SOC Automation Project-Navjot Singh

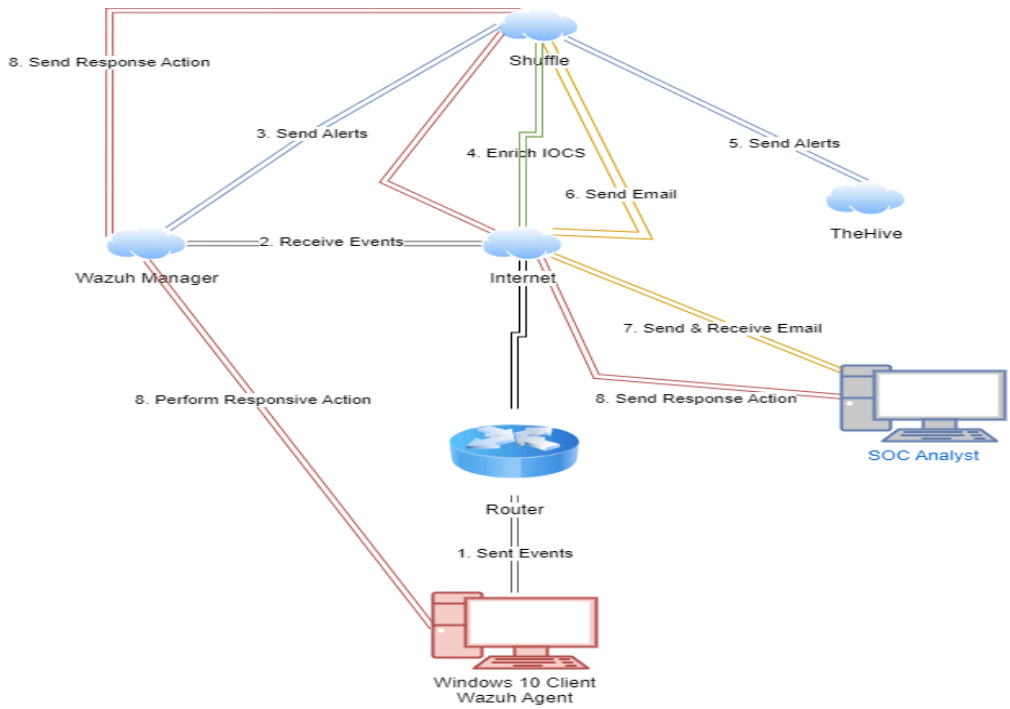
Objective: To learn and understand Identification, Containment, and Eradication with various different tools in a SOC analysts environment.

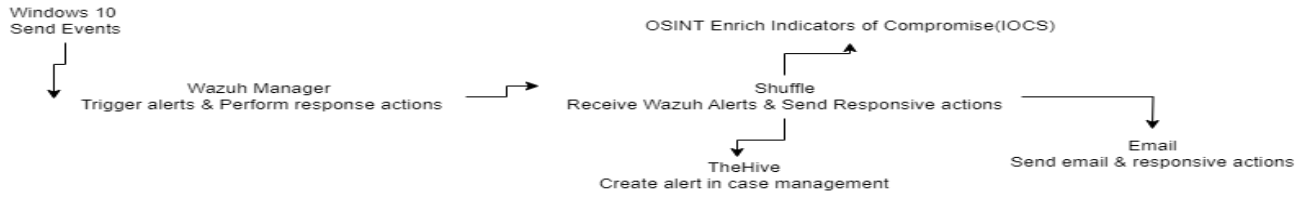
Tools/Machines:

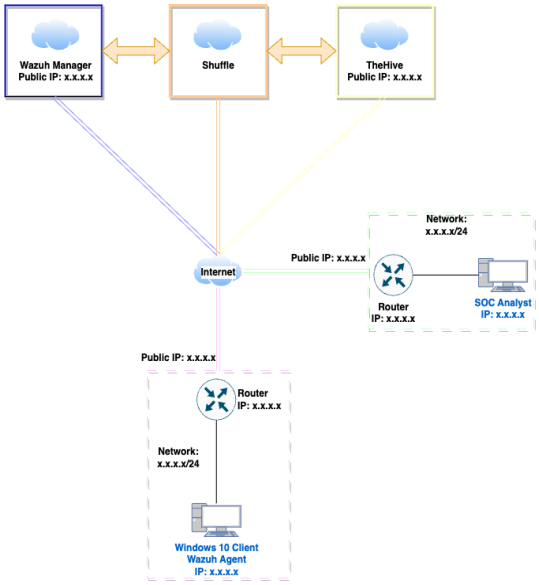
Draw.io-Design environment
Wazuh Manager- Extended detection and response(XDR) and Security information and event management (SIEM)-Ubuntu 22.04
TheHive-Open source Security Incident Response Platform-Ubuntu 22.04
Shuffle->Security orchestration, automation and response (SOAR)
Windows 10 Wazuh agent/client
Sysmon-System Monitor is a Windows system service and device driver

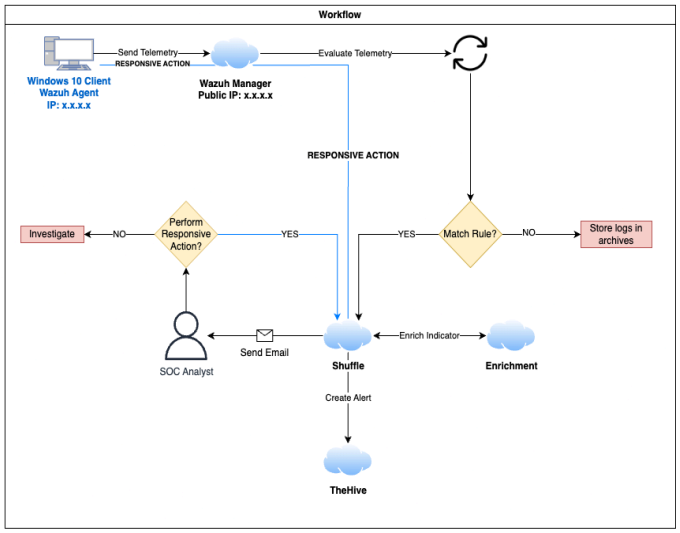
Design:

Draw.io was used to design the logical structure of data flow. Draw.io is an open source diagram maker. This design visual can help me understand where and how the data flow will be implemented in the project. It also points out different connections between tools and machines. Below is my Draw.io diagram that I referenced during the course of the project. Screenshot Below ↓↓









Credits^: https://www.youtube.com/@MyDFIR

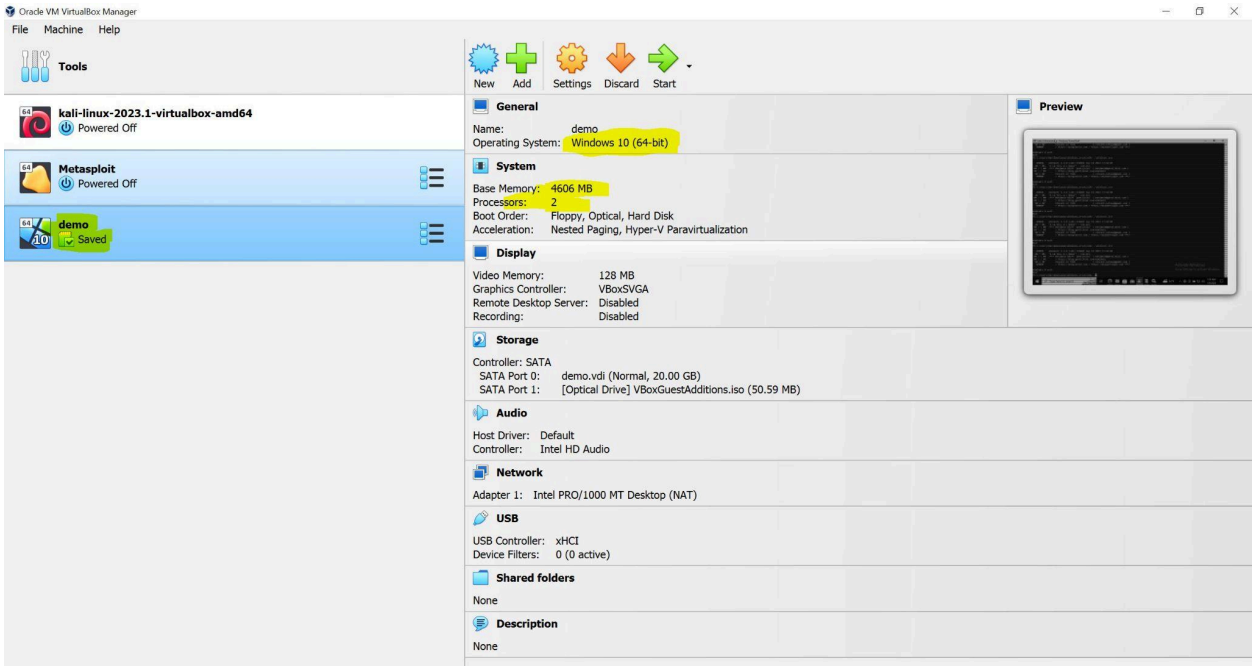
Setup Explanation:

1. A Windows 10 client with Wazuh agent will send events through the internet to the Wazuh manager that will host a Wazuh dashboard which I will showcase further in the project.
2. The Wazuh manager/dashboard will send the alert through the Shuffle-SOAR platform and add it under case management in Thehive.
3. Shuffle not only aids in enriching the Indicators of Compromise (IOCs) but also facilitates the exchange of emails between Shuffle and the Security Operations Center (SOC) Analyst.
    a. I am in the process of establishing a lab that involves the utilization of Mimikatz, a program designed for extracting passwords, hashes, PINs, and Kerberos tickets from Windows memory. In the event that the sysmon on the Windows 10 client detects the presence of the Mimikatz application, the Wazuh client will promptly send an alert to Shuffle.
    b. Shuffle will extract the SHA 256 hash to check reputation score with virustotal-Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, and automatically share them with the security community.
    c. Shuffle will then send updated information to the Thehive for case management.
    d. Lastly, send an email to an SOC analyst.
4. The SOC analyst will receive an email containing an option to respond to the alert, which will follow a path through Shuffle, the dashboard, and ultimately reach the Windows 10 client.

