White paper

Sentinel

La guida completa alla gestione di log ed eventi

Un white paper del Dott. Anton Chuvakin, sponsorizzato da NetIQ

Tutti hanno a che fare con i log, il che significa che tutti devono gestirli, non da ultimo per il fatto che lo impongono molti obblighi normativi. In questa guida, il Dr. Anton Chuvakin analizzerà la relazione tra la Security Information and Event Management (SIEM) e la gestione dei log, concentrandosi non solo sulle differenze tecniche e sui diversi usi di queste due tecnologie, ma anche sull'architettura della loro installazione congiunta. Oltre a ciò, fornirà alcune raccomandazioni per le aziende che hanno installato solo la tecnologia di gestione dei log o solo SIEM per aiutarle a sviluppare linee guida volte a migliorare, ottimizzare ed espanderne l'installazione. Offrirà inoltre linee guida per le aziende che hanno già installato entrambe le tecnologie.

NetIQ

Sommario

pagina

Introduzione 1
Funzionalità di Security, Information and Event Management 2
Funzionalità di gestione dei log 3
Comparazione ad alto livello: SIEM vs. gestione dei log 4
Casi d'uso delle tecnologie SIEM e di gestione dei log 5
Tendenze tecnologiche 8
Scenario di esempio relativo a SIEM e gestione dei log 8
Architettura di gestione dei log e della SIEM 9
Conclusioni 22
Informazioni sull'autore 22
Informazioni su NetIQ 23

Introduzione

La tecnologia Security, Information and Event Management (SIEM) esiste sin dai tardi anni '90, ma ha sempre generato controversie nel settore della sicurezza per via della sua iniziale promessa di offrire "un'unica console di controllo della sicurezza" e della sua lenta adozione da parte delle aziende di dimensioni più piccole. Recentemente, alla SIEM tradizionale si è affiancato l'ampio uso di tecnologie di gestione dei log, mirato a raccogliere log di diversi tipi per una grande varietà di scopi, dalla risposta agli incidenti di sicurezza alla conformità normativa, fino alla gestione dei sistemi e alla risoluzione dei problemi delle applicazioni.

In questo documento analizzeremo la relazione tra la Security Information and Event Management (SIEM) e la gestione dei log, concentrandoci non solo sulle differenze tecniche e sui diversi usi di queste due tecnologie, ma anche sull'architettura della loro installazione congiunta. Ad esempio, per soddisfare i requisiti di registrazione del Payment Card Industry-Data Security Standard (PCI DSS), qual è la tecnologia giusta da installare? Quale tecnologia è più adatta a ottimizzare la risposta agli incidenti e le procedure di indagine? Quale è in grado di fornire dati in tempo reale sugli attacchi? Oltre a ciò, forniremo alcune raccomandazioni per le aziende che hanno installato solo la gestione dei log o solo la SIEM per aiutarle a sviluppare linee guida volte a migliorare, ottimizzare ed espanderne l'installazione. Offriremo infine linee guida per le aziende che hanno già installato entrambe le tecnologie.

Gli strumenti SIEM hanno fatto la loro comparsa sul mercato nel 1997. Originariamente, loro scopo era ridurre i falsi positivi generati dai NIDS (Network Intrusion Detection System), al tempo un problema quotidiano di questi sistemi. Gli strumenti erano complessi da installare e utilizzare e venivano impiegati solo dalle organizzazioni più grandi, dotate

dei programmi di sicurezza più avanzati. Nei tardi anni '90, le dimensioni del mercato si attestavano intorno a pochi milioni di dollari mentre, secondo alcuni analisti, negli anni a venire potranno raggiungere somme nell'ordine dei miliardi. Gli strumenti SIEM oggi disponibili, come NetIQ Sentinel, sono utilizzati da aziende grandi e piccole, dalle imprese Fortune 1000 o Global 2000 alle PMI.

Prima di iniziare la nostra analisi, è bene definire le tecnologie SIEM e di gestione dei log e spiegare in cosa si differenziano. *La* SIEM *si occupa di: raccolta, aggregazione, normalizzazione e permanenza di log rilevanti; raccolta di dati contestualizzati; analisi, incluse correlazione e prioritizzazione; presentazione, incluse reportistica e visualizzazione; workflow e contenuti correlati alla sicurezza.* Tutti i casi d'uso della SIEM riguardano la sicurezza delle informazioni, la sicurezza della rete, la sicurezza dei dati e la conformità normativa.

La gestione dei log, invece, include: raccolta di log completi, aggregazione, permanenza dei log originali (non elaborati, non modificati); analisi del testo dei log; presentazione, prevalentemente in forma di ricerca ma anche reportistica; workflow e contenuti correlati. Se parliamo di gestione dei log, i casi d'uso sono tanti e coprono tutti gli usi possibili dei dati dei log, sia nell'IT che in altri ambiti.

La principale differenza evidenziata da quanto sopra esposto è che la SIEM è mirata principalmente alla sicurezza (a cui fa riferimento la prima lettera dell'acronimo) e all'uso delle diverse informazioni IT per scopi di sicurezza. La gestione dei log, invece, è mirata ai log e ai diversi usi dei dati dei log, sia in ambito di sicurezza che in altri ambiti.

SIEM:

- Raccolta, aggregazione, normalizzazione e permanenza di log rilevanti
- Raccolta di dati contestualizzati
- Analisi, incluse correlazione e prioritizzazione
- Presentazione, incluse reportistica e visualizzazione
- Workflow e contenuti correlati alla sicurezza
- Sicurezza delle informazioni, sicurezza della rete, sicurezza dei dati e conformità normativa

Funzionalità di Security, Information and Event Management

Passiamo ora a definire le funzionalità che caratterizzano la SIEM, ovvero quelle che la maggior parte dei clienti ricercherà al momento di scegliere il prodotto SIEM. Tali funzionalità sono:

- **Raccolta di log e dati contestualizzati.** *Include la raccolta di log e dati contestualizzati quali le informazioni sulle identità o i risultati della valutazione delle vulnerabilità per mezzo di una combinazione di metodi senza agente e basati su agente.*
- **Normalizzazione e categorizzazione.** *Conversione dei log originali raccolti in un formato universale che ne permetta l'uso nel prodotto SIEM. Gli eventi, inoltre, sono categorizzati in pratici contenitori classificati come "modifiche di configurazione", "accesso ai file" o "attacco di overflow del buffer" e così via.*

Gestione dei log:

- Raccolta di log completi, aggregazione, permanenza dei log originali (non elaborati, non modificati)
- Analisi del testo dei log
- Presentazione, prevalentemente in forma di ricerca ma anche reportistica
- Workflow e contenuti correlati
- I casi d'uso coprono tutti gli usi possibili dei dati dei log, sia nell'IT che in altri ambiti

- **Correlazione.** *Include la correlazione basata su regole, la correlazione statistica o algoritmica e altri metodi che includono la correlazione tra eventi diversi e quella tra eventi e dati contestuali. La correlazione può avvenire in tempo reale, ma non tutti gli strumenti la supportano mentre potrebbero correlare i dati cronologici dei vari database. Altri metodi di analisi dei log sono a volte raggruppati in pacchetti, sotto l'etichetta della correlazione.*
- **Notifiche e avvisi.** *Notifiche o avvisi generati e quindi inviati a operatori o manager. I meccanismi di avviso più diffusi includono e-mail, SMS o semplici messaggi SNMP (Simple Network Management Protocol).*
- **Prioritizzazione.** *Include diverse funzionalità che aiutano a mettere in evidenza gli eventi importanti rispetto a quelli meno critici. La prioritizzazione può essere eseguita correlando gli eventi di sicurezza ai dati sulla vulnerabilità o ad altre informazioni sulle risorse. Gli algoritmi di prioritizzazione possono anche utilizzare le informazioni sulla gravità fornite dalla fonte originale del log.*
- **Visualizzazioni in tempo reale.** *Dashboard di monitoraggio della sicurezza e display utilizzati dal personale operativo. Tali display mostrano agli analisti le informazioni raccolte e i risultati di correlazione in tempo quasi reale. Le visualizzazioni possono contenere anche i dati cronologici archiviati.*
- **Reportistica.** *La reportistica, anche quella pianificata, riguarda tutte le visualizzazioni cronologiche dei dati che il prodotto SIEM raccoglie. Alcuni prodotti dispongono anche di un meccanismo per distribuire i rapporti al personale addetto alla sicurezza o ai responsabili IT, sia tramite e-mail che tramite un portale Web sicuro e dedicato.*
- **Workflow dei ruoli di sicurezza.** *Funzionalità di gestione degli incidenti, quali l'apertura di casi e l'esecuzione di attività di indagine, oppure l'esecuzione automatica o semiautomatica di tipiche attività per le operazioni di sicurezza. Alcuni prodotti includono anche funzionalità di collaborazione che permettono a più analisti di collaborare sulla stessa azione di risposta.*

La funzionalità sopra descritta è disponibile nella maggior parte dei prodotti SIEM commerciali presenti sul mercato. Quasi tutti questi prodotti, tuttavia, presentano punti deboli e forti, oltre che ulteriori funzionalità speciali.

