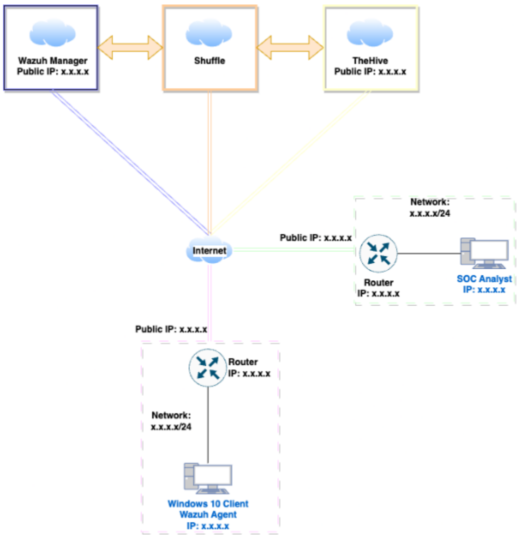
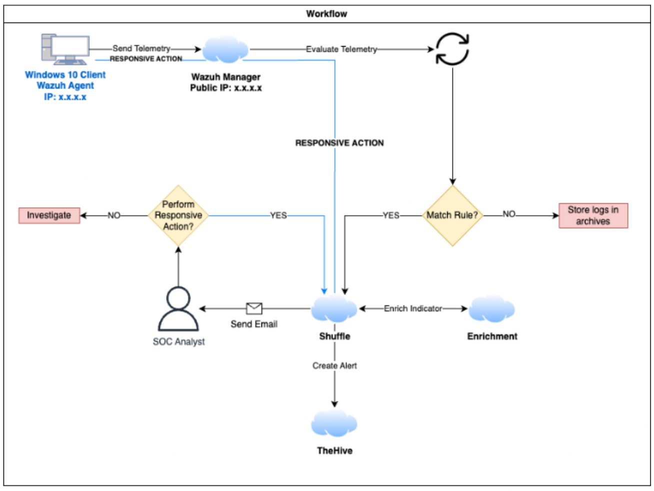
SOC Automation Project

The basic planning of the SOC automation can be seen below:

DFD:





It explains the process being conducted with the help of shuffle and making it automatic such that it automatically collects the alarms by wazuh and sends them to hive to make a ticket, it also sends it to the Email address specified in shuffle to inform the security engineer regarding the ticket and the alert such that continuous monitoring of wazuh dashboard is not required.

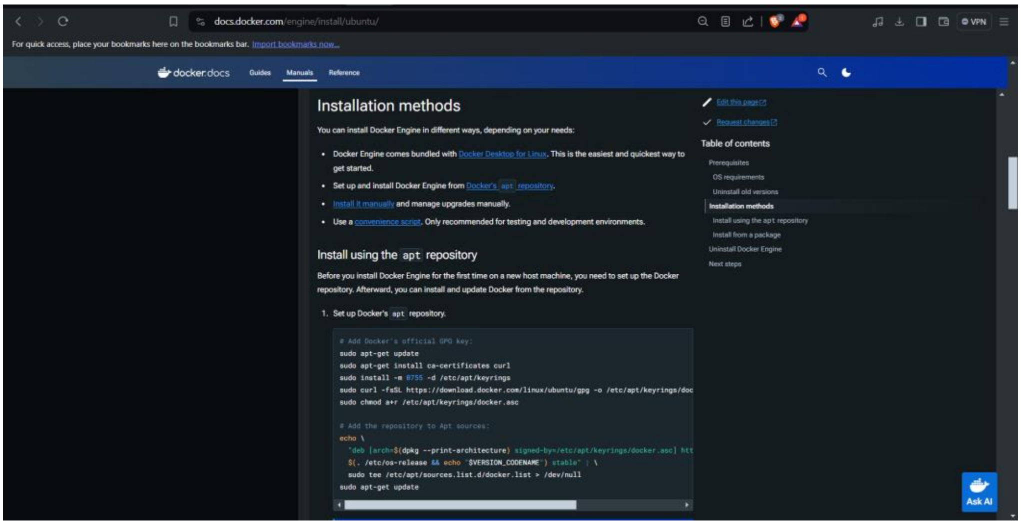
Following the procedure mentioned below shows the steps involved in installing and configuring the software required in this SOC Automation.

Installing docker

The first pre-requisite is to have docker engine and docker composed installed on the system where shuffle is going to be installed. The following screenshot shows the installation and the steps involved in the process.

Step 1: Go to the website https://docs.docker.com/engine/install/ubuntu

Note: This is the installation process for ubuntu host systems only.



Installation methods

You can install Docker Engine in different ways, depending on your needs:

- Docker Engine comes bundled with Docker Desktop for Linux. This is the easiest and quickest way to get started.
- Set up and install Docker Engine from Docker's `apt` repository.
- Install it manually and manage upgrades manually.
- Use a convenience script. Only recommended for testing and development environments.

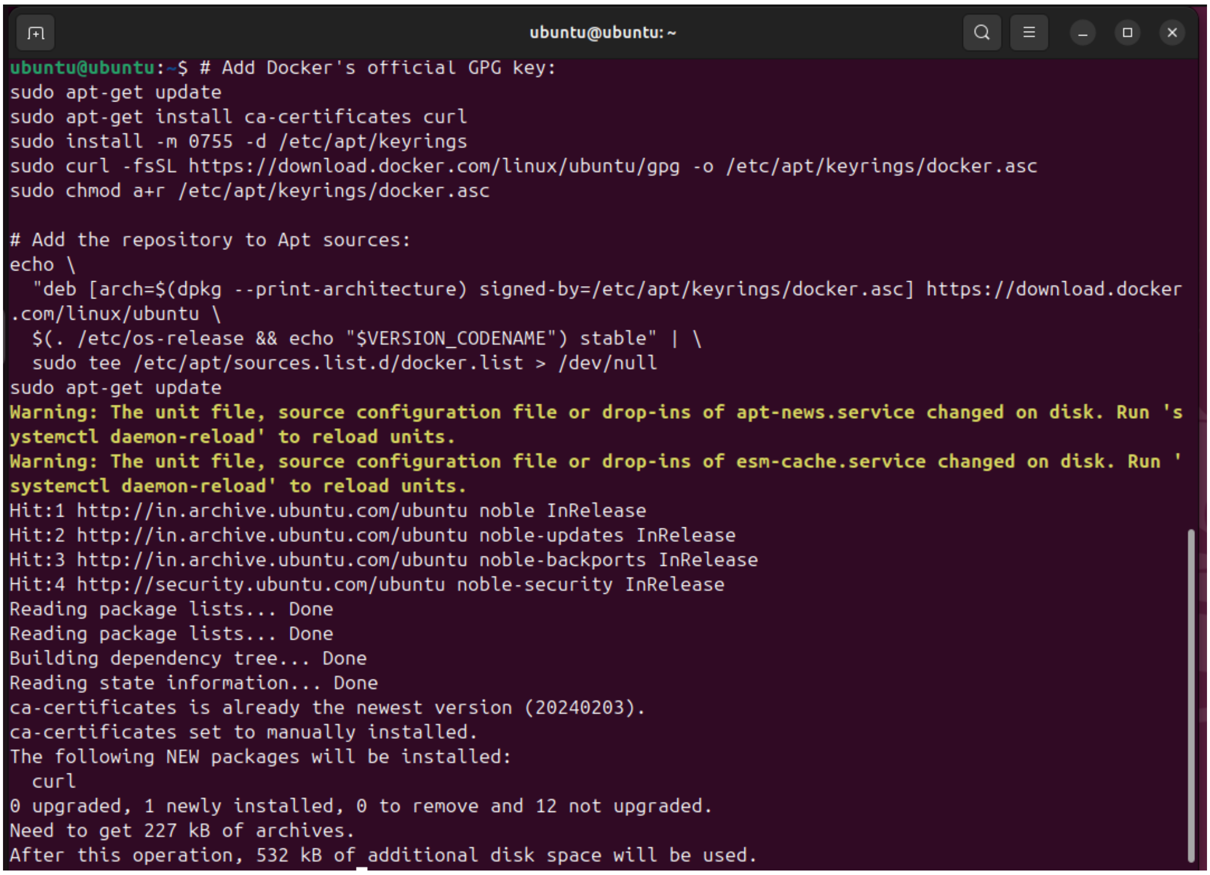
Install using the `apt` repository

Before you install Docker Engine for the first time on a new host machine, you need to set up the Docker repository. Afterward, you can install and update Docker from the repository.

1. Set up Docker's `apt` repository.

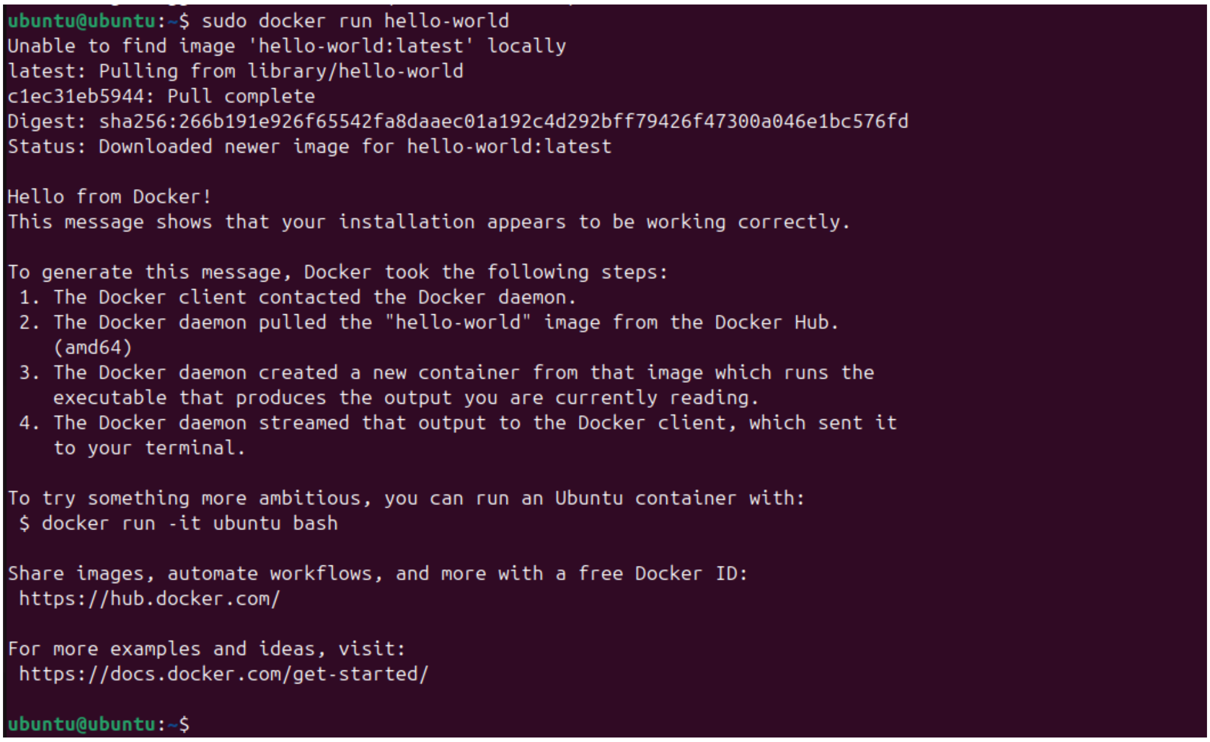
```
# Add Docker's official GPG key:
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/doc
sudo chmod a+r /etc/apt/keyrings/docker.asc

# Add the repository to Apt sources:
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] htt
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```

Step 2: Follow the commands shown in documentation by docker installation guide.



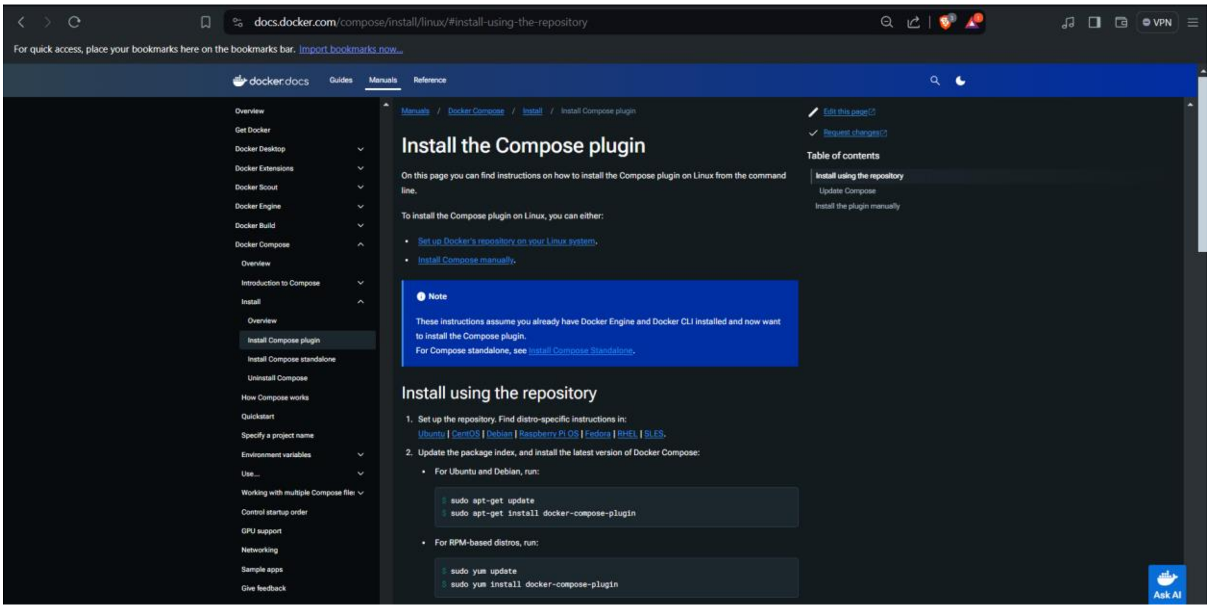
```
ubuntu@ubuntu:~$ # Add Docker's official GPG key:
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc