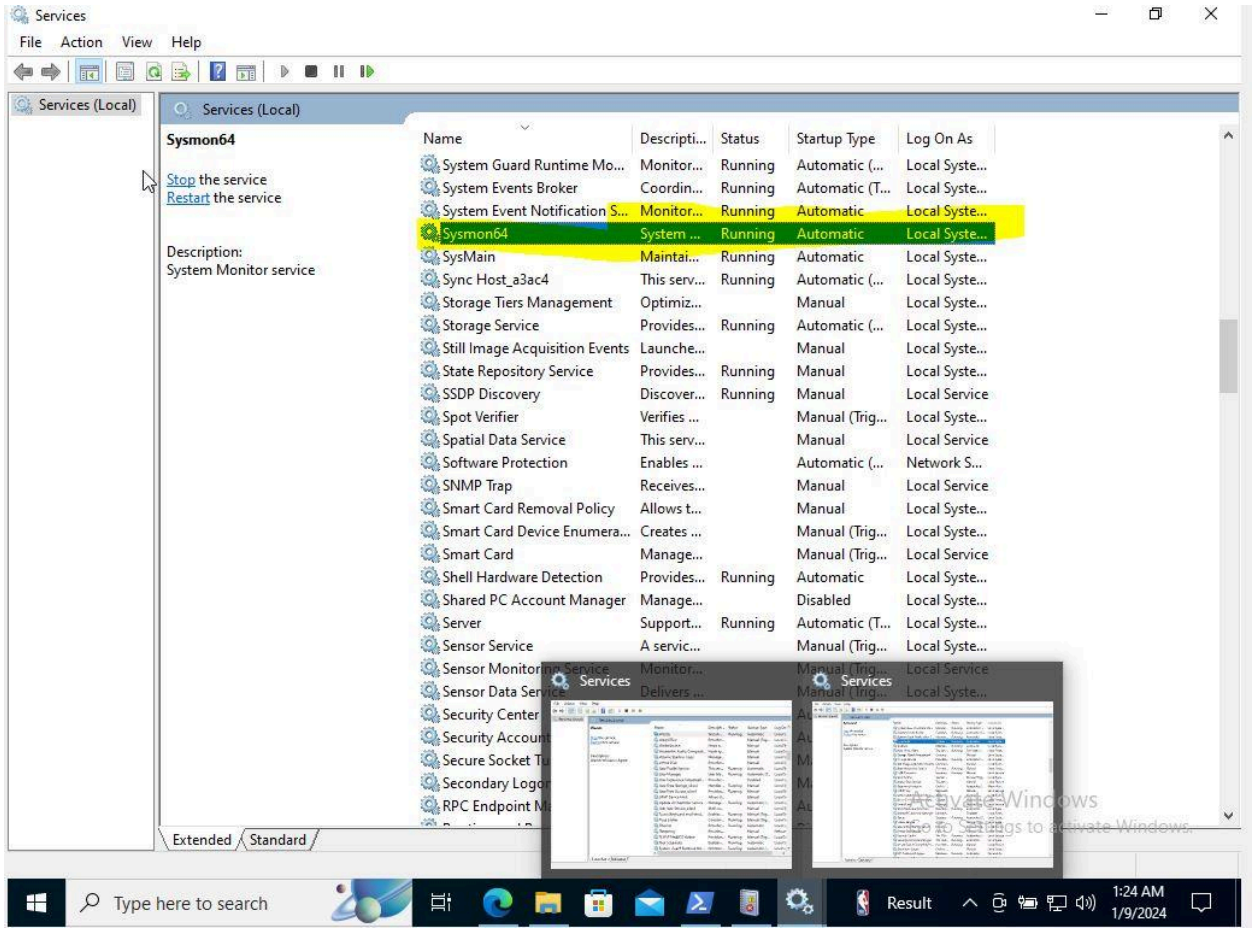
Machine configurations:

Windows 10 and sysmon setup: My Github instruction:-https://github.com/872941/Soc-Automation-Project/blob/main/Windows%2010%20and%20Sysmon%20Setup

A. I utilized Virtualbox where I set up Windows 10 ISO from Microsoft: https://www.microsoft.com/en-us/software-download/windows10 .



B. Sysmon on windows 10:



WAZUH manager server and thehive Setup: https://youtu.be/YxpUx0czgx4?t=917

A. I used a digitalocean(https://www.digitalocean.com/)-online cloud provider and set up 2 Ubuntu 22.04 machines: 1 for the Wazuh manager that will serve the dashboard and the other for Thehive for case management.
B. Specifications:
   CPU: 2 CPU Cores
   RAM: 8GB+
   HDD: 50GB+
   OS: Ubuntu 22.04 LTS
   Make sure to write down passwords for both machines.

Name	IP Address	State	Added
Wazuh 8 GB / 2 Intel vCPUs / 160 GB / TOR1		Up-to-date	18 minutes ago
thehive 8 GB / 2 Intel vCPUs / 160 GB / TOR1		Updating...	Just now

C. Setup firewall for both machines:
   a. Click on the networking tab and set up the firewall with the rules below and assign firewall to both machines.

Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All other traffic will be blocked.

Type	Protocol	Port Range	Sources	
ICMP	ICMP		[redacted]	More
All TCP	TCP	All ports	[redacted]	More
SSH	TCP	22	[redacted]	More
HTTP	TCP	80	[redacted]	More
HTTPS	TCP	443	[redacted]	More
Custom	TCP	9000	All IPv4	More
Custom	TCP	55000	All IPv4	More
All UDP	UDP	All ports	[redacted]	More

New rule

Outbound Rules

Set the Firewall rules for outbound traffic. Outbound traffic will only be allowed to the specified ports. All other traffic will be blocked.

Type	Protocol	Port Range	Destinations	
ICMP	ICMP		All IPv4 All IPv6	More
All TCP	TCP	All ports	All IPv4 All IPv6	More
All UDP	UDP	All ports	All IPv4 All IPv6	More

D. Run the droplet and run updates: apt-get update && apt-get upgrade

a. Specifications
b. RAM: 8GB+
c. HDD: 50GB+
d. OS: Ubuntu 22.04 LTS

e. Install Wazuh 4.7
f. curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
g. Make sure to write down username and password at the end of the command.

```
08/01/2024 00:44:55 INFO: --- Removing existing Wazuh installation ---
08/01/2024 00:44:55 INFO: Removing Wazuh manager.
08/01/2024 00:45:04 INFO: Wazuh manager removed.
08/01/2024 00:45:04 INFO: Removing Wazuh indexer.
08/01/2024 00:45:08 INFO: Wazuh indexer removed.
08/01/2024 00:45:08 INFO: Removing Filebeat.
08/01/2024 00:45:11 INFO: Filebeat removed.
08/01/2024 00:45:11 INFO: Removing Wazuh dashboard.
08/01/2024 00:45:22 INFO: Wazuh dashboard removed.
08/01/2024 00:45:23 INFO: Installation cleaned.
08/01/2024 00:45:31 INFO: Wazuh web interface port will be 443.
08/01/2024 00:45:38 INFO: Wazuh repository added.
08/01/2024 00:45:38 INFO: --- Configuration files ---
08/01/2024 00:45:38 INFO: Generating configuration files.
08/01/2024 00:45:39 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necess
ary for installation.
08/01/2024 00:45:40 INFO: --- Wazuh indexer ---
08/01/2024 00:45:40 INFO: Starting Wazuh indexer installation.
08/01/2024 00:46:40 INFO: Wazuh indexer installation finished.
08/01/2024 00:46:40 INFO: Wazuh indexer post-install configuration finished.
08/01/2024 00:46:40 INFO: Starting service wazuh-indexer.
08/01/2024 00:46:58 INFO: wazuh-indexer service started.
08/01/2024 00:46:58 INFO: Initializing Wazuh indexer cluster security settings.
08/01/2024 00:47:09 INFO: Wazuh indexer cluster initialized.
08/01/2024 00:47:09 INFO: --- Wazuh server ---
08/01/2024 00:47:09 INFO: Starting the Wazuh manager installation.
08/01/2024 00:47:55 INFO: Wazuh manager installation finished.
08/01/2024 00:47:55 INFO: Starting service wazuh-manager.
08/01/2024 00:48:13 INFO: wazuh-manager service started.
08/01/2024 00:48:13 INFO: Starting Filebeat installation.
08/01/2024 00:48:19 INFO: Filebeat installation finished.
08/01/2024 00:48:19 INFO: Filebeat post-install configuration finished.
08/01/2024 00:48:19 INFO: Starting service filebeat.
08/01/2024 00:48:20 INFO: filebeat service started.
08/01/2024 00:48:20 INFO: --- Wazuh dashboard ---
08/01/2024 00:48:20 INFO: Starting Wazuh dashboard installation.
08/01/2024 00:48:57 INFO: Wazuh dashboard installation finished.
08/01/2024 00:48:57 INFO: Wazuh dashboard post-install configuration finished.
08/01/2024 00:48:57 INFO: Starting service wazuh-dashboard.
08/01/2024 00:48:58 INFO: wazuh-dashboard service started.
08/01/2024 00:49:28 INFO: Initializing Wazuh dashboard web application.
08/01/2024 00:49:30 INFO: Wazuh dashboard web application initialized.
08/01/2024 00:49:30 INFO: --- Summary ---
08/01/2024 00:49:30 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: vUQdm*FdBVu9b??2p6ibkezyWO?2lc?P
08/01/2024 00:49:30 INFO: Installation finished.
root@Wazuh:~# _
```

h. Extract Wazuh Credentials
i. sudo tar -xvf wazuh-install-files.tar

E. Use https://WAZUH-Droplet-Address to access dashboard

Thehive: https://youtu.be/YxpUx0czgx4?t=1258 -Mydfir

A. Setup the droplet with the same Specs as the Wazuh manager and same configured firewall
B. Open Thehive and install the prerequisites in order: Java, Cassandra, Elastic search and thehive; all the command are in instruction file in github: https://github.com/872941/Soc-Automation-Project/blob/main/TheHive-Install-Instructions.txt
C. When everything is installed use systemctl status to check if they are active and running.