Funzionalità di gestione dei log

Iniziamo analizzando le funzionalità che caratterizzano un sistema di gestione dei log. Tali funzionalità includono:

- **Raccolta dei dati di log.** *Include la raccolta di tutti i log utilizzando metodi senza agente o basati su agente oppure una combinazione dei due.*
- **Permanenza efficiente.** *Se la raccolta e il salvataggio dei dati dei log non sembrano rappresentare di per sé una grande sfida ingegneristica, la raccolta efficiente di gigabyte e persino di terabyte di dati - e la loro permanenza associata alle capacità di ricerca e accesso rapido a tali dati - non è un problema da poco. Dal momento che molte normative impongono termini specifici per la permanenza dei dati dei log, spesso corrispondenti a diversi anni, questa funzionalità si rivela critica per un sistema di gestione dei log.*
- **Ricerca.** *Si tratta del metodo di accesso primario alle informazioni di tutti i log, inclusi quelli registrati dalle applicazioni personalizzate. La ricerca è indispensabile per l'uso dei log a fini di indagine, per la documentazione legale dei log e per la ricerca degli errori quando i log sono impiegati per la risoluzione dei problemi delle applicazioni. Un'interfaccia di ricerca interattiva che sia chiara e veloce è pertanto essenziale per un sistema di gestione dei log.*

- **Indicizzazione o analisi dei log.** *Queste funzionalità sono componenti chiave di un sistema di gestione dei log. L'indicizzazione può centuplicare la velocità di ricerca. La tecnologia di indicizzazione crea una struttura di dati chiamata indice che consente di effettuare rapidamente ricerche, sia booleane che per parola chiave, nello storage dei log. Talvolta, l'indicizzazione viene utilizzata per altre tecniche di analisi full-text. Ad esempio, può essere paragonata a una sorta di Google per i log. Poiché non tutti gli strumenti di gestione dei log supportano l'indicizzazione oppure vengono indicate velocità di raccolta dei log che non considerano l'indicizzazione, è necessario prestare molta attenzione alle promesse dei fornitori.*
- **Reportistica e reportistica pianificata.** *Queste funzionalità coprono tutti i dati raccolti dal prodotto di gestione dei log e sono simili alla reportistica SIEM. Il principale vantaggio della reportistica - indipendentemente dal fatto che venga utilizzata per motivi di sicurezza, conformità o gestione - è che può fare o disfare la soluzione di gestione dei log. La reportistica deve essere veloce, personalizzabile e facile da usare per una vasta gamma di finalità. La distinzione tra ricerche e rapporti è molto netta: la ricerca agisce su tutti i log raccolti nel loro formato originale e non elaborato (la stessa modalità con cui Google tratta le pagine Web), mentre il rapporto opera su log che sono analizzati in un database (come un foglio di calcolo Excel). È necessario valutare con attenzione la facilità con cui è possibile creare un rapporto personalizzato in uno strumento di gestione dei log. È su questo punto che molte soluzioni si dimostrano carenti, richiedendo agli operatori di studiare gli aspetti più sofisticati delle strutture di storage dei log prima di poter personalizzare i rapporti.*

Poiché non tutti gli strumenti di gestione dei log supportano l'indicizzazione oppure vengono indicate velocità di raccolta dei log che non considerano l'indicizzazione, è necessario prestare molta attenzione alle promesse dei fornitori.

Ora passiamo alla comparazione delle funzionalità e delle caratteristiche della SIEM e della gestione dei log ad alto livello.

Comparazione ad alto livello: SIEM vs. gestione dei log

Nella tabella che segue sono evidenziate le aree chiave di funzionalità e le differenze tra la SIEM e la gestione dei log:

Funzionalità	Security Information and Event Management (SIEM)	Gestione dei log
Raccolta dei log	Raccolta dei log importanti per la sicurezza	Raccolta di tutti i log, inclusi log operativi e log delle applicazioni personalizzati
Conservazione dei log	Conservazione limitata dei dati dei log analizzati	Conservazione dei dati dei log analizzati e non elaborati per lunghi periodi
Reportistica	Reportistica incentrata sulla sicurezza, reportistica in tempo reale	Reportistica a uso diffuso, reportistica cronologica
Analisi	Correlazione, classificazione delle minacce, prioritizzazione degli eventi	Analisi full-text, assegnazione di tag
Segnalazioni e notifiche	Reportistica avanzata incentrata sulla sicurezza	Segnalazioni semplici su tutti i log
Altre funzioni	Gestione degli incidenti, analisi di altri dati relativi alla sicurezza	Alta scalabilità per la raccolta e la ricerca

Vediamo insieme come vengono utilizzate le tecnologie SIEM e di gestione dei log.

Tre tipi di casi d'uso:

- Sicurezza – rilevazione e indagine
- Conformità – alle normative (globale) e alle policy (locale)
- Risoluzione dei problemi operativi, di sistema e di rete e normali operazioni

Recentemente, alla SIEM tradizionale si è affiancato l'ampio uso di tecnologie di gestione dei log, mirato a raccogliere log di diversi tipi per una grande varietà di scopi, dalla risposta agli incidenti di sicurezza alla conformità normativa, fino alla gestione dei sistemi e alla risoluzione dei problemi delle applicazioni..

Casi d'uso delle tecnologie SIEM e di gestione dei log

Prima di discutere l'architettura congiunta di SIEM e gestione dei log, è necessario presentare i tipici casi d'uso che richiedono l'installazione di un prodotto SIEM da parte di un'organizzazione. Inizieremo dal livello più elevato dei tre principali casi d'uso:

1. **Sicurezza – rilevazione e indagine.** Si tratta di quella che, a volte, viene definita la gestione delle minacce e riguarda principalmente il rilevamento e la risoluzione di problemi quali attacchi, malware, furto di dati e altri problemi di sicurezza.
2. **Conformità – alle normative (globale) e alle policy (locale).** Riguarda la soddisfazione dei requisiti di molteplici leggi, mandati, framework e policy aziendali locali.
3. **Risoluzione dei problemi operativi, di sistema e di rete e normali operazioni.** Questo caso d'uso è specifico soprattutto della gestione dei log e consiste nell'indagine dei problemi dei sistemi e nel monitoraggio della disponibilità di sistemi e applicazioni.

A un livello più dettagliato, i casi d'uso relativi a sicurezza e conformità rientrano in diversi scenari. Esaminiamoli in dettaglio.

Il primo scenario è un Security Operations Center (SOC) di tipo tradizionale. Un SOC, ovvero un centro operativo per la sicurezza, fa normalmente un uso massiccio di funzionalità SIEM quali la correlazione e le visualizzazioni in tempo reale. L'organizzazione di un cliente SIEM sarà dotata di analisti online 24x7 impegnati nell'identificazione degli avvisi di sicurezza non appena vengono visualizzati. Questo era il caso d'uso SIEM originario, quando questa tecnologia fece la sua comparsa negli anni '90. Oggi questo caso riguarda solo le organizzazioni di grandi dimensioni.

Il prossimo caso d'uso è quello che viene a volte definito uno scenario di mini-SOC. In questo caso, il personale addetto alla sicurezza si avvale di visualizzazioni non in tempo reale per controllare i problemi di sicurezza, in quanto gli analisti iniziano il loro lavoro la mattina. Gli analisti sono online solo per poche ore al giorno e revisionano gli avvisi e i rapporti in base alla necessità e non in tempo quasi reale - salvo nei casi in cui si verifichino degli eventi mentre gli analisti sono collegati al prodotto.

