Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

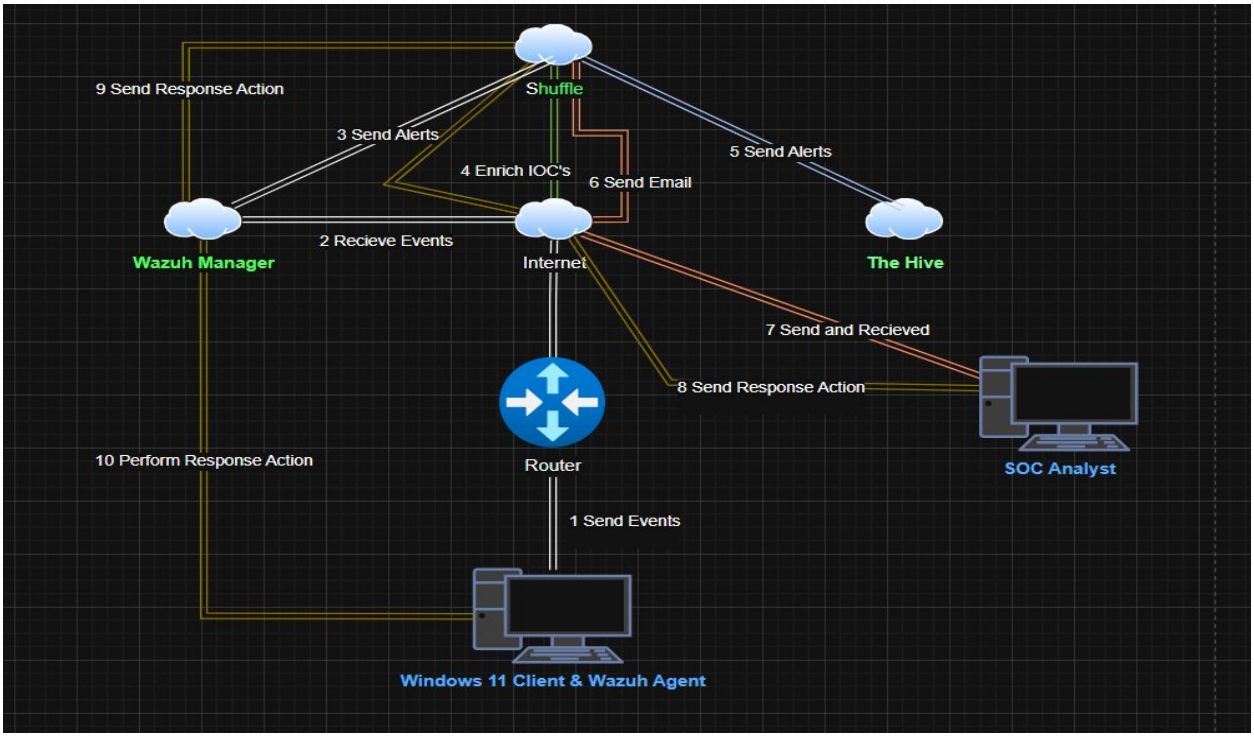
Project Name: SOC Automation Project (Home Lab)

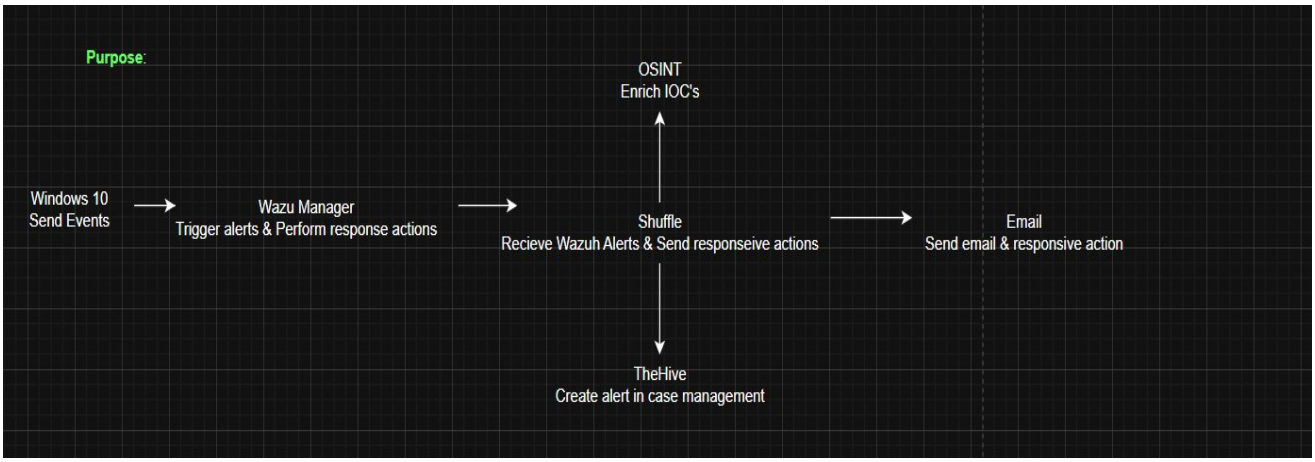
Project Overview

This project presents a simplified yet functional **Security Operations Center (SOC)** architecture designed for home lab experimentation and learning. It simulates real-world task of **Security Analyst** workflows using open-source tools, **enabling hands-on experience with threat detection, incident response, and automation.**

The **goal** is to empower aspiring **SOC analysts and cybersecurity enthusiasts** with a practical environment to understand how data flows through a security ecosystem, from endpoint agents to centralized analysis platforms.

1. I developed a simplified **Home SOC (Security Operations Center) architecture** for use in the **SOC Automation Project Leo Home Lab**. This setup provides a clear visualization of system flow - from the **Wazuh Agent,** simulated with **Mimikatz** connecting through the internet to the **Wazuh Manager (SIEM)**, then integrating with **Shuffle (SOAR)**, also utilized the **Virus total** for **reputation** checking and **TheHive** to create an alert for **case management**, all culminating in a centralized interface for the **Cybersecurity | SOC Analyst**. This architecture serves as a practical tool for understanding and simulating real-world SOC operations.





2. **Operating system/Devices: Ubuntu and Windows 11 or Server 2022 | Applications: Wazuh, Shuffle, Virus Total, and TheHive** are the applications needed for Home Lab setup.

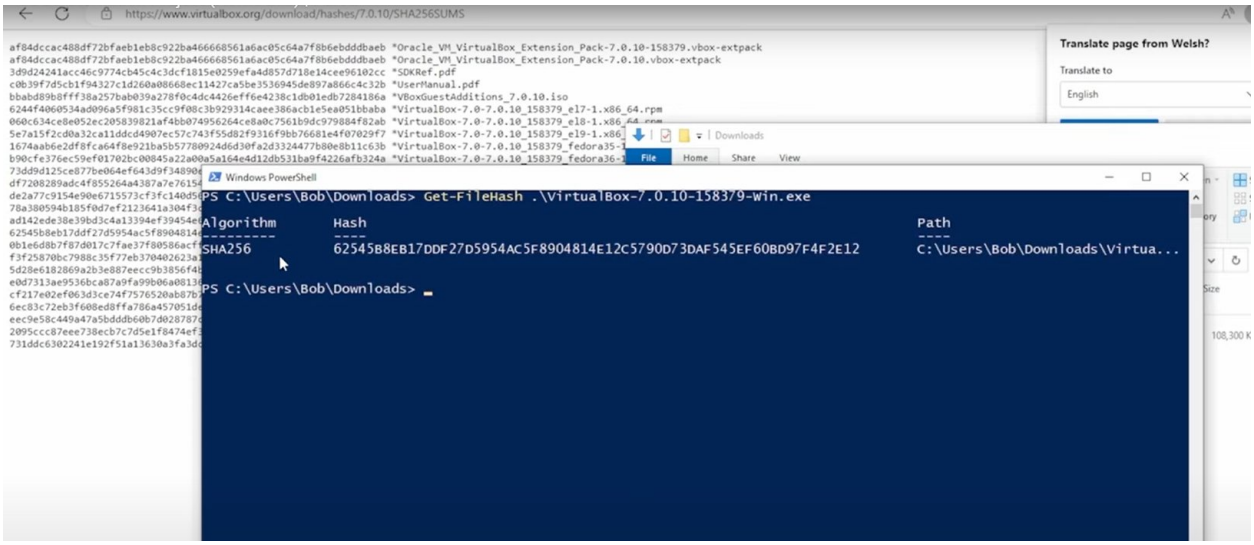
   https://wazuh.com/
   Wazuh is a **threat prevention, detection, and response platform** that is free and open source. It safeguards workloads on-premises, in virtualized, containerized, and cloud settings. Wazuh is utilized by hundreds of companies worldwide, ranging from tiny firms to major corporations.

   https://strangebee.com/thehive/
   TheHive is a versatile tool designed for incident management and response. It is purpose-built for SOC, CERT, and CSIRT teams to minimize the time between actions taken by a bad actor and a team's security response unit. TheHive allows users to track down and assign tasks to teammates, ensuring efficient collaboration during incident resolution.