# Add the repository to Apt sources:
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker
.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
Warning: The unit file, source configuration file or drop-ins of apt-news.service changed on disk. Run 's
ystemctl daemon-reload' to reload units.
Warning: The unit file, source configuration file or drop-ins of esm-cache.service changed on disk. Run '
systemctl daemon-reload' to reload units.
Hit:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20240203).
ca-certificates set to manually installed.
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 12 not upgraded.
Need to get 227 kB of archives.
After this operation, 532 kB of additional disk space will be used.
```

Step 3: Check the installation and working of docker by running a sample image hello-world.



```
ubuntu@ubuntu:~$ sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
c1ec31eb5944: Pull complete
Digest: sha256:266b191e926f65542fa8daaec01a192c4d292bff79426f47300a046e1bc576fd
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/

ubuntu@ubuntu:~$
```

Step 4: Using the documentation on https://docs.docker.com/compose/install/linux/#install-using-the-repository to install the Docker compose which is a requirement to run shuffle.



Install the Compose plugin

On this page you can find instructions on how to install the Compose plugin on Linux from the command line.

To install the Compose plugin on Linux, you can either:

- Set up Docker's repository on your Linux system.
- Install Compose manually.

Note

These instructions assume you already have Docker Engine and Docker CLI installed and now want to install the Compose plugin.
For Compose standalone, see Install Compose Standalone.

Install using the repository

1. Set up the repository. Find distro-specific instructions in:
   Ubuntu | CentOS | Debian | Raspberry Pi OS | Fedora | RHEL | SLES.
2. Update the package index, and install the latest version of Docker Compose:
   - For Ubuntu and Debian, run:

```
$ sudo apt-get update
$ sudo apt-get install docker-compose-plugin
```

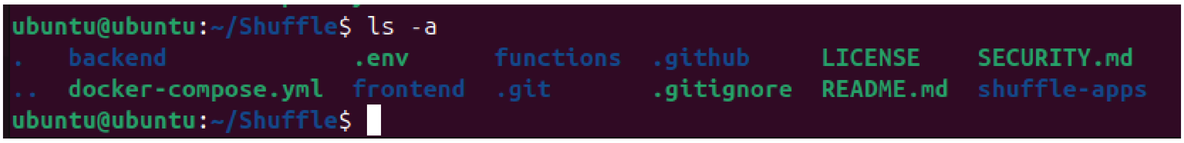
   - For RPM-based distros, run:

```
$ sudo yum update
$ sudo yum install docker-compose-plugin
```

Installing Shuffle

In this project, Shuffle is used as the bridge between the tools and helps transfer collected logs from the SIEM and create tickets in platforms such as TheHive and help in automating the process whenever an irregularity is found.

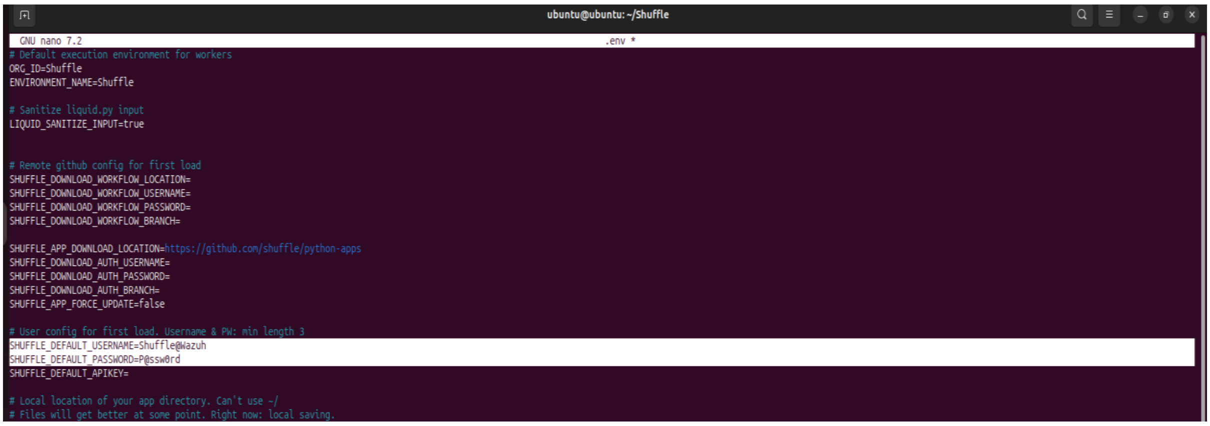
Step 1: Go to the website https://github.com/shuffle/shuffle/blob/main/.github/install-guide.md and follow the steps mentioned to install shuffle, refer the images attached below for easier understanding of the project.



```
ubuntu@ubuntu:~/Shuffle$ ls -a
.   backend             .env      functions  .github     LICENSE    SECURITY.md
..  docker-compose.yml  frontend  .git       .gitignore  README.md  shuffle-apps
ubuntu@ubuntu:~/Shuffle$ 
```

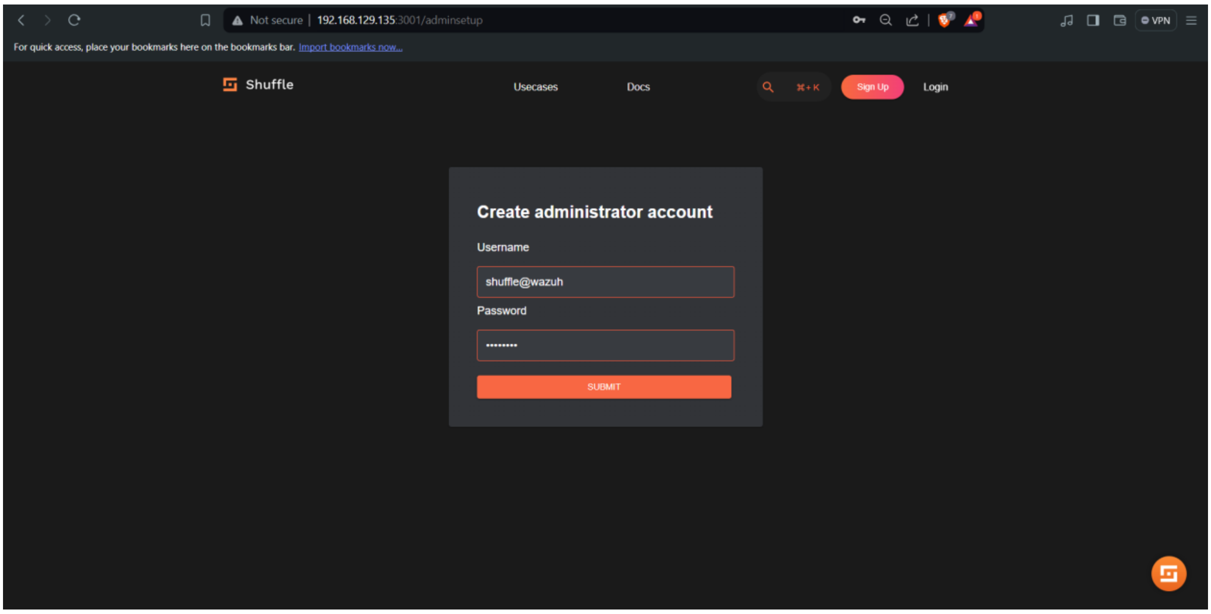
Once the Docker is installed all there is left is to clone the git repository of shuffle and run the shuffle in docker as shown below:

Step 2: Next Configure the .env file from the repository cloned where u can change the shuffle admin password.



```
  GNU nano 7.2                                                    .env *
# Default execution environment for workers
ORG_ID=Shuffle
ENVIRONMENT_NAME=Shuffle

# Sanitize liquid.py input
LIQUID_SANITIZE_INPUT=true


# Remote github config for first load
SHUFFLE_DOWNLOAD_WORKFLOW_LOCATION=
SHUFFLE_DOWNLOAD_WORKFLOW_USERNAME=
SHUFFLE_DOWNLOAD_WORKFLOW_PASSWORD=
SHUFFLE_DOWNLOAD_WORKFLOW_BRANCH=

SHUFFLE_APP_DOWNLOAD_LOCATION=https://github.com/shuffle/python-apps
SHUFFLE_DOWNLOAD_AUTH_USERNAME=
SHUFFLE_DOWNLOAD_AUTH_PASSWORD=
SHUFFLE_DOWNLOAD_AUTH_BRANCH=
SHUFFLE_APP_FORCE_UPDATE=false

# User config for first load. Username & PW: min length 3
SHUFFLE_DEFAULT_USERNAME=Shuffle@Wazuh
SHUFFLE_DEFAULT_PASSWORD=P@ssw0rd
SHUFFLE_DEFAULT_APIKEY=

