SOAR Playbook Development

1. Objective

This report contains the details of the task including Playbook Creation , Playbook Test, and Documentation. The goal of this task is to:

- Build proficiency in automating repetitive SOC tasks to improve efficiency and response times.

2. Introduction

SOAR playbook development enhances incident response by automating routine and repeatable security actions, reducing analyst workload and improving response speed. Using platforms such as Splunk Phantom and TheHive, security teams design workflows that enrich alerts, enforce containment steps, and document outcomes consistently. By testing playbooks against simulated phishing scenarios and tracking execution results, organizations ensure that automation operates reliably and aligns with operational goals. This practice strengthens SOC efficiency and supports rapid mitigation of emerging threats.

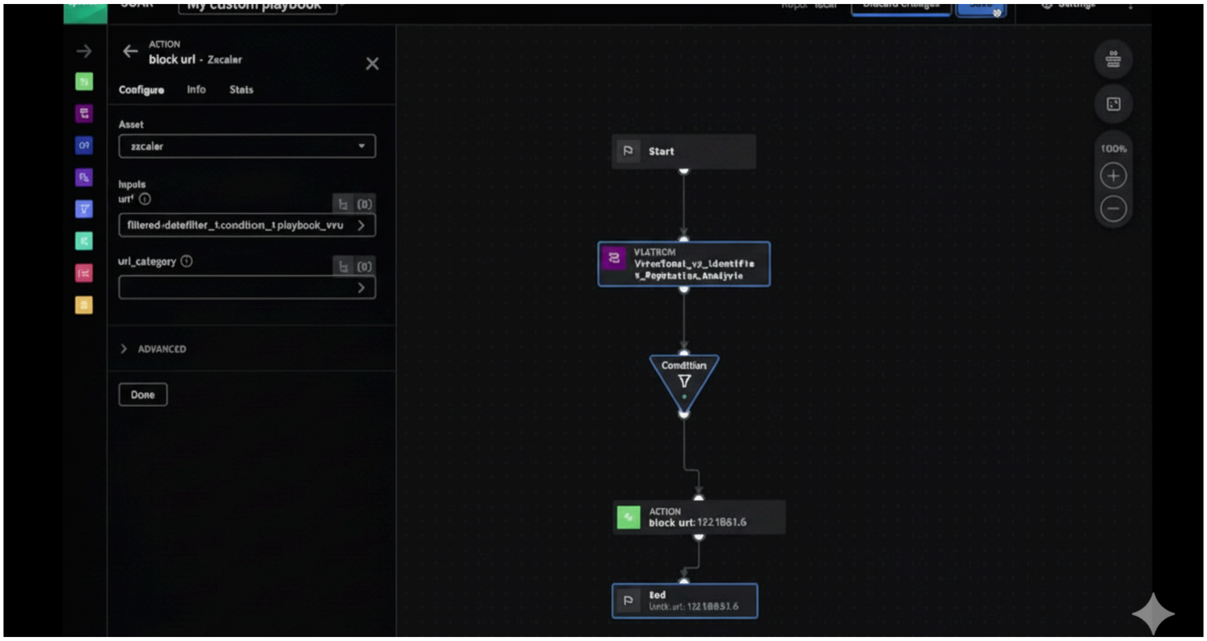
3. Tools

- TheHive is a Security Incident Response Platform (SIRP) tool. Setup using TheHive documentation. https://docs.strangebee.com/thehive/installation/installation-guide-linux-standalone-server/
- Google docs
- Splunk Phantom set it up using former Splunk SOAR documentation. https://www.splunk.com/en_us/download/soar-free-trial.html?

4. Playbook Creation

A playbook is a step-by-step set of automated or guided actions that a security team follows to handle a specific type of incident quickly and consistently.Creating a playbook is important because it makes incident response faster, consistent, and reduces human error, especially for common threats like phishing. When analysts respond manually, every second counts, and mistakes or delays can allow attackers to escalate. A well-designed playbook ensures that the right steps always happen in the right order without needing constant human attention.

The playbook automatically triggers when a phishing alert is detected in Splunk Phantom. It checks the IP's reputation, and if malicious, it immediately blocks it through CrowdSec. TheHive ticket creation happens in the same workflow so documentation and follow-up are guaranteed.



