SOAR Playbook Development

This SOAR playbook enhances phishing incident response by automatically ingesting alerts from Wazuh and extracting associated IP indicators. It performs multi-source threat intelligence enrichment to evaluate reputation and risk. Based on predefined decision thresholds, malicious IPs are blocked through CrowdSec, and a comprehensive case is created in TheHive with supporting evidence. The automation reduces analyst workload, improves response time, enforces standardized containment actions, and maintains full audit visibility for investigation and compliance purposes.