SOC Automation Workflow Overview

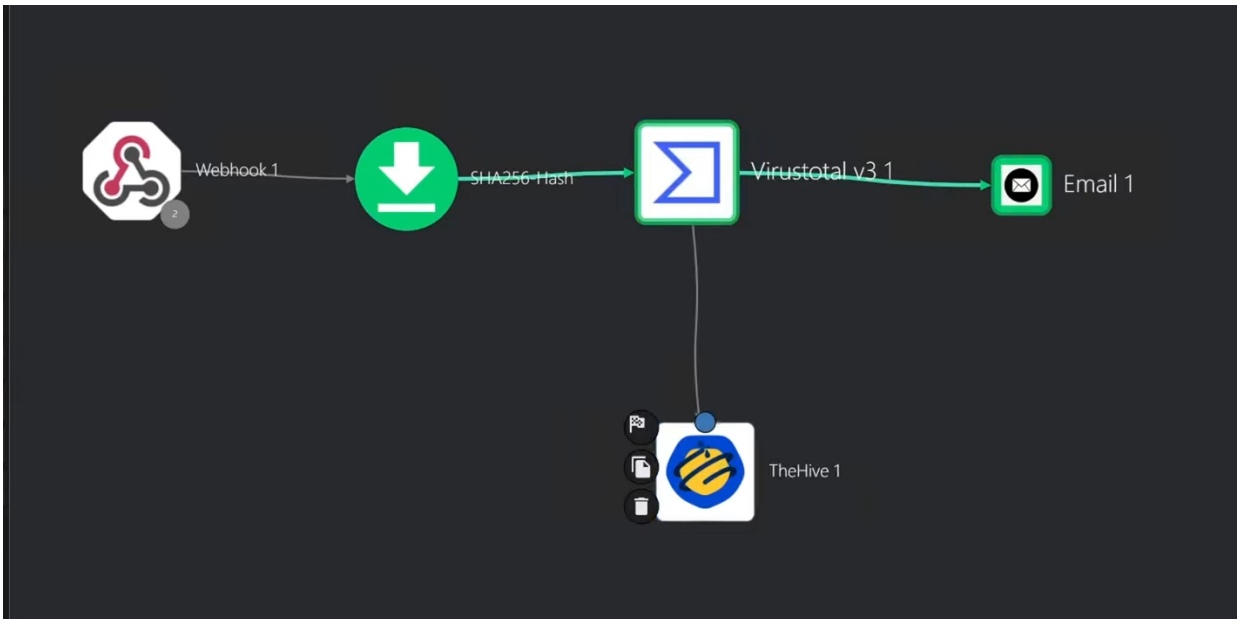
```
<!--
  Wazuh - Manager - Default configuration for ubuntu 24.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <integration>
    <name>shuffle</name>
    <hook_url>https://shuffler.io/api/v1/hooks/webhook_77b3d111-4e06-4cee-95b4-60173af00763</hook_url>
    <rule_id>100002</rule_id>
    <alert_format>json</alert_format>
  </integration>
```

This image shows a portion of the Wazuh Manager configuration file

This configuration enables automated SOC workflows by: Forwarding Wazuh alerts to Shuffle in real time, eliminating manual alert triage.



This image illustrates an automated SOC incident response workflow built using Shuffle SOAR and integrated with multiple security tools.

Workflow Breakdown:

Webhook Trigger

a. The workflow begins with a Webhook that receives alerts from the SIEM (Wazuh).
b. The alert contains file-related indicators generated from Sysmon events on the Windows 11 endpoint.

SHA-256 Hash Extraction

c. The incoming alert is parsed to extract the SHA-256 file hash associated with the suspicious activity.
d. This hash is used as the primary indicator for threat of intelligence enrichment.

VirusTotal v3 Integration

e. The extracted SHA-256 hash is automatically submitted to VirusTotal v3.
f. VirusTotal analyzes the hash and returns reputation data, detection ratios, and threat classifications.

Automated Actions

g. Based on the VirusTotal results:
    i. An email notification is sent to the SOC analyst with enrichment details.
    ii. A case is created in TheHive for incident tracking, investigation, and escalation.

Purpose and Value:

This automation reduces manual SOC effort by:

- Automatically enriching alerts with threat intelligence
- Improving detection-to-response time
- Creating structured incident cases for proper SOC workflow management

The playbook demonstrates practical SOC automation by integrating SIEM, SOAR, threat intelligence, alerting, and case management into a single automated