# Local location of your app directory. Can't use ~/
# Files will get better at some point. Right now: local saving.
```

Step 4: Lookup localhost address and check the working of Shuflle.


Not secure | 192.168.129.135:3001/adminsetup
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Shuffle
Usecases
Docs
⌘+K
Sign Up
Login
VPN

Create administrator account

Username: shuffle@wazuh

Password: ••••••••

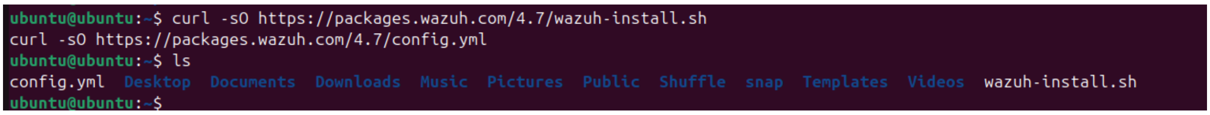
SUBMIT

Inatalling Wazuh:

Wazuh is an open-source security platform that provides unified security monitoring, detection, and response across various environments, including cloud, on-premises, and hybrid. It integrates host-based intrusion detection, log analysis, vulnerability detection, and configuration assessment into a single platform, making it a versatile solution for comprehensive security management and compliance.

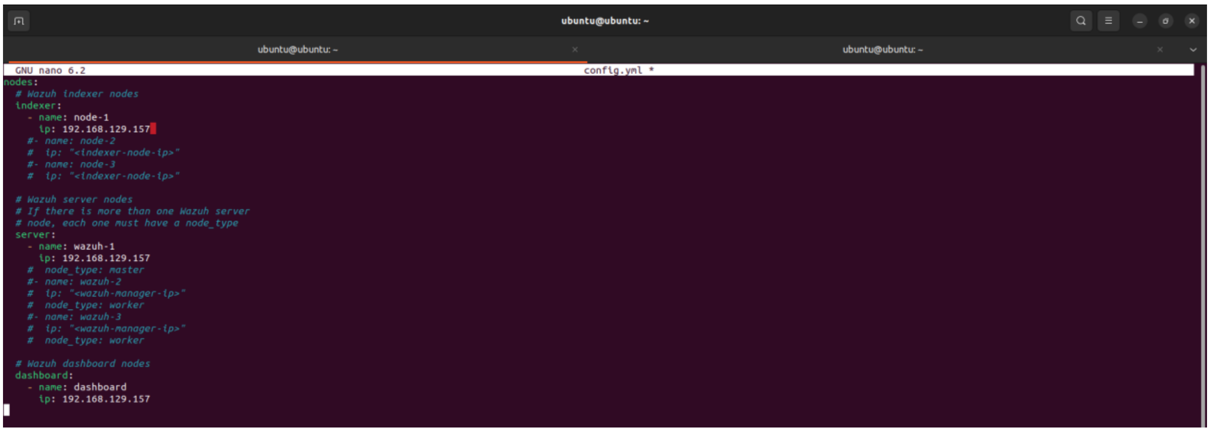
Follow these steps for installation of wazuh:

Step 1: download the configuration file and setup file of wazuh using the commands: “curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh curl -sO https://packages.wazuh.com/4.7/config.yml”



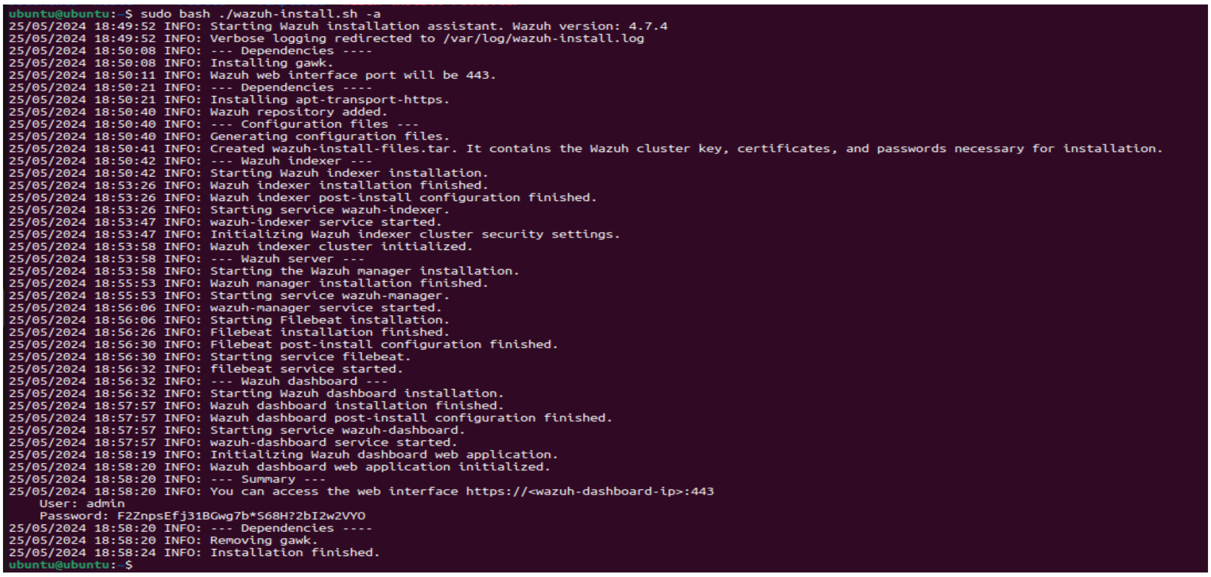
```
ubuntu@ubuntu:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.7/config.yml
ubuntu@ubuntu:~$ ls
config.yml  Desktop  Documents  Downloads  Music  Pictures  Public  Shuffle  snap  Templates  Videos  wazuh-install.sh
ubuntu@ubuntu:~$
```

Step 2: Next open the configuration file and configure the IP address to the host systems IP address and then save the configuration file.



```
  GNU nano 6.2                                config.yml *
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: 192.168.129.157
    #- name: node-2
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: 192.168.129.157
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: 192.168.129.157
```

Step 2: Now after changing the IP in configuration file, run the installation script downloaded in the first step, using the command “sudo bash wazuh-install.sh –a”, save the password shown at the last for future logins.



```
ubuntu@ubuntu:~$ sudo bash ./wazuh-install.sh -a
25/05/2024 18:49:52 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.4
25/05/2024 18:49:52 INFO: Verbose logging redirected to /var/log/wazuh-install.log
25/05/2024 18:50:08 INFO: --- Dependencies ----
25/05/2024 18:50:08 INFO: Installing gawk.
25/05/2024 18:50:11 INFO: Wazuh web interface port will be 443.
25/05/2024 18:50:21 INFO: --- Dependencies ----
25/05/2024 18:50:21 INFO: Installing apt-transport-https.
25/05/2024 18:50:40 INFO: Wazuh repository added.
25/05/2024 18:50:40 INFO: --- Configuration files ---
25/05/2024 18:50:40 INFO: Generating configuration files.
25/05/2024 18:50:41 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
25/05/2024 18:50:42 INFO: --- Wazuh indexer ---
25/05/2024 18:50:42 INFO: Starting Wazuh indexer installation.
25/05/2024 18:53:26 INFO: Wazuh indexer installation finished.
25/05/2024 18:53:26 INFO: Wazuh indexer post-install configuration finished.
25/05/2024 18:53:26 INFO: Starting service wazuh-indexer.
25/05/2024 18:53:47 INFO: wazuh-indexer service started.
25/05/2024 18:53:47 INFO: Initializing Wazuh indexer cluster security settings.
25/05/2024 18:53:58 INFO: Wazuh indexer cluster initialized.
25/05/2024 18:53:58 INFO: --- Wazuh server ---
25/05/2024 18:53:58 INFO: Starting the Wazuh manager installation.
25/05/2024 18:55:53 INFO: Wazuh manager installation finished.
25/05/2024 18:55:53 INFO: Starting service wazuh-manager.
25/05/2024 18:56:06 INFO: wazuh-manager service started.
25/05/2024 18:56:06 INFO: Starting Filebeat installation.
25/05/2024 18:56:26 INFO: Filebeat installation finished.
25/05/2024 18:56:30 INFO: Filebeat post-install configuration finished.
25/05/2024 18:56:30 INFO: Starting service filebeat.
25/05/2024 18:56:32 INFO: filebeat service started.
25/05/2024 18:56:32 INFO: --- Wazuh dashboard ---
25/05/2024 18:56:32 INFO: Starting Wazuh dashboard installation.
25/05/2024 18:57:57 INFO: Wazuh dashboard installation finished.
25/05/2024 18:57:57 INFO: Wazuh dashboard post-install configuration finished.
25/05/2024 18:57:57 INFO: Starting service wazuh-dashboard.
25/05/2024 18:57:57 INFO: wazuh-dashboard service started.
25/05/2024 18:58:19 INFO: Initializing Wazuh dashboard web application.
25/05/2024 18:58:20 INFO: Wazuh dashboard web application initialized.
25/05/2024 18:58:20 INFO: --- Summary ---
25/05/2024 18:58:20 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: F2ZnpsEfj31BGwg7b*S68H?2bI2w2VYO
25/05/2024 18:58:20 INFO: --- Dependencies ----
25/05/2024 18:58:20 INFO: Removing gawk.
25/05/2024 18:58:24 INFO: Installation finished.
ubuntu@ubuntu:~$
```

Installing The hive

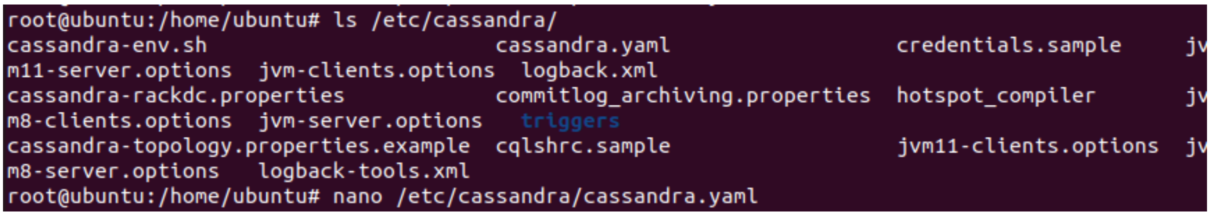
The Hive is an open-source Security Incident Response Platform (SIRP) designed for managing and resolving security incidents efficiently. It supports collaboration among security teams by enabling the tracking, analysis, and response to security threats. With its powerful case management and automation capabilities, The Hive streamlines incident response workflows and enhances overall security operations.

Follow the following steps to configure the dependencies for Hive.

Installing dependency Cassandra for hive

Cassandra as a dependency for Hive enables seamless integration, allowing Hive to efficiently store and query large datasets.

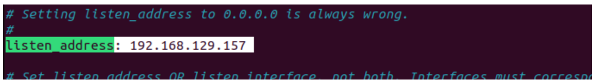
Step 1: Using the script attached in the repository, install Cassandra. Then go the etc directory where Cassandra is installed to configure it as shown below:



```
root@ubuntu:/home/ubuntu# ls /etc/cassandra/
cassandra-env.sh                      cassandra.yaml                  credentials.sample      jv
m11-server.options  jvm-clients.options  logback.xml
cassandra-rackdc.properties           commitlog_archiving.properties  hotspot_compiler        jv
m8-clients.options  jvm-server.options   triggers
cassandra-topology.properties.example cqlshrc.sample                  jvm11-clients.options   jv
m8-server.options   logback-tools.xml
root@ubuntu:/home/ubuntu# nano /etc/cassandra/cassandra.yaml
```

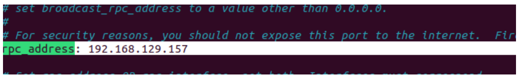
Step 2: Modify the listen, rpc and seed address to the address of the host machine as shown below.

Changing Listen Address:



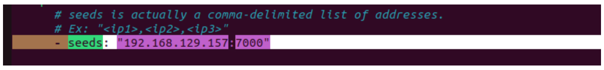
```
# Setting listen_address to 0.0.0.0 is always wrong.
#
listen_address: 192.168.129.157

# Set listen_address OR listen_interface, not both. Interfaces must correspo
```

Changing RPC Address:



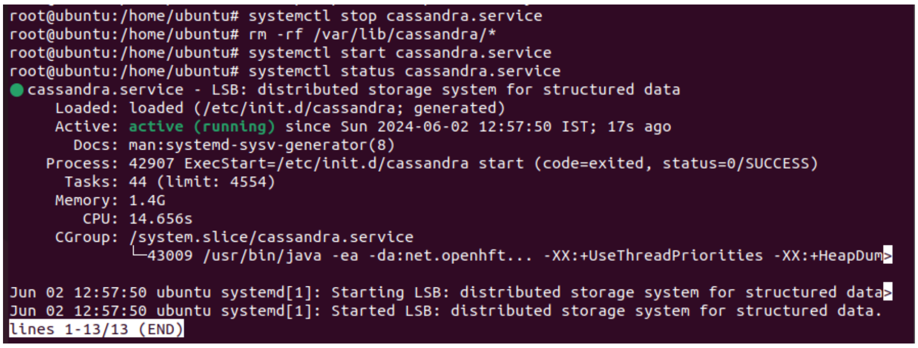
```
# set broadcast_rpc_address to a value other than 0.0.0.0.
#
# For security reasons, you should not expose this port to the internet.  Fir
rpc_address: 192.168.129.157