Il terzo scenario riguarda un SOC automatizzato in cui un'organizzazione configura la sua SIEM in modo che generi avvisi sulla base di determinate regole e quindi non si occupa del prodotto fin quando non viene generato un avviso. Gli analisti non accedono mai al prodotto

a meno che non vi sia la necessità di investigare sugli avvisi, revisionare i rapporti su base settimanale o mensile o eseguire altre attività non di routine. Questo è il tipico caso d'uso per molte piccole organizzazioni e sono pochi i prodotti SIEM in grado di soddisfare questa esigenza - e comunque non senza un notevole intervento di personalizzazione. Vale la pena aggiungere che molti prodotti SIEM vengono venduti con l'aspettativa di rappresentare un SOC automatizzato, ma raramente questa aspettativa viene soddisfatta.

La risoluzione dei problemi delle applicazioni e l'amministrazione del sistema sono altri due importanti casi d'uso per i sistemi di gestione dei log.

Le tecnologie di gestione dei log sono presenti anche in scenari non strettamente legati alla sicurezza. La risoluzione dei problemi delle applicazioni e l'amministrazione del sistema sono altri due importanti casi d'uso per i sistemi di gestione dei log. Una volta installata l'applicazione e configurata la registrazione, il sistema di gestione dei log viene utilizzato per sottoporre rapidamente a revisione errori e log di eccezioni. Oppure per revisionare i riepiloghi della normale attività dell'applicazione allo scopo di stabilire lo stato di quest'ultima e risolverne le eventuali irregolarità.

Uno scenario che rientra in questa categoria è la reportistica sullo stato di conformità. Qui analisti o manager della sicurezza revisionano i rapporti allo scopo di rilevare eventuali problemi di conformità. La revisione viene condotta a cadenza settimanale o mensile o in base a quanto indicato da uno specifico regolamento e non a scopo di sicurezza o di operatività. Questo caso d'uso rappresenta solitamente una fase di transizione che le organizzazioni sperimentano prima di diventare più mature e passare a uno dei casi summenzionati. Gli strumenti di gestione dei log sono quasi sempre installati per questo tipo di scenario, ma non è raro che un prodotto SIEM venga utilizzato anche per fini di conformità. I requisiti di permanenza a lungo termine dei log rappresentano spesso una sfida per l'installazione.

Dal momento che i log sono molto importanti ai fini degli obblighi di conformità, osserviamo nel dettaglio alcune leggi.

PCI-DSS

Lo standard Payment Card Industry Data Security (PCI-DSS) si applica alle organizzazioni che gestiscono transazioni con carte di credito e obbliga alla registrazione di dettagli specifici, alla permanenza dei log e a procedure di revisione giornaliera dei log.

Sebbene la registrazione sia presente in tutti i requisiti PCI, il PCI DSS include anche il requisito 10 che è espressamente dedicato a registrazione e gestione dei log. In base a tale requisito, i log di tutti i componenti del sistema devono essere sottoposti a revisione almeno una volta al giorno. In più, lo standard PCI DSS impone all'organizzazione di garantire l'integrità dei suoi log installando un software per il rilevamento delle modifiche e il monitoraggio dell'integrità dei file. Inoltre, stabilisce di conservare per almeno un anno i log dei sistemi che rientrano nell'ambito di applicazione dello standard.

L'HITECH (Health Information Technology for Economic and Clinical Health) del 2009 mira a promuovere su vasta scala le installazioni HIPAA negli anni a venire.

FISMA

Il Federal Information Security Management Act (FISMA) del 2002 mette in evidenza l'esigenza, da parte delle agenzie federali, di sviluppare, documentare e adottare un programma di ampia portata finalizzato alla protezione dei sistemi informativi che supportano le loro operazioni e risorse. La SP 800-53 del NIST (Recommended Security Controls for Federal Information Systems) descrive i controlli per la gestione dei log, incluse la generazione, la revisione, la protezione e la permanenza dei record dei controlli, oltre alle misure da intraprendere in caso di mancato superamento del controllo.

La SP 800-92 del NIST (Guide to Computer Security Log Management) semplifica la conformità FISMA e assicura che sia totalmente dedicata alla gestione dei log. Questa pubblicazione speciale descrive l'esigenza della gestione dei log nelle agenzie federali e le modalità per creare e amministrare al meglio le infrastrutture di gestione dei log, incluse le modalità di generazione, analisi, storage e monitoraggio dei log. La SP 800-92 del NIST tratta l'importanza di analizzare vari tipi di log provenienti da varie origini e di definire chiaramente ruoli e responsabilità specifici dei team e degli individui coinvolti nella loro gestione.

HIPAA

L'HIPAA (Health Insurance Portability and Accountability Act) del 1996 illustra a grandi linee gli standard di sicurezza relativi alle informazioni sanitarie. La SP 800-66 del NIST (An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule) descrive in dettaglio i requisiti di gestione dei log ai fini di protezione delle informazioni sanitarie. La Sezione 4.1 della SP 800-66 descrive l'esigenza di una regolare revisione dell'attività del sistema informativo, ad esempio log di revisione, rapporti sull'accesso e rapporti sul controllo degli incidenti di sicurezza. La Sezione 4.22 specifica che la documentazione relativa ad azioni e attività deve permanere per un minimo di sei anni. I log a volte sono considerati parte di tale documentazione. L'HITECH (Health Information Technology for Economic and Clinical Health) del 2009 mira a promuovere su vasta scala le installazioni HIPAA negli anni a venire.

Gli strumenti SIEM oggi disponibili, come NetIQ® Sentinel™, sono utilizzati da aziende di tutte le dimensioni, dalle imprese Fortune 1000 o Global 2000 alle piccole e medie imprese.

Tendenze tecnologiche

La tecnologia SIEM ha ormai più di 10 anni e ha attraversato numerose fasi, così tante da potervi dedicare un intero white paper. Tuttavia, scopo di questo documento è esaminare solo alcune delle tendenze tecnologiche della SIEM. Nonostante sia nata come tecnologia rivolta alle grandi aziende di portata globale e alle agenzie governative operanti nei settori più delicati, la SIEM continua la sua strada verso i mercati rappresentati dalle aziende di minori dimensioni. Secondo quanto previsto da molti analisti, nel 2011 i principali produttori SIEM si sarebbero dati battaglia per la conquista dei middle market. Il risultato di questa lotta è stata la nascita di strumenti di gestione della sicurezza migliorati e adatti ai clienti più piccoli.

Un'altra tendenza è la definitiva accettazione di ruoli distinti per SIEM e gestione dei log. La maggioranza dei produttori SIEM offre oggi anche soluzioni di gestione dei log. Ciò significa anche altri usi degli strumenti SIEM, ad esempio: operazioni IT, analisi delle frodi, risoluzione dei problemi delle applicazioni, e altro ancora, fino alla governance IT, usi per rischio e conformità (GRC) per la governance ad alto livello e obiettivi di misurazione del rischio.

Stiamo anche assistendo al delinearsi della convergenza di operazioni e gestione IT e gestione della sicurezza. Anche se gli analisti lo avevano previsto già molti anni fa, solo ora tale tendenza si è materializzata pienamente. Nonostante ciò, molti prevedono che la tendenza di questa convergenza continuerà e che gli strumenti di sicurezza saranno sempre più collegati agli strumenti operativi dell'IT, come quelli per la gestione delle reti e dei sistemi.

Molti prevedono che la tendenza di questa convergenza continuerà e che gli strumenti di sicurezza saranno sempre più collegati agli strumenti operativi dell'IT, come quelli per la gestione delle reti e dei sistemi.

Scenario di esempio relativo a SIEM e gestione dei log

Questo case study illustra l'installazione di una soluzione SIEM e di gestione dei log per soddisfare i requisiti PCI-DSS nell'ambito di una grande catena di vendita al dettaglio. Il rivenditore aveva deciso di installare una soluzione di gestione dei log di tipo commerciale quando il suo consulente PCI gli ha detto che avrebbe dovuto sottoporsi a una valutazione. Un produttore di soluzioni di gestione dei log gli ha a sua volta suggerito di acquistare contemporaneamente una soluzione SIEM e una soluzione di gestione dei log. Il rivenditore si è così trovato a passare direttamente dal non considerare nemmeno i suoi log al gestire un sistema avanzato di gestione dei log e una correlazione in tempo reale.

Molte organizzazioni hanno installato sia la SIEM che la gestione dei log o stanno pensando di integrare una delle due tecnologie nell'installazione esistente.