Configuration of thehive and Wazuh manager: https://youtu.be/VuSKMPRXN1M?t=37

** Make sure to restart after each config; as this is important to apply necessary changes. Systemctl restart **

Thehive config:

A. Cassandra config: Nano into /etc/cassandra/cassandra.yaml and change cluster name to whatever you would like and change listen, RPC, and seed provider address to the public ip address of the thehive server. Remove any old files: rm -rf /var/lib/cassandra/*
B. Elasticsearch config:
    a. nano /etc/elasticsearch/elasticsearch.yml.
    b. Uncomment cluster name and put thehive.
    c. Uncomment node-name
    d. Uncomment network host and put in public ip of thehive and remember that default port is 9200
    e. Uncomment cluster.initial_master_nodes:["node-1"]-here we can setup to scale the elasticsearch

C. Thehive
    a. Ls -la /opt/thp
    b. Chown -R thehive:thehive /opt/thp—--------->> changing ownership of user/group to run the hive
    c. Nano /etc/thehive/application.conf
    d. Change database and index config ip address to the thhive public address
    e. Under service config: Application.baseurl should have thehive public address on port 9000 so you can access the dashboard.

```
root@thehive:~# systemctl status cassandra.service
● cassandra.service - LSB: distributed storage system for structured data
     Loaded: loaded (/etc/init.d/cassandra; generated)
     Active: active (running) since Mon 2024-01-08 21:57:19 UTC; 37min ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 71 (limit: 9492)
     Memory: 2.2G
        CPU: 1min 46.830s
     CGroup: /system.slice/cassandra.service
             └─15944 /usr/bin/java -ea -da:net.openhft... -XX:+UseThreadPriorities -XX:+HeapDumpOnOutOfMemoryError -Xss256k -XX>

Jan 08 21:57:19 thehive systemd[1]: Starting LSB: distributed storage system for structured data...
Jan 08 21:57:19 thehive systemd[1]: Started LSB: distributed storage system for structured data.
root@thehive:~# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-01-08 22:33:59 UTC; 1min 20s ago
       Docs: https://www.elastic.co
   Main PID: 20024 (java)
      Tasks: 64 (limit: 9492)
     Memory: 2.5G
        CPU: 44.553s
     CGroup: /system.slice/elasticsearch.service
             ├─20024 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.ca>
             └─20208 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jan 08 22:33:39 thehive systemd[1]: Starting Elasticsearch...
Jan 08 22:33:42 thehive systemd-entrypoint[20024]: Jan 08, 2024 10:33:42 PM sun.util.locale.provider.LocaleProviderAdapter <cli>
Jan 08 22:33:42 thehive systemd-entrypoint[20024]: WARNING: COMPAT locale provider will be removed in a future release
Jan 08 22:33:59 thehive systemd[1]: Started Elasticsearch.
root@thehive:~# systemctl status thehive
● thehive.service - Scalable, Open Source and Free Security Incident Response Solutions
     Loaded: loaded (/lib/systemd/system/thehive.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-01-08 22:04:09 UTC; 31min ago
       Docs: https://thehive-project.org
   Main PID: 16807 (java)
      Tasks: 101 (limit: 9492)
     Memory: 893.3M
        CPU: 2min 58.461s
     CGroup: /system.slice/thehive.service
             └─16807 java -Dfile.encoding=UTF-8 -Dconfig.file=/etc/thehive/application.conf -Dlogger.file=/etc/thehive/logback.>

Jan 08 22:04:09 thehive systemd[1]: Started Scalable, Open Source and Free Security Incident Response Solutions.
root@thehive:~# _
```

Default Credentials on port 9000
credentials are 'admin@thehive.local' with a password of 'secret'

ERROR code: if thehive is giving errors or not starting up then its most likely elasticsearch, if that is the case then add more computing power to the droplet.

** Make sure to restart after each config; as this is important to apply necessary changes. Systemctl restart **

Wazuh Config and dashboard:

A. Extract Wazuh Credentials: sudo tar -xvf wazuh-install-files.tar
B. We need to extract wazuh-passwords.txt: the file should be in /wazuh-install-files—------->> take a note of user API username and pass(this will be used with shuffle for automation)and the admin username and pass

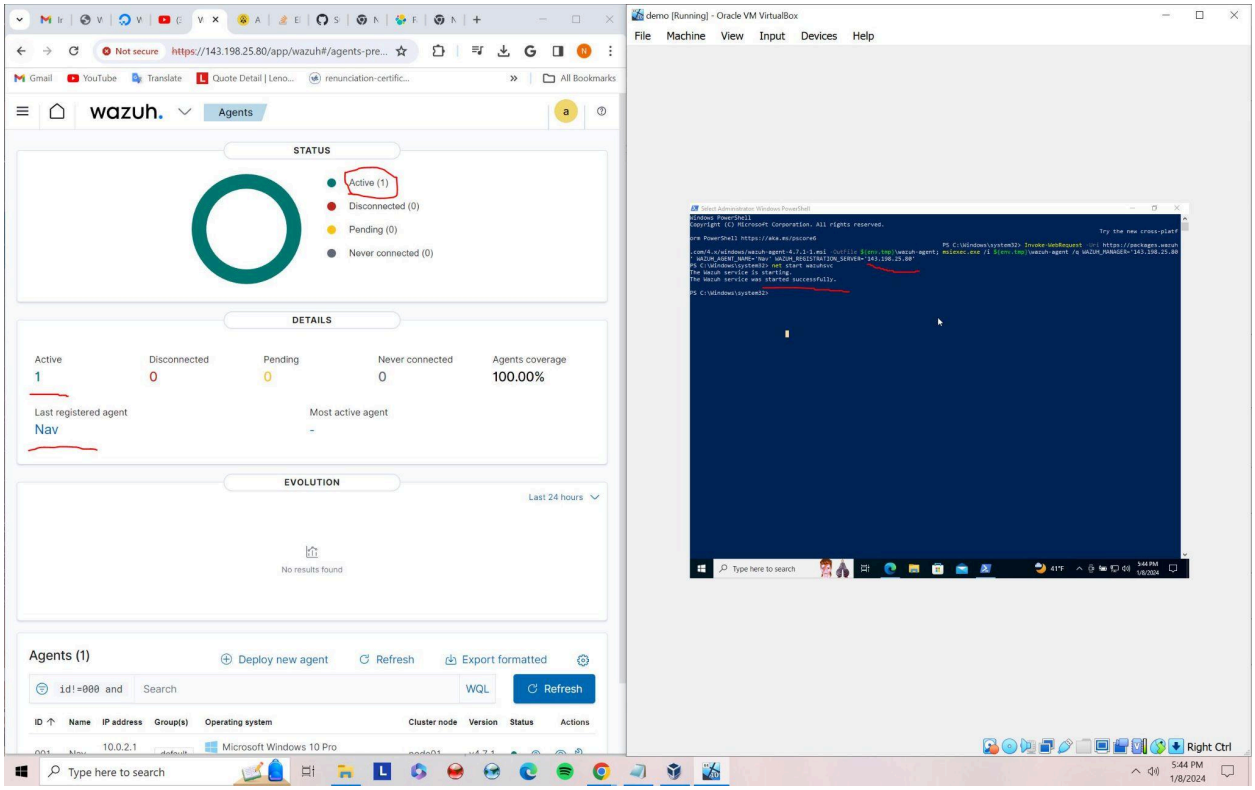
```
wazuh-install-files/wazuh-dashboard-key.pem
wazuh-install-files/wazuh-dashboard.pem
wazuh-install-files/admin-key.pem
wazuh-install-files/config.yml
wazuh-install-files/root-ca.key
wazuh-install-files/wazuh-passwords.txt
wazuh-install-files/wazuh-indexer.pem
wazuh-install-files/admin.pem
wazuh-install-files/wazuh-indexer-key.pem
wazuh-install-files/wazuh-server.pem
root@Wazuh:~# cd wazuh-install-files/
root@Wazuh:~/wazuh-install-files# ls
admin-key.pem  config.yml   root-ca.pem              wazuh-dashboard.pem    wazuh-indexer.pem    wazuh-server-key.pem
admin.pem      root-ca.key  wazuh-dashboard-key.pem  wazuh-indexer-key.pem  wazuh-passwords.txt  wazuh-server.pem
root@Wazuh:~/wazuh-install-files# cat wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: 'vUQdm*FdBVu9b?72p6ibkezyWO?2lc?P'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
  indexer_username: 'kibanaserver'
  indexer_password: 'vom1wG+Xw8Lbl27inFh03G+zp9WoLHJV'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
  indexer_username: 'kibanaro'
  indexer_password: 'ifW0dSo5L4VVJzYA3PxAdAeL.eLT.F0v'

# Filebeat user for CRUD operations on Wazuh indices
  indexer_username: 'logstash'
  indexer_password: 'jdN43x7O3ug7hbfpf9.SL9A8EJYy2zU6'

# User with READ access to all indices
  indexer_username: 'readall'
  indexer_password: '.Hi6owb+AMTgHQ3Hcp0oW+HXo6fD9Ib1'

# User with permissions to perform snapshot and restore operations
  indexer_username: 'snapshotrestore'
  indexer_password: 'TgupjSw7bKj2rL480VWIZShf3.QK3Mzb'

# Password for wazuh API user
  api_username: 'wazuh'
  api_password: '2SvecJwN5jR1S7nYHeVMYd8Tse+y5+a7'

# Password for wazuh-wui API user
  api_username: 'wazuh-wui'
  api_password: 'psWf80vQma+G90HYjw+?b7LfuO6gAF13'

root@Wazuh:~/wazuh-install-files# _
```