3. **Start the installation of Virtual Machine (Virtual Box or Hyper-V)**

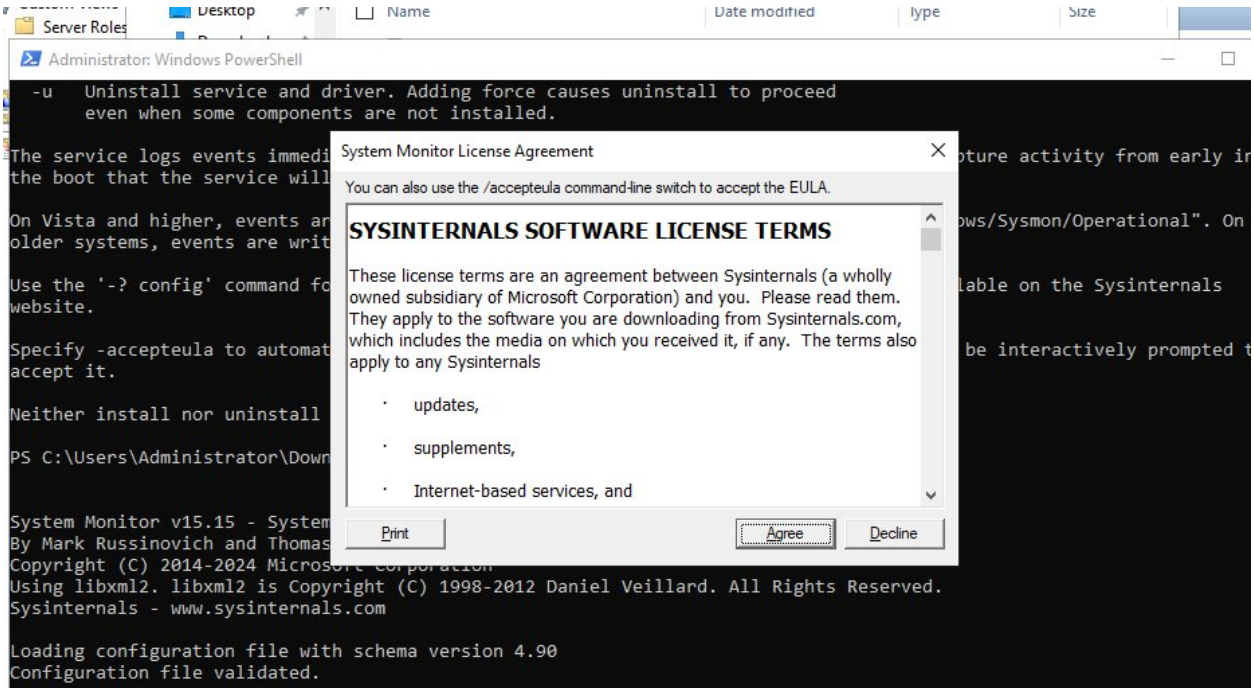
   - To check that the downloaded file is legit, check and get/download the SHA 5 Hash to verify the legitimacy of the downloaded file, once downloaded open this and match with the download file HASH.
   - In Windows > Open **PowerShell(admin)** > locate the location of your downloaded file and run below

     Get-FileHash .\VirtualBox-7.0.10-158379-win.exe



- Install Windows 11 (SysMon), Ubuntu, and Kali Linux

4. **Sysmon** Installation in Windows Machine.
    - Download the Sysmon = https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
    - Extract the downloaded files and find the sysmonconfig.xml
    - Download the sysmonconfig.xml = https://github.com/olafhartong/sysmon-modular > Right-click RAW > Save As > sysmonconfig
    - Once, finished download extract your sysmon.zip
    - Open PowerShell (Admin) > Go to the directory where your extracted Sysmon is located > e.g. C:\Users\administrator\Downloads\sysmon
    - Make sure that your **sysmconfig.xml** is in the same directory of your sysmon extracted.
    - In your PowerShell type **.\sysmon64.exe** (to check if there is existing sysmon installed > Check this in Windows services if sysmon is installed).
    - Now, type **.\sysmon64.exe .\sysmonconfig.xml** and below will popup



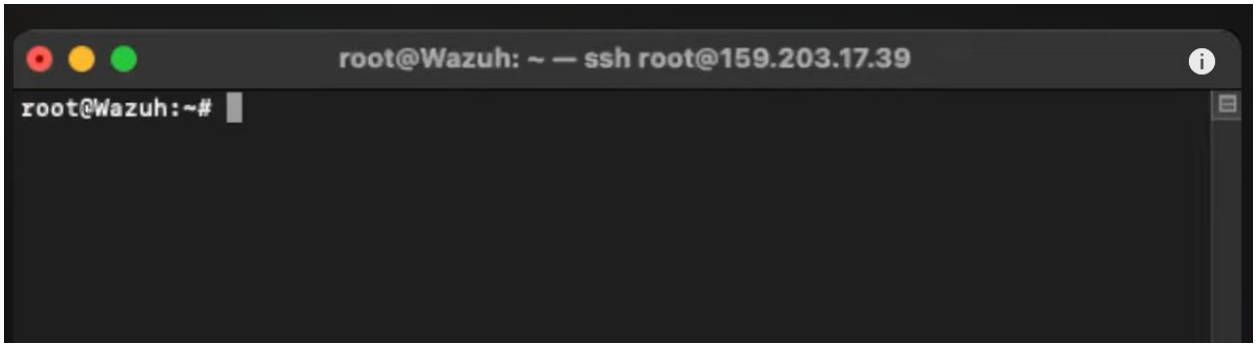
- Click Agree > Sysmon will now install

4. **Wazuh Installation in the Cloud or on a Virtual Machine (VM)**
   To install Wazuh, you'll need a cloud provider to host and manage your application. For this setup, I used DigitalOcean - https://cloud.digitalocean.com/projects

   Note: If you'd prefer not to pay for lab practice, you can install the required tools directly onto your Ubuntu or Windows virtual machine (VM). This allows you to practice locally without relying on paid lab environments.

   - Login to your account in digital ocean > Click create droplets > Choose Ubuntu > Basic > Password > at the buttom hostname = change this to Wazuh > Click create (wait for the droplet to be created)
   - Create a firewall > click Firewall in the left > Create Firewall > **Inbound Rules**: **Type** = All TCP, **Source** = Remove all IP & **add your public IP** (to get your **public IP**, open > "whatismyIPaddress" = https://whatismyipaddress.com/
   - Create as well for UDP and follow above > Click create firewall
   - Once firewall has been created > Click Networking
   - Click Droplets > Check you Wazuh IP Address > Click Wazuh > Click Networking (scroll down) until you see firewall > Click Edit and select firewall that you have created > Click Droplets and look for your VM (e.g Wazuh) > Add droplet (Now the firewall will protect the virtual machine)
   - To access your VM > Click Droplets > Click Access > Select Launch Droplet Console

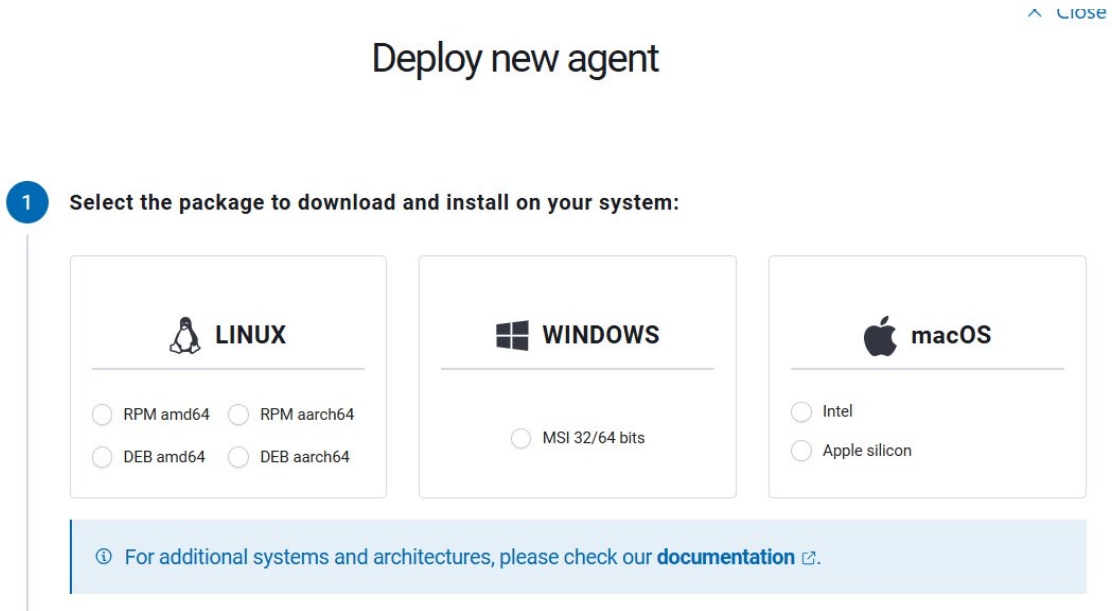
- We can now perform the update and upgrade.