La realizzazione del progetto è durata alcuni mesi, seguendo un approccio per fasi. Il personale IT del rivenditore ha deciso di installare il sistema procedendo dall'esterno verso l'intero, sulla base di una valutazione iniziale del rischio. Il personale è partito dai firewall della rete perimetrale (DMZ) per poi passare all'inserimento di nuovi log in un apposito sistema di gestione, definendo al contempo le regole di correlazione ed eseguendo rapporti con il pacchetto per la conformità PCI DSS fornito dal produttore. Man mano che il personale ha imparato a rispondere agli avvisi, i processi sono diventati più maturi e il personale ha quindi iniziato a utilizzare anche altre funzionalità SIEM.

Nel complesso, il progetto ha consentito la creazione di un'installazione perfettamente conforme ai requisiti di registrazione PCI. L'organizzazione ha superato molto bene la valutazione PCI ed è stata lodata per il suo approccio globale alla registrazione e al monitoraggio della sicurezza. Oltre a ciò, il team addetto alla sicurezza ha dimostrato che la sua installazione SIEM PCI riesce effettivamente a soddisfare i nuovi requisiti normativi, dal momento che lo standard PCI DSS arriva a un maggiore livello di dettaglio pur coprendo essenzialmente le stesse aree di governance IT. Allo stesso tempo, gli strumenti di gestione dei log hanno anche supportato le capacità operative e l'efficienza generale dell'IT, mentre la SIEM ha offerto all'organizzazione la base per le sue capacità future di rilevamento e risposta in tempo reale.

Architettura di gestione dei log e della SIEM

Date le differenze tra le due tecnologie, molte organizzazioni hanno installato sia la SIEM che la gestione dei log o stanno pensando di integrare una delle due tecnologie nell'installazione esistente. Quali sono alcune delle più diffuse architetture congiunte di SIEM e gestione dei log?

In questa sede tratteremo quello che è lo scenario più comune: il "SIEM shield", ovvero lo "scudo SIEM". Molte delle organizzazioni che hanno installato una soluzione SIEM esistente hanno inviato troppi dati al loro sistema, sovraccaricandolo con il rischio di perdere funzionalità e dati critici. Per risolvere questo problema, hanno acquistato anche uno strumento di gestione dei log installandolo davanti alla soluzione SIEM.

Fig. 1

In questo modo, l'uso di uno strumento di gestione dei log, intrinsecamente più scalabile, davanti alla SIEM funziona da scudo e da filtro e protegge lo strumento SIEM, meno scalabile, da flussi di log eccessivamente lunghi. Non è raro che, su dieci eventi ricevuti, lo scudo ne invii uno solo alla SIEM che si trova dietro di esso. Contemporaneamente, tutti gli eventi ricevuti sono archiviati dallo strumento di gestione dei log. Ad esempio, se il volume totale dei log è di 40.000 messaggi al secondo, lo strumento SIEM riceverà solo 4.000 messaggi al secondo.

Non è raro che, su dieci eventi ricevuti, lo scudo ne invii uno solo alla SIEM che si trova dietro di esso. Contemporaneamente, tutti gli eventi ricevuti sono archiviati dallo strumento di gestione dei log.

Fig. 2

Un altro scenario è quello che vede la gestione dei log installata per prima, per creare una piattaforma aziendale di registrazione. La SIEM viene aggiunta successivamente, come una delle applicazioni di questa piattaforma. Questo scenario può essere definito una sorta di "percorso di crescita verso la SIEM" e oggi rappresenta fino al 50% delle installazioni SIEM. È il tipico caso in cui un'organizzazione si dota di uno strumento di gestione dei log e pian piano si rende conto di avere l'esigenza - oltre che di avere sviluppato una capacità - di correlazione, visualizzazione, monitoraggio, workflow e così via. Si tratta dello scenario più logico per la maggior parte delle organizzazioni, come vedremo in seguito.

Se un'organizzazione si rende conto di avere un'esigenza di correlazione, avrà bisogno di raccogliere e salvare tutti i log per poter eseguire ricerche efficienti e analizzare i dati non elaborati.

Bisogna essere pronti a rispondere meglio, prima di essere costretti a reagire in fretta. È molto più facile essere preparati a rispondere che non a monitorare.

Nel prossimo caso, SIEM e gestione dei log vengono installate una accanto all'altra, contemporaneamente. Questo è uno "scenario emergente", da momento che ormai sono in aumento i clienti che acquistano in contemporanea entrambe le tecnologie - spesso dallo stesso produttore. In effetti, se un'organizzazione si rende conto di avere un'esigenza di correlazione, avrà bisogno di raccogliere e salvare tutti i log per poter eseguire ricerche efficienti e analizzare i dati non elaborati.

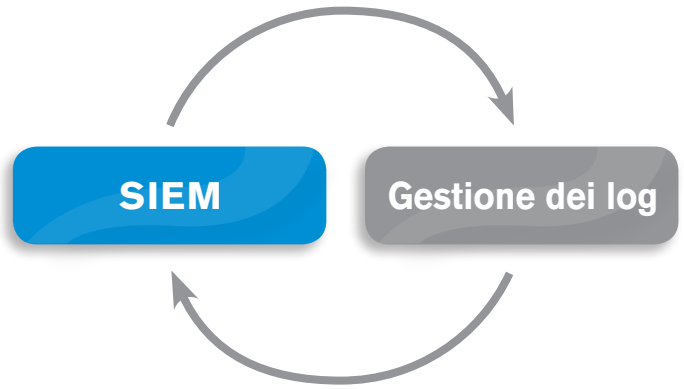

Fig. 3

L'installazione successiva è un'installazione SIEM con la gestione dei log utilizzata come archivio per i log elaborati e di altro tipo. Questo scenario si delinea quando si acquista una grande soluzione SIEM per monitorare la sicurezza e, successivamente, ci si rende conto che manca qualcosa. Di conseguenza, viene installato uno strumento di gestione dei log per il dump di tutti i log e per eseguire l'analisi dei dati non elaborati che la SIEM rifiuta, ad esempio quelli che non sa analizzare, normalizzare o categorizzare. Tutto questo porta a un caso d'uso in cui si amplia la soluzione passando dal monitoraggio della sicurezza alla risposta agli incidenti e alla conformità PCI DSS.

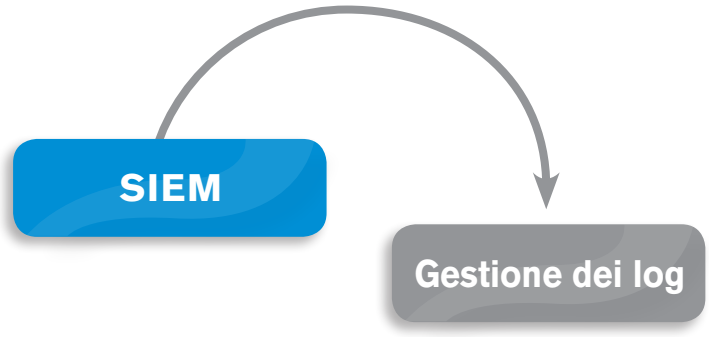

Fig. 4

Una recente analisi condotta da Gartner su come adottare la tecnologia SIEM ("How to Implement SIEM Technology", Gartner, 2009) suggerisce inequivocabilmente di "installare le funzioni di gestione dei log prima di tentare un'installazione su vasta scala della gestione degli eventi in tempo reale".

Ci sono anche molti casi di sola gestione dei log (ancora in aumento) e alcuni scenari di installazione della sola SIEM (probabilmente in calo).

Cosa installare per prima: SIEM o gestione dei log?

Fortunatamente, la domanda che verte su quale tecnologia debba essere installata per prima ha una risposta molto semplice. Se ci sono dei log, è necessaria la gestione dei log. Questo principio si applica indifferentemente alle organizzazioni dotate di un solo server e a quelle che di server ne hanno 100.000. Ovviamente, la tecnologia che queste organizzazioni dovranno installare per gestire i log sarà diversa, ma l'esistenza dei log implica la necessità di gestirli. Ad esempio, se è necessario revisionare i log da un'unica macchina, saranno sufficienti degli strumenti integrati nel sistema operativo. Se, invece, il volume quotidiano dei log raggiunge i 100 GB (una situazione non impossibile, nonostante la cifra impressionante), saranno necessari strumenti sofisticati, e quindi costosi.