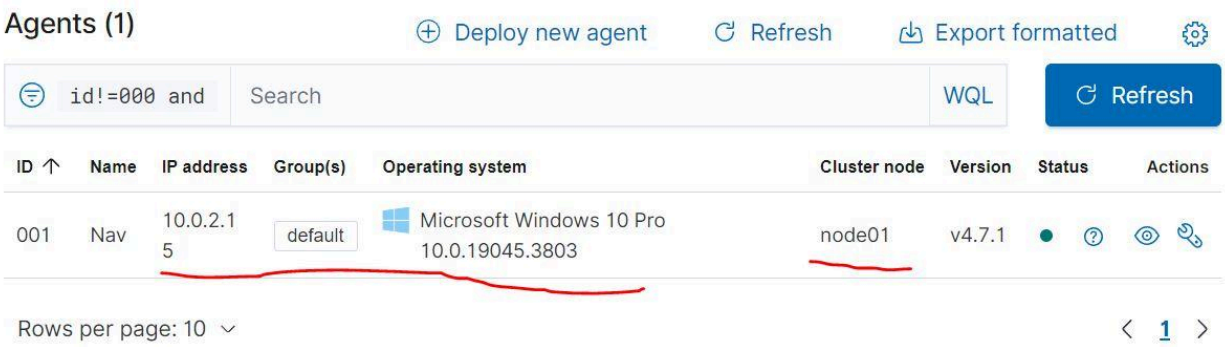
C. Using the admin username and pass, the dashboard can be accessed.

** Make sure to restart after each config; as this is important to apply necessary changes. Systemctl restart **

Wazuh dashboard:

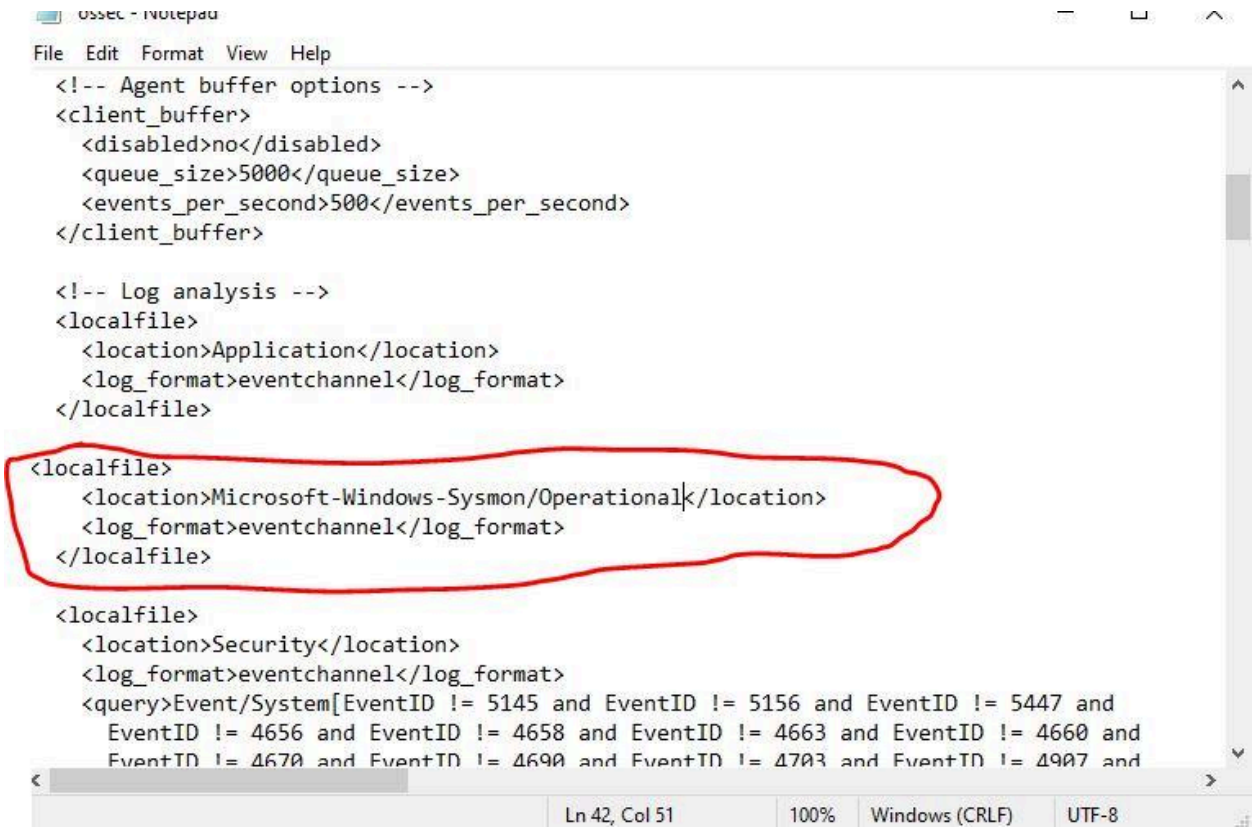
A. Click add agent on the dashboard and select windows 10 option that should be MSI 32/64 bits.
B. Add Wazuh public address in the server address box
C. Add name for the windows 10 agent and select default group
D. Open admin powershell and copy and run command; Start Wazuh agent
E. Double check in services if the Sysmon and Wazuh services are running(net start wazuhsvc).
F. Now there should be active agents on the dashboard:
G. End goal is to detect Mimikatz on the client machine





Windows 10 Telemetry:

A. This telemetry is needed for sysmon and wazuh dashboard to communicate with each other.
B. Go to local disk>program files x86 > ossec agent:---open ossec conf file using admin privileges notepad
C. Under log analysis add the red circled text in the ossec conf file(show in the pic below)



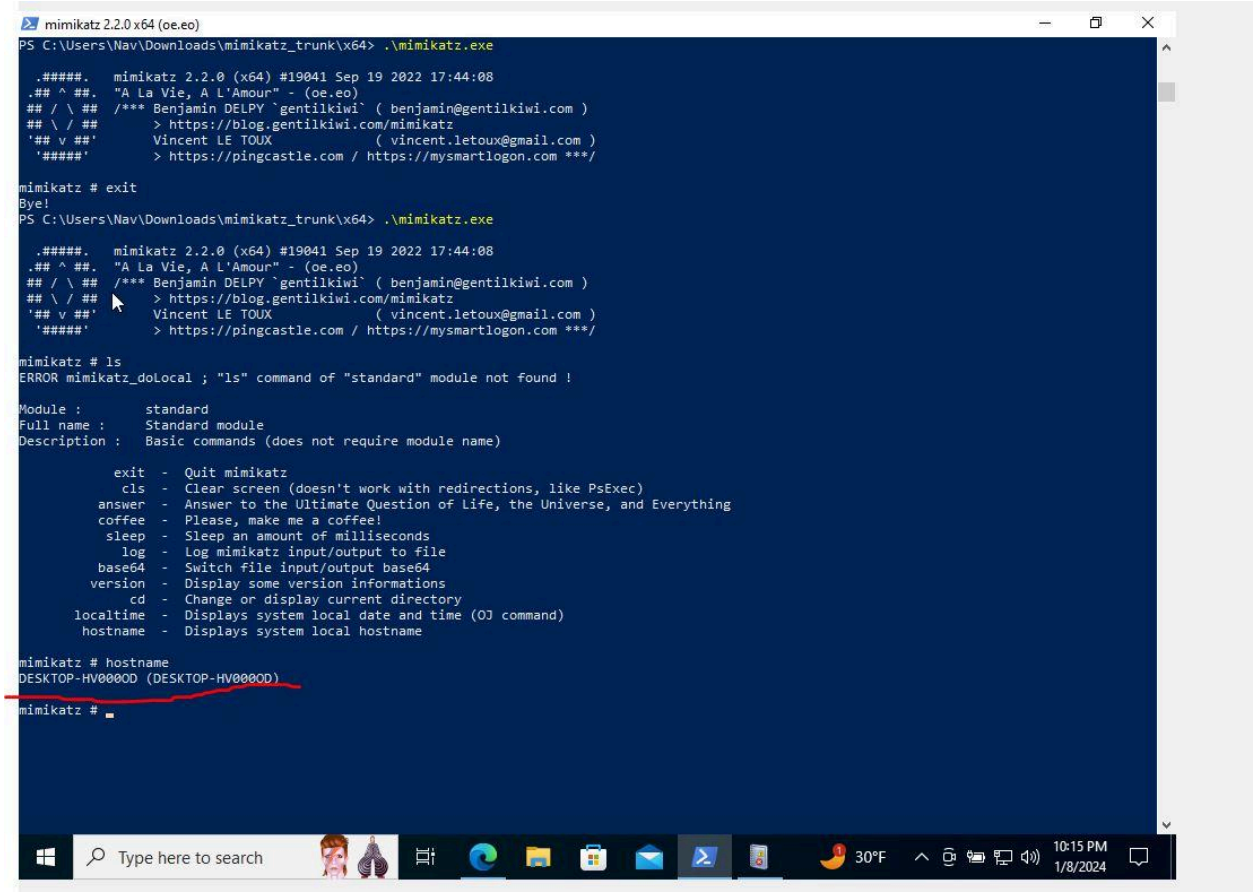
D. Save file and restart wazuh service
E. Open the wazuh dashboard and notice the agent that you named.
F. In security events tab search for sysmon and wazuh should detect the usage of sysmon.