# Set rpc_address OR rpc_interface, not both. Interfaces must correspond
```

Changing Seed Address:



```
      # seeds is actually a comma-delimited list of addresses.
      # Ex: "<ip1>,<ip2>,<ip3>"
      - seeds:  "192.168.129.157:7000"
```

Step 3: Start the Cassandra service and check if its running properly.



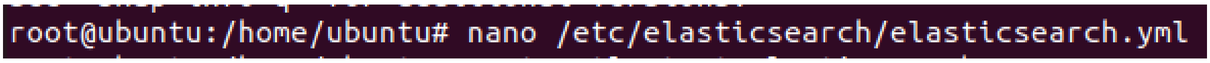
```
root@ubuntu:/home/ubuntu# systemctl stop cassandra.service
root@ubuntu:/home/ubuntu# rm -rf /var/lib/cassandra/*
root@ubuntu:/home/ubuntu# systemctl start cassandra.service
root@ubuntu:/home/ubuntu# systemctl status cassandra.service
● cassandra.service - LSB: distributed storage system for structured data
     Loaded: loaded (/etc/init.d/cassandra; generated)
     Active: active (running) since Sun 2024-06-02 12:57:50 IST; 17s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 42907 ExecStart=/etc/init.d/cassandra start (code=exited, status=0/SUCCESS)
      Tasks: 44 (limit: 4554)
     Memory: 1.4G
        CPU: 14.656s
     CGroup: /system.slice/cassandra.service
             └─43009 /usr/bin/java -ea -da:net.openhft... -XX:+UseThreadPriorities -XX:+HeapDum>

Jun 02 12:57:50 ubuntu systemd[1]: Starting LSB: distributed storage system for structured data>
Jun 02 12:57:50 ubuntu systemd[1]: Started LSB: distributed storage system for structured data.
lines 1-13/13 (END)
```

Configuring elastic search used in hive

Elasticsearch for use in Hive enhances data indexing and search capabilities, allowing for faster and more efficient querying of large datasets, ultimately improving Hive's performance and scalability in handling complex data operations.

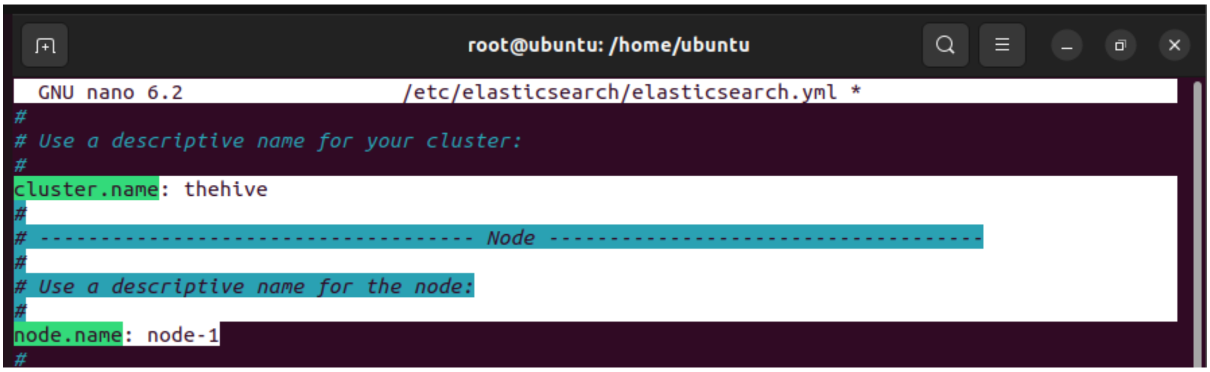
Follow the steps to configure Elastic Search for hive:

Step 1: After installing Elastic Search using the provided bash script, go the following path where the configuration file for Elastic Search is present as shown below:



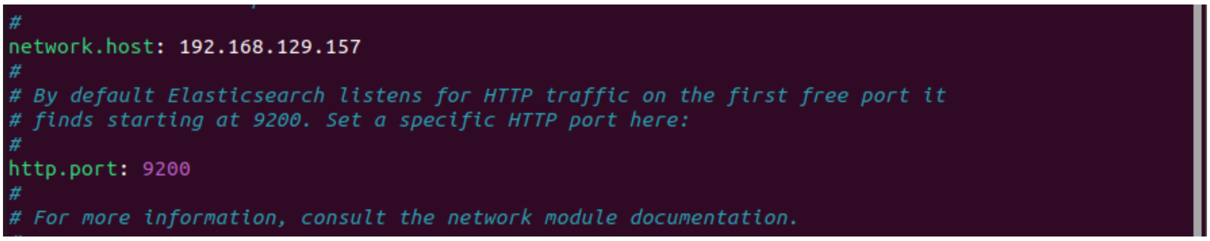
```
root@ubuntu:/home/ubuntu# nano /etc/elasticsearch/elasticsearch.yml
```

Step 2: Now set the cluster name as shown below:



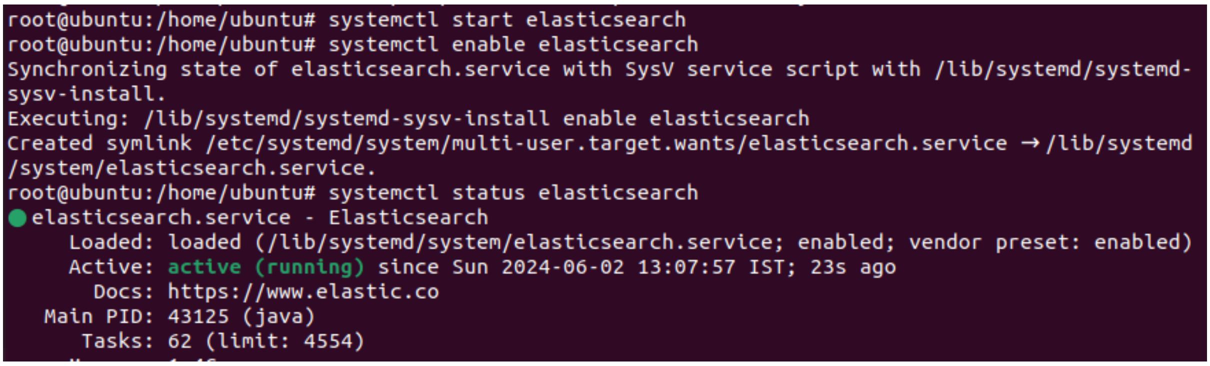
```
  GNU nano 6.2                 /etc/elasticsearch/elasticsearch.yml *
#
# Use a descriptive name for your cluster:
#
cluster.name: thehive
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: node-1
#
```

Step 3: Also set the IP Address of the host/server machine to the “network.host” option.



```
#
network.host: 192.168.129.157
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
```

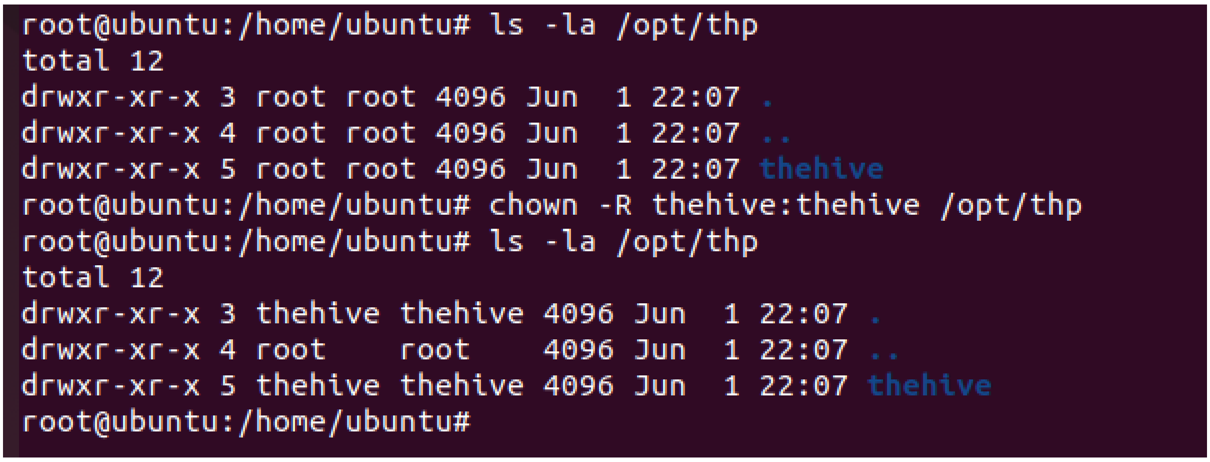
Step 4: Lastly start the elastic search service and check if its running without any issues:



```
root@ubuntu:/home/ubuntu# systemctl start elasticsearch
root@ubuntu:/home/ubuntu# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-
sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd
/system/elasticsearch.service.
root@ubuntu:/home/ubuntu# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-06-02 13:07:57 IST; 23s ago
       Docs: https://www.elastic.co
   Main PID: 43125 (java)
      Tasks: 62 (limit: 4554)
```

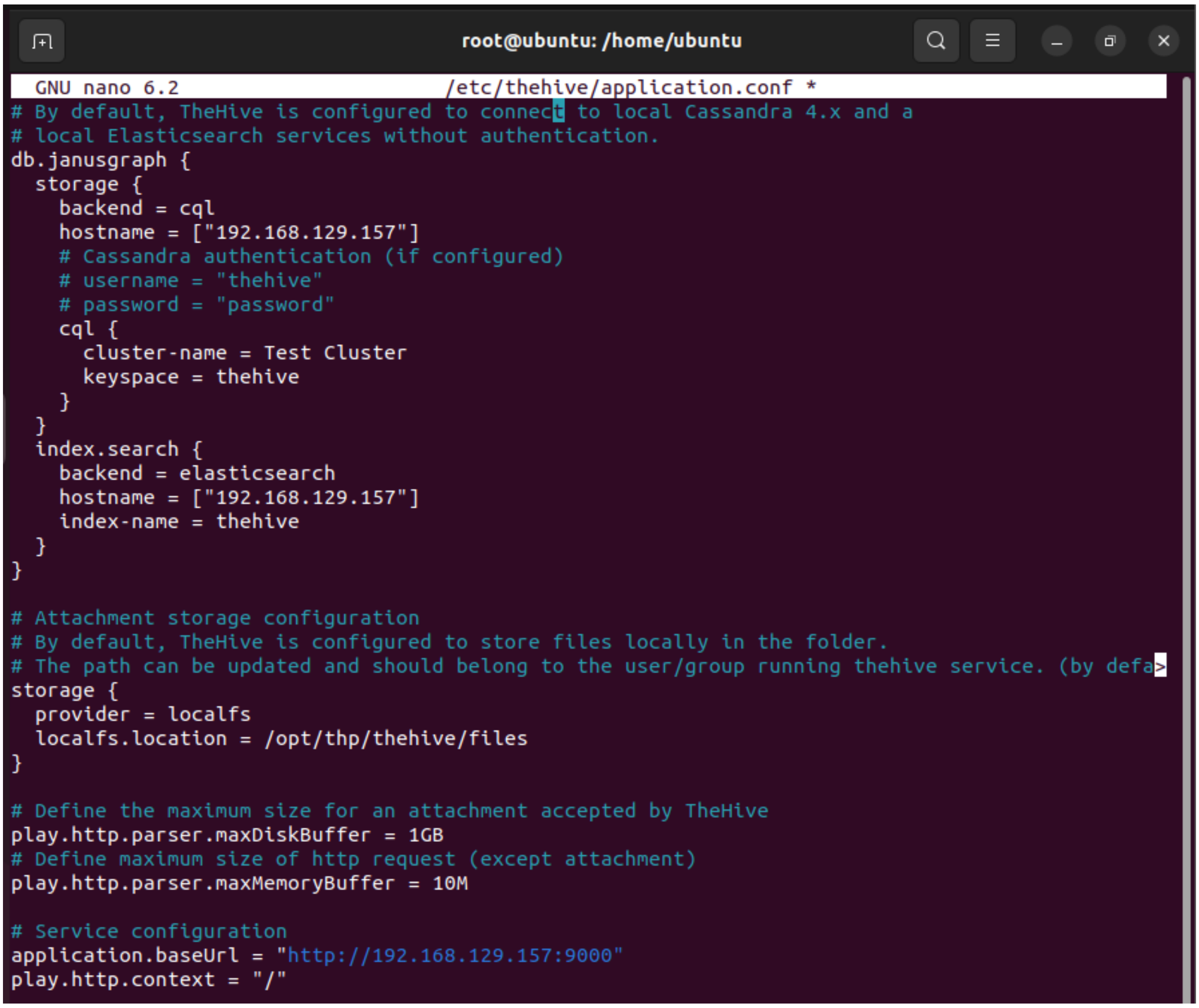
Configuring The hive

Step 1: After installing Hive using the bash script, we need to change the ownership of the `/opt/thp` directory and all of its contents to the user `thehive` and the group `thehive suing the commands`: “chown -R thehive:thehive /opt/thp” u can replace the “thehive” with the cluster name that u added when configuring the Elastic Search file.



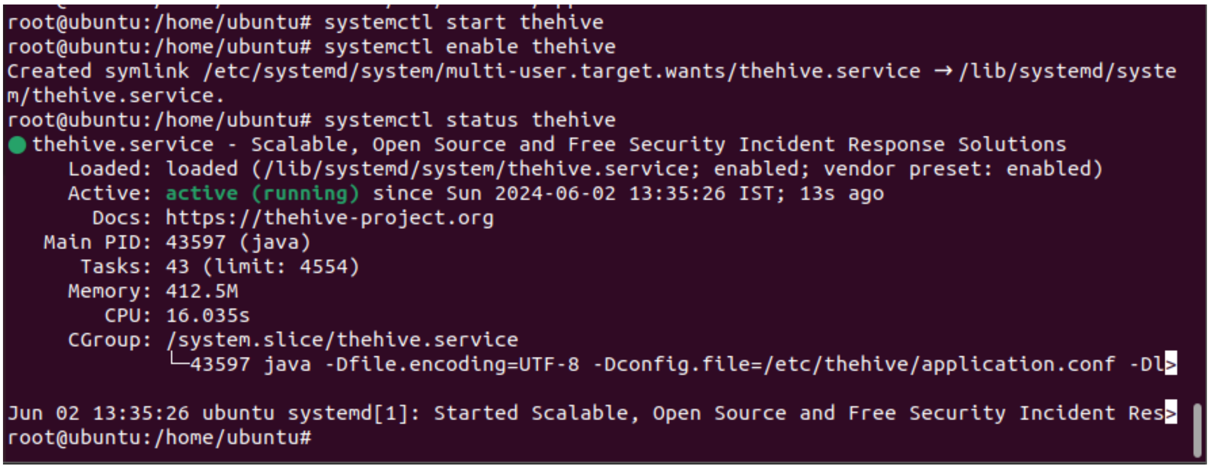
```
root@ubuntu:/home/ubuntu# ls -la /opt/thp
total 12
drwxr-xr-x 3 root root 4096 Jun  1 22:07 .
drwxr-xr-x 4 root root 4096 Jun  1 22:07 ..
drwxr-xr-x 5 root root 4096 Jun  1 22:07 thehive
root@ubuntu:/home/ubuntu# chown -R thehive:thehive /opt/thp
root@ubuntu:/home/ubuntu# ls -la /opt/thp
total 12
drwxr-xr-x 3 thehive thehive 4096 Jun  1 22:07 .
drwxr-xr-x 4 root    root    4096 Jun  1 22:07 ..
drwxr-xr-x 5 thehive thehive 4096 Jun  1 22:07 thehive
root@ubuntu:/home/ubuntu#
```

Step 2: Now go to the directory where hive files exist and open application.conf file in an text editor as shown below and configure the details as shown below such as IP Address and index name:



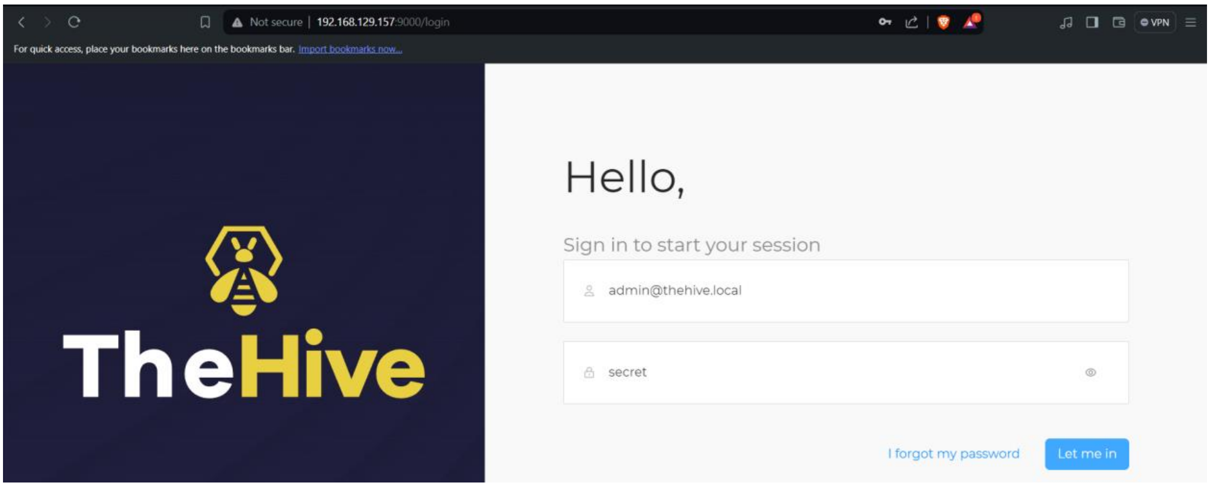
```
  GNU nano 6.2                   /etc/thehive/application.conf *
# By default, TheHive is configured to connect to local Cassandra 4.x and a
# local Elasticsearch services without authentication.
db.janusgraph {
  storage {
    backend = cql
    hostname = ["192.168.129.157"]
    # Cassandra authentication (if configured)
    # username = "thehive"
    # password = "password"
    cql {
      cluster-name = Test Cluster
      keyspace = thehive
    }
  }
  index.search {
    backend = elasticsearch
    hostname = ["192.168.129.157"]
    index-name = thehive
  }
}

# Attachment storage configuration
# By default, TheHive is configured to store files locally in the folder.
# The path can be updated and should belong to the user/group running thehive service. (by defa>
storage {
  provider = localfs
  localfs.location = /opt/thp/thehive/files
}

# Define the maximum size for an attachment accepted by TheHive
play.http.parser.maxDiskBuffer = 1GB
# Define maximum size of http request (except attachment)
play.http.parser.maxMemoryBuffer = 10M

# Service configuration
application.baseUrl = "http://192.168.129.157:9000"
play.http.context = "/"
```

Step 3: Now enable the hive as a service and run it, check if it the service is running properly:



```
root@ubuntu:/home/ubuntu# systemctl start thehive
root@ubuntu:/home/ubuntu# systemctl enable thehive
Created symlink /etc/systemd/system/multi-user.target.wants/thehive.service → /lib/systemd/syste
m/thehive.service.
root@ubuntu:/home/ubuntu# 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 Sun 2024-06-02 13:35:26 IST; 13s ago
       Docs: https://thehive-project.org
   Main PID: 43597 (java)
      Tasks: 43 (limit: 4554)
     Memory: 412.5M
        CPU: 16.035s
     CGroup: /system.slice/thehive.service
             └─43597 java -Dfile.encoding=UTF-8 -Dconfig.file=/etc/thehive/application.conf -Dl>