Una recente analisi condotta da Gartner su come adottare la tecnologia SIEM ("How to Implement SIEM Technology", Gartner, 2009) suggerisce inequivocabilmente di "installare le funzioni di gestione dei log prima di tentare un'installazione su vasta scala della gestione degli eventi in tempo reale". Inoltre dichiara che, se la tecnologia SIEM è richiesta per motivi di conformità, l'ordine di installazione non varia: "Le prime fasi di una installazione SIEM richiesta principalmente dal PCI dovrebbe installare funzioni di gestione dei log per i sistemi che rientrano nell'ambito della valutazione PCI". In questo caso, il punto principale è che è necessario essere pronti a rispondere meglio, prima di essere costretti a rispondere in fretta.

Se ci sono dei log, è necessaria la gestione dei log. Questo principio si applica indifferentemente alle organizzazioni dotate di un solo server e a quelle che di server ne hanno 100.000.

Prima di installare la SIEM, chiedetevi quanto la vostra sicurezza è in tempo reale.

Per quanto riguarda invece le organizzazioni che hanno già installato degli strumenti SIEM, considerare al più presto una soluzione di gestione dei log è senz'altro la cosa più giusta da fare. Essere in grado di analizzare una raccolta completa di record di log potenzierà le loro capacità di indagine e le aiuterà a rispettare i requisiti di conformità.

È un'esigenza di tutte le aziende quella di passare dalla gestione dei log alla SIEM?

Cosa succede dopo che un'organizzazione installa uno strumento di gestione dei log e inizia a utilizzarlo correttamente sia per scopi di sicurezza e conformità, sia per scopi operativi? La naturale e logica evoluzione di questa situazione è il passaggio a un livello superiore con uno strumento SIEM che consenta di gestire gli eventi in tempo quasi reale.

Questo white paper è il primo documento che formula i criteri di questo passaggio. Le organizzazioni che passano troppo presto al livello superiore rischiano di sprecare tempo e lavoro, senza ottenere una maggiore efficienza nella gestione della sicurezza. Aspettare troppo a lungo, d'altra parte, può far sì che l'organizzazione non riesca mai a sviluppare le capacità necessarie per garantire la sicurezza.

In breve, i criteri sono:

- **Capacità di risposta.** *L'organizzazione deve essere pronta a rispondere agli avvisi non appena vengono generati.*
- **Funzionalità di monitoraggio.** *L'organizzazione deve disporre di funzionalità di monitoraggio della sicurezza o deve iniziare ad approntarne, istituendo un centro per le operazioni di sicurezza (SOC) o almeno un team dedicato al monitoraggio periodico continuativo.*
- **Capacità di ottimizzazione e personalizzazione.** *L'organizzazione deve accettare la responsabilità di provvedere all'ottimizzazione e alla personalizzazione dello strumento SIEM installato. Difficilmente le soluzioni SIEM pronte all'uso hanno successo o riescono a esprimere il loro potenziale completo.*

Rivediamo questi criteri in dettaglio.

In primo luogo, l'organizzazione deve essere pronta a rispondere agli avvisi non appena vengono generati. Anche se sentiamo spesso i produttori affermare che "oggi il business funziona in tempo reale, quindi anche la sicurezza dovrebbe fare altrettanto", sono poche le organizzazioni che sembrano essere in grado di raggiungere questo traguardo al momento. Prima di installare la SIEM, chiedetevi quanto la vostra sicurezza è in tempo reale. Potreste pensare che la maggior parte del tempo la sicurezza è effettivamente in tempo reale o molto vicina a questo standard. I sistemi di rilevamento delle intrusioni di rete o NIDS (Network Intrusion Detection System) individuano gli attacchi esterni in microsecondi, i firewall bloccano le connessioni non appena vengono stabilite e la tecnologia antivirus fa di tutto per catturare i virus non appena si manifestano.

Ecco perché sono poche le organizzazioni disposte ad acquistare un sistema NIDS in grado di notificare un attacco solo dopo che ne sono stati subiti altri due. Queste stesse organizzazioni, tuttavia, si limiteranno a fare controllare gli avvisi IDS agli analisti solo la mattina. Nel caso di una compromissione critica, il tempo di risposta di un millisecondo del sistema NIDS non è rilevante, mentre quello di un'ora da parte del personale lo è. Quindi, le indagini "del giorno dopo" che con l'analisi degli avvisi fanno scoprire una compromissione critica del sistema sono ancora accettabili.

Analogamente, se un file infetto arriva e il software antivirus può pulirlo in tempo reale, il problema è risolto. Se, invece, il software antivirus rileva il malware ma non può automaticamente pulirlo o metterlo in quarantena e si limita a generare un errore (ciò che succede nel caso di alcuni codici back door e trojan), la risposta spetta agli analisti che, probabilmente, sono in ritardo di alcune ore. Con le minacce sofisticate di oggi, questo tempo è spesso sufficiente perché si verifichi una violazione grave che potrebbe richiedere mesi per essere riparata. In pratica, è vero che delle regole avanzate per gli avvisi e la correlazione stateful possono fornire risposte in poche frazioni di secondo, ma è necessario essere preparati a rispondere.

Se un'organizzazione non dispone di un SOC o di capacità di monitoraggio (per scopi di sicurezza o operativi) supportate da SLA (Service Level Agreement) rigorosi, molte delle funzionalità SIEM non verranno sfruttate completamente. La prima cosa che si fa per passare dall'uso puramente reattivo dei log al monitoraggio totale della sicurezza è l'uso del monitoraggio periodico ritardato, che consiste nella revisione giornaliera dei i rapporti sui log. Questa operazione può essere svolta con l'ausilio di uno strumento di gestione dei log o di uno strumento SIEM.

L'ultimo criterio per il passaggio riguarda la capacità di ottimizzazione e personalizzazione. L'organizzazione deve accettare la responsabilità di occuparsi dell'attività di ottimizzazione e personalizzazione dello strumento SIEM installato per adattarne le potenti funzionalità al problema che l'organizzazione deve affrontare. Una seconda opzione è affidare l'ottimizzazione a un'azienda di consulenza esterna. Ogni azienda ha le sue caratteristiche e, per essere più efficace, una soluzione SIEM deve essere adatta ai processi specifici dell'azienda che la usa. In pratica, può rendersi necessario creare avvisi, scrivere regole di correlazione o personalizzare i rapporti per conoscere meglio il comportamento aziendale nei confronti di sicurezza o conformità. Le installazioni pronte all'uso che promettono una funzionalità SIEM in grado di garantire analisi ottimali raramente funzionano.

Se un'organizzazione non dispone di un SOC o di capacità di monitoraggio (per scopi di sicurezza o operativi) supportate da SLA (Service Level Agreement) rigorosi, molte delle funzionalità SIEM non verranno sfruttate completamente.

La curva della maturità si estende dalla più completa ignoranza dei log fino alla loro raccolta e permanenza, all'attività di indagine occasionale, alla revisione periodica dei log, via via fino al monitoraggio della sicurezza in tempo quasi reale.

Le organizzazioni che non hanno piani immediati per passare a un livello superiore da - ad esempio - una gestione dei log mirata alla conformità, dovrebbero scegliere uno strumento di registrazione che permetta loro di passare alla SIEM in un momento successivo. Anche in assenza di piani iniziali per andare oltre le funzioni per la conformità, molte installazioni di SIEM e gestione dei log seguono i cosiddetti modelli "compliance-plus", il che significa che lo strumento viene acquistato per un particolare framework normativo ma viene utilizzato anche per molti altri problemi di IT e sicurezza.

È interessante notare che alcuni degli strumenti di gestione dei log non permettono questo percorso di upgrade alla SIEM. In particolare, gli strumenti più semplici che permettono solo di raccogliere log non elaborati ed eseguire ricerche in tali log potrebbero essere estremamente utili e, tuttavia, non offrire un percorso semplice per ottenere anche funzioni complete per la normalizzazione e la categorizzazione dei dati dei log, nonché altre caratteristiche correlate alla sicurezza. In generale, se lo strumento scelto si occupa della raccolta e della permanenza dei record dei log e non può essere associato a una soluzione SIEM che può utilizzare tali dati per scopi di monitoraggio e analisi, l'upgrade al monitoraggio non sarà possibile e sarà necessario acquistare altri strumenti, quando l'organizzazione è pronta per il monitoraggio in tempo reale.

Dal momento che un uso efficace di una soluzione SIEM offre vantaggi diretti per quanto riguarda la riduzione delle minacce, grazie alla sua capacità di analisi avanzata mirata alla sicurezza (ma solo se l'organizzazione è pronta alla SIEM), il modello compliance-plus può essere considerato valido. Nel complesso, permette all'organizzazione di avvicinarsi di più al mito del modello "unica console di controllo della sicurezza".

