Automated Security Operations Center (SOC)

1. Introduction

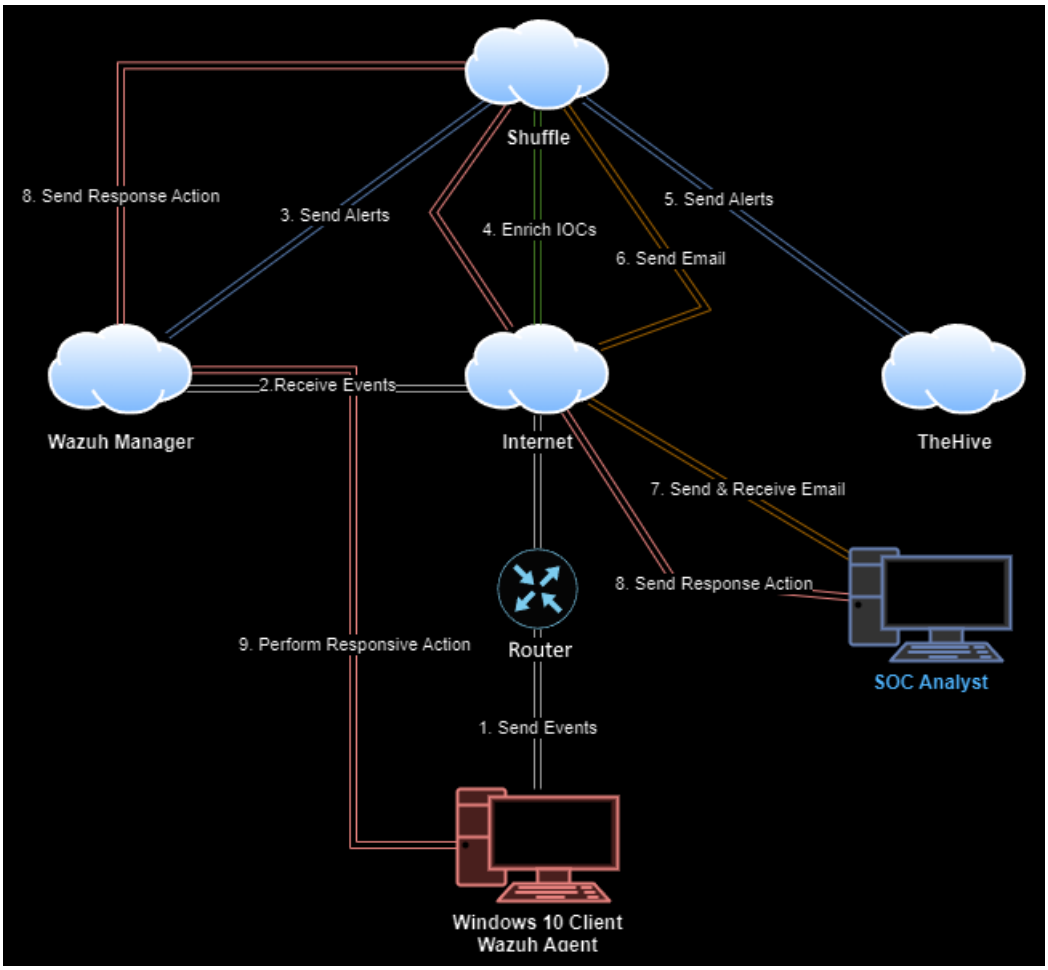
1.1 Overview

The **SOC Automation Project** is designed to create an **automated Security Operations Center (SOC) workflow** that enhances **event monitoring, alerting, and incident response**. By leveraging powerful **open-source security tools** such as **Wazuh, Shuffle, and TheHive**, this project **optimizes SOC operations** by **automating repetitive tasks, reducing the workload** on security analysts, and **improving overall efficiency in security monitoring**.

1.2 Purpose and Goals

- **Automate Event Collection and Analysis** – Ensures security events are collected, logged, and analyzed in real-time, reducing manual intervention.
- **Streamline the Alerting Process** – Automates the process of generating, forwarding, and triaging alerts to minimize response times.
- **Enhance Incident Response Capabilities** – Introduces automated response actions for security incidents, ensuring a swift and structured response.
- **Improve SOC Efficiency** – Reduces analyst workload by automating **log analysis, threat correlation, and case management**.

1.3 SOC Automation Diagram



2. Prerequisites

2.1 Hardware Requirements

To successfully set up the SOC Automation Lab, ensure your system meets the following hardware requirements:

- **Host machine** capable of running multiple virtual machines (VMs).
- **Minimum 16GB RAM** and **4 vCPUs** (recommended **32GB RAM** for smoother performance).
- **500GB+ disk space** to store log files and system images.

2.2 Software Requirements

- **VMware Workstation/Fusion or VirtualBox** – Used for virtualization.
- **Windows 10 ISO** – Acts as the client machine for security event generation.
- **Ubuntu 22.04 ISO** – Serves as the operating system for **Wazuh** and **TheHive**.