Jun 02 13:35:26 ubuntu systemd[1]: Started Scalable, Open Source and Free Security Incident Res>
root@ubuntu:/home/ubuntu#
```

Step 4: Now that the hive is successful been installed and is running, go to the browser and lookup the server IP along with the port number 9000 which is the default port where hive service will run.



Not secure | 192.168.129.157:9000/login

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Hello,

Sign in to start your session

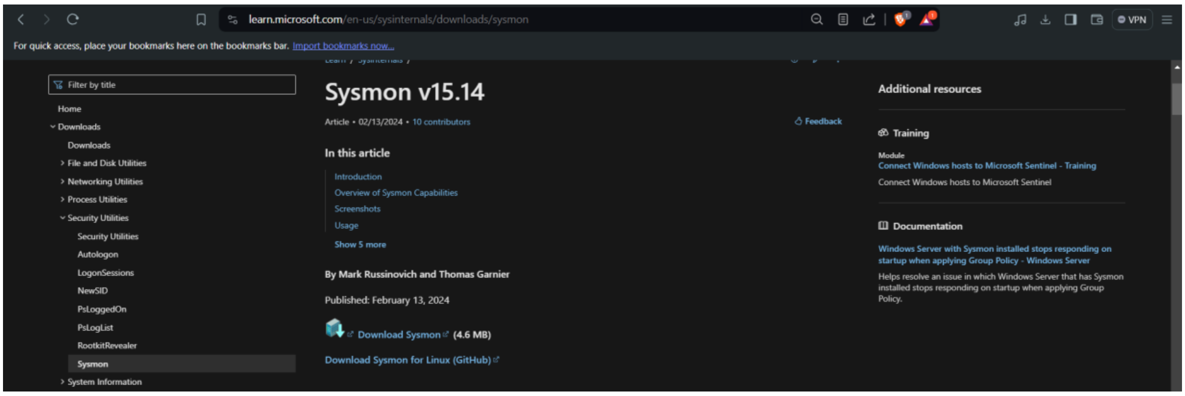
admin@thehive.local

secret

Installing Monitoring Services on Windows System

Installing Sysmon

- Download Sysmon from the Sysinternals website.



learn.microsoft.com/en-us/sysinternals/downloads/sysmon

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Filter by title

- Home
- Downloads
  - Downloads
  - File and Disk Utilities
  - Networking Utilities
  - Process Utilities
  - Security Utilities
    - Security Utilities
    - Autologon
    - LogonSessions
    - NewSID
    - PsLoggedOn
    - PsLogList
    - RootkitRevealer
    - Sysmon
  - System Information

Sysmon v15.14

Article • 02/13/2024 • 10 contributors

Feedback

In this article

- Introduction
- Overview of Sysmon Capabilities
- Screenshots
- Usage
- Show 5 more

By Mark Russinovich and Thomas Garnier

Published: February 13, 2024

Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

Additional resources

Training

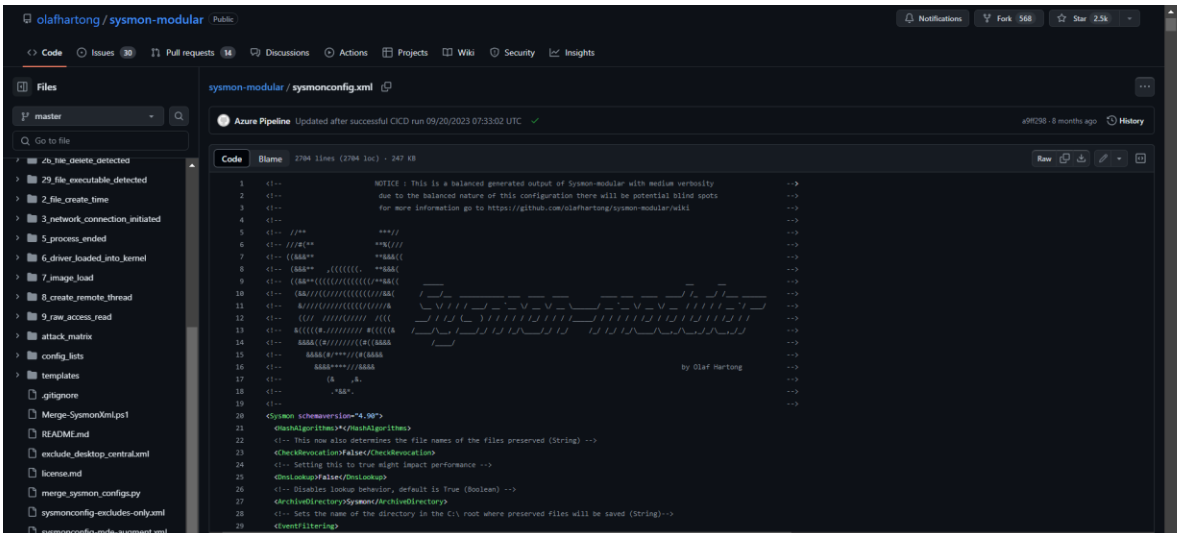
Module
Connect Windows hosts to Microsoft Sentinel - Training
Connect Windows hosts to Microsoft Sentinel

Documentation

Windows Server with Sysmon installed stops responding on startup when applying Group Policy - Windows Server

Helps resolve an issue in which Windows Server that has Sysmon installed stops responding on startup when applying Group Policy.

- Download the Sysmon configuration file from GitHub.



olafhartong / sysmon-modular Public

- 26_file_delete_detected
- 29_file_executable_detected
- 2_file_create_time
- 3_network_connection_initiated
- 5_process_ended
- 6_driver_loaded_into_kernel
- 7_image_load
- 8_create_remote_thread
- 9_raw_access_read
- attack_matrix
- config_lists
- templates
- .gitignore
- Merge-SysmonXml.ps1
- README.md
- exclude_desktop_central.xml
- license.md
- merge_sysmon_configs.py
- sysmonconfig-excludes-only.xml
- sysmonconfig-mde-augment.xml

sysmon-modular / sysmonconfig.xml

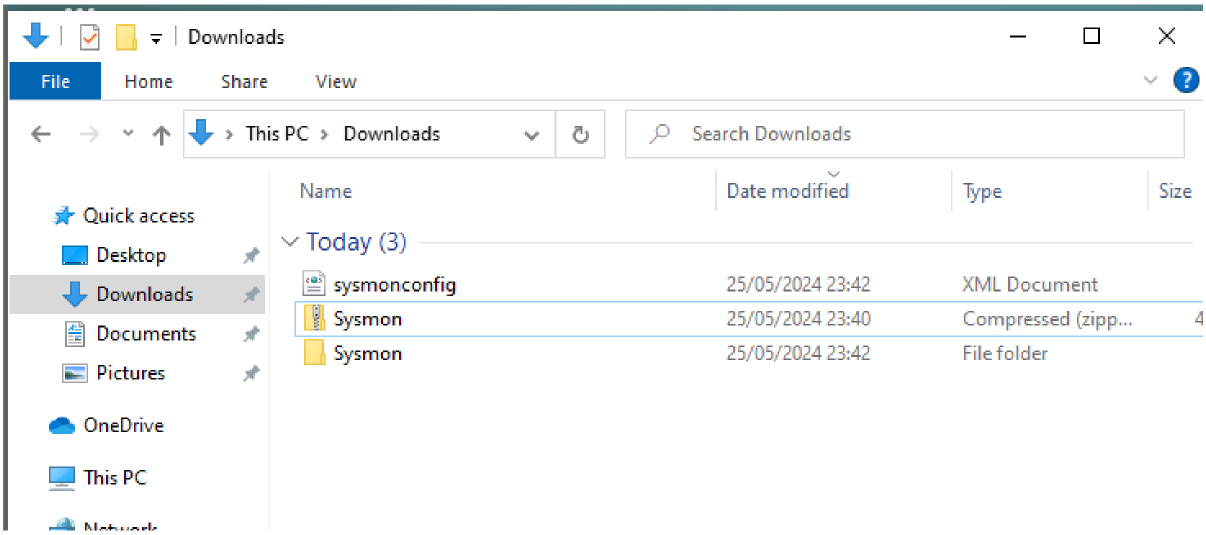
Azure Pipeline Updated after successful CICD run 09/20/2023 07:33:02 UTC ✓

a9ff298 · 8 months ago History

2704 lines (2704 loc) · 247 KB

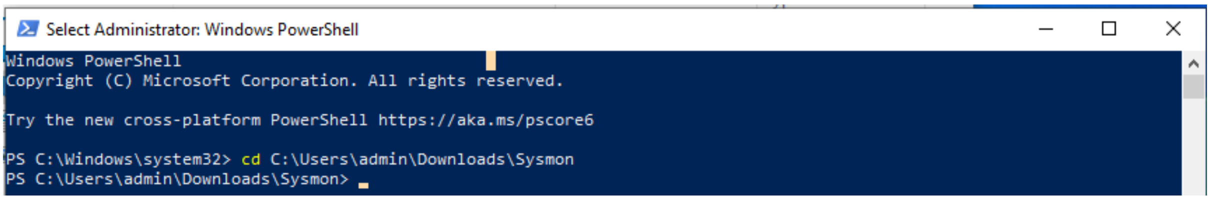
```
<!--                     NOTICE : This is a balanced generated output of Sysmon-modular with medium verbosity       -->
<!--                      due to the balanced nature of this configuration there will be potential blind spots      -->
<!--                      for more information go to https://github.com/olafhartong/sysmon-modular/wiki            -->
<!--                                                                                                                 -->
<!--  //**                  ***//                                                                                    -->
<!-- ///#(**               **%(///                                                                                   -->
<!-- ((&&&**               **&&&((                                                                                   -->
<!--  (&&&**   ,(((((((.   **&&&(                                                                                    -->
<!--  ((&&**(((((//(((((((/**&&((                                                                                    -->
<!--   (&&///((////(((((((///&&(                                                                                     -->
<!--    &////(/////(((((/(////&                                                                                      -->
<!--    ((//  /////(/////  /(((                                                                                      -->
<!--   &(((((#.///////// #(((((&                                                                                     -->
<!--    &&&&((#///////((#((&&&&                                                                                      -->
<!--      &&&&(#/***//(#(&&&&                                                                                        -->
<!--        &&&&****///&&&&                                                             by Olaf Hartong             -->
<!--           (&    ,&.                                                                                             -->
<!--            .*&&*.                                                                                               -->
<!--                                                                                                                 -->
<Sysmon schemaversion="4.90">
  <HashAlgorithms>*</HashAlgorithms>
  <!-- This now also determines the file names of the files preserved (String) -->
  <CheckRevocation>False</CheckRevocation>
  <!-- Setting this to true might impact performance -->
  <DnsLookup>False</DnsLookup>
  <!-- Disables lookup behavior, default is True (Boolean) -->
  <ArchiveDirectory>Sysmon</ArchiveDirectory>
  <!-- Sets the name of the directory in the C:\ root where preserved files will be saved (String)-->
  <EventFiltering>
```

- Extract Sysmon and move the configuration file to the same directory.



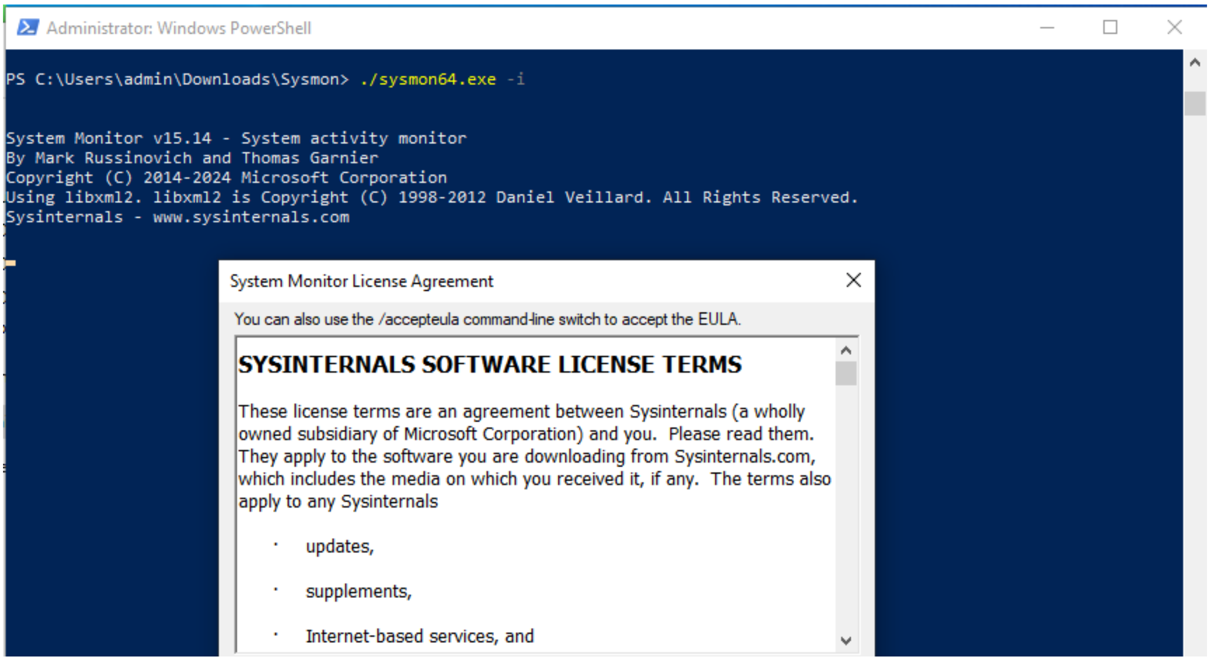
Name	Date modified	Type	Size
Today (3)			
sysmonconfig	25/05/2024 23:42	XML Document	
Sysmon	25/05/2024 23:40	Compressed (zipp...	4
Sysmon	25/05/2024 23:42	File folder	

- Open PowerShell as an administrator, navigate to the Sysmon directory.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd C:\Users\admin\Downloads\Sysmon
PS C:\Users\admin\Downloads\Sysmon> _
```

- Install Sysmon using the configuration file. Verify Sysmon installation by checking services and event logs.



```
PS C:\Users\admin\Downloads\Sysmon> ./sysmon64.exe -i


System Monitor v15.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
```

System Monitor License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

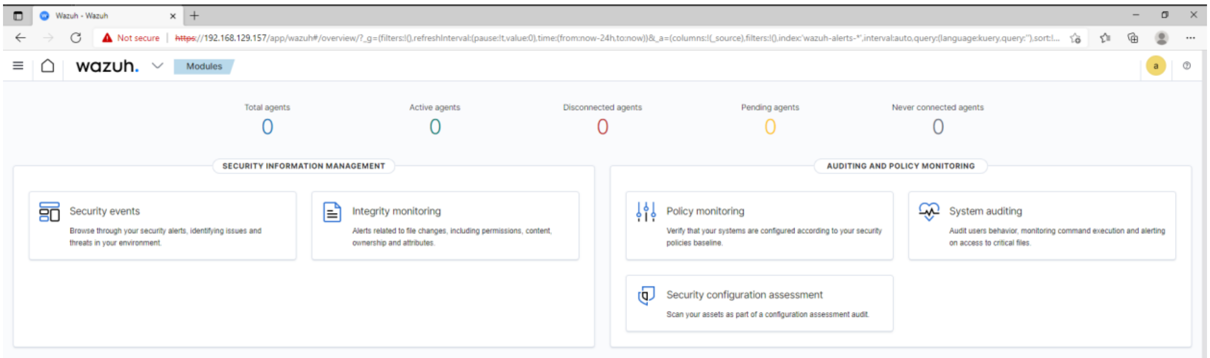
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Access the Wazuh Dashboard

- Use the **admin credentials** to log in.
- If you don’t have the credentials:

```
bash
ls /var/ossec/etc/
tar -xvf wazuh-install.tar
cat wazuh-install/wazuh-password.txt
```


Wazuh - Wazuh
Not secure
https://192.168.129.157/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(),index:'wazuh-alerts-*',interval:auto,query:(language:kuery,query:''),sort:!...
wazuh.
Modules
a

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
0	0	0	0	0

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

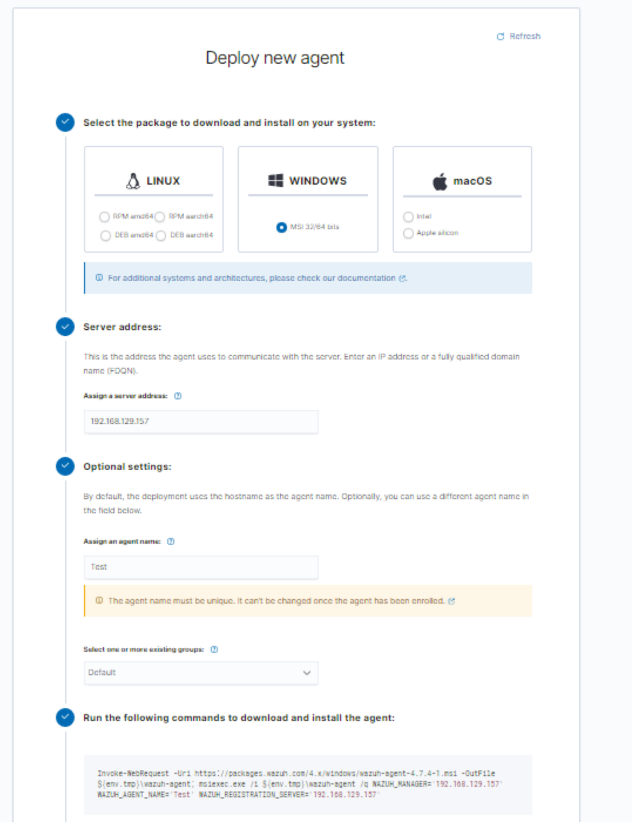
Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

Add a Windows Agent

- In the Wazuh dashboard, click **Add Agent**.
- **Select OS:** Windows
- **Server Address:** Enter your **Wazuh public IP** (e.g., 192.168.129.157).
- **Optional:** Assign an agent name (e.g., Test).



