XSECURE

LA SOLUZIONE DI LOG-MANAGEMENT

LE ESIGENZE DI MERCATO

Le norme e le direttive europee sulla privacy richiedono la raccolta sicura dei dati, la loro conservazione per lunghi periodi di tempo e la revisione regolare dei file di log; tutto questo serve a verificare che siano stati introdotti i controlli informatici necessari a proteggere la riservatezza dei dati sensibili, come le informazioni legate alle carte di credito, le diagnosi cliniche o i dati di carattere finanziario.

L'afflusso di dati sulla sicurezza produce milioni di messaggi ogni giorno, con un sovraccarico di informazioni generate in modi diversi, presentate in formati non omogenei, memorizzate o utilizzate per attività di reporting in luoghi differenti. In un ambiente di questo tipo, diventa praticamente impossibile individuare gli eventi che richiedono attenzione immediata o, cosa ancora più importante, quali di essi rappresentano l'inizio di un attacco in grado di paralizzare le attività. Altrettanto difficile è individuare la vulnerabilità, la causa alla base delle violazioni della sicurezza, soprattutto in un ambiente configurato in modo inadeguato.

Avviene così che, da un lato, le imprese sono continuamente sollecitate a fornire puntualmente report e ad identificare rapidamente eventuali violazioni delle regole, mentre, dall'altro lato, le misure di sicurezza preventiva e la rispondenza alle norme richiedono una analisi quotidiana di informazioni provenienti dalle fonti più disparate.

I FILE DI LOG

I file di log contengono informazioni relative alla gestione della sicurezza e sono generati da molte fonti eterogenee tra cui: Sistemi Operativi, Applicazioni, Apparati di Networking, Firewall, sistemi di Intrusion detection e prevention. Molte organizzazioni ignorano i file di log finchè non si verifica un problema di sicurezza.

IL LOG MANAGEMENT

La raccolta dei log, la loro memorizzazione e la successiva analisi sono compiti di per sé scoraggianti: un normale ambiente elaborativo può generare milioni di eventi al giorno, l'equivalente di terabyte di dati in un mese; per di più, così come sono diversificate le sorgenti dei dati di log, anche i loro formati risultano eterogenei. Individuare chi ha assegnato un privilegio ad un utente, chi ha avuto accesso ad un certo dato, quando è stata creata un'utenza o quando una configurazione è stata modificata è un compito arduo. Le soluzioni di Log Management permettono una forte riduzione dei costi informatici e una notevole diminuzione dei rischi di inadempienza rispetto ai requisiti normativi.

Grazie all'automazione della raccolta e dell'elaborazione dei log, si evita di dover effettuare costosi ed inefficienti processi manuali, mentre ai dati rilevanti che riguardano la sicurezza viene attribuito il giusto livello di attenzione. Infine, come ulteriore vantaggio, vi è la possibilità di fornire agli auditor sia interni che esterni le informazioni di cui hanno bisogno nel momento stesso in cui le chiedono.

Questo tipo di analisi può aiutare a identificare le cause degli incidenti e spesso aiuta a prevenirle e non può che essere fatta attraverso l'uso di strumenti appropriati.

LA SOLUZIONE: XSECURE

Xech ha realizzato XSecure, la soluzione per aiutare le imprese a raggiungere gli obiettivi di sicurezza e conformità normativa sia attuali che futuri.

XSecure, caratterizzata da ristretti tempi di implementazione, gestisce elevati volumi di log, facilita le analisi e la produzione di report, semplifica le attività di audit, le analisi di sicurezza, le attività di conformità.

XSecure raccoglie, filtra, normalizza, archivia e centralizza i log provenienti da fonti eterogenee. Permette la correlazione di eventi e rende disponibili funzionalità di ricerca. Riduce in modo significativo il costo e la complessità delle attività di analisi.

Grazie ad allarmi generati in caso di violazione delle policy definite dall'organizzazione XSecure consente una reazione in tempo reale mentre la ricca reportistica immediatamente disponibile alleggerisce il compito, altrimenti gravoso, di fornire le prove delle conformità normative.

XSecure garantisce la raccolta e l'aggregazione dei dati di log ed è in grado di comprimere ed archiviare i dati di audit sia grezzi che normalizzati. Utilizzando le capacità di ricerca risulta possibile investigare rapidamente sulle attività degli utenti e sui loro accessi alle risorse.