Dopo la gestione dei log e la SIEM: la curva della maturità

Cosa succede subito dopo che la gestione dei log e la SIEM sono state entrambe installate e rese operative per consentire all'organizzazione di raggiungere la conformità e ottenere vantaggi in termini di sicurezza? La curva della maturità si estende dalla più completa ignoranza dei log fino alla loro raccolta e permanenza, all'attività di indagine occasionale, alla revisione periodica dei log, via via fino al monitoraggio della sicurezza in tempo quasi reale.

La tendenza della curva può essere descritta in questo modo: si parte ignoranti per divenire lentamente reattivi, poi rapidamente reattivi e infine proattivi e consapevoli di ciò che succede nell'ambiente IT. Tentare di passare direttamente dall'ignoranza alla proattività funziona solo raramente o addirittura mai.

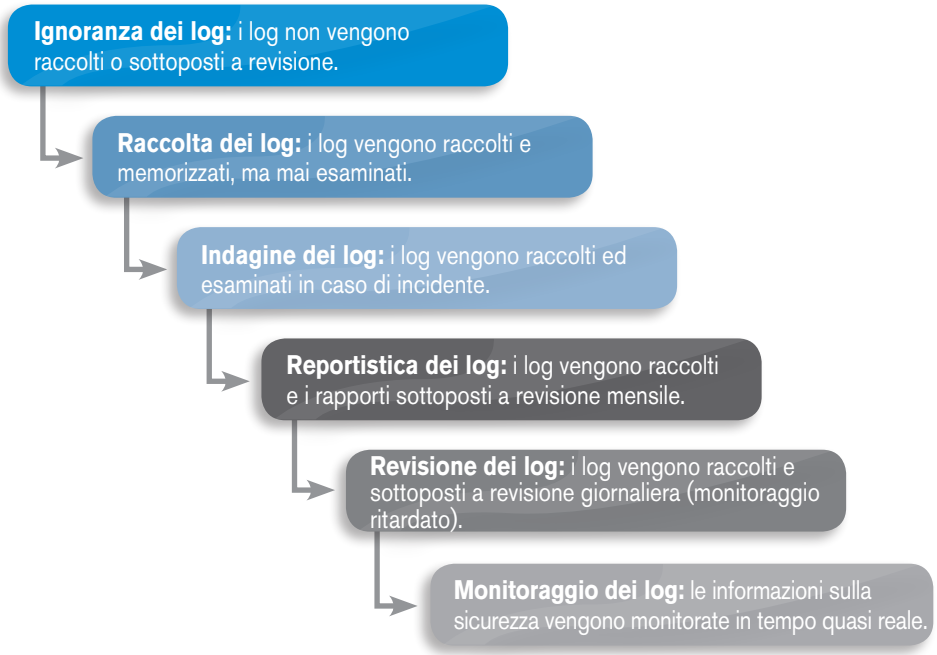

Fig. 5

Le organizzazioni dovrebbero migliorare costantemente la portata e profondità dell'installazione SIEM integrandola con più sistemi per poterne sfruttare meglio le capacità di analisi.

Qual è il passo successivo? Tanto per iniziare, le organizzazioni dovrebbero migliorare costantemente la portata e profondità della propria installazione SIEM integrandola con più sistemi per poterne sfruttare meglio le capacità di analisi. Questo comportamento permette di arrivare al centro della missione SIEM - il monitoraggio della sicurezza - e di risolvere nuovi problemi quali frodi, minacce interne, monitoraggio delle applicazioni e monitoraggio dell'attività generale degli utenti. La SIEM inizia ad acquisire più informazioni e ad ampliare il suo raggio d'azione passando dalla rete all'applicazione, da un numero limitato di origini dati all'installazione a livello aziendale. Contemporaneamente, al suo fianco comincia a crescere un'organizzazione di sicurezza che sviluppa procedure operative migliori, che rendono l'azienda più agile. Mentre si espande l'installazione, è importante ricordare che la chiave del successo risiede in un approccio per fasi.

Quali sono i sistemi che dovrebbero migliorare lo scopo della SIEM e permettere di risolvere anche altri problemi? Uno degli esempi più interessanti riguarda l'uso delle informazioni provenienti da sistemi per la gestione delle identità come, ad esempio, NetIQ Identity Manager. Le informazioni disponibili in questo sistema includono le identità degli utenti (ad esempio, nome, funzione e Business Unit) e i diritti di accesso a vari sistemi e applicazioni. Sapere chi è l'utente e cosa è autorizzato/a a fare è indispensabile per il monitoraggio delle attività interne ai fini della sicurezza.

La cosa da tenere presente è che anche se molti produttori vantano la funzione di integrazione delle identità, la maggior parte di essi garantisce esclusivamente una semplice ricerca LDAP (Lightweight Directory Access Protocol). Questi sistemi non assicurano i dati elaborati che un sistema per la gestione delle identità dovrebbe fornire per consentire alla SIEM di stabilire se alcune attività sono dannose o hanno rilevanza ai fini della conformità.

Ad esempio, permette di creare un'identità unificata per un utente e utilizzarla per monitorare le azioni di tale utente sui vari sistemi, anche se l'utente è associato a nomi e account diversi.

Inoltre, l'integrazione di Identity Manager permette al prodotto SIEM di riconoscere i login ufficiali e autorizzati dai tentativi di login back door, non autorizzati. Questa integrazione supporta anche il monitoraggio di separazione dei compiti automatizzato, consentendo al prodotto SIEM di riconoscere i ruoli non autorizzati all'esecuzione di determinate azioni.

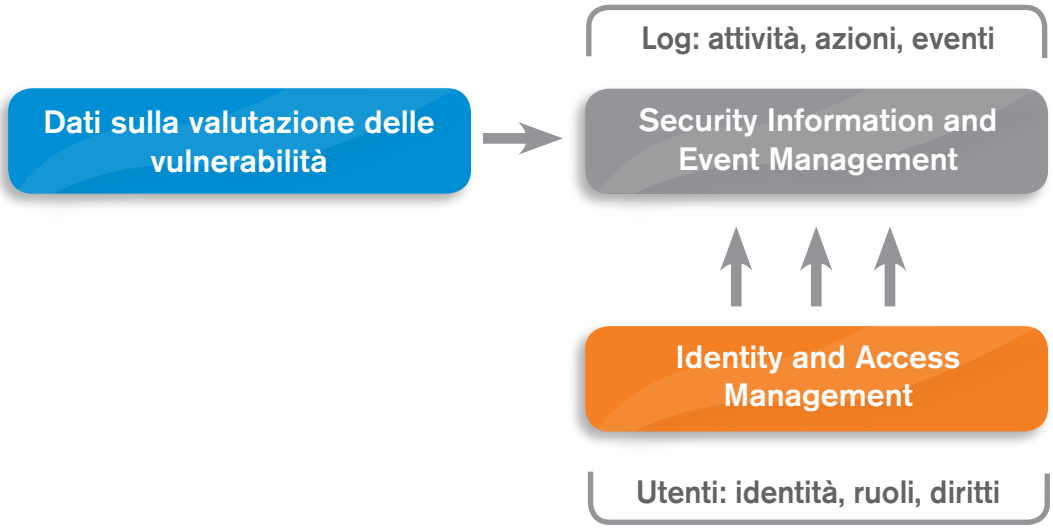

Fig. 6

In più, un sistema di gestione delle risorse conterrà informazioni dettagliate dello stesso tipo su tutte le risorse IT dell'organizzazione. Come nel caso degli utenti, è possibile estrarre i ruoli aziendali delle risorse, la criticità aziendale, la rilevanza per la conformità, i nomi degli amministratori e le ubicazioni, nonché altre informazioni sulla funzione svolta e sui responsabili. Tali informazioni migliorano notevolmente il calcolo del rischio e le funzioni di prioritizzazione degli eventi della SIEM. La cosa da tenere presente è che anche se molti produttori vantano la funzione di integrazione delle identità, la maggior parte di essi garantisce esclusivamente una semplice ricerca LDAP (Lightweight Directory Access

Protocol). Questi sistemi non assicurano i dati elaborati che un sistema per la gestione delle identità dovrebbe fornire per consentire alla SIEM di stabilire se alcune attività sono dannose o hanno rilevanza ai fini della conformità.

