PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 5026 di Mercoledì 13 ottobre 2021

Sicurezza informatica: gli acronimi SIEM e SOAR

Nel mondo dell'informatica gli acronimi rappresentano uno standard espressivo, che talvolta mette in difficoltà i lettori. È opportuno offrire aggiornamenti periodici su nuovi acronimi, che spesso rapidamente dilagano nei testi di sicurezza informatica.

Ecco due acronimi che stanno apparendo sempre più spesso sui testi di sicurezza informatica:

SIEM e SOAR.

Vediamone il significato, tenendo presente che le funzionalità degli interventi descritti da questi acronimi sono spesso collegate.

SIEM- Security Information and Event Management

Questo acronimo fa riferimento a un approccio tecnologico alla gestione della sicurezza informatica, grazie al quale le squadre addette alla sicurezza aggregano dati significativi, che vengono dall'intero sistema informativo, analizzano ed identificano delle possibili deviazioni da comportamenti, che vengono normalmente ritenuti come accettabili; sulla base dell'analisi e della valutazione di queste deviazioni, si possono prendere appropriate azioni correttive.

Questo primo acronimo fa riferimento ad attività che sono già da tempo presenti nella gestione dei sistemi informativi, mentre, come vedremo in seguito, il secondo acronimo fa riferimento ad attività relativamente innovative.

Le applicazioni SIEM effettuano un'analisi in tempo reale del flusso dei dati e del loro trattamento, allertando i responsabili della sicurezza quando vengono individuate situazioni anomale. Queste situazioni anomale possono fare riferimento a una possibile violazione in corso, ma, se l'applicativo è correttamente gestito, ISO può anche predire la possibilità di una violazione, attivando tempestivamente i processi di messa sotto controllo.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

SOAR - Security Orchestration, Automation and Response

Ci troviamo davanti a un gruppo di programmi, fra loro collegati, che aiutano la squadra addetta alla sicurezza informatica nel raccogliere dati afferenti a minacce per la sicurezza e, nei limiti del possibile, automatizzare la risposta a possibili incidenti. La piattaforma SOAR si indirizza evidentemente a situazioni similari, ma l'obiettivo di questi programmi è quello di garantire il regolare funzionamento di un sistema operativo, cercando di rendere automatica la identificazione dei rischi e l'attivazione di procedure di risposta.

Un vantaggio di questa piattaforma sta nel fatto che la discrezionalità, che talvolta è presente nell'attivazione di programmi di risposta a possibili rischi, viene fortemente ridotta, lasciando poco spazio a possibili distrazioni da parte degli operatori.

Adalberto Biasiotti

Licenza Creative Commons

---

www.puntosicuro.it