SOAR Playbook Development – Automated Phishing Response

Security Orchestration, Automation, and Response (SOAR) platforms are designed to automate repetitive SOC tasks and improve incident response speed. In this exercise, a playbook was designed to automatically respond to phishing-related alerts by validating IP reputation, blocking malicious sources, and generating an incident case.

Playbook Objective

The objective of the playbook is to automatically handle High-priority phishing alerts by performing validation, containment, and case creation without requiring manual Tier 1 intervention.

Playbook Workflow (Splunk Phantom)

The following automated workflow was designed:

1. Trigger when a phishing alert is generated in the SIEM.
2. Extract source IP from the alert.
3. Check IP reputation using threat intelligence integration.
4. If IP is malicious → block using CrowdSec.
5. Automatically create a case in TheHive.
6. Notify SOC Tier 2 if severity remains High.

This workflow ensures faster containment and reduces Mean Time to Respond (MTTR).

Playbook Test Simulation

A mock phishing alert was simulated in the SIEM environment to validate automation execution.

Playbook Step	Status	Notes
Check IP	Success	IP flagged as malicious

Block IP	Success	CrowdSec blocked 192.168.1.102
Create Case	Success	TheHive case generated automatically

The automation executed successfully, confirming that the IP was validated, blocked, and logged for further investigation.

Playbook Summary

The SOAR playbook automated phishing incident response by validating IP reputation, blocking malicious sources, and creating an incident case in TheHive. Automation reduced manual workload, improved response consistency, and accelerated containment. Implementing structured playbooks enhances SOC efficiency and ensures standardized handling of high-severity alerts.