SOAR Playbook Development – Automated Phishing Response

Tools Used

- **Splunk Phantom** – Playbook creation and automation
- **TheHive** – Incident case management
- **Wazuh** – Phishing alert simulation
- **CrowdSec** – Automated IP blocking
- Google Docs – Documentation

Playbook Creation

A SOAR playbook was designed in **Splunk Phantom** to handle phishing alerts automatically.

Playbook Workflow

1. **Trigger**: Receive phishing alert from Wazuh
2. **Extract Indicator**: Source IP address
3. **Enrichment**: Check IP reputation using threat intelligence
4. **Decision**: If IP is malicious
5. **Response**: Block IP using CrowdSec
6. **Case Management**: Create an incident ticket in TheHive
7. **Logging**: Record all actions for audit purposes

Playbook Test (Performed)

A simulated phishing alert was generated in Wazuh to validate the playbook execution.

Test Results Documentation

Playbook Step	Status	Notes
Check IP	Success	IP flagged as malicious
Block IP	Success	CrowdSec blocked 192.168.1.102
Create Ticket	Success	Incident created in TheHive

50-Word Playbook Summary

This SOAR playbook automates phishing incident response by validating source IP reputation, blocking confirmed malicious IPs through CrowdSec, and creating investigation cases in TheHive. Automation ensures faster response, consistent containment actions, reduced analyst workload, and proper incident documentation across the SOC environment.