LE FUNZIONALITÀ

RACCOLTA DI DATI

XSecure è in grado di raccogliere log da varie sorgenti come sistemi operativi, data base, applicazioni, apparati di networking. L'architettura del prodotto permette di effettuare la ricerca e la raccolta distribuita dei log con la scalabilità necessaria a supportare elevati volumi di eventi provenienti da numerose sorgenti di dati.

SCALABILITA' E PERFORMANCE

XSecure è stato progettato per sostenere un alto numero di eventi raccolti dai log. A tal fine utilizza Oracle Berkeley DB per la gestione e la memorizzazione delle informazioni.

In una delle sue reali applicazioni XSecure raccoglie oltre 5 miliardi di eventi al giorno e sono stati effettuati test di performance che hanno dimostrato la capacità di raggiungere picchi di 400.000 eventi al secondo (singola CPU).

COMPRESSIONE E ARCHIVIAZIONE DEI LOG

XSecure è progettato per comprimere in modo efficiente i log con un rapporto fino a 10:1, contribuendo così a ridurre i costi dello storage.

ENCRYPTION E SIGNATURE

XSecure è progettato per criptare, totalmente o in parte, i dati raccolti. Inoltre, è possibile aggiungere delle signature al fine di proteggere le informazioni raccolte e di verificare l'eventuale modifica non autorizzata dei dati archiviati.

REPORTISTICA

XSecure offre modelli predefiniti e personalizzabili per la creazione di report, mappati sulle linee guida più comuni in merito alle verifiche di sicurezza e alle normative. I report possono essere generati a richiesta o su base regolare e possono essere automaticamente inviati via e-mail. Inoltre, XSecure permette di personalizzare report specifici per le proprie necessità.

FACILITÀ DI IMPLEMENTAZIONE E GESTIONE

L'implementazione di XSecure è estremamente semplice e produce da subito benefici tangibili mediante la raccolta dati, strumenti per la ricerca e l'analisi, nonché report e query immediatamente utilizzabili.

PROFILAZIONE UTENTI

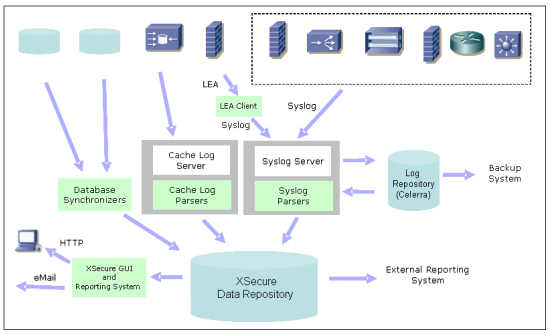
XSecure permette la profilazione degli utenti in modo da definirne varie tipologie con molteplici possibilità di analisi di fonti differenti.

PLUG-IN

XSecure utilizza le tecnologie che i vari sistemi mettono a disposizione e consente quindi differenti tipologie di raccolta dei log, sia agent che agent-less. In modalità agent-less (per esempio syslog) non è necessario installare alcun tipo di software all'interno del sistema da cui si vuole raccogliere i log. In modalità agent è possibile installare software proprietari particolarmente efficienti che raccolgono le informazioni e le inviano al sistema.

FILTRI

I plug-in hanno la possibilità di definire filtri per raccogliere e inviare a XSecure esclusivamente le informazioni ritenute importanti al fine di non saturare le infrastrutture di network.



ALLARMI

XSecure permette l'attivazione di allarmi che segnalano il verificarsi di particolari condizioni. Inoltre, consente di verificare che le fonti stiano effettivamente trasmettendo le informazioni e segnala eventuali anomalie. È possibile definire differenti canali (e-mail, sms, ...) per segnalare gli eventi.

WEB-BASED

XSecure è una soluzione web-based che permette non solo la consultazione dei dati raccolti e la produzione e distribuzione di adeguata reportistica, ma anche la configurazione delle fonti e dei dati da raccogliere

XECH S.r.l.
via Cesare Ajraghi 30 - 20156 Milano
Tel: +39 0239219548 | Fax: +39 02700403123
P.IVA e C.F. 04029390962