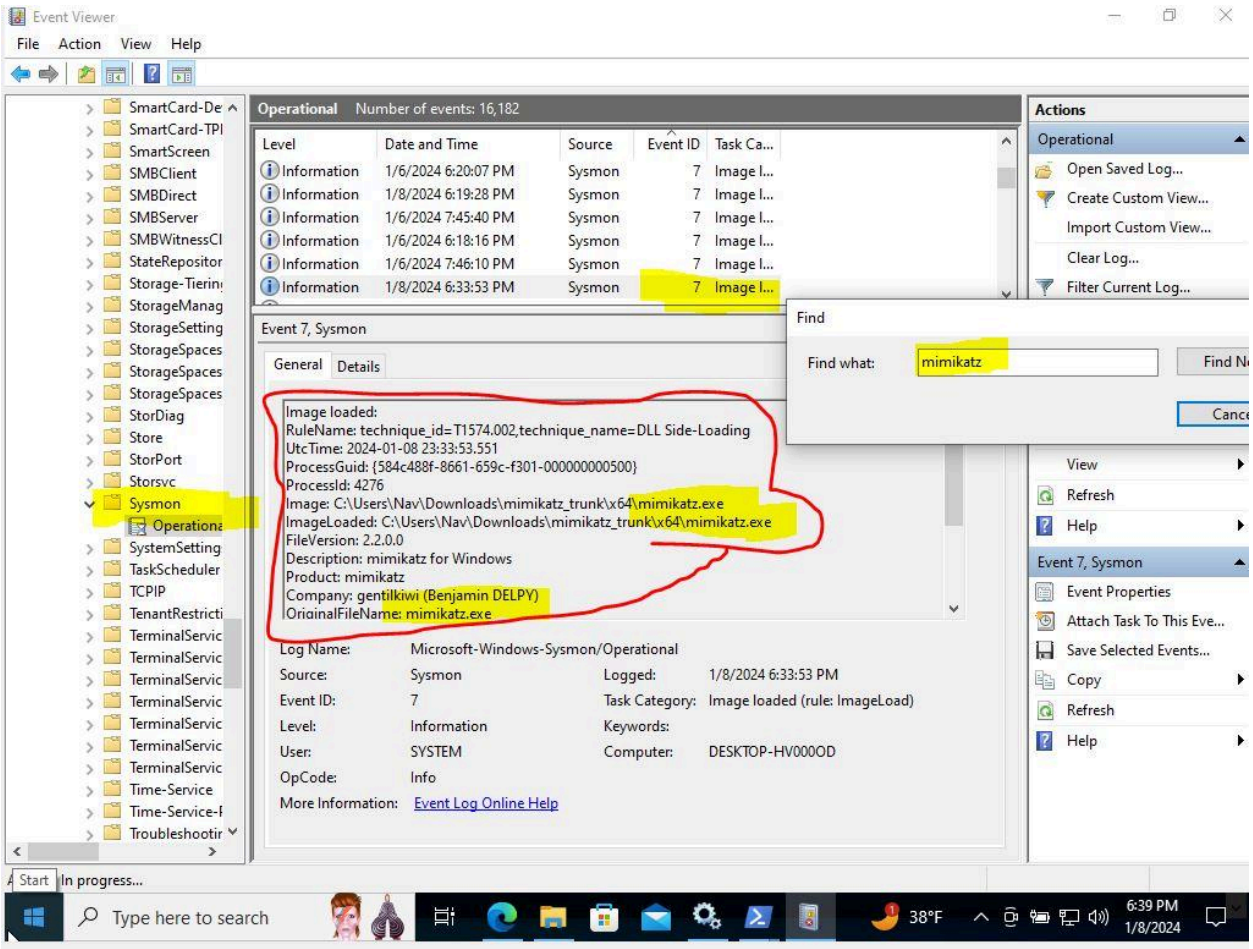
Mimikatz detection:

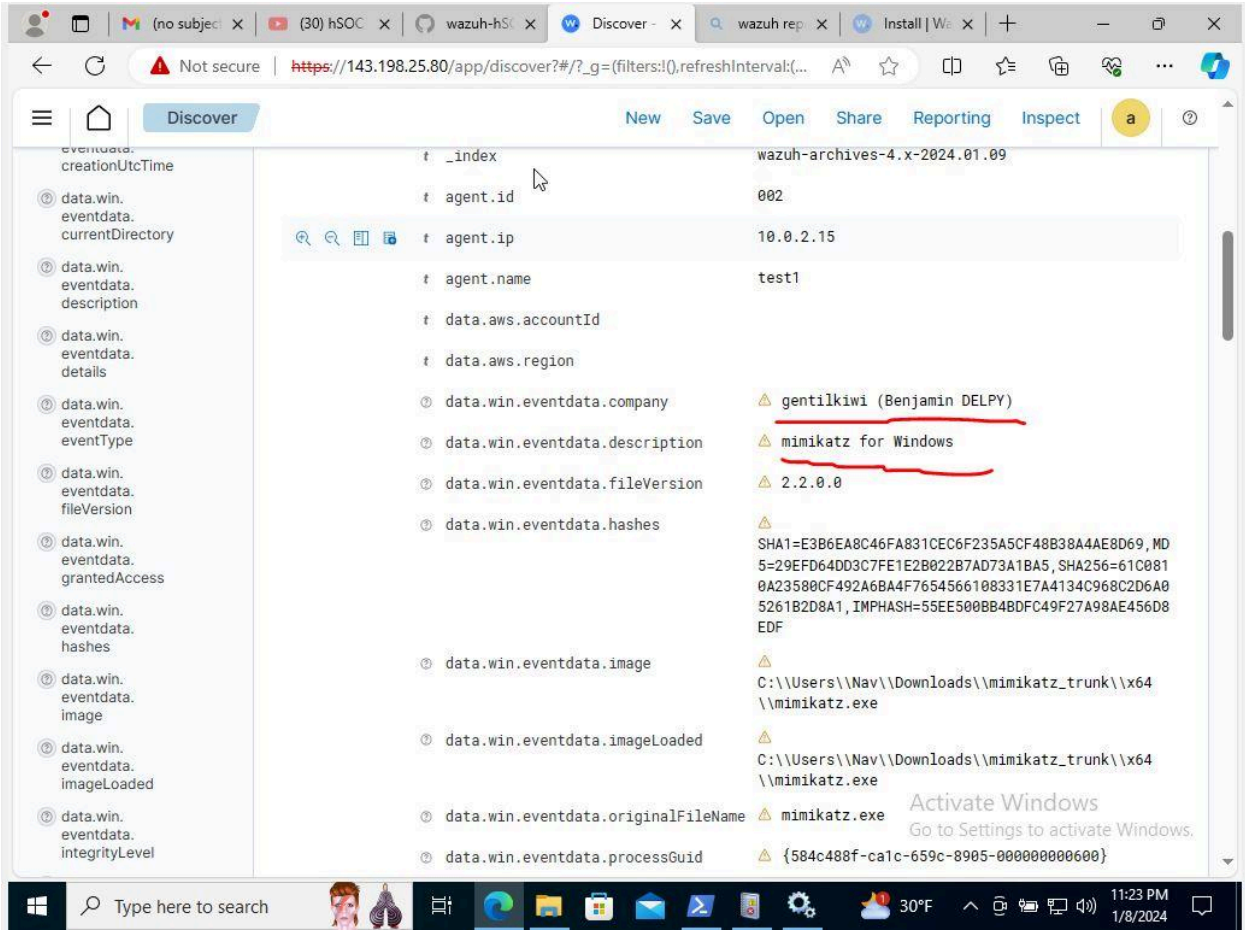
Mimikatz github link–https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20220919

A. Unzip mimikatz zip folder and using admin privileges; run Mimikatz on the agent - .\mimikatz.exe
B. Return to wazuh dashboard and search for security events mimikatz.
C. If mimikatz is not detected then head over to wazuh manager and nano into /var/ossec/etc/ossec.conf and change ossec.conf setting of logall and logall_json to yes and save the file. Additionally this can be done through the dashboard using the rule editor.
D. In the directory /var/ossec/logs/archives: nano into /etc/filebeat/filebeat.yml—-and under filebeat.modules change archives enabled to true.
   ** Make sure to restart after each config; as this is important to apply necessary changes. Systemctl restart **
E. In the dashboard, under stack management click create index pattern and name it wazuh-archives-* and click next and select timestamp, and finally create an index pattern.

