SOAR Playbook Development Report

1. Executive Summary

The objective of this activity was to design, implement, and validate a SOAR playbook that automates phishing incident response. The playbook evaluates IP reputation, applies preventive containment using CrowdSec, and creates an incident ticket in TheHive to ensure visibility and auditability of response actions.

2. Playbook Steps

Step 1: Playbook Creation

Playbook Created

Step 2: IP Reputation Check

The playbook evaluated the extracted IP to determine maliciousness.

- The IP 192.168.1.102 was identified as a private/internal address
- No malicious reputation was detected
- The IP was classified as not suspicious

Despite the clean reputation result, the playbook continued execution based on phishing alert context and zero-trust policy.

Step 3: Preventive IP Blocking via CrowdSec

As a precautionary containment measure:

- The IP was blocked locally using CrowdSec
- A temporary ban of 12 hours was applied
- The action was documented as preventive containment, not confirmed malicious activity

Step 4: TheHive Ticket Creation

An alert was created in TheHive with the following details:

- Alert Type: Phishing
- Severity: Medium
- TLP: Amber

- Artifact: Internal IP address
- Tasks: Analyst validation and IT notification

3. Playbook Test Results

Playbook Step	Status	Notes
Check IP	Success	IP found not suspicious
Block IP	Success	IP blocked as preventive control
Create Ticket	Success	Alert created in TheHive
Assign Tasks	Success	Case created and response tasks added

Table 1: Playbook Notes

4. Summary

This SOAR playbook automates phishing response by evaluating source IP reputation and applying preventive containment using CrowdSec, even when no malicious reputation is found. A TheHive alert is created to document actions, ensure analyst validation, and maintain consistent incident handling across the SOC.