- **Apt-get update && apt-get upgrade** > Package will run just hit enter >

5. **Now, install Wazuh Manager in your Ubuntu VM.**
   - Run = sudo apt update && sudo apt dist-upgrade -y
   - Sudo apt install curl
   - Sudo apt install default-jdk
   - curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
   - bash ./wazuh-install.sh -a -i
   - **Note** = get user name & password

6. Install the **Wazuh Agent** > In HOME click Agents Summary (Active or Disconnected) > Click **Deploy New Agent** and fill up below.



2 **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

172.20.135.157

Remember server address

3 **Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

Agent name

The agent name must be unique. It can't be changed once the agent has been enrolled.

In your agent machine/endpoint > Run the following below in PowerShell (Admin)

4 **Run the following commands to download and install the agent:**

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.2-1.msi -OutFile
${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='172.20.135.157'
WAZUH_AGENT_NAME='LizJamesDC1'
```

Requirements

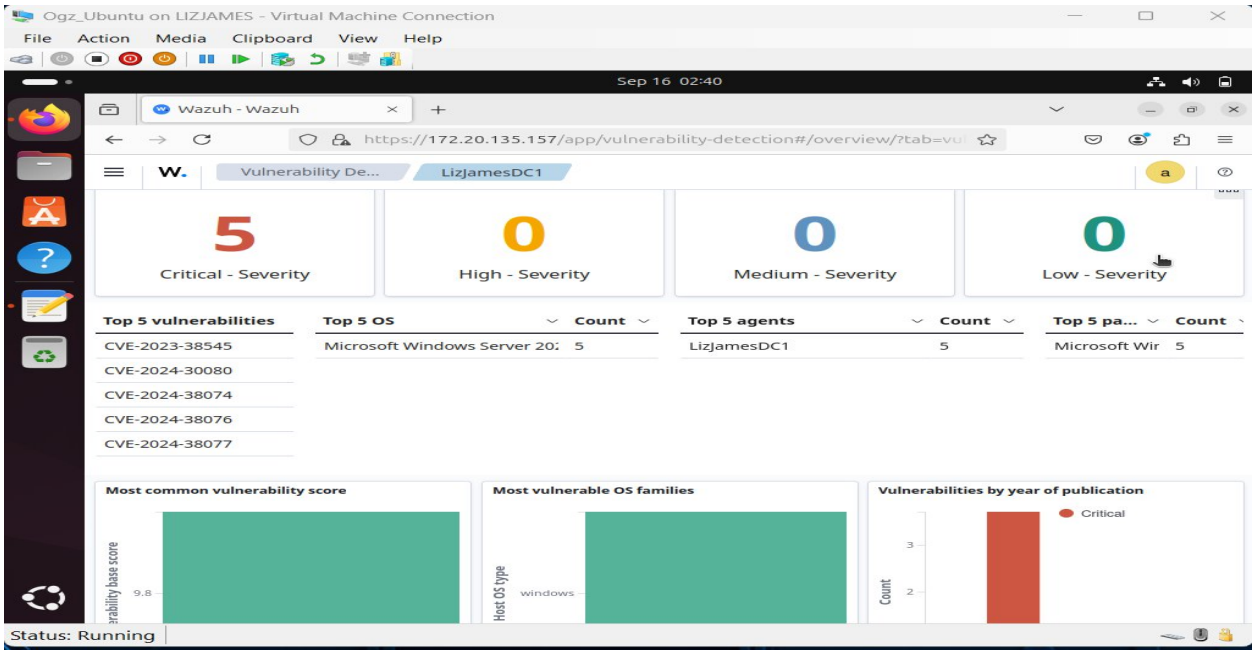
- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

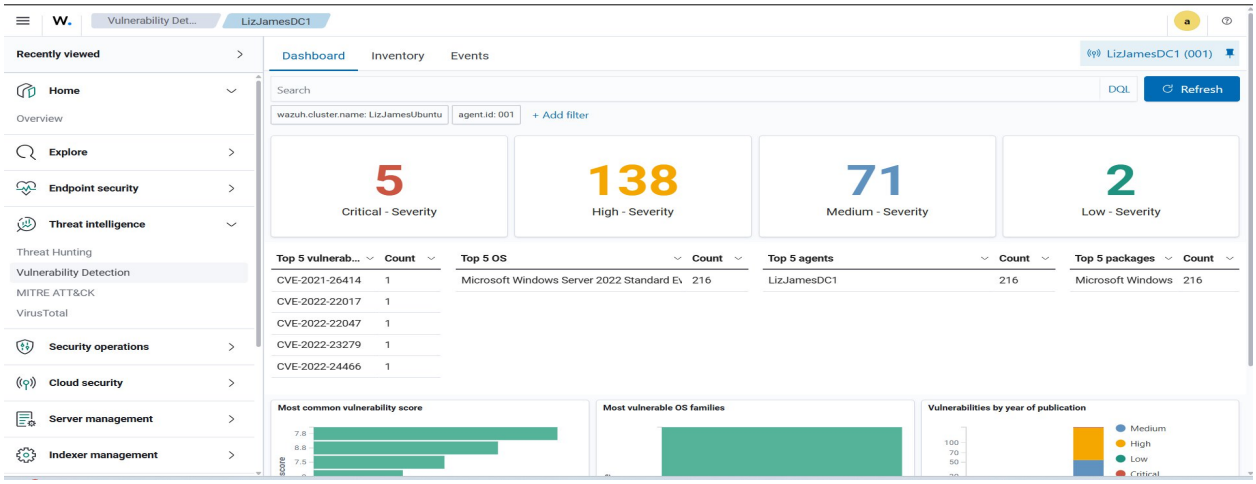
5 **Start the agent:**

```
NET START WazuhSvc
```

This is an example agent deployed on my **Ubuntu-based Wazuh Server Manager**: **Agent** is LizJamesDC1, a **Windows Server 2022** machine.



This is an example of **Vulnerability Scanning Detection** on my **Ubuntu-based Wazuh Server Manager**: **Agent** is LizJamesDC1, a **Windows Server 2022** machine.



- For an in-depth introduction to **Wazuh**, refer to the official tutorial available on YouTube.

  https://www.youtube.com/watch?v=mKijuwrTeRM&list=PLI0vJRMEGNYRVuQWxO7BPZAe_G_mM9d66

Troubleshooting:

- If there is an issue encountered "Wasuh dashboard server is not ready yet". Initial steps of troubleshooting are to restart your Wazuh-dashboard and Wazuh-indexer.

```
Systemctl stop wazuh-dashboard
Systemctl start wazuh-dashboard
Systemctl status wazuh-dashboard

Systemctl stop wazuh-indexer
Systemctl start wazuh-indexer
Systemctl status wazuh-indexer
```

- If Wazuh server IP/Hostname was changed. In your Wazuh client navigate to C:\Program Files (x86)\ossec-agent and edit the **ossec.conf and edit below.**

