Title: Splunk Phantom Playbook Design (Auto-Block IP for Phishing Alerts)

Date: 24 Nov 2025
Prepared by: Mayuri Sawle

Objective:
Automate containment actions in response to phishing alerts detected by Wazuh or Elastic.

1. **Work flow steps**
    1. Check IP reputation via AlienVault OTX.
    2. If malicious → Block using local iptables or CrowdSec API.
    3. Create a case in TheHive and attach related logs.
    4. Record action in evidence log (playbook_actions.log).

2. Playbook Test Documentation

Playbook Step	Status	Notes
Check IP	Success	IP flagged as malicious by OTX & VT
Block IP	Success	CrowdSec blocked 192.168.1.102
Create Ticket	Success	TheHive case created with full details
Notify SOC	Success	Slack alert sent to SOC team

Summary (50 words)

The SOAR playbook automates phishing alert response by validating IP reputation, blocking malicious IPs through CrowdSec, and creating a case in TheHive for SOC investigation. This reduced manual analyst intervention and improved containment time from 10 minutes to under 2 minutes.