Practical Alert Management Using TheHive and Wazuh

Introduction

This document outlines the practical exercise for alert management using TheHive, Wazuh, and Google Sheets. It covers creating mock alerts, classifying and prioritizing them, drafting incident tickets in TheHive, and practicing escalation procedures. Alert management is crucial for detecting, prioritizing, and responding to cybersecurity incidents. The exercise simulates alerts of varying severity, maps them to MITRE ATT&CK tactics, and creates incident tickets in TheHive for structured response.

Tools Used:

- **Google Sheets**: For alert classification and prioritization.
- **TheHive**: For incident ticket creation, management, and escalation practice. On Ubuntu. IP: 192.168.1.35.
- **Wazuh**: For monitoring alerts and visualizing alert dashboards. On Ubuntu. IP: 192.168.1.35.

Creating Mock Alerts

Three mock alerts were created to simulate real incidents:

A	B	C	D	E	F
Alert ID	**Alert Title**	**Severity**	**CVSS**	**Priority**	**MITRE Tactic**
ALERT-001	Phishing Email: Suspicious Link	Medium	5	Medium	Initial Access (TA0001)
ALERT-002	Ransomeware Detected on Server-X	High	9.8	Critical	Impact (TA0040)
ALERT-003	Unauthorized Port Scan Detected	Low	3	Low	Reconnaissance (TA0043)

1: Mapping Alerts on Google Sheet

The alerts were formatted as JSON files (alert1.json, alert2.json, alert3.json) for importing into TheHive.

Example JSON Structure for ALERT-001:

{
"title": "Phishing Email: Suspicious Link",
"type": "external",
"source": "MockAlerts",
"sourceRef": "ALERT-001",
"description": "User received a suspicious email with a link to fake login page.",
"tags": ["phishing","mock"],
"severity": 2,
"tlp": 2
}

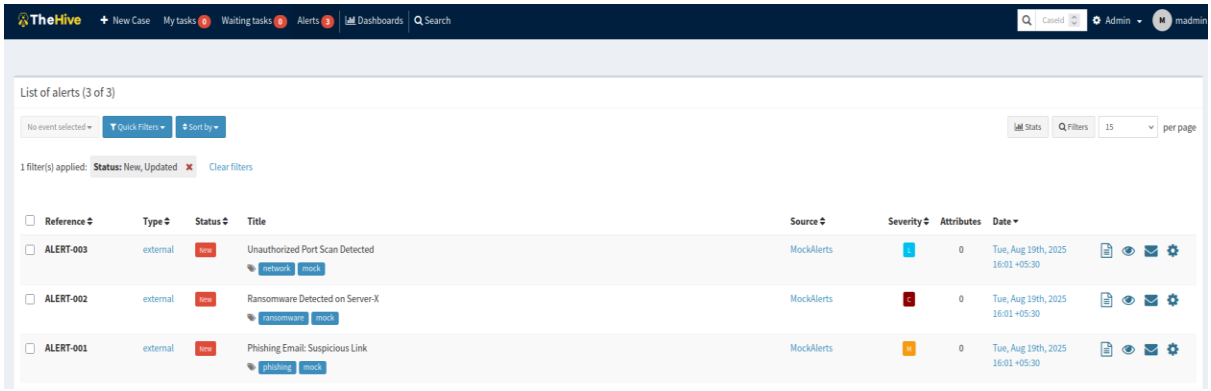
Importing Alerts to TheHive

Use the following curl command to import alerts:

```
curl -X POST -H "Content-Type: application/json" \
    -H "Authorization: Bearer <API_KEY>" \
    -d @"$HOME/alert1.json" \
    http://<192.168.1.35>:9000/api/alert
```

Repeated for alert2.json and alert3.json.

Verify the alerts appear in TheHive dashboard under **Alerts**.