Livelli successivi di integrazione - e quindi di consapevolezza - possono essere raggiunti integrando il prodotto SIEM con i Configuration Management Database. Grazie a tali integrazioni, il prodotto SIEM può correlare le modifiche rilevate nei sistemi e nelle applicazioni con quelle approvate e autorizzate.

Errori

Al momento di pianificare e installare la raccolta dei log e un'infrastruttura di analisi - si tratti di SIEM o di gestione dei log - le organizzazioni spesso scoprono che le promesse di tali sistemi non vengono sfruttate appieno. Di fatto, a volte, notano una perdita di efficienza. Ciò si verifica frequentemente a causa di alcuni tipici errori di installazione.

In primo luogo, l'errore più ovvio - e purtroppo fin troppo comune - è la mancanza completa di registrazione di log, persino nell'epoca del Sarbanes-Oxley (SOX) e del PCI DSS. Questo errore impedisce qualsiasi possibilità di trarre vantaggio tanto dalla gestione dei log che dalla SIEM.

Un'altra variante di questo stesso errore è non avere nessuna registrazione e rendersene conto solo quando ormai è troppo tardi.

Come è possibile che sia troppo tardi? Non disporre di registrazione, e quindi di log, può comportare la perdita di guadagno: il mancato rispetto dei requisiti di registrazione PCI-DSS può portare all'annullamento dei privilegi di elaborazione delle carte di credito da parte di Visa o MasterCard e all'esclusione dal giro di affari; di reputazione: qualcuno ha rubato solo alcuni numeri di carta di credito dal database, ma i media hanno riferito che i numeri rubati sono quelli di tutti e 40 milioni di carte di credito, visto che non è possibile provare il contrario; e addirittura della libertà: in questo caso, è sufficiente leggere le numerose storie sul SOX apparse sui media.

Il mancato rispetto dei requisiti di registrazione PCI-DSS può portare all'annullamento dei privilegi di elaborazione delle carte di credito da parte di Visa o MasterCard e all'esclusione dal giro di affari.

Una volta che sia la SIEM sia la gestione dei log sono state rese operative, l'organizzazione può proseguire lungo la curva della maturità per passare alla visibilità completa della rete e delle applicazioni, al monitoraggio delle attività degli utenti e all'integrazione con altri sistemi.

Il traguardo è sapere cosa sta succedendo nell'ambiente ed essere in grado di rispondere agli eventi, nonché riuscire a prevedere cosa succederà in seguito.

Anche le organizzazioni più preparate incorrono spesso in questo errore. Consideriamo questo esempio. Sul vostro server Web, la funzione di registrazione è abilitata? Certo, è un'opzione di default sui due server Web più diffusi, ovvero Apache e Microsoft IIS. Il sistema operativo del vostro server registra i messaggi?

Certamente, nessuno ha cancellato */var/log/messages*. Ma riguardo al vostro database? L'opzione di default in Oracle è di non generare alcun log di controllo dei dati di accesso. Con Microsoft SQL la cosa va meglio? Purtroppo no. È necessario analizzare a fondo il sistema per poter avviare un livello, anche moderato, di generazione di audit trail.

Pertanto, per evitare questo errore, si rivela spesso necessario cambiare i valori di default e assicurarsi che su software e hardware venga abilitato un qualche livello di registrazione. Nel caso di Oracle, ad esempio, la cosa potrebbe ridursi a controllare che la variabile "audit trail" sia impostata su "db", mentre per altri sistemi la faccenda potrebbe essere più complicata.

Non sottoporre a revisione i log è il secondo errore più comune. Anche se accertarsi che i log esistano e vengano raccolti e memorizzati è importante, questa è solo una tappa del percorso. Il traguardo è sapere cosa sta succedendo nell'ambiente ed essere in grado di rispondere agli eventi, nonché riuscire a prevedere cosa succederà in seguito. Come abbiamo già detto, questa è solo una tappa, non la meta finale. Se l'azienda è appena passata dalla fase di totale ignoranza dei log a quella di raccolta, è importante sapere che alla fine sarà necessario sottoporre a revisione questi log. Raccogliere i log senza revisionarli significa solo documentare la propria negligenza, soprattutto se la policy di sicurezza IT dell'azienda prescrive tali revisioni.

Ecco perché, una volta che la tecnologia è stata approntata e i log sono stati raccolti, è necessario disporre di un processo di monitoraggio e revisione continui che si agganci a ogni eventuale azione o passaggio successivo che si renda necessario. Inoltre, il personale che revisiona o monitora i log deve disporre di informazioni sufficienti per capire bene cosa sta succedendo, se è richiesta un'azione e quale.

C'è da sottolineare che alcune organizzazioni si muovono solo parzialmente nella giusta direzione: revisionano i log dopo un incidente grave - una compromissione, una fuga di informazioni o un misterioso crash del server - ma evitano il monitoraggio e la revisione continua, trincerandosi spesso dietro la scusa della solita carenza di risorse. Questa condizione permette loro di sfruttare il vantaggio reattivo dell'analisi dei log, un fattore importante ma che impedisce di avvalersi del vantaggio proattivo: sapere quando un evento negativo è in procinto di verificarsi o sta peggiorando. Ad esempio, revisionando i log è possibile sapere che è stato attivato il failover su un firewall e, anche se questo non ha

comportato la perdita di connessione, è senz'altro un evento su cui indagare più a fondo. Se non lo si fa e la connettività di rete va perduta, sarà necessario affidarsi ai sempre utili log per capire come mai entrambi i dispositivi di failover si sono arrestati.

È anche importante sottolineare che alcuni tipi di organizzazione *hanno l'obbligo di esaminare i file di log e le tracce di controllo per conformarsi a un particolare requisito normativo*. Come già menzionato, le regole HIPAA impongono alle organizzazioni del settore sanitario di creare un programma di analisi e registrazione dei controlli. Lo standard PCI-DSS per la sicurezza dei dati include disposizioni per la raccolta e il monitoraggio dei log e per la loro revisione periodica, evidenziando il fatto che la raccolta dei log da sola non è sufficiente.

Il terzo errore comune è mantenere i log per un periodo troppo breve. Nell'archivio dei log operativi di un sistema SIEM, la permanenza degli eventi normalizzati può essere di 30 giorni, mentre per un periodo di permanenza più lungo è necessario un sistema di gestione dei log. Ciò induce i team addetti alla sicurezza o alle operazioni IT a credere di disporre di tutti i log necessari ai fini del monitoraggio, dell'indagine o della risoluzione dei problemi. Di conseguenza, dopo il verificarsi di un incidente, accade che ci si renda drammaticamente conto che tutti i log sono andati perduti a causa di una policy di permanenza poco lungimirante. Troppo spesso - soprattutto nel caso di attacchi interni - succede che l'incidente venga scoperto molto tempo - a volte molti mesi - dopo che il crimine o l'abuso sono stati commessi. In questi casi, per ottenere un qualche risparmio sull'hardware di storage si rischia di pagare una somma dieci volte superiore per sanzioni amministrative.

Troppo spesso - soprattutto nel caso di attacchi interni - succede che l'incidente venga scoperto molto tempo - a volte molti mesi - dopo che il crimine o l'abuso sono stati commessi.

Se il fattore costo è importante, la soluzione può essere quella di dividere la permanenza in due parti: storage online (che costa di più) a breve termine e storage offline (che è molto più economico) a lungo termine. Un efficace strumento di gestione dei log permette di effettuare le ricerche in modo trasparente in entrambi questi tipi di archivio, senza alcun trasferimento dei dati. Un approccio altrettanto diffuso e più consigliabile è quello a tre livelli, che risolve i limiti del precedente. In questo approccio, lo storage online a breve termine è integrato da uno storage nearline, in cui è possibile accedere ai log ed effettuare ricerche. I record dei log meno recenti e rilevanti vengono scaricati sul terzo livello, quale un nastro o un DVD, con un considerevole contenimento dei costi di storage. Questo approccio, però, non permette l'accesso selettivo ai log desiderati. Nello specifico, questo significa ad esempio che un istituto finanziario può memorizzare i log per 90 giorni nello storage online, quindi per due anni nello storage ricercabile nearline del sistema di gestione dei log e, infine, per sette anni o più su un nastro.