- **Sysmon** – Provides detailed Windows event logging for advanced **threat detection**.

2.3 Tools and Platforms

- **Wazuh** – A powerful **open-source SIEM and XDR platform** for log collection and analysis.
- **Shuffle** – A **SOAR (Security Orchestration, Automation, and Response)** tool that automates security workflows.
- **TheHive** – A **Security Incident Response Platform (SIRP)** for managing security investigations and response actions.
- **VirusTotal** – A **cloud-based malware scanning and intelligence platform** for file and URL analysis.

2.4 Required Skills & Knowledge

- Familiarity with **Virtual Machines (VMs)** and virtualization platforms.
- Basic **Linux command-line experience** (file manipulation, installing packages, editing config files).
- Understanding of **SOC operations, log analysis, threat detection, and security automation**.

---

3. Setup Guide

3.1 Install and Configure Windows 10 with Sysmon

3.1.1 Install Windows 10 on VMware/VirtualBox

1. Download and install **VMware Workstation** or **VirtualBox**.
2. Create a new virtual machine with:
    - **4GB RAM**, **2 vCPUs**, and **50GB storage**.
    - Attach the **Windows 10 ISO** and complete the installation.

3.1.2 Install Sysmon for Advanced Logging

1. Download **Sysmon** from the Sysinternals website.
2. Obtain a **Sysmon configuration file** (from GitHub or **DFIR resources**).
3. Extract the Sysmon archive and navigate to the extracted folder in PowerShell.
4. Install Sysmon using:

```
.\Sysmon64.exe -i .\sysmonconfig.xml
```

5. Verify Sysmon installation:
    - Open **Services.msc** and check for **Sysmon64**.
    - Open **Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon**.

3.2 Set Up Wazuh Server

3.2.1 Deploy Wazuh on a Cloud Server (DigitalOcean)

1. Create a **DigitalOcean Droplet** with **Ubuntu 22.04**.
2. Set a **strong root password** and name the droplet **Wazuh**.
3. Configure a firewall:
    - Navigate to **Networking > Firewalls**.
    - Restrict inbound traffic and allow only trusted IPs.
4. Connect to the server via SSH:

```
ssh root@[WAZUH-SERVER-IP]
```

5. Update and upgrade packages:

```
sudo apt-get update && sudo apt-get upgrade -y
```

6. Install Wazuh:

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

7. Access the Wazuh Web Interface at:

```
https://[WAZUH-SERVER-IP]/
```

3.2.2 Deploy Wazuh Locally (On-Premises)

- Install **Ubuntu 22.04**.
- Allocate **8GB RAM, 4 vCPUs, and 50GB Storage**.
- Follow the **Wazuh Quickstart Guide**.

3.3 Install TheHive

3.3.1 Deploy TheHive on a Cloud Server (DigitalOcean)

1. Create a **DigitalOcean Droplet** for **TheHive (Ubuntu 22.04)**.
2. Install dependencies:

```
sudo apt install wget gnupg apt-transport-https git ca-certificates curl -y
```

3. Install **Java, Cassandra, and Elasticsearch**.
4. Install TheHive:

```
sudo apt-get install -y thehive
```

5. Access **TheHive Web Interface** at:

```
http://[THEHIVE-SERVER-IP]:9000
```

---

4. Automation with Shuffle

4.1 Integrate Wazuh with Shuffle

1. Create a **Webhook** in **Shuffle** and copy the URL.
2. Modify Wazuh Configuration:

```
<integration>
  <name>shuffle</name>
  <hook_url>https://shuffler.io/api/v1/hooks/webhook</hook_url>
  <level>3</level>
  <alert_format>json</alert_format>
</integration>
```

3. Restart Wazuh:

```
systemctl restart wazuh-manager.service
```

4.2 Automate Incident Handling with TheHive

1. Extract **SHA256 hash** from alerts.
2. Query **VirusTotal** for threat intelligence.
3. Forward alerts to **TheHive** for investigation.
4. Send **Email Notifications** to SOC Analysts.

---

5. Conclusion

This project successfully integrates **Wazuh, TheHive, and Shuffle** to create an **automated SOC environment**. The implementation ensures:

- **Real-time event monitoring and automated alerting**.
- **Seamless integration between security tools for automation**.
- **Incident response workflows using SOAR capabilities**.

Future improvements can include **advanced correlation rules**, **integrating additional threat intelligence sources**, and **refining automation workflows**.

---

6. References

- Microsoft Docs. "Sysmon for Windows". Accessed March 2025.
- Wazuh. "Wazuh Documentation". Accessed March 2025.
- TheHive Project. "TheHive Documentation". Accessed March 2025.
- DigitalOcean. "How to Set Up a SOC Environment". Accessed March 2025.