Screenshots below:







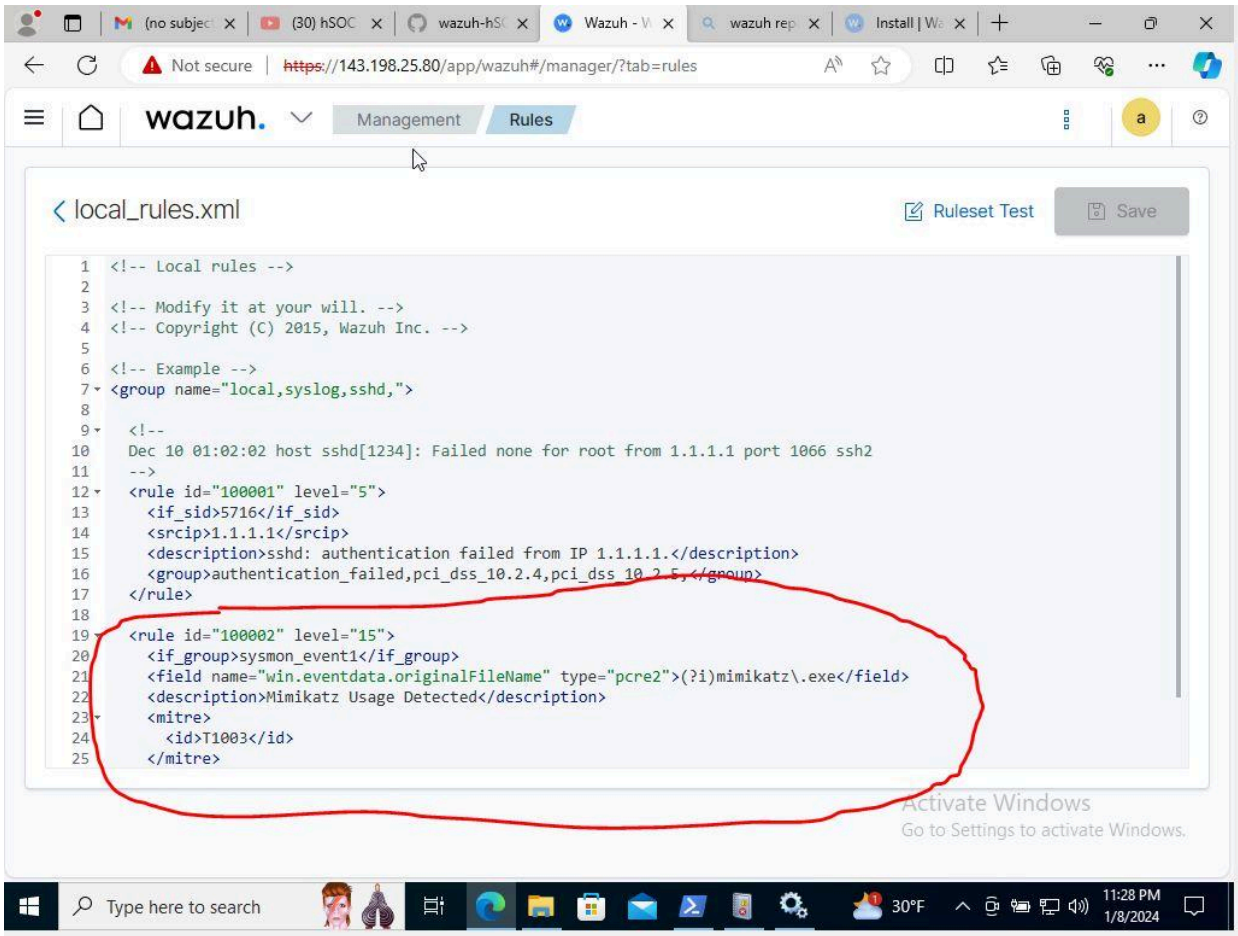
Rule Creation for detecting sysmon event ID 1:

A. Head over to wazuh management on the dashboard and click rules and then custom rules.
B. Edit local_rules.xml and type in exactly the rule that is below in the screenshot.

```
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <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>
```

C. There are more rules if you just google search or github search or you are able to configure your own rules. So with this rule creation, even if the attacker changes the file name, we will still know based on event ID and sysmon logs.

D. Restart and run mimikatz again and test the rule.



SOAR(Security orchestration, automation and response)and Shuffle automation setup:
Objective: Shuffle website–https://shuffler.io/

- Connect SOAR(Shuffle)
- Send alert to thehive
- Send alert via email to SOC analyst

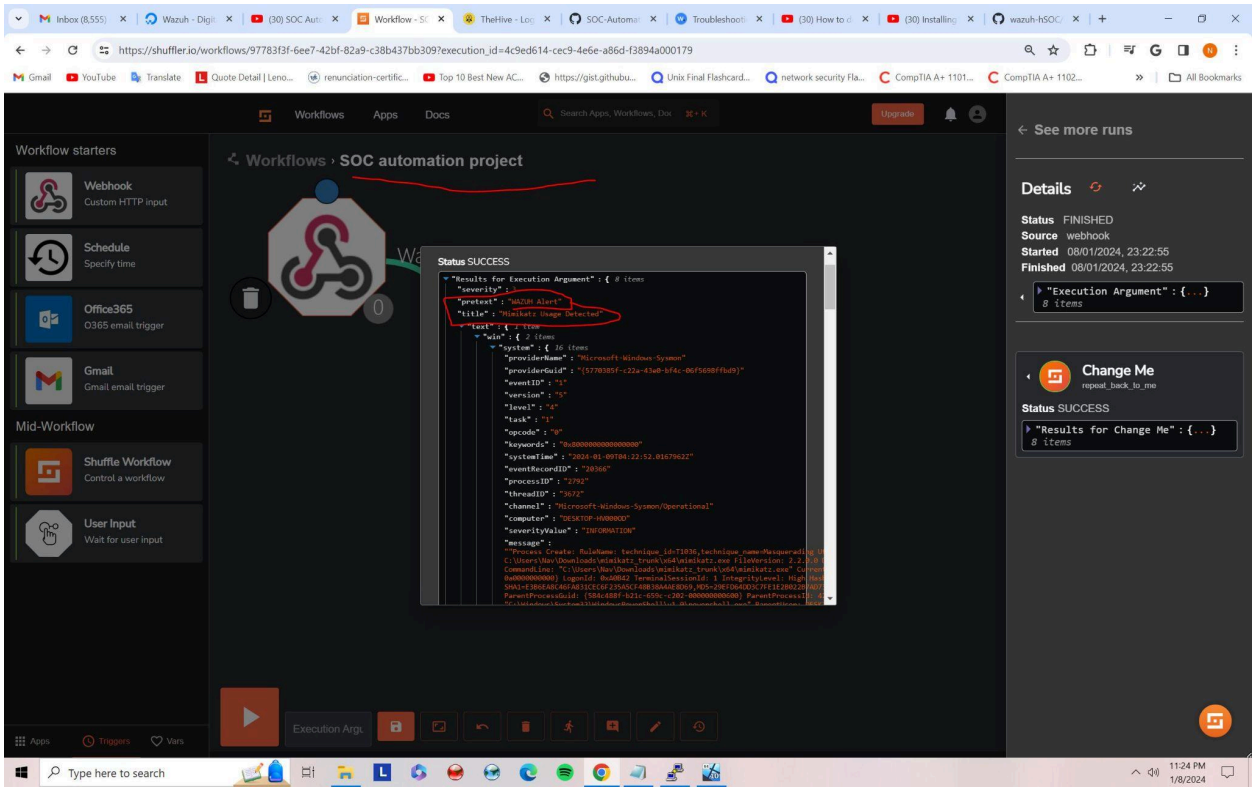
** I have summarized my instructions for this portion of the lab because there are many little bits and pieces that need to connect together and activate all the capabilities. It is better to watch mydfir's videos for a more perfect guide-https://www.youtube.com/watch?v=GNXK00QapjQ**

A. Create a new workflow and add all apps that are show in my workflow pic below
   a. Wazuh alerts(requires api or authentication)
   b. Get API-uses Wazuh api(requires api or authentication)
   c. Wazuh- active response(requires api or authentication)
   d. User input

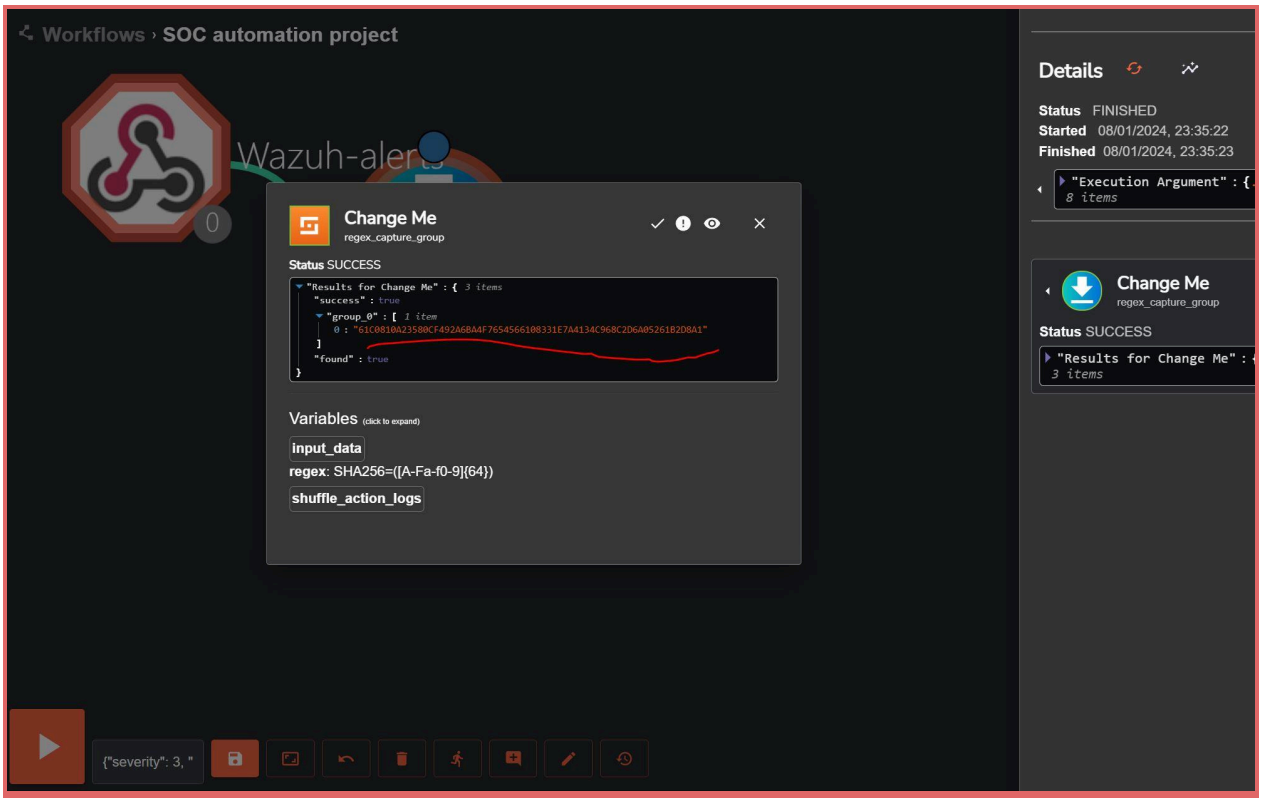
e. Sha-256 Regex
f. Email
g. TheHive(requires api or authentication)
h. Virustotal-requires authentication or API key

Workflow:

1. Mimikatz alert to shuffle via wazuh alerts
2. Shuffle will extract sha 256 hash
3. Virustotal will be used to check the reputation score
4. Shuffle will send details from wazuh alert and virustotal to TheHive to open a new case and insert all details
5. Shuffle will send email to SOC analyst to alert the analyst and also ask for response to block based on event ID.