Il quarto errore riguarda la prioritizzazione dei record dei log. Dal momento che l'esigenza di stabilire un ordine di priorità per organizzare meglio le attività di analisi dei log è molto sentita, l'errore più comune è quello di prioritizzare i record dei log prima ancora della raccolta. Effettivamente, anche alcuni dei documenti di best practice consigliano

È necessario assicurarsi che i log delle applicazioni siano raccolti e disponibili per l'analisi e anche per la permanenza a lungo termine. Per fare in modo che questo accada, è necessario configurare il software di gestione dei log in modo che questi vengano raccolti e stabilire una policy di revisione dei log che includa sia la revisione contestualizzata in caso di incidente che la revisione periodica proattiva.

di raccogliere solo "i dati importanti". Ma quali sono i dati importanti? Ecco il punto in cui questi documenti guida si rivelano carenti, non offrendo spiegazioni chiare in merito. Esistono, è vero, diversi approcci possibili a questo problema, ma possono portare a evidenti falle nella sicurezza o addirittura compromettere le iniziative per la conformità normativa. Ad esempio, molti potrebbero affermare che i log sulla prevenzione e il rilevamento delle intrusioni di rete siano per loro natura più importanti dei log sui concentratori VPN (Virtual Private Network). Questo può essere vero in un mondo in cui le minacce esterne sono predominanti ed è possibile avere fiducia in dipendenti e partner. I log sulle VPN, insieme a quelli su server e workstation, sono quelli più utili quando bisogna condurre un'indagine interna su una perdita di informazioni o anche un'infezione da malware. Affermazioni simili sulla maggiore importanza di qualsiasi altro tipo di log sono altrettanto discutibili e questo potrebbe portarci alla triste constatazione che è necessario raccogliere tutti i record di log prodotti o almeno la maggior parte di essi. Ma sarebbe possibile? Prima di rispondere a questa domanda, proviamo a capire se è possibile richiamare i log più importanti prima di averli esaminati e questo problema non sembrerà più irrisolvibile. Di fatto, esistono delle soluzioni convenienti che garantiscono esattamente ciò.

Il modo per evitare questo errore è installare la gestione dei log prima della SIEM, come indicato in precedenza. In questo modo, tutti i log necessari saranno disponibili per l'analisi, anche se solo una percentuale di questi è visibile dal motore di correlazione di una SIEM.

L'ultimo errore è quello di ignorare i log registrati dalle applicazioni, concentrandosi solo su quelli dei dispositivi di rete interni e sul perimetro, magari anche dei server.

L'insieme delle applicazioni aziendali va da applicazioni SAP e PeopleSoft a piccole applicazioni fatte in casa che comunque gestiscono processi di importanza critica per molte aziende. Poi ci sono anche le applicazioni esistenti ed eseguite su sistemi mainframe e midrange che, a loro volta, eseguono spesso i processi aziendali di base. La disponibilità e la qualità dei log varia notevolmente da un'applicazione all'altra e va da un livello di carenza totale (nel caso di molte applicazioni sviluppate internamente) a un livello estremamente dettagliato e voluminoso (come nel caso di molte applicazioni mainframe). La mancanza di standard di registrazione comuni e anche di una guida alla registrazione per gli sviluppatori di software fa sì che i log delle applicazioni siano alquanto problematici. Per fortuna sono in corso iniziative come la Common Event Expression (CEE) di MITRE che risolveranno questo problema in futuro.

Nonostante i problemi, è necessario assicurarsi che i log delle applicazioni siano raccolti e disponibili per l'analisi e anche per la permanenza a lungo termine. Per fare in modo che questo accada, è necessario configurare il software di gestione dei log in modo che questi

vengano raccolti e stabilire una policy di revisione dei log che includa sia la revisione contestualizzata in caso di incidente che la revisione periodica proattiva. Occorre pertanto scegliere un produttore che garantisca una facile configurazione del sistema per la raccolta dei log dalle applicazioni personalizzate, che spesso si rivelano quelle più importanti. Successivamente, è possibile configurare la SIEM in modo che analizzi questi log ai fini della sicurezza, insieme ai log della rete e di altro tipo.

È possibile che un'organizzazione debba tornare a scuola di registrazione prima di potersi "laureare in SIEM". Questa "laurea" richiede la capacità di rispondere agli avvisi e di personalizzare e ottimizzare i prodotti.

Conclusioni

Una delle principali conclusioni di questo lavoro è che tutti hanno a che fare con i log, il che significa che tutti hanno in ultimo bisogno di un qualche sistema di gestione dei log. Nella sua accezione più ampia, gestione dei log significa semplicemente utilizzo dei log. Chiunque abbia a che fare con i log deve utilizzarli, se non altro perché ciò viene imposto do molti dei più recenti requisiti normativi.

È anche importante ricordare che i log vengono utilizzati in moltissime situazioni, che vanno dalla tradizionale risposta agli incidenti a quella più sofisticata. Nella maggior parte dei casi, i log vengono utilizzati molto tempo dopo che l'evento si è verificato ed è stato registrato nei log. È molto più facile essere preparati a rispondere che non a monitorare.

È possibile che un'organizzazione debba tornare a scuola di registrazione prima di potersi "laureare in SIEM". Questa "laurea" richiede la capacità di rispondere agli avvisi e di personalizzare e ottimizzare i prodotti.

Una volta che sia la SIEM sia la gestione dei log sono state rese operative, l'organizzazione può proseguire lungo la curva della maturità per passare alla visibilità completa della rete e delle applicazioni, al monitoraggio delle attività degli utenti e all'integrazione con altri sistemi.

Informazioni sull'autore

Il Dott. Anton Chuvakin (**www.chuvakin.org**) è un affermato esperto di sicurezza nel settore della gestione dei log e della conformità PCI-DSS. È l'autore dei libri "Security Warrior" e "PCI Compliance" e ha collaborato con "Know Your Enemy II", "Information Security Management Handbook" e altre pubblicazioni. Chuvakin ha pubblicato numerosi

Clienti e partner scelgono NetIQ per risolvere in modo economicamente conveniente le problematiche di protezione delle informazioni e le complessità degli ambienti IT.

documenti su argomenti quali gestione dei log, correlazione, analisi dei dati, PCI-DSS e gestione della sicurezza (per un elenco, visitate **www.info-secure.org**). Il suo blog **www.securitywarrior.org** è uno dei più visitati del settore. A queste attività affianca quella dell'insegnamento ed è spesso impegnato in conferenze sulla sicurezza in vari paesi del mondo, tra cui, di recente, Stati Uniti, Regno Unito, Singapore, Spagna Russia e altri ancora. È un esperto degli standard di sicurezza emergenti ed è consulente per numerose start-up operanti nel settore della sicurezza.

Al momento Chuvakin è impegnato nello sviluppo della sua attività di consulenza sulla sicurezza, **www.securitywarriorconsulting.com**, la cui area di interesse è la conformità al PCI-DSS per i produttori di soluzioni di sicurezza e le organizzazioni Fortune 500. Il Dott. Anton Chuvakin è stato Director of PCI Compliance Solutions di Qualys. Prima di tale incarico, ha lavorato in Log Logic come Chief Logging Evangelist per insegnare al mondo l'importanza della registrazione per scopi operativi, di sicurezza e di conformità. Ancora prima, ha ricoperto un ruolo strategico di gestione dei prodotti per un fornitore di soluzioni di sicurezza. Ha conseguito la laurea presso la Stony Brook University.

Informazioni su NetIQ

NetIQ è un produttore di software costantemente impegnato nella realizzazione di soluzioni che favoriscono il successo dei clienti. Clienti e partner scelgono NetIQ per risolvere in modo economicamente conveniente le problematiche di protezione delle informazioni e le complessità degli ambienti IT. Il portafoglio di soluzioni scalabili e automatizzate per la gestione di sicurezza e conformità, identità e accessi e prestazioni e disponibilità, oltre all'approccio pratico alla soluzione delle problematiche IT, aiuta i clienti a ottenere risparmi sui costi e miglioramenti aziendali dimostrabili e di più alto valore strategico rispetto agli approcci alternativi.

Per ulteriori informazioni, visitare il sito: **www.netiq.com**

NetIQ
Milano
Via Enrico Cialdini, 16
20161 Milano (MI)
Italia
Tel: +39 02 36634900

Roma
Palazzo dell'Arte Moderna – EUR
P.zza Marconi 15
00144 Roma
Italia
Tel: +39 06 32803663

info@netiq.com
www.netiq.com/communities
www.netiq.com

Per un elenco completo dei nostri uffici in Nord America, Europa, Medioriente, Africa, Asia-Pacifico e America Latina, visitate www.netiq.com/contacts.

www.netiq.com

www.netiq.com