**SOC Capstone — Suricata + Wazuh (GitHub)**

**Use Case:** Debian 22.x VM running Suricata sensor + Wazuh Manager/Indexer/Dashboard on Windows 11 (WSL Ubuntu)

**1. Goal**

Assemble a compact SOC pipeline that:

* Detects anomalous network activity with Suricata.
* Forwards Suricata alerts into Wazuh.
* Correlates and displays events in the Wazuh dashboard.
* Records evidence, escalates, and responds.

**2. Topology**

[Debian 22.x VM: Suricata sensor (192.168.204.137)] ---> [Windows 11 VM (WSL Ubuntu): Wazuh Manager/Indexer/Dashboard (192.168.204.138)]

**3. Requirements**

* Debian 22.x virtual machine (Suricata sensor) — IP: 192.168.204.137
* Windows 11 VM with WSL (Ubuntu) running the Wazuh stack — IP: 192.168.204.138
* Administrative privileges (root / sudo) on both systems
* Network connectivity between the VMs

**4. Install & Configure Suricata on Debian 22.x**

# Update system

sudo apt update && sudo apt upgrade -y

# Install Suricata

sudo apt install -y suricata

# Enable promiscuous mode

sudo ip link set eth0 promisc on

# Test run

sudo suricata -i eth0 -l /var/log/suricata/

**Troubleshooting:**

* If Suricata loads no rules → install rule set:

sudo suricata-update

sudo systemctl restart suricata

* Logs of interest: /var/log/suricata/eve.json

**5. Configure Wazuh Agent to Collect Suricata Logs**

Add a localfile entry to the agent configuration (/var/ossec/etc/ossec.conf):

<localfile>

<log\_format>json</log\_format>

<location>/var/log/suricata/eve.json</location>

</localfile>

Restart the agent to apply the change:

sudo systemctl restart wazuh-agent

**6. Generate Test Alerts Using Hydra (attacker)**

Use hydra to create rapid authentication attempts that Suricata should detect (target Windows 11 VM). Install and run hydra on an attacker system (this can be a separate Kali VM or the Debian sensor if you’re testing locally).

sudo apt update && sudo apt install -y hydra

# Replace 'user' and target host accordingly. This will send many SSH authentication attempts to the Windows 11 VM.

hydra -l user -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.204.138 -s 22

**Why:** Generates noisy network traffic and authentication failures that should trigger Suricata IDS alerts and be forwarded to Wazuh.

**7. Create a Custom Rule in Wazuh**

Add a local rule to map Suricata signatures into higher-priority Wazuh alerts. Edit /var/ossec/etc/rules/local\_rules.xml:

<rule id="100100" level="10">

<decoded\_as>json</decoded\_as>

<field name="alert.signature">ET MALWARE</field>

<description>Suricata detected ET MALWARE event</description>

<mitre>

<id>T1071</id>

</mitre>

</rule>

Then restart the Wazuh manager so the rule takes effect:

sudo systemctl restart wazuh-manager

**8. Escalation: Creating a TheHive Case**

Open TheHive and create a case through the UI or via API.

**100-word summary template:**

Suricata on Debian detected suspicious traffic from an external IP attempting to exploit a network service. The alert was ingested into Wazuh and correlated to MITRE ATT&CK technique T1071. Payload indicators and source behavior align with a known exploitation pattern. Impact: possible lateral movement and compromise if exploitation succeeded. Actions performed: triage, temporary IP blocking, and evidence capture. Recommended next steps: full packet capture analysis, IOC extraction, endpoint inspection, and notify the incident response team for containment.

**TheHive JSON template (case import):**

{

"title": "Suricata Alert - ET MALWARE",

"description": "Suricata detected malware traffic (ET MALWARE). Event ingested in Wazuh, MITRE T1071. Action taken: IP blocked.",

"severity": 2,

"tlp": 2,

"pap": 2,

"status": "New"

}

**9. Reporting: Executive & Technical Summary (Google Docs)**

**200-word template:**

Executive Summary:

On [date], the Suricata sensor on the Debian host detected suspicious network activity that was ingested and correlated by the Wazuh stack (running on Windows 11 WSL). The event was mapped to MITRE ATT&CK T1071 indicating potential command-and-control or data transfer activity. The source IP attempted exploit-like behavior against a service on the monitored host. The alert was escalated to TheHive and assigned medium priority. Immediate containment included blocking the offending IP. Recommended actions: extract IOCs, perform endpoint scans, and collect full packet captures for forensic analysis.

Technical Details:

- Source IP: [IP]

- Destination IP: [IP]

- Signature: ET MALWARE

- Log path: /var/log/suricata/eve.json → Wazuh agent → Wazuh manager

- MITRE: T1071

- Response: IP blocked and evidence archived

Outcome:

Detection, triage, and containment were successfully completed by the SOC pipeline.

**10. Evidence Handling Checklist**

* Preserve raw eve.json logs.
* Export packet captures when available.
* Document incidents in TheHive with proper TLP/PAP.
* Store artifacts in the repository under /evidence.
* Keep a CHAIN\_OF\_CUSTODY.md to track evidence handling.

**11. Useful Scripts**

scripts/start-suricata.sh:

#!/bin/bash

sudo ip link set eth0 promisc on

sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -D

scripts/collect-logs.sh:

#!/bin/bash

tar -czvf evidence\_$(date +%F).tar.gz /var/log/suricata/eve.json

scripts/push-evidence.sh:

#!/bin/bash

git add evidence\_\*.tar.gz

git commit -m "Add evidence logs $(date)"

git push origin main

**12. Troubleshooting Guidance**

* **No Suricata alerts:** Ensure rules are installed and the correct interface is monitored (suricata-update and check suricata.yaml).
* **Empty eve.json:** Verify Suricata has the correct interface and that traffic is observed on that NIC.
* **Agent not forwarding logs:** Inspect /var/ossec/logs/ossec.log on the agent and ensure the localfile entry is correct.
* **Wazuh dashboard empty:** Confirm Filebeat is running and the indexer is healthy.

**13. Reproduction Quickstart**

# On Windows PowerShell, open WSL

wsl -d Ubuntu

# On WSL Ubuntu – ensure Wazuh services are running

sudo systemctl enable --now wazuh-manager wazuh-indexer wazuh-dashboard filebeat

# On Debian VM (192.168.204.137) – install Suricata and start sensor

sudo apt update && sudo apt install -y suricata

sudo ip link set eth0 promisc on

sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -D

# On attacker (or Debian if testing locally) – generate hydra traffic to Windows 11 VM (192.168.204.138)

sudo apt update && sudo apt install -y hydra

hydra -l user -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.204.138 -s 22

# Collect evidence

tar -czvf evidence\_$(date +%F).tar.gz /var/log/suricata/eve.json