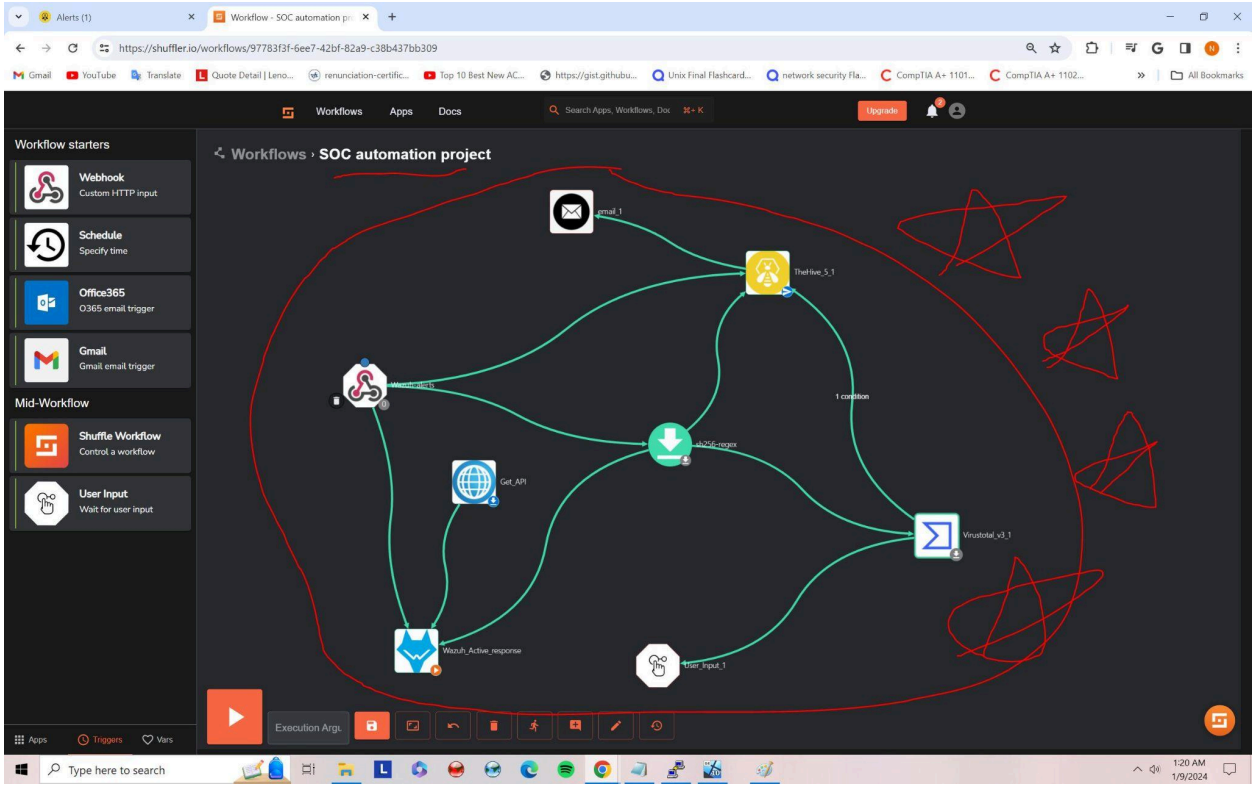


This screenshot shows alert on wazuh alert on shuffle ↑↑



This screenshot shows Extracted sha-256 hash which later can be add to virustotal for reputation score ↑↑↑↑

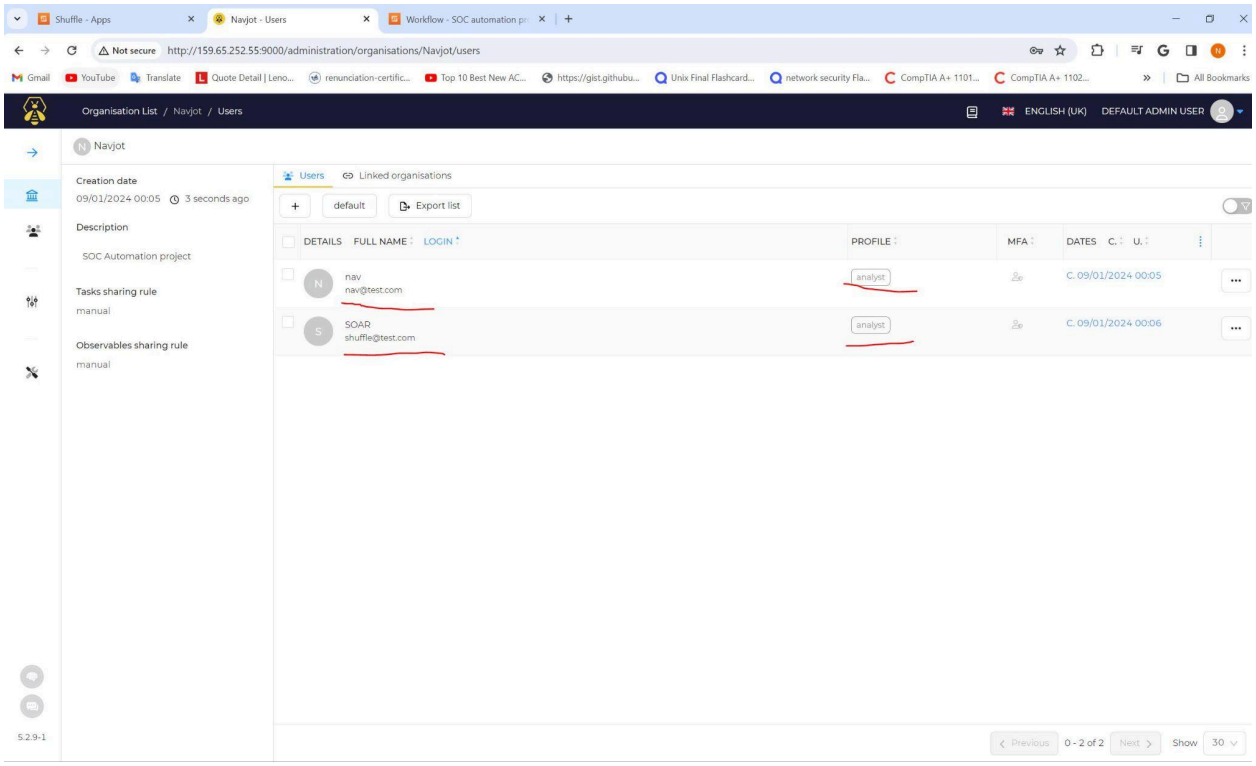
END GOAL OF SHUFFLE:

