PLAYBOOK DEVELOPMENT

Notes: Phishing IP Response

Objective:

Simulate a simplified SOAR playbook for phishing alert response, focusing on verifying and blocking a malicious IP without automated tools (Phantom or Cortex).

Tools Used:

- TheHive (for alert/case management)
- CrowdSec (for manual IP blocking)
- VirusTotal / AlienVault OTX (for threat intelligence)

Procedure:

1. Ingest Alert in TheHive:
2. A phishing alert was manually ingested via JSON with relevant artifacts (IP and URL).
   Alert ID: ~8343800.
3. **Check IP Reputation (Manual):** IP 192.168.1.102 was checked using VirusTotal and AlienVault OTX.
4. Determined to be malicious.
5. Findings documented in TheHive case notes.
6. **Block Malicious IP (Manual):** IP was manually blocked using CrowdSec:
   ```
   sudo cscli decisions add --ip 192.168.1.102 --duration 1h --reason "Phishing alert"
   ```
7. Block verified via:
   ```
   sudo cscli decisions list | grep 192.168.1.102
   ```

Results:

Playbook Step	Status	Notes
Check IP	Success	IP 192.168.1.102 verified as malicious via VirusTotal/OTX
Block IP	Success	IP 192.168.1.102 manually blocked using CrowdSec (cscli ban)

Summary:

The workflow demonstrates end-to-end phishing incident handling using manual IP verification and blocking. Even without automated SOAR tools, this approach ensures that malicious activity is identified and mitigated effectively, with all steps documented in TheHive for incident tracking.