

Il Security Information Management (SIM)

Come ridurre gli eventi indesiderati nell'infrastruttura informatica aziendale?

L'architettura di rete e di sicurezza informatica di ogni azienda è composta da molti elementi quali ad esempio router, firewall, IDS, sistemi antivirus, server applicativi, etc.

Normalmente questi elementi richiedono competenze specifiche e sono gestiti da persone diverse: allarmi, segnalazioni e log non vengono quasi mai raffrontati per determinare se sono in corso attacchi o abusi di risorse sensibili.

Analogamente, è difficile controllare che tutti i sistemi rispettino le policy di sicurezza aziendale, generando ad esempio delle segnalazioni utili all'analisi forense successiva ad un evento che impatta sulla sicurezza informatica, nel rispetto delle normative vigenti.

Premessa

Disporre di una **piattaforma centralizzata** di raccolta e correlazione dei log, segnalazioni ed allarmi **di tutti gli apparati e servizi di rete e sicurezza**, consente agli amministratori ICT di rilevare con un elevato grado di efficienza le violazioni alle politiche di sicurezza o gli abusi da parte di soggetti autorizzati.

La possibilità di **generare allarmi** (p.e. con invio di email o sms) che vengono innescati al **verificarsi di eventi di particolare gravità** su uno o più sistemi, e la disponibilità di report con il massimo livello di dettaglio sull'utilizzo di risorse o minacce alla sicurezza, diventano quindi strumenti indispensabili per sapere in tempo reale cosa sta accadendo sulla propria rete.



Obiettivi e funzionalità del servizio

NEST2 offre un servizio centralizzato per gestire e monitorare lo stato dell'infrastruttura di rete aziendale.

Il servizio prevede la collocazione nella sede del centro stella del cliente di un server che si interfaccia con tutti gli elementi sensibili dell'architettura di rete e sicurezza del cliente.

Il server raccoglie e storicizza tutti i log generati da firewall, router, sistemi operativi e da altri apparati e li trasferisce in modo autenticato e crittografato (in modo da garantirne integrità e confidenzialità) alla **piattaforma di analisi e correlazione** collocata presso il **SOC (Security Operation Center)** di NEST2.



Le principali caratteristiche della piattaforma sono le seguenti:

- **Log Management.** Gestione dei log provenienti dagli apparati della sede cliente
- **Analisi delle vulnerabilità.** Consente di raffrontare i dati raccolti con le vulnerabilità riscontrate nei sistemi
- **Monitoring e alerting.** Monitoraggio e sistema di allarme in tempo reale
- **Compliance Management.** Consente di gestire l'archiviazione dei log e la produzione di report secondo le regole dettate dai più importanti standard internazionali, quali SOC, PCI, GLBA, HIPAA, FISMA
- **Forensics Analysis.** Consente di effettuare ricerche storiche su ampi volumi di log provenienti da sorgenti diverse, allo scopo di supportare l'investigazione nel caso di incidenti di sicurezza o comportamenti dubbi da parte di impiegati

Sono inoltre disponibili **ampie funzionalità di reporting** (più di 1200 tipologie di report personalizzabili) e la possibilità da parte del personale

autorizzato del cliente, di accedere ad un portale web dove è possibile:

- Accedere a dei cruscotti (dashboard) personalizzati che sintetizzano lo stato di sicurezza e disponibilità dell'infrastruttura
- Eseguire dei report customizzati
- Accedere direttamente ai log prodotti dagli apparati (se autorizzati)

Vantaggi

- Visione "integrata" degli eventi e dei trend di sicurezza a livello di architettura e non più a livello di singolo apparato o tecnologia
- Rilevazione immediata di eventi/attacchi non facilmente identificabili da un singolo apparato (ad esempio abusi da parte di utenti leciti)
- Alerting via mail o sms sugli eventi
- Visuale immediata dello stato e del trend di rischio (grazie a report e dashboard)
- Gestione completa dei log nel rispetto delle più recenti normative
- Supporto di un team di specialisti di sicurezza per analisi e consulenze
- Piattaforma di altissimo livello ad una frazione del costo (grazie all'economia di scala su molti clienti)

Applicazioni

- Aziende di qualsiasi dimensione che gestiscono dati sensibili
- Ambienti che gestiscono transazioni economiche
- Aziende che vogliono massimizzare gli investimenti già effettuati in tecnologie di comunicazione e sicurezza