```
<server>
  <address>ServerIP/Host</address>
  <port>1514</port>
  <protocol>tcp</protocol>
```

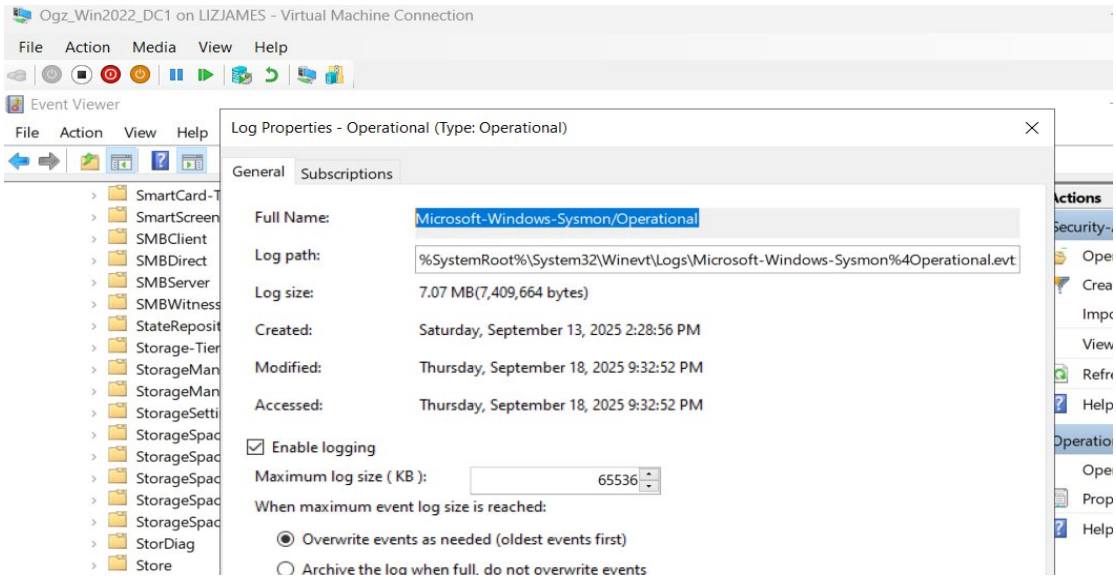
7. Installation of **theHive in Ubuntu**.

   Sources:
   a. https://www.youtube.com/watch?v=61t4qouh7tc
   b. https://github.com/lovnishverma/bigdataecosystem/blob/main/HiveInstallation.md
   c. https://www.youtube.com/watch?v=VuSKMPRXN1M

8. **Windows Server Telemetry (sysmon)**. We need to edit the ossec.conf for the sysmon monitoring.

   Telemetry = is the automatic remote collection and analysis of data from sensors and systems to monitor their internal state and performance in real-time.

   - In C:\Program Files (x86)\ossec-agent open the ossec.conf. Check because there is some Events ID that are excluded.
   - Use SysMon > to check **SysMon channel name** open the Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > right click operational > properties > Now, get the full name = Microsoft-Windows-Sysmon/Operational



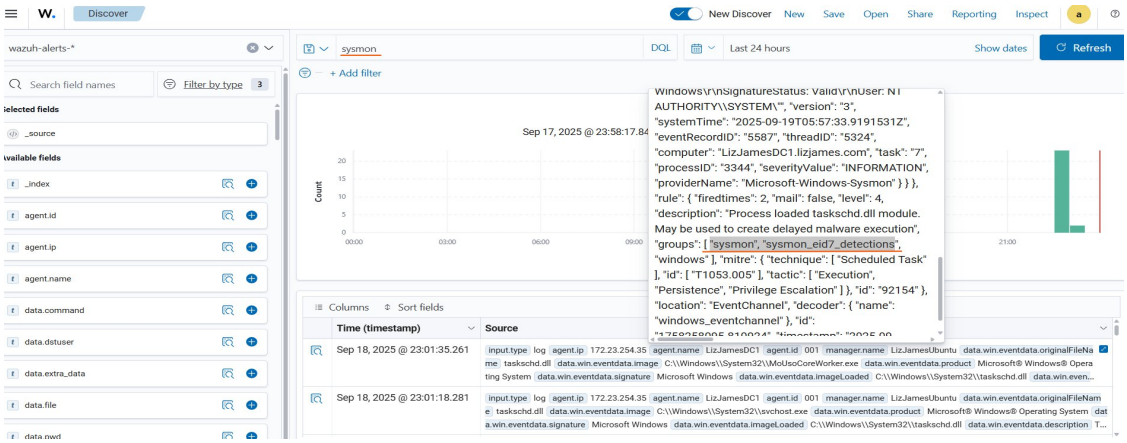
- Now add and put this in your ossec.conf.

```
<!-- Log analysis -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

<!-- Log analysis -->
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Security</location>
```

- Next, Remove the **local file application, security, and system**.

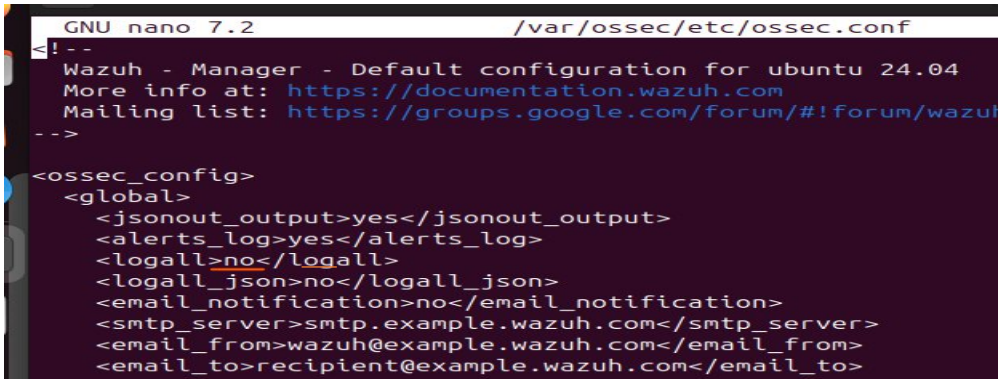
```
<!-- Log analysis -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

<!-- Log analysis -->
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
    EventID != 5152 and EventID != 5157]</query>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>
```

- In your Wazuh manager click **Explore > Discover > and DQL type sysmon**

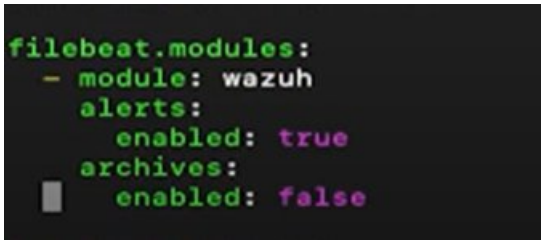


9. Installation of **Mimikatz – Mimikatz** is the application used by the attacker and Red Team to extract credential from your machine.

- We need to exclude our download folder in Virus & Threat Protection
- In Windows search type Windows security > Enable the Virus & Threat Protection > in Virus & Threat Protection click Manage settings > Click Add or remove exclusion > Add an exclusion > Folder > The path of your **download** folder.
- Download Mimikatz = https://sourceforge.net/projects/mimikatz.mirror/files/2.2.0-20220919/mimikatz_trunk.zip/download > "Note you will encounter error since Virus & Threat will verify this, just click **keep anyway.**
- Open your PowerShell (Admin) > change your directory to your downloaded Mimikatz 64 (C:\Users\Administrator\Downloads\mimikatz_trunk\x64) > Run your Mimikatz in PowerShell > **.\Mimikatz.exe**
- Navigate to your Wazuh Manager and check if there is a Mimikatz alert, if there is none? do the following in the next steps.
- Backup your Wazuh ossec.conf > In your Ubuntu terminal run the following # cp/var/ossec/etc/ossec.conf ~/ossec-backup.conf or you can do it manually.
- Now, in your terminal run # nano /var/ossec/etc/ossec.conf once open change your **logall and logall_json** from **No to Yes and save** (ctrl+x and Y).

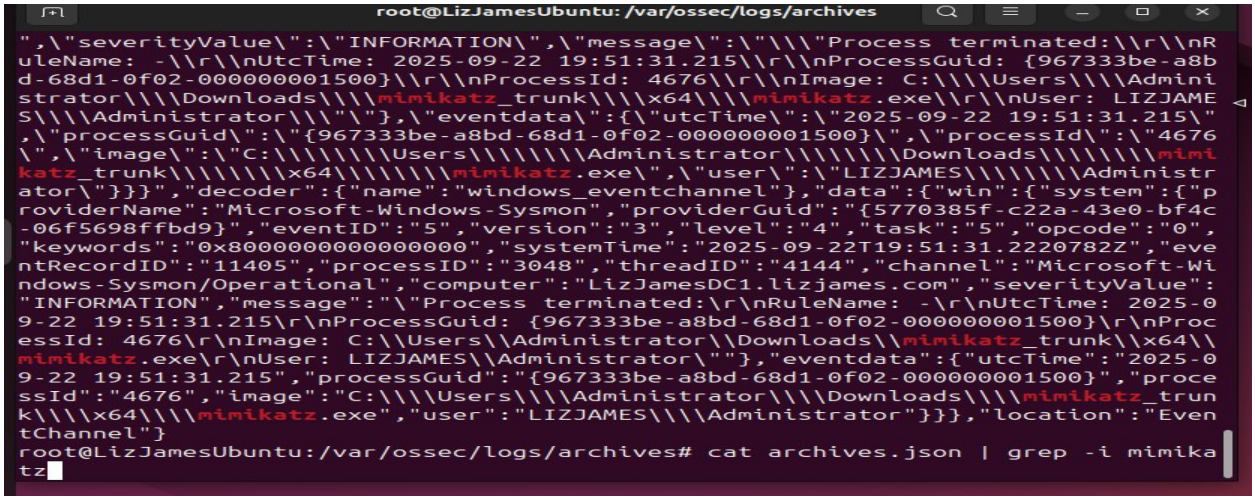


- Now, restart your Wazuh manager = systemctl restart wazuh-manager.service
- All logs will be located in /var/ossec/log/archives = json file
- Now in-order to Wazuh start ingesting this logs we need to change the location of filebeat.yml run > nano /etc/filebeat/filebeat.yml module from **false to TRUE.**

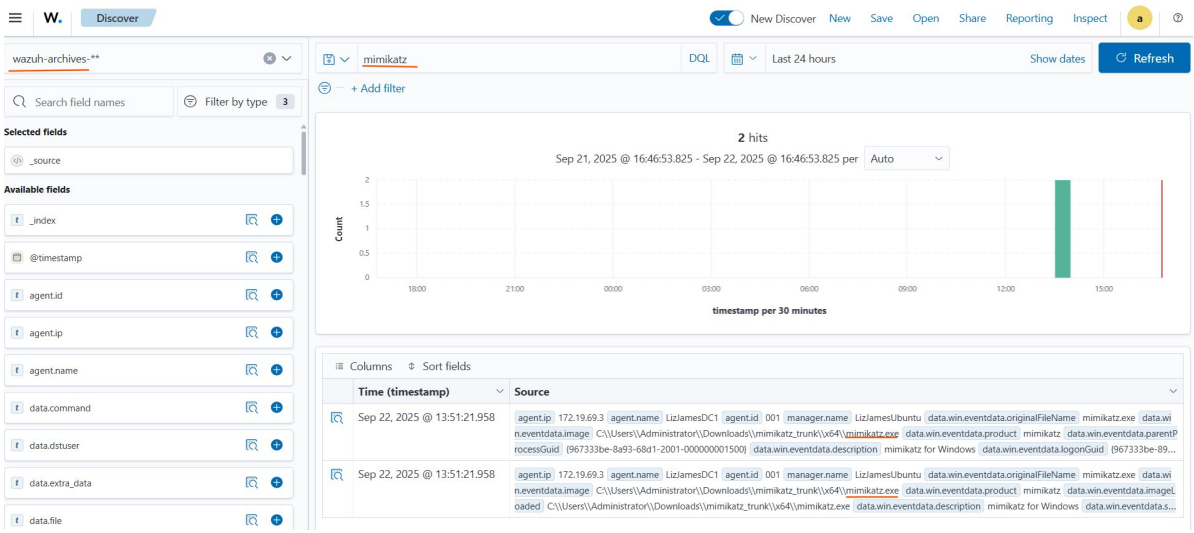


- Now, restart your filebeat run > # **systemctl restart filebeat**
- Now, we need to create a new Index > In your Wazuh Manager > Click the hamburger > Dashboard Management > Dashboard management > Index Pattern > Create Index > Index Pattern Name = wazuh-archives-** > click Next > Time field = timestamp
- Note: In Wazuh we cannot see all the logs, that is the reason we need to configure Wazuh to see all the logs and everything.

10. **How to Test the Mimikatz:**
    - In your Windows Server (Device) where Wazuh Agent and Mimikatz downloaded, start the Mimikatz for testing.
    - In your Wazuh Manager | Ubuntu, navigate to # /var/ossec/logs/archive and run # cat archives.json | grep -I mimikatz, see sample output below.



- Now, verify the tested Mimikatz to Wazuh > Click Hamburger > Exlplore > Discover > **choose wazuh-archives-** > mimikatz**



- Server Management > Rules > in search type Sysmon 0r 0800-sysmon_id_1 > check the ID 92000 > Open the .xml file

  Now, copy the rule id=”92000”