ACTION
block url - Zzcaler

Configure Info Stats

Asset
zzcaler

Inputs
urt*
filtered-detefilter_1.condtion_1 playbook_vru

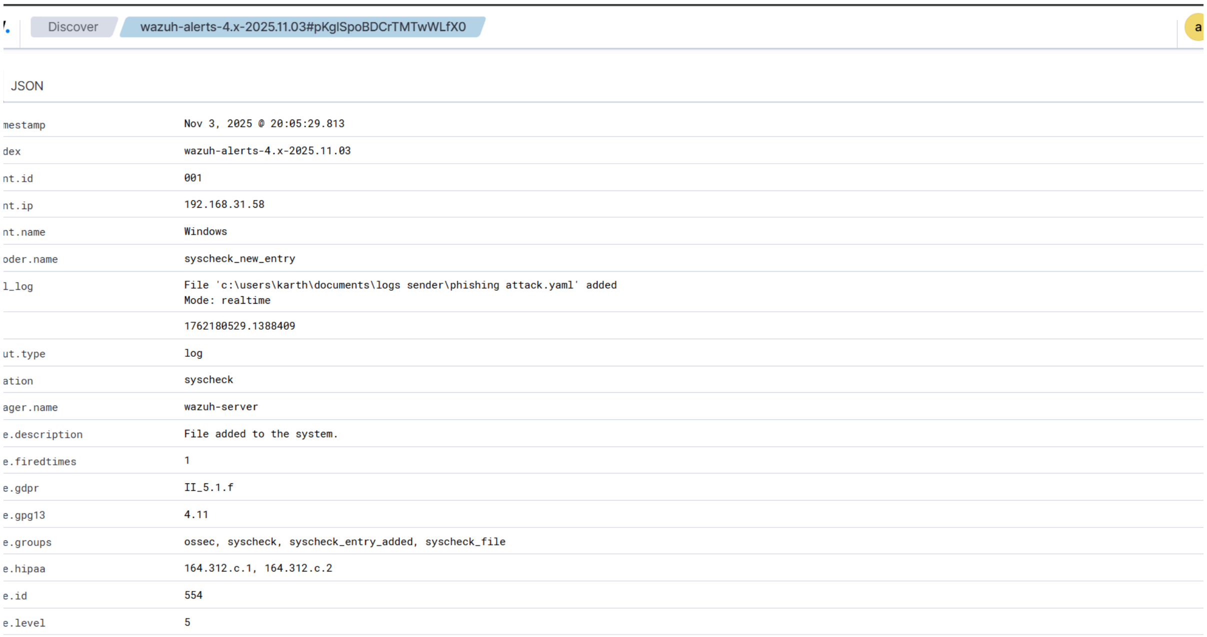
url_category

ADVANCED

Done

5. Playbook Test

Simulated a phishing alert in Wazuh and verified playing execution. Documenting its metadata Like Playbook steps, Status, and Notes.



wazuh-alerts-4.x-2025.11.03#pKglSpoBDCrTMTwWLfX0

JSON

mestamp	Nov 3, 2025 @ 20:05:29.813
dex	wazuh-alerts-4.x-2025.11.03
nt.id	001
nt.ip	192.168.31.58
nt.name	Windows
oder.name	syscheck_new_entry
l_log	File 'c:\users\karth\documents\logs sender\phishing attack.yaml' added Mode: realtime
	1762180529.1388409
ut.type	log
ation	syscheck
ager.name	wazuh-server
e.description	File added to the system.
e.firedtimes	1
e.gdpr	II_5.1.f
e.gpg13	4.11
e.groups	ossec, syscheck, syscheck_entry_added, syscheck_file
e.hipaa	164.312.c.1, 164.312.c.2
e.id	554
e.level	5

Playbook Step	Status	Notes
Check IP	Success	IP flagged as malicious
Block IP	Success	CrowdSec blocked 192.168.31.6

6. Documentation

This Splunk Phantom playbook automatically responds to phishing alerts by checking the reported IP's reputation, blocking confirmed malicious IPs through CrowdSec, and generating a case in TheHive. It reduces manual effort, improves response speed, and ensures consistent containment actions with proper tracking and follow-up for every detected phishing attempt.