Il SIEM cresce e sfocia in altri servizi

Dic 19, 2019 Giancarlo Calzetta Approfondimenti, In evidenza, RSS, Software 1

Sviluppare un SIEM efficace al giorno d'oggi significa mettere le mani in pasta in moltissimi aspetti della sicurezza e questo permette di creare nuovi servizi.

I software SIEM sono da sempre degli ottimi alleati dei responsabili della sicurezza. Considerato quanti prodotti bisogna inserire nella infrastruttura per proteggere utenti e dati da **una quantità di minacce sempre maggiore**, al giorno d'oggi non può mancare un aiuto nella gestione degli eventi e delle segnalazioni che arrivano da decine di console diverse.

"Per questo" – dice Massimo Turchetto, CEO e fondatore di SGbox – "le aziende apprezzano sempre di più i SIEM, soprattutto dalle medie dimensioni in su". In effetti, tutti gli strati che compongono la difesa di un'azienda moderna generano una **quantità di allarmi ingestibile** per un team "umano" senza un aiuto tecnologico concreto.

SGBox sviluppa SIEM in Italia da sette anni e il suo prodotto si è sempre distinto per performance e comodità d’uso. Oltre al classico motore di Log Management, che da sempre è alla base di questo tipo di soluzioni, la piattaforma si è sviluppata fino a garantire anche una funzione di Log Correlation, ovvero **un sistema che mettere in relazione tra loro gli eventi registrati da prodotti diversi** per scovare segni di compromissione o di attacco ed elevare il livello della segnalazione.

“A breve” – continua Turchetto – “arriverà anche un motore di analisi del comportamento degli utenti che migliorerà ulteriormente la qualità delle rilevazioni”.

Il SIEM, quindi, non è più solo un "punto di raccolta" per gli allarmi, ma **un sistema intelligente in grado di fornire un aiuto notevole** nel catalogare e gerarchizzare le investigazioni.

Un sistema che, inevitabilmente, **crea fortissime competenze in molti settori della sicurezza informatica** e che SGBox va a sfruttare tramite una offerta di servizi alle aziende che andrebbe vista come un percorso.

I primi due sono assessment, ovvero **analisi e report, rispettivamente sulle vulnerabilità e sullo stato della rete aziendale** (dispositivi presenti, appliance, connessioni e così via). Condotti tramite procedure automatizzate e operazioni manuali, forniscono la base per organizzare la vera e propria difesa, partendo da un quadro completo sul quale operare.

A seguire, è disponibile un servizio di **penetration testing** volto a verificare quanto le contromisure in essere riescano a far fronte agli attacchi. Le operazioni sono molto flessibili e si basano sulle linee guida del NIST (National Institute of Standards and Technology).

"In futuro" – conclude Turchetto – "andremo a raffinare sempre più i prodotti disponibili e a crearne di nuovi per sostenere anche la nostra crescita sul mercato estero."

Condividi l'articolo

Attenti agli insider: spesso la minaccia arriva dall'interno

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/12/19/il-siem-cresce-e-sfocia-in-altri-servizi/