Contribution ID: **367** Type: **Presentazione orale**

Progettazione e test di un NextGen SOC "Security Onion" AI-Based

Wednesday, 28 May 2025 12:00 (30 minutes)

Nel panorama attuale della cybersecurity, minacce sempre più sofisticate come APT, ransomware e attacchi zero-day richiedono strategie di difesa reattive ma soprattutto proattive, in grado di rilevare e mitigare rapidamente attività anomale e malevole. La realizzazione di un Security Operations Center (SOC) è una delle risposte più efficaci, ma spesso è percepita come una soluzione accessibile solo a realtà di grandi dimensioni, a causa dei costi elevati delle piattaforme commerciali.
In questo contesto si inserisce Security Onion, una piattaforma open source che consente di costruire un SOC completo e modulare. L'architettura del SOC qui presentata è costituita da una macchina centrale su cui è installato Security Onion in modalità standalone. Abbiamo collegato alcuni nodi configurati per generare e ricevere traffico benigno e malevolo rappresentativo di situazioni reali, al fine di condurre test realistici di detection e risposta.
Il flusso operativo si sviluppa in tre fasi principali:
1) SIEM: Raccolta, parsing e correlazione dei log
2) SOAR: Automazione della risposta e gestione degli incidenti
3) Monitoraggio degli host
Per migliorare il framework è stato sviluppato e integrato nella pipeline di Security Onion un modulo IDS AI-based per analizzare in tempo reale il traffico di rete. Questo modulo applica modelli di machine learning per rilevare comportamenti anomali e potenziali attacchi sconosciuti, con l'obiettivo di ridurre i falsi positivi e migliorare la capacità di individuare minacce emergenti.
L'intero sistema è stato implementato in ambiente di test, sfruttando una macchina fisica del CNAF per la parte centrale e un'infrastruttura virtualizzata per i test. Abbiamo collegato alcuni nodi configurati per generare e ricevere traffico benigno e malevolo rappresentativo di situazioni reali, al fine di valutare l'efficacia del sistema in scenari concreti.
Lo scopo finale del progetto è arrivare a una configurazione granulare e distribuita, in cui un SOC centrale sarà in grado di permettere un monitoraggio attivo e proattivo della sicurezza informatica dell'intera organizzazione, con un'infrastruttura modulare, scalabile e sostenibile.

Primary authors: STELLACCI, Simona Maria (INFN); Mr REGA, Vincenzo (Istituto Nazionale di Fisica Nucleare)

Presenter: Mr REGA, Vincenzo (Istituto Nazionale di Fisica Nucleare)

Session Classification: Security e compliance

Track Classification: Security e compliance