```
<group name="sysmon,sysmon_eid1_detections,windows,">

  <rule id="92000" level="4">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.parentImage" type="pcre2">(?i)\\(c|w)script\.exe</field>
    <options>no_full_log</options>
    <description>Scripting interpreter spawned a new process</description>
    <mitre>
      <id>T1059.005</id>
    </mitre>
  </rule>

  <rule id="92001" level="6">
```

- Click back button > click Custom rules > **1 local_rules.xml files are available** > click the local_rules.xml > Copy the rules that we copied a while ago and paste this to the local file

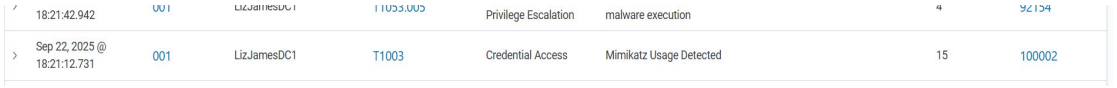
```
<rule id="92000" level="4">
  <if_group>sysmon_event1</if_group>
  <field name="win.eventdata.parentImage"
type="pcre2">(?i)\\(c|w)script\.exe</field>
  <options>no_full_log</options>
  <description>Scripting interpreter spawned a new process</description>
  <mitre>
    <id>T1059.005</id>
  </mitre>
</rule>
```

- Note: Alert is case sensitive and follow the spacing > Custom rules start with 100k

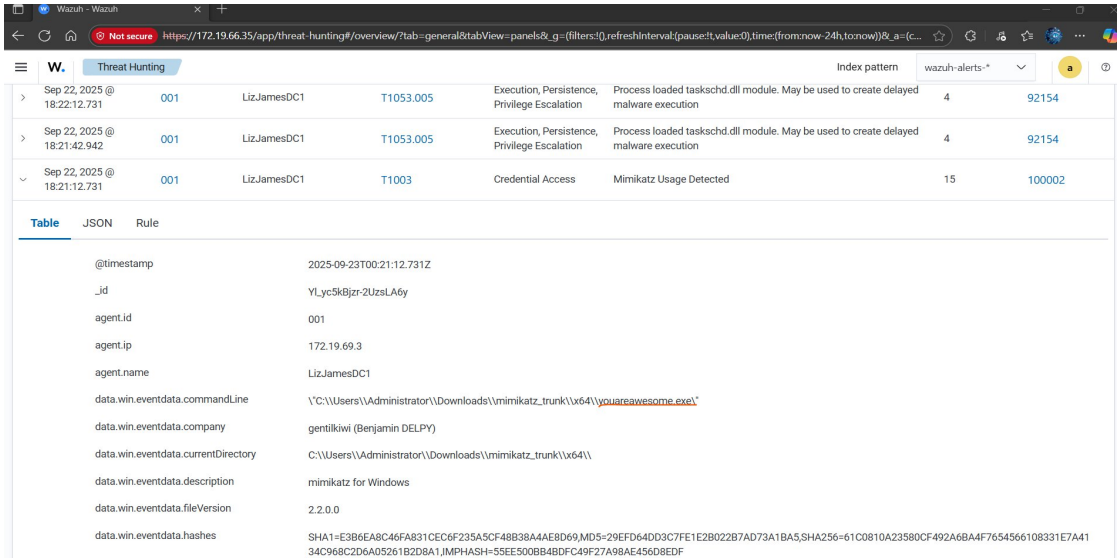
See the changes below:

