Contribution ID: **30** Type: **Presentazione orale**

Integrazioni Avanzate tra OpenSearch (BDP), Wazuh, MISP e Suricata

Friday, 24 May 2024 09:00 (25 minutes)

Per tenere sotto controllo la postura di sicurezza del CNAF abbiamo installato e configurato un'istanza Clusterizzata di Wazuh, integrandola con la Big Data Platform (BDP) invece di utilizzare il suo Opensearch nativo.

Questa istanza e' stata in seguito Customizzata sia abilitando capacita' disattivate di default come il System Integrity Monitoring e la Vulnerability Detection, che integrandolo con prodotti esterni come il Suricata Intrusion Detection e usando MISP (Malware Information Sharing Platform) come sorgente di eventi interessanti da rilevare qualora capitassero sulle nostre macchine.

Queste integrazioni hanno richiesto cambiamenti a livello di codice sia nella parte OSSEC per la gestione delle opzioni, delle regole, e delle directory di osservazione, che al livello di codice data la necessità di script in Pyhton per consentire la comunicazione tra le varie piattaforme mediante servizi RestAPI.

L'utilizzo congiunto del MISP e del sistema IDS permette inoltre di personalizzare anche le regole che generano gli allarmi, cosi facendo vi è la possibilità di utilizzare l'Active Response di Wazuh per poter agire immediatamente non appena viene trovata un'anomalia.

Primary author: AMORI, Francesco (Istituto Nazionale di Fisica Nucleare)

Presenter: AMORI, Francesco (Istituto Nazionale di Fisica Nucleare)

Session Classification: Sessione "Servizi ICT"

Track Classification: Servizi ICT