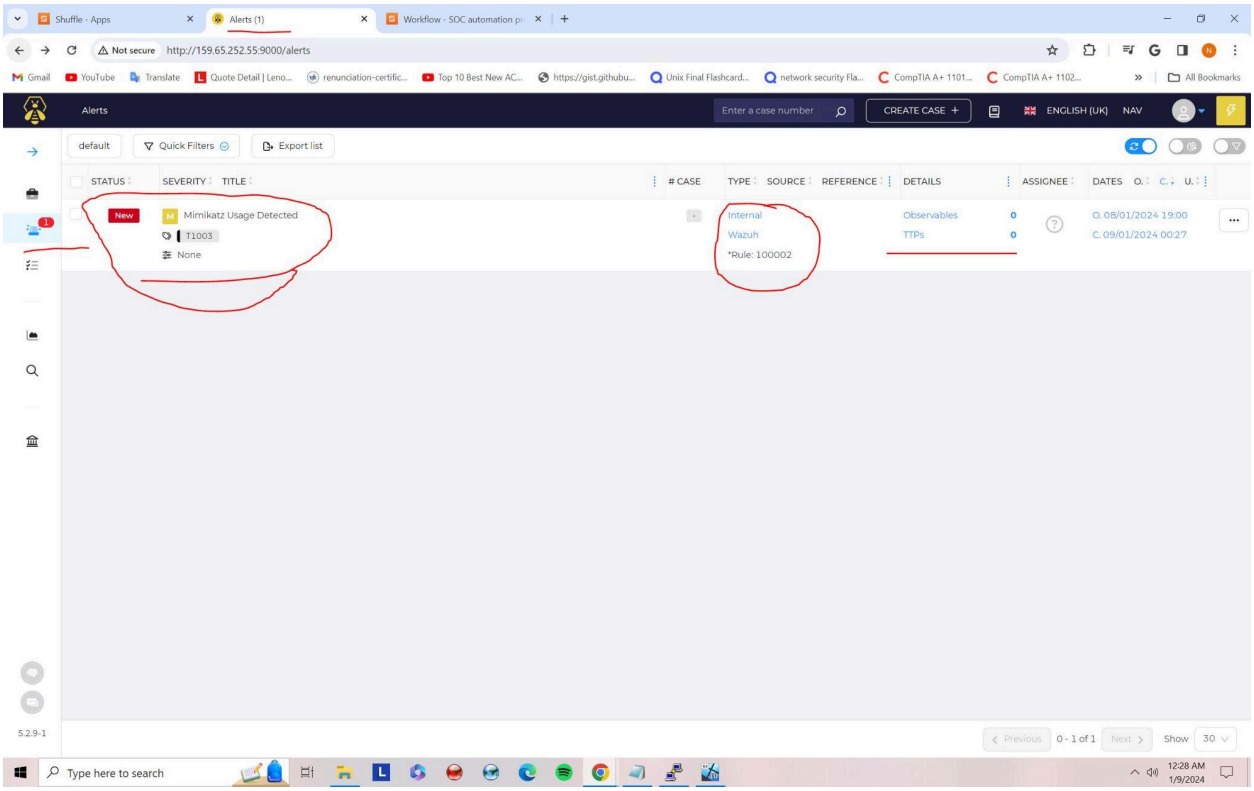


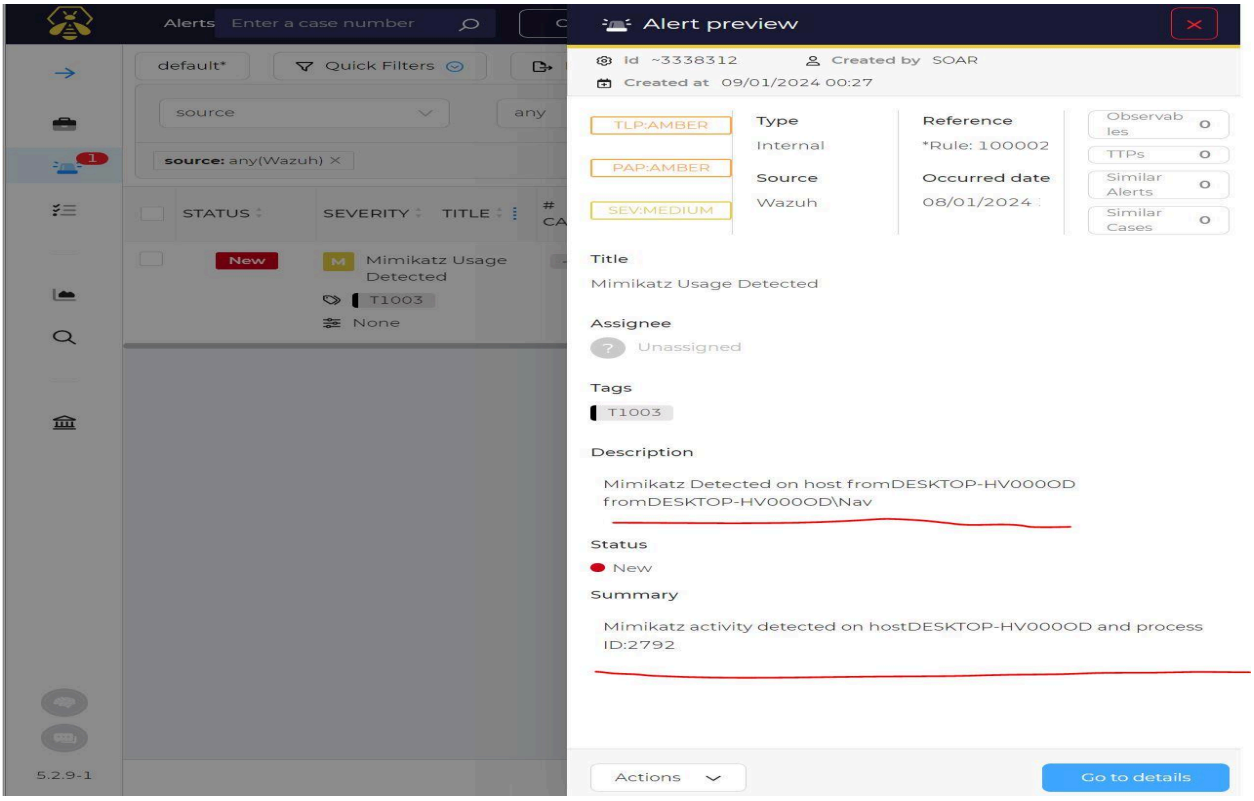
TheHive:

Log into thehive using: admin@thehive.local and password-secret

A. Create and name organizations, select normal type at the top and add login information like for me I added nav@test.com and select analyst profile
B. Add another: Create and name SOAR organizations, select service type at the top and add login information like for me I added shuffle@test.com and select analyst profile—Make sure that this account is following the principle of least privilege such as read-only.
C. Click on the soar account and add a password, make to save this or you can also create an API key and add that on thehive in shuffle.

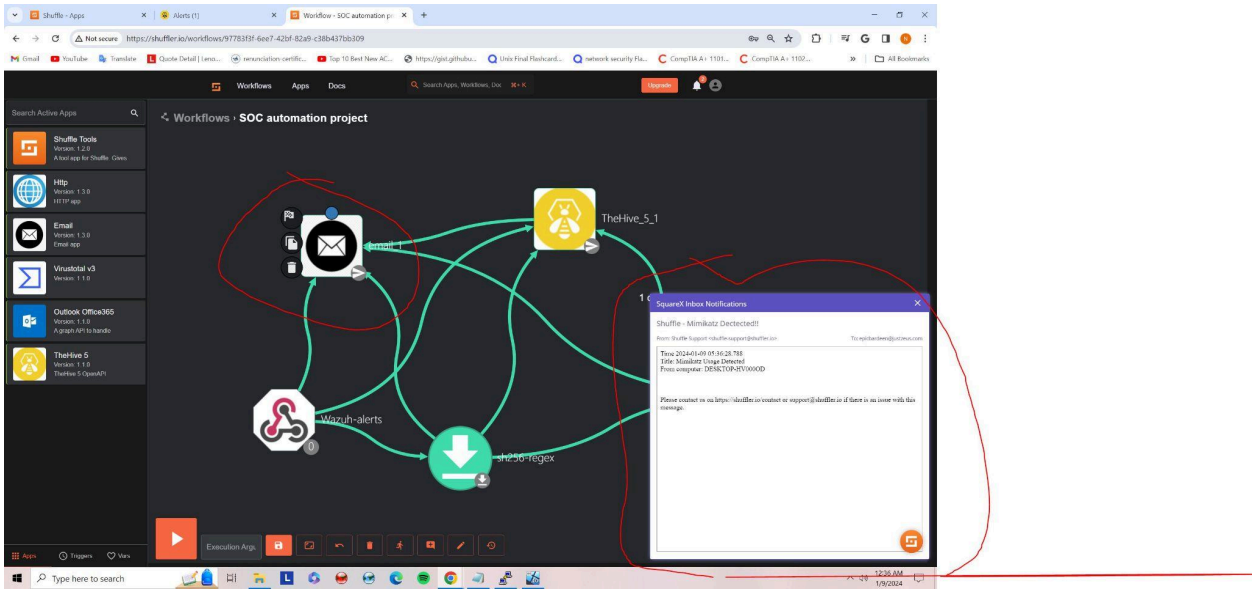

Shuffle - Apps
Navjot - Users
Workflow - SOC automation pr
Not secure
http://159.65.252.55:9000/administration/organisations/Navjot/users
Organisation List / Navjot / Users
ENGLISH (UK)
DEFAULT ADMIN USER
Navjot
Creation date
09/01/2024 00:05
3 seconds ago
Description
SOC Automation project
Tasks sharing rule
manual
Observables sharing rule
manual
Users
Linked organisations
default
Export list
DETAILS
FULL NAME
LOGIN
PROFILE
MFA
DATES
nav
nav@test.com
analyst
C. 09/01/2024 00:05
SOAR
shuffle@test.com
analyst
C. 09/01/2024 00:06
Previous
0 - 2 of 2
Next
Show
30
5.2.9-1


Shuffle - Apps
Alerts (1)
Workflow - SOC automation pr
Not secure
http://159.65.252.55:9000/alerts
Alerts
Enter a case number
CREATE CASE
ENGLISH (UK)
NAV
default
Quick Filters
Export list
STATUS
SEVERITY
TITLE
CASE
TYPE
SOURCE
REFERENCE
DETAILS
ASSIGNEE
DATES
New
Mimikatz Usage Detected
T1003
None
Internal
Wazuh
*Rule: 100002
Observables 0
TTPs 0
O. 08/01/2024 19:00
C. 09/01/2024 00:27
Previous
0 - 1 of 1
Next
Show
30
5.2.9-1
Type here to search
12:28 AM
1/9/2024



Email: For this setup I used Square X which is a free browser extension that can generate email and has an inbox.

A. All you need to do is add the Square X email and add subject and body.



B. User Input will send a separate email for response that will go all the way back to window 10 client through shuffle.

Shuffle - User input required

from: Shuffle Support <shuffle-support@shuffler.io>
to: stoicellis@imcourageous.com
on: 12/10/2023, 9:27:48 PM

Action required!
Would you like block this source IP: 103.180.149.26

If this is TRUE click this: https://shuffler.io/workflows/e9539563-4ee3-4317-9afc-d266c9d0f025/run?authorization=713b979b-1454-445d-b39a-bf065192e622&start=4d29821e-aac3-4ff2-becf-dca1198052ea&reference_execution=bf9ce30e-ce88-4fcd-b2b0-d0c457dddaa5&answer=true

IF THIS IS FALSE, click this: https://shuffler.io/workflows/e9539563-4ee3-4317-9afc-d266c9d0f025/run?authorization=713b979b-1454-445d-b39a-bf065192e622&start=4d29821e-aac3-4ff2-becf-dca1198052ea&reference_execution=bf9ce30e-ce88-4fcd-b2b0-d0c457dddaa5&answer=false

Please contact us at shuffler.io/contact or support@shuffler.io if there is an issue with this message.

Throughout this project, I learned a ton about SOC workflows, tool integrations, and the importance of systematic configurations. It was a hands-on journey into the world of security incident handling, and I'm pretty proud of the setup. Many humble thanks to Mydfir(https://www.youtube.com/@MyDFIR) for setting a good example of the project. –Thank you so much

If you have any questions or need more details on a specific aspect, feel free to ask!😄