```
<rule id="100002" level="15">
  <if_group>sysmon_event1</if_group>
  <field name="win.eventdata.originalFileName"
type="pcre2">(?i)mimikatz\.exe</field>
  <description>Mimikatz Usage Detected</description>
  <mitre>
    <id>T1003</id>
  </mitre>
</rule>
```

- Now, click Save > Restart > Confirm
- Now, in your Windows Server where Mimikatz located (C:\Users\Administrator\Downloads\mimikatz_trunk\x64) rename your .exe file >
- Now, click **Threat intelligence > Threat Hunting** > Verify Mimikatz Usage Detected



18:21:42.942	001	LizJamesDC1	T1053.005	Privilege Escalation	malware execution	4	92154
Sep 22, 2025 @ 18:21:12.731	001	LizJamesDC1	T1003	Credential Access	Mimikatz Usage Detected	15	100002

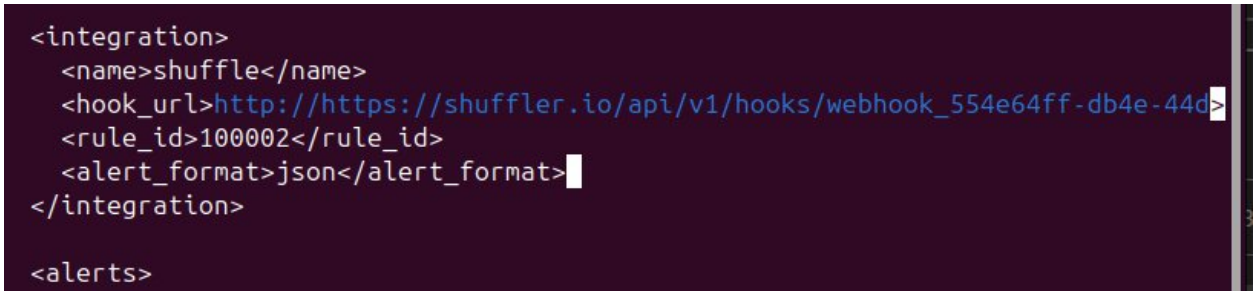


11. We will now proceed to install the www.shuffler.io > create an account > Login to Shuffle

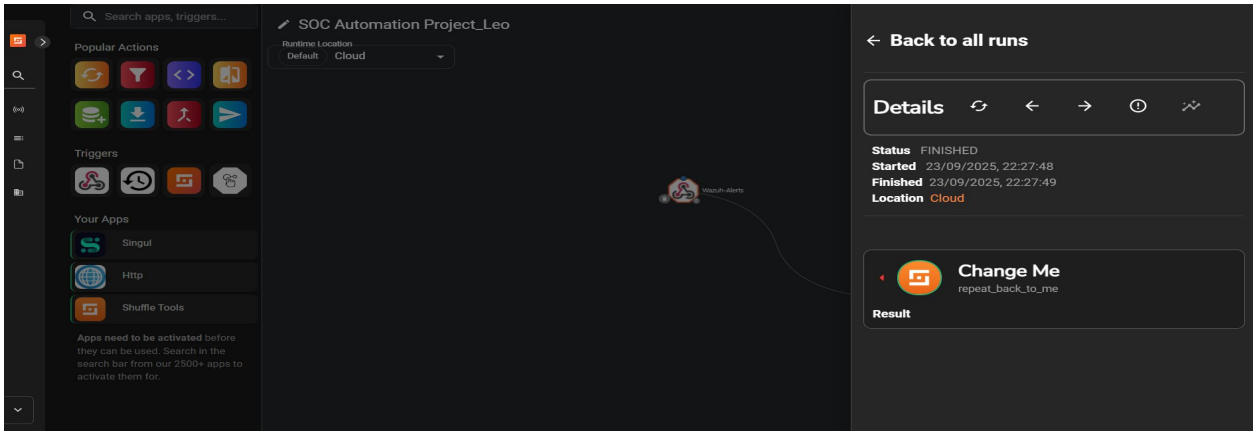
    What is Shuffle: "Shuffle workflow" is a set of automated tasks within Shuffle, an open-source platform for Security Orchestration, Automation, and Response **(SOAR).** These workflows connect various security and technical tools, automating processes like threat detection and incident response by using triggers to initiate actions and apps to interact with different services. Organizations use Shuffle workflows to streamline security operations, reduce manual tasks, and efficiently manage and respond to security incidents.

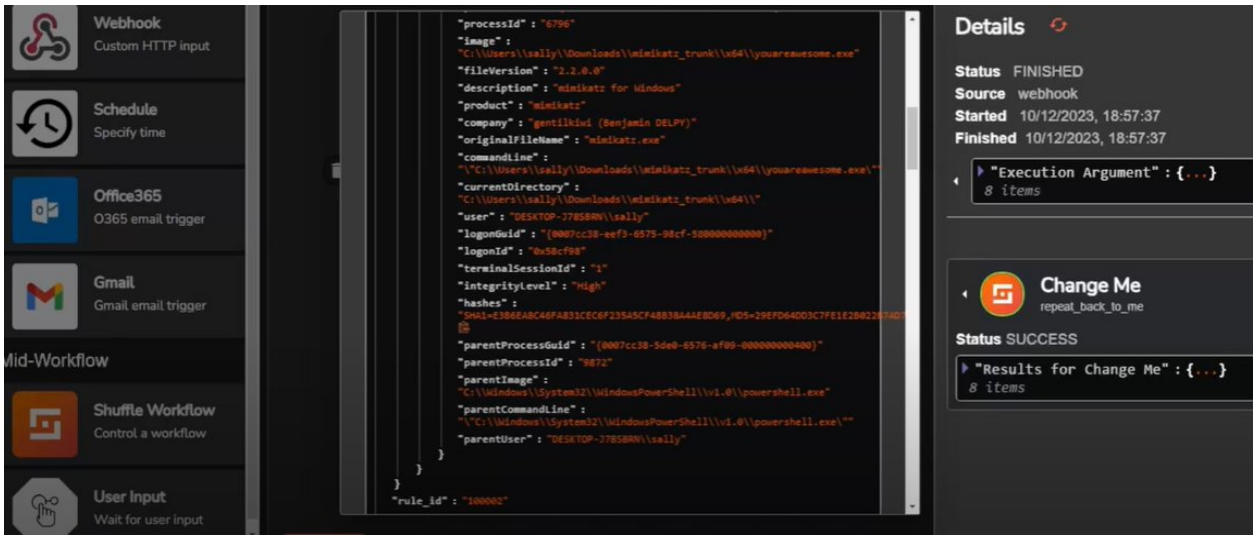
- Click Automate > Workflows > Create Workflow > > Name: , Description: Usecases
- To open your project, click Automate > Workflow > your project > Triggers > Webhook > Click the Webhook and rename this e.g. Wazuh-Alerts > In Parameters copy the Webhook URI = https://shuffler.io/api/v1/hooks/webhook_554e64ff-db4e-44d5-abe9-8c1880c6ed63
- Click your Change Me icon and make it sure that Find Actions “Repeat back to me” > Change the Call > Remove the Hello world > Click the + sign > Change with Runtime Argument > Click Save Workflow
- Now, go to your Wazuh Server (Ubuntu) > Edit the ossec.conf, navigate to terminal and run # nano /var/ossec/etc/ossec.conf

  <integration>
  <name>shuffle</name>
