha bisogno per identificare i rischi e gli attacchi prima che possano causare dei danni?
- Quale sarebbe l'impatto sulla sicurezza e le risorse se tu utilizzassi una soluzione SIEM con approfondimenti intuitivi e visualizzazioni facilmente personalizzabili?
- In che modo l'integrazione nella tua infrastruttura migliorerebbe sicurezza, visibilità, processi e reattività?

Quello che funzionava dieci anni fa con i SIEM legacy non è più in grado di soddisfare le esigenze odierne. Con le nuove esigenze legate ai Big Data, alle informazioni di sicurezza, alla consapevolezza sulla situazione, alle prestazioni, usabilità e integrazione, i casi di utilizzo del SIEM si sono ampliati. Le soluzioni SIEM devono ridurre la complessità, non crearla. Chiedi di più al tuo SIEM.

Oggi le soluzioni SIEM devono operare nell'ambito di una cornice di protezione ampia e connessa, nella quale le priorità dell'azienda e della sicurezza sono allineate. Il SIEM gioca un ruolo importante nel rendere la sicurezza più strategica e nel fornire all'impresa un valore reale.

Per saperne di più sulle soluzioni SIEM di McAfee, visita: www.mcafee.com/it/products/siem/index.aspx.

Security Connected

La piattaforma Security Connected di McAfee fornisce una cornice unificata per centinaia di prodotti, servizi e partner che possono apprendere l'uno dall'altro, condividere dati contestuali in tempo reale e agire in squadra per mantenere al sicuro reti e informazioni. Grazie ai concetti innovativi, ai processi ottimizzati e ai risparmi concreti offerti dalla piattaforma, qualsiasi organizzazione può migliorare la propria condizione di sicurezza e ridurre al minimo i costi operativi.

McAfee
An Intel Company

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

61099brf_focus-5-siem_0514_fnl_ETMG