Deploy new agent

Select the package to download and install on your system:

LINUX
○ RPM amd64 ○ RPM aarch64
○ DEB amd64 ○ DEB aarch64

WINDOWS
● MSI 32/64 bits

macOS
○ Intel
○ Apple silicon

For additional systems and architectures, please check our documentation.

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: 192.168.129.157

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: Test

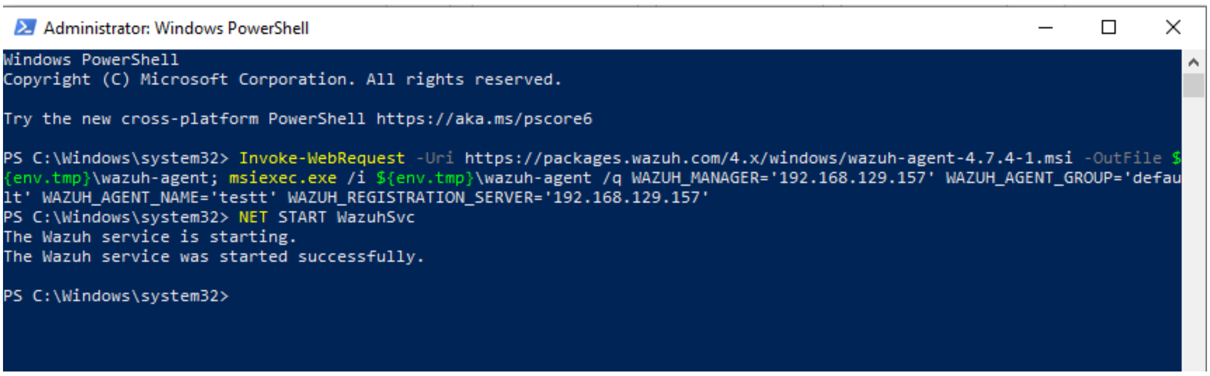
The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups: Default

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile
${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.129.157'
WAZUH_AGENT_NAME='Test' WAZUH_REGISTRATION_SERVER='192.168.129.157'
```

- Copy the generated command and **run it in PowerShell** (as Administrator) on the Windows machine:

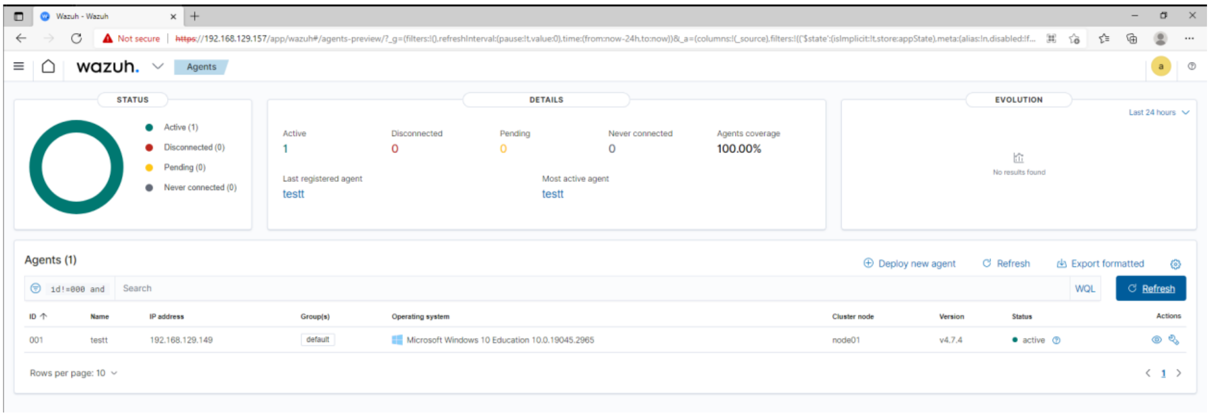


Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile ${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.129.157' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='testt' WAZUH_REGISTRATION_SERVER='192.168.129.157'
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

Verify Agent Connection

- Go to Wazuh Dashboard → Check Agents.
- If it shows `disconnected`, wait a moment. It should connect shortly, showing 1 active agent.
- Once connected, click on Security Events to query logs.



Wazuh - Wazuh
Not secure
https://192.168.129.157/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isImplicit:!t,store:appState),meta:(alias:!n,disabled:!f...
wazuh.
Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
EVOLUTION
Last 24 hours
No results found
Deploy new agent
Refresh
Export formatted
WQL
Refresh
Rows per page: 10

Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last registered agent: testt

Most active agent: testt

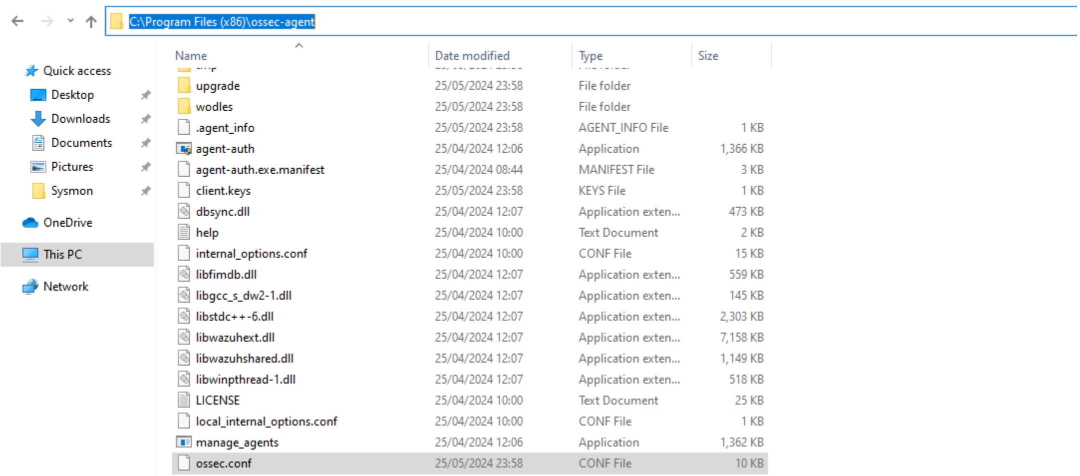
Agents (1)

id!=000 and Search

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	testt	192.168.129.149	default	Microsoft Windows 10 Education 10.0.19045.2965	node01	v4.7.4	● active	

Navigate to Wazuh Configuration:

- On the Windows 10 machine, locate the Wazuh configuration file under Program Files (x86) > ossec-agent.



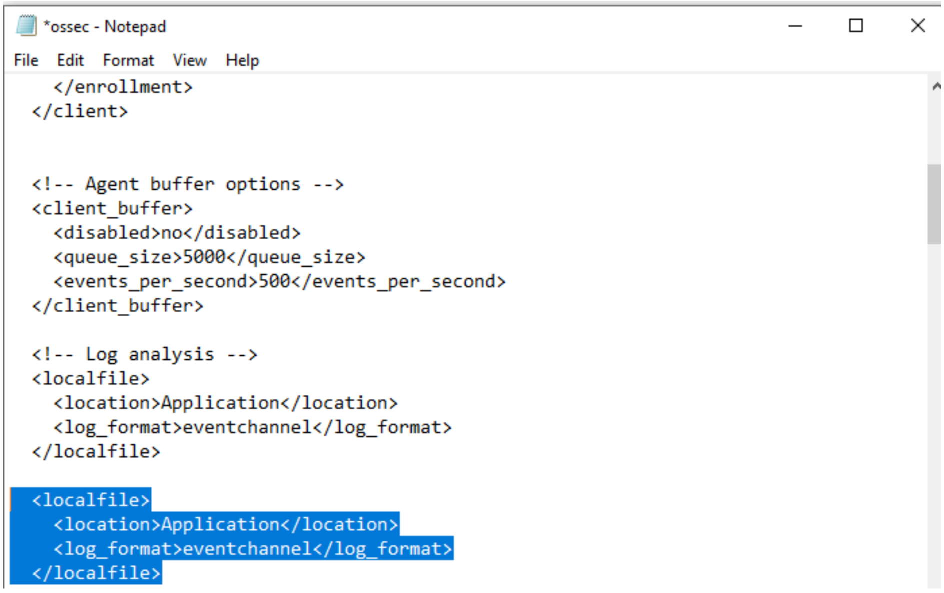
C:\Program Files (x86)\ossec-agent

Name	Date modified	Type	Size
upgrade	25/05/2024 23:58	File folder	
wodles	25/05/2024 23:58	File folder	
.agent_info	25/05/2024 23:58	AGENT_INFO File	1 KB
agent-auth	25/04/2024 12:06	Application	1,366 KB
agent-auth.exe.manifest	25/04/2024 08:44	MANIFEST File	3 KB
client.keys	25/05/2024 23:58	KEYS File	1 KB
dbsync.dll	25/04/2024 12:07	Application exten...	473 KB
help	25/04/2024 10:00	Text Document	2 KB
internal_options.conf	25/04/2024 10:00	CONF File	15 KB
libfimdb.dll	25/04/2024 12:07	Application exten...	559 KB
libgcc_s_dw2-1.dll	25/04/2024 12:07	Application exten...	145 KB
libstdc++-6.dll	25/04/2024 12:07	Application exten...	2,303 KB
libwazuhext.dll	25/04/2024 12:07	Application exten...	7,158 KB
libwazuhshared.dll	25/04/2024 12:07	Application exten...	1,149 KB
libwinpthread-1.dll	25/04/2024 12:07	Application exten...	518 KB
LICENSE	25/04/2024 10:00	Text Document	25 KB
local_internal_options.conf	25/04/2024 10:00	CONF File	1 KB
manage_agents	25/04/2024 12:06	Application	1,362 KB
ossec.conf	25/05/2024 23:58	CONF File	10 KB

- Open the ossec.conf file using Notepad (ensure you have administrative privileges).

Modifying Configuration:

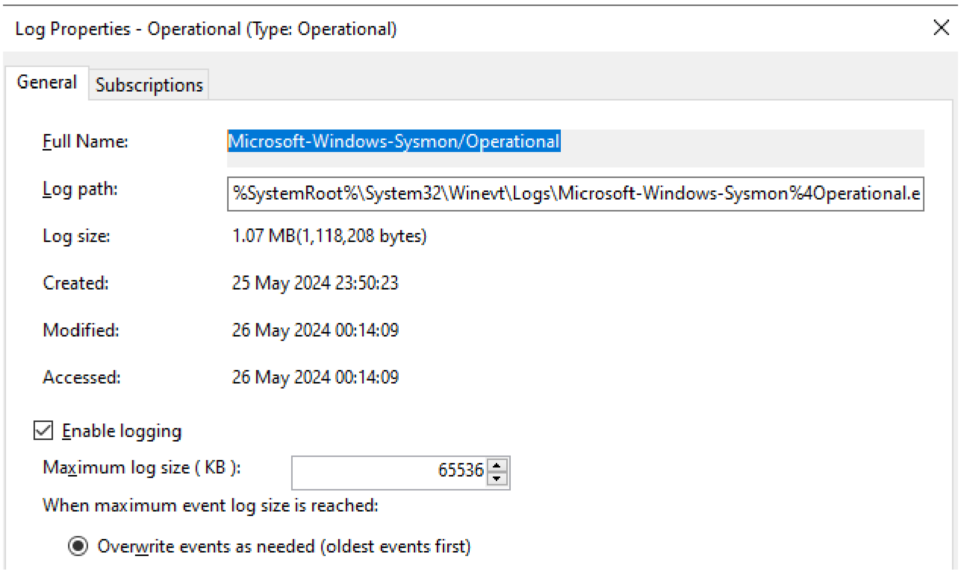
- Look for the log_analysis section.
- To monitor for specific events, such as Mimikatz, Sysmon logs need to be ingested.
- First, create a backup of the configuration file before making changes.