  <hook_url>https://”yourshuffleURL”</hook_url>
  <rule_id>100002</rule_id>
  <alert_format>json</alert_format>
  </integration>



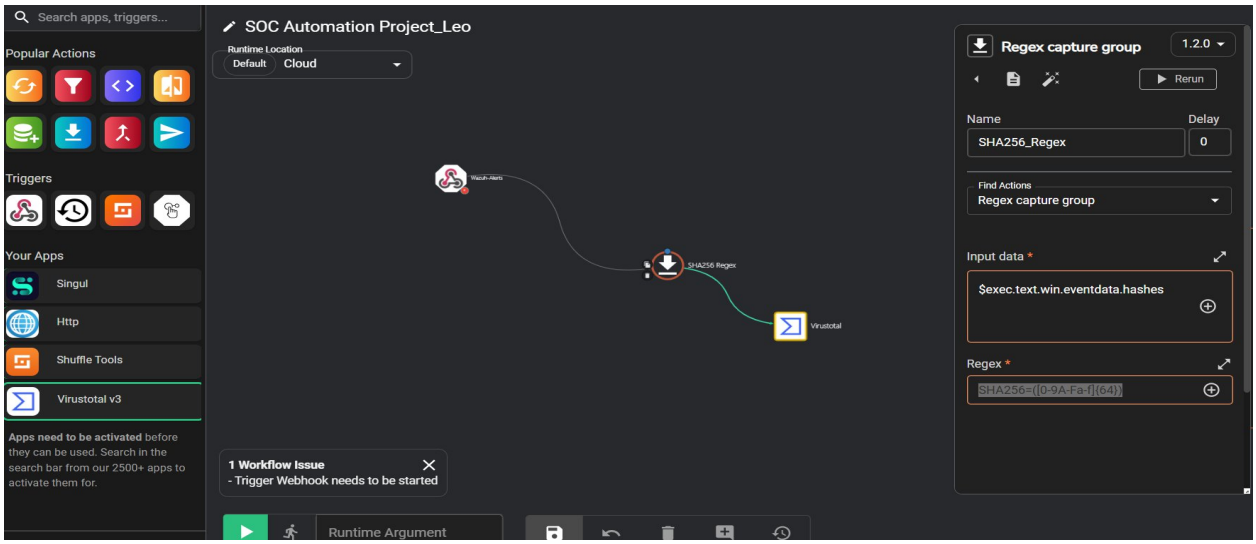
- Run systemctl daemon-reload and systemctl restart wazuh-manager.service
- Now, in your www.shuffler.io > Automate > Workflows > Click your WebHook Wazuh-Alerts> Click the running person and click Test Workflow



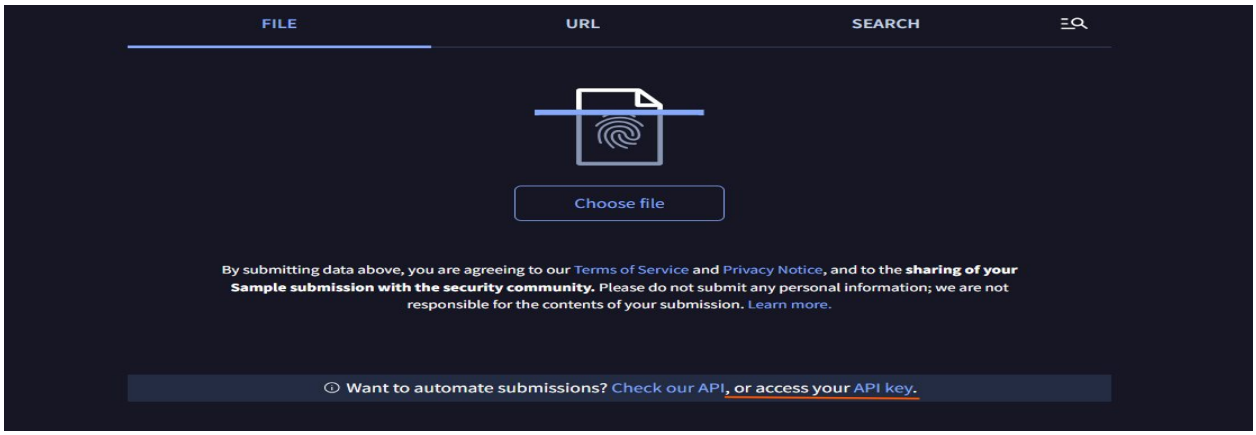


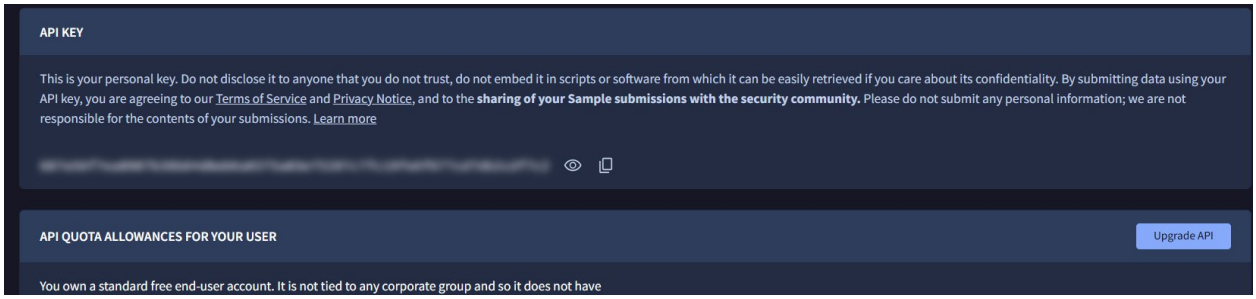
12. In **Change Me** icon > Rename this to **SHA256_Regex** > Find Actions = Regex capture group > Input data = $exec.text.win.eventdata.hashes Regex = SHA256=([0-9A-Fa-f]{64}) > Click Save button

    Note: to create a Regex = use ChatGPT or Copilot and prompt like: “create a regex to parse the sha256 value”

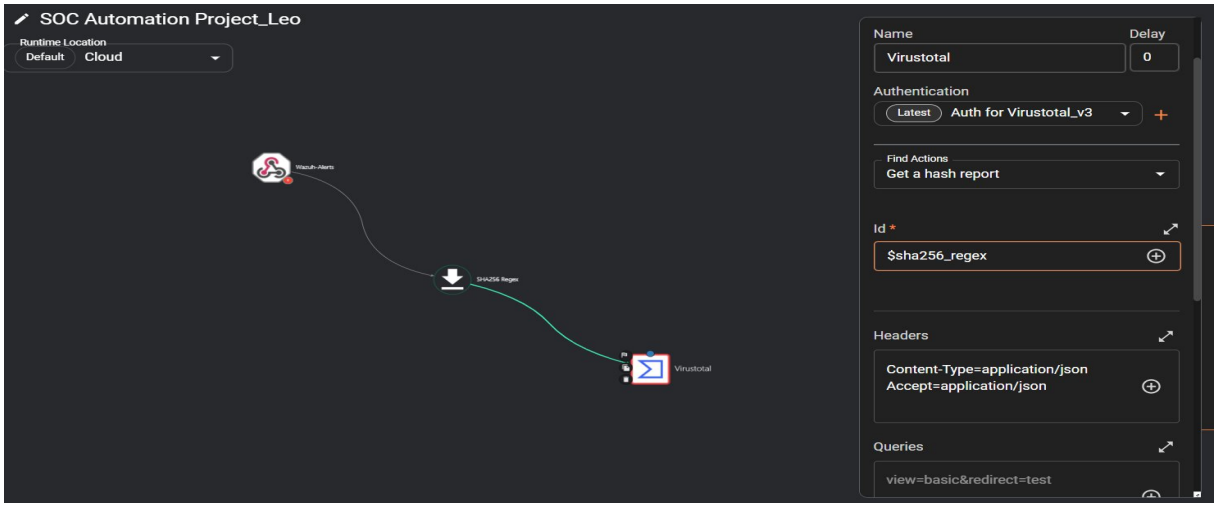


13. We will now use and utilize **Virus Total** to check the **Reputation** > Sign in to Virus Total https://www.virustotal.com/ and create an account > Now in Virus Total click below the access your API Key > Now you can see your API key above in blurry.



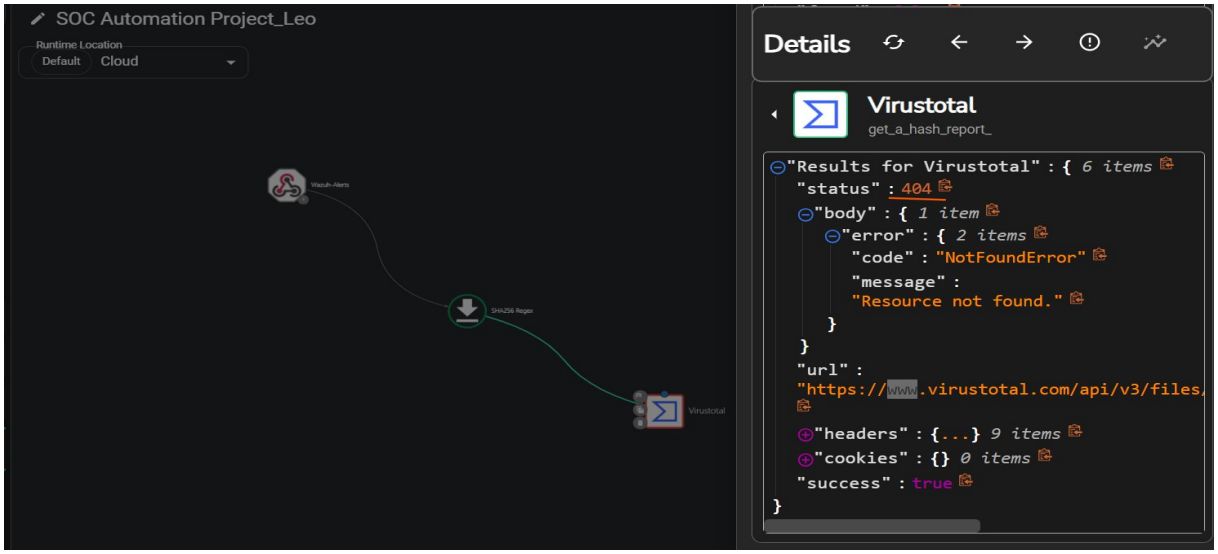


- Go-back to your Shuffle > in search app, triggers type Virus Total > click to be activated > Drag your Virus Total and it will automatically connect to your SHA256 Regex
- Configure your Virus total > Name = Virus total > Find Actions = Get a hash report > Click authenticate Virustotal v3 > paste your API key and copy this to your Virustotal see above > click Submit > ID click + and choose SHA256 Regex = $sha256_regex > Headers = default > Click Save

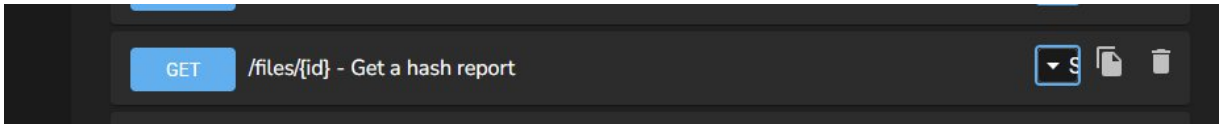


- Now click Person Test Run again.

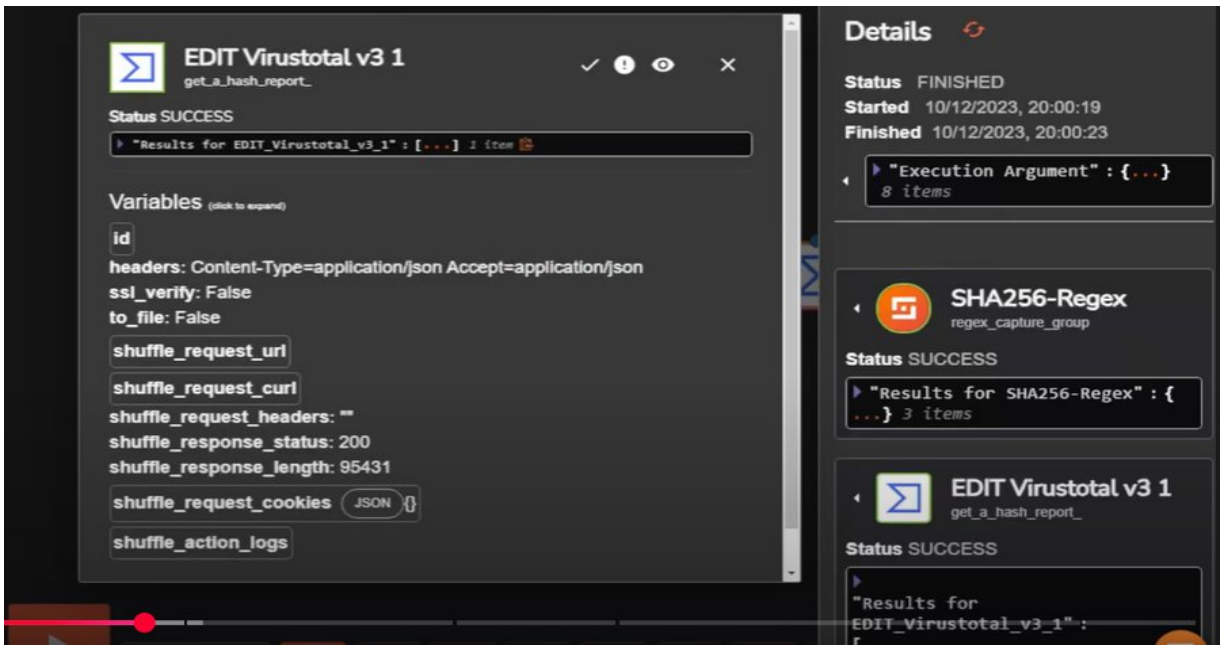
- On this, you will encounter an error 404.



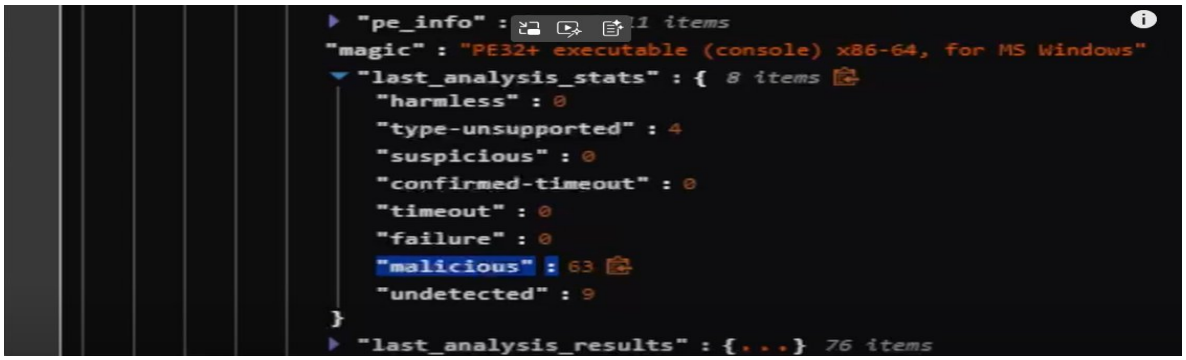
- **How to fix this?** > Now, in the left > Click APP > Click Virus total view App details > Go down and find the Get a hash report > Click GET



- Now, test to **Run** again



- To check the **Reputation**: Identify that there is a 63 malicious, **meaning that there are 63 scanners detected that is malicious.**

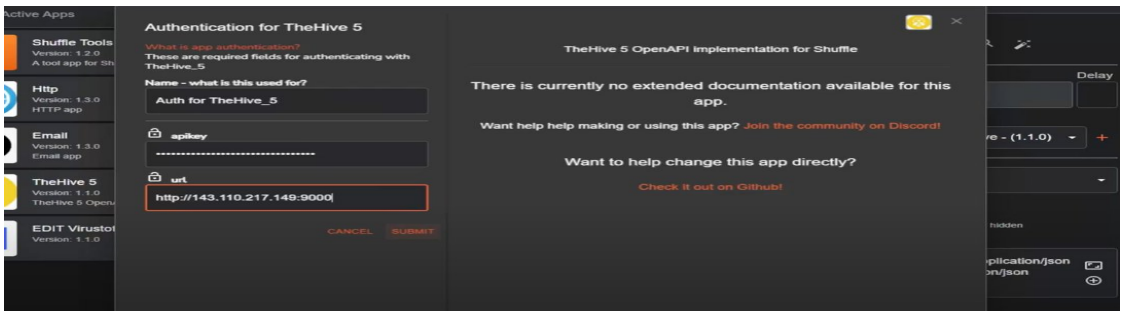