2: Alets on TheHive

Prioritizing Alerts

1. Using Google Sheets, each alert was assigned a priority based on CVSS scores:

    - **Critical:** CVSS ≥ 9 (e.g., Ransomware)
    - **Medium:** CVSS 4-6 (e.g., Phishing)
    - **Low:** CVSS 0-3 (e.g., Port Scan)

2. Alerts were mapped to MITRE ATT&CK tactics:
    - **T1566:** Phishing
    - **T1486:** Data Encrypted for Impact (Ransomware)
    - **T1046:** Network Service Scanning

Dashboard Creation in Wazuh

1. Log into Wazuh web interface.
2. Create a new dashboard for alert visualization.
3. Add widgets:

    - Pie chart for **Alert Priority Distribution**
    - Table for **Alert Types**
    - Time-series chart for **Alert Volume Over Time**

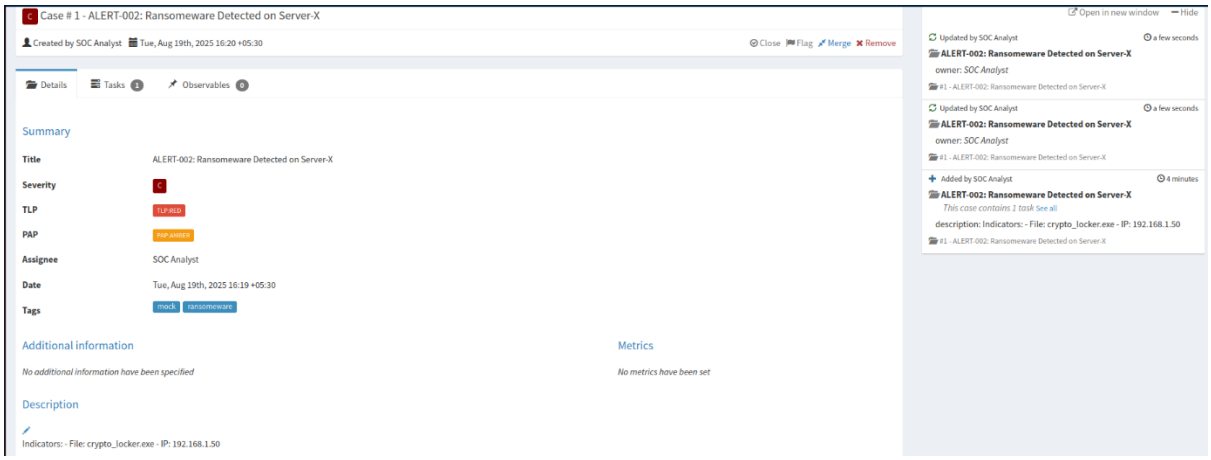
Creating Incident Tickets in TheHive

Example Ticket for ALERT-002 (Ransomware):

Field	Value
Title	[Critical] Ransomware Detected on Server-X
Description	Indicators: - File: crypto_locker.exe - IP: 192.168.1.50
Priority	Critical
Assignee	SOC Analyst
Tags	ransomware, mock
Source	MockAlerts
TLP	2

Artifacts:

- **File:** crypto_locker.exe
- **IP:** 192.168.1.50



3: Critical Alert Case

Escalation Role-Play

Escalation Email Example (100 words):

Subject: [Critical] Ransomware Incident on Server-X – Immediate Attention Required

Body:

Hello Tier 2 Team,

We have detected a critical ransomware incident on Server-X. Indicators of Compromise include the file crypto_locker.exe and suspicious communication from IP 192.168.1.50.

Immediate containment is recommended to prevent lateral movement. All relevant logs and artifacts have been attached in TheHive case [Critical] Ransomware Detected on Server-X. Please prioritize investigation and initiate response procedures per SOP. We will monitor the situation and provide updates as necessary.

Thank you,
SOC Analyst.

References

- https://thehive-project.org/documentation/
- https://documentation.wazuh.com/current/index.html
- https://attack.mitre.org/
- https://www.xmatters.com/blog/how-to-build-an-escalation-policy-for-effective-incident-management
- https://docs.strangebee.com/thehive/download/#debian-ubuntu
- https://hub.docker.com/r/thehiveproject/thehive
- https://sbscyber.com/blog/top-5-most-common-incident-response-scenarios