Contribution ID: **147** Type: **Presentazione orale**

Il SOC dell'INFN: fare tesoro delle esperienze locali per costruire un SOC nazionale - Endpoint Detection and Response all'INFN

Thursday, 25 May 2023 17:30 (45 minutes)

Descriveremo una proposta operativa per l'implementazione di una piattaforma distribuita di analisi e ricerca di correlazioni tra eventi di sicurezza, dispiegabile nel neonato SOC INFN. Mostreremo alcune possibili soluzioni per l'integrazione di strumenti per la raccolta di metriche e log partendo dalle esperienze fatte nelle varie sedi INFN tentando di metterle a fattor comune. Mostreremo lo stato di dispiegamento del sistema di EDR basato su tecnologia Microsoft. Descriveremo le differenti funzionalita'e disponibilita'per i vari sistemi operativi supportati. Analizzeremo l'organizzazione logica dell'infrastruttura: policy, onboarding, gestione console. Proporremo un possibile piano operativo per il dispiegamento della piattaforma stessa. Approfondiremo le possibili integrazioni tra i vari strumenti : Wazuh (log and event analysis - SIEM), Microsoft Defender (Enpoint Detection and Response - EDR), MISP (Threat intelligence), Splunk (Security Information Event Management - SIEM).

Primary author: PECO, Gianluca (Istituto Nazionale di Fisica Nucleare)

Presenter: PECO, Gianluca (Istituto Nazionale di Fisica Nucleare)

Session Classification: Servizi ICT

Track Classification: Servizi ICT