14. **TheHive** – it will create an alert for case management

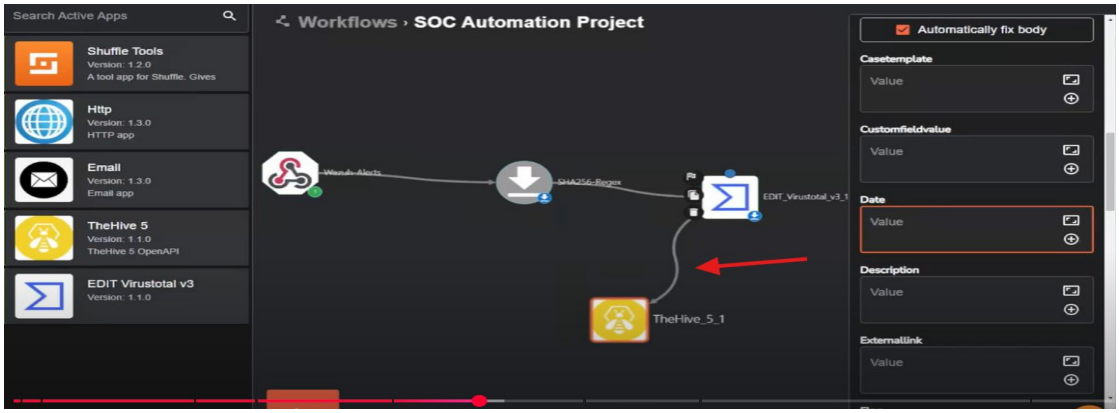
- In Search Active Apps > Type TheHive > Click TheHive to activate this in your SOAR (Shuffle) > Drag TheHive to your project
- How to install TheHive in your Ubuntu machine

  https://docs.strangebee.com/thehive/installation/installation-guide-linux-standalone-server/#step-3-install-and-configure-apache-cassandra

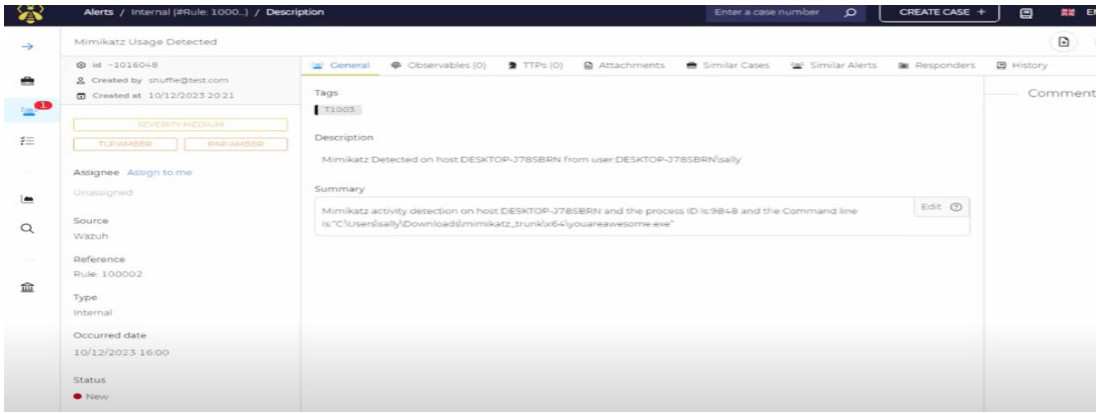
- Now, login to your TheHive > Click the + button > Name: SOC Home Project_Leo > Click Confirm.
- Add 2 users: Add a user > Normal > Login = leo@test.com, Name = Leo, Profile = Analyst > Click confirm
- Create a password in the account > click preview > set a new password > hit confirm
- Add a user > Service > Login = shuffle@test.com, Name = SOAR, Profile = Analyst > Click confirm
- Create a password in the account > click preview > Create API Key > Copy the API > This you will use this in your Shuffle TheHive
- Now, go back to **Shuffle** and configure the TheHive > Click the + button beside authenticate > Now, provide the APIKEY from TheHive a while ago > URL: provide the IP address of your TheHive and port number = http://143.110.217.149:9000



- Now connect your Wazuh to TheHive



- Find Actions = **select create alert** > Date = Select Execution Argument (SHA256 Regex) > Select UTC Time > Title = Mimikatz Detected on host:$exec.test.win.system.computer from user > Status = New > Summary = Mimikats activity detection on $exec (Execution Argument) > Tags = [“T1003”] > Type = Internal > Save the workflow
- Modify your firewall to open this enable all communication will pass thru in your Shuffle > Save the workflow
- Now Rerun the workflow > Click the person icon > Click Rerun the workflow > see output below > Automatically the alert was created



15. Next steps, is to send an email to the Analyst.

- In the Search Active Apps > Click the Email and drag this to your project > Connect the Virtus Total to your Email and configure the Email.
- Use https://sqrx.com/ for some investigation like file viewer and browser

” When you train Smarter, you defend Stronger”
Leonard Estos