```
  </enrollment>
</client>


<!-- Agent buffer options -->
<client_buffer>
  <disabled>no</disabled>
  <queue_size>5000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

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

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

Configure Sysmon Log Ingestion:

- Add a new configuration for Sysmon log ingestion.
- Open Event Viewer and get the Sysmon channel name from Open Windows Event Viewer → Applications & Services → Microsoft → Windows → Sysmon → Operational → Properties.



Full Name: Microsoft-Windows-Sysmon/Operational

Log path: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Sysmon%4Operational.e

Log size: 1.07 MB(1,118,208 bytes)

Created: 25 May 2024 23:50:23

Modified: 26 May 2024 00:14:09

Accessed: 26 May 2024 00:14:09

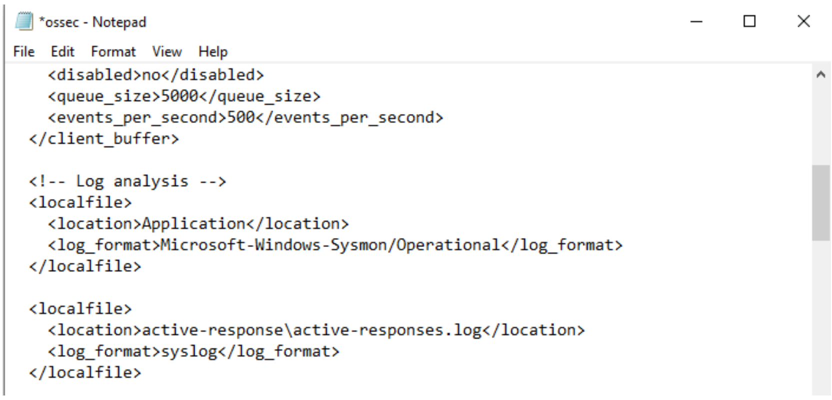
☑ Enable logging

Maximum log size (KB): 65536

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

- Replace the default application location with the Sysmon channel name



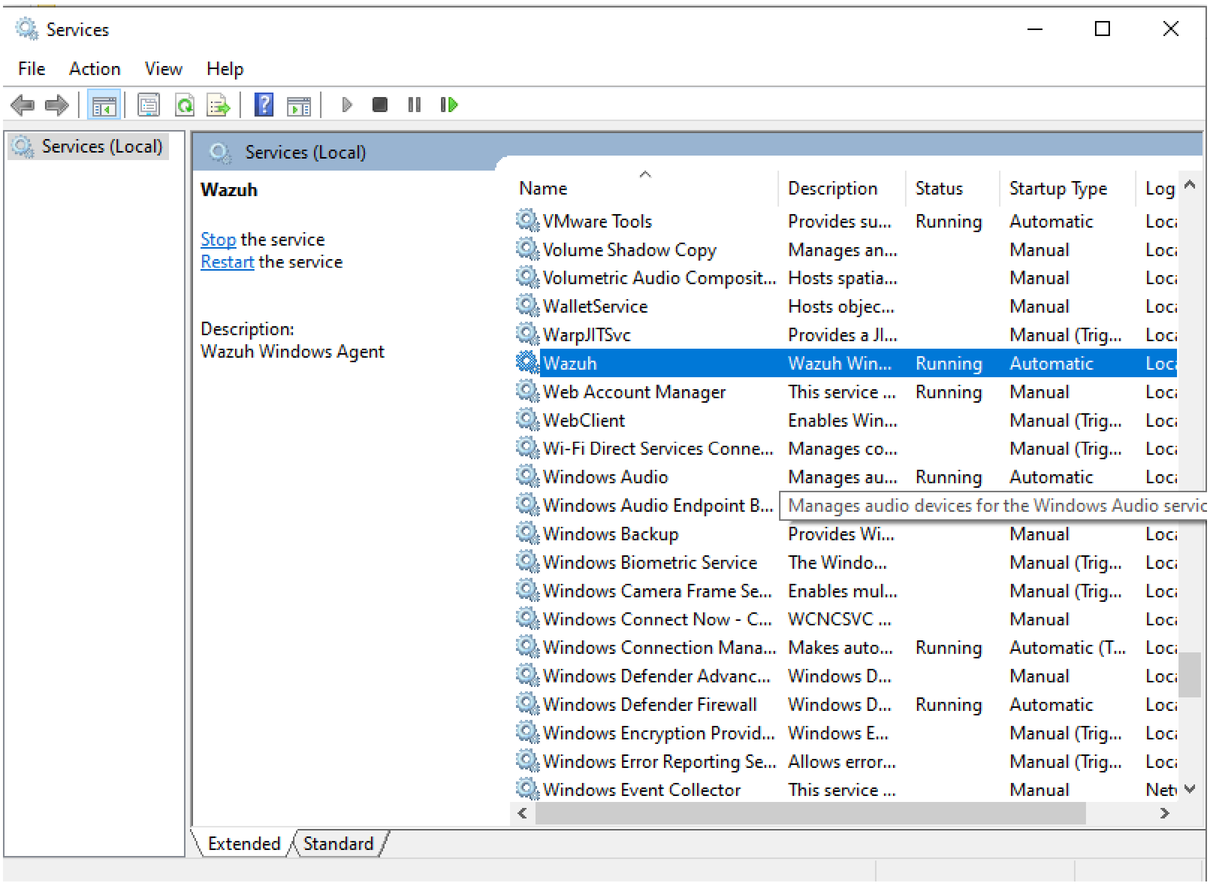
```
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

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

  <localfile>
    <location>active-response\active-responses.log</location>
    <log_format>syslog</log_format>
  </localfile>
```

Save Changes:

- After making the necessary changes, save the file.
- Use administrative privileges to overwrite the configuration file.

Restart Wazuh Service:

- Restart the Wazuh service using services.msc.
- Remember, any configuration change requires a service restart.



Wazuh

Stop the service
Restart the service

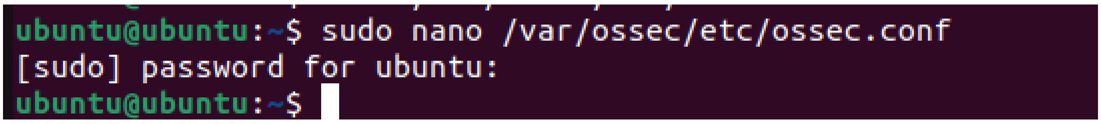
Description:
Wazuh Windows Agent

Name	Description	Status	Startup Type	Log
VMware Tools	Provides su...	Running	Automatic	Loc
Volume Shadow Copy	Manages an...		Manual	Loc
Volumetric Audio Composit...	Hosts spatia...		Manual	Loc
WalletService	Hosts objec...		Manual	Loc
WarpJITSvc	Provides a JI...		Manual (Trig...	Loc
Wazuh	Wazuh Win...	Running	Automatic	Loc
Web Account Manager	This service ...	Running	Manual	Loc
WebClient	Enables Win...		Manual (Trig...	Loc
Wi-Fi Direct Services Conne...	Manages co...		Manual (Trig...	Loc
Windows Audio	Manages au...	Running	Automatic	Loc
Windows Audio Endpoint B...	Manages audio devices for the Windows Audio servic			
Windows Backup	Provides Wi...		Manual	Loc
Windows Biometric Service	The Windo...		Manual (Trig...	Loc
Windows Camera Frame Se...	Enables mul...		Manual (Trig...	Loc
Windows Connect Now - C...	WCNCSVC ...		Manual	Loc
Windows Connection Mana...	Makes auto...	Running	Automatic (T...	Loc
Windows Defender Advanc...	Windows D...		Manual	Loc
Windows Defender Firewall	Windows D...	Running	Automatic	Loc
Windows Encryption Provid...	Windows E...		Manual (Trig...	Loc
Windows Error Reporting Se...	Allows error...		Manual (Trig...	Loc
Windows Event Collector	This service ...		Manual	Net

Modify Wazuh to Log All Events

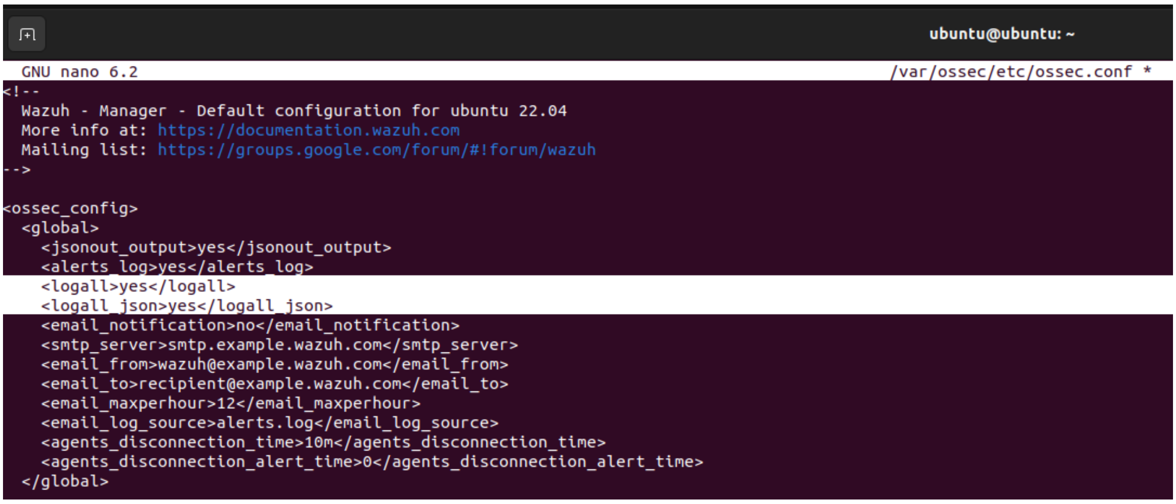
Backup & Modify `ossec.conf` in Wazuh Manager:

- Create a backup: cp /var/ossec/etc/ossec.conf ~/ossec_backup.conf.



```
ubuntu@ubuntu:~$ sudo nano /var/ossec/etc/ossec.conf
[sudo] password for ubuntu:
ubuntu@ubuntu:~$
```

- In osc.conf, set log_all and logall_json to yes.

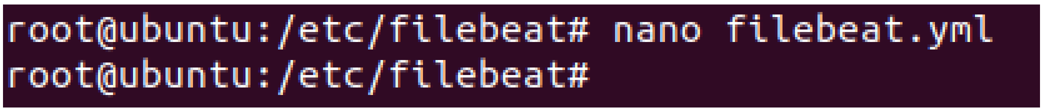


ubuntu@ubuntu: ~

```
  GNU nano 6.2                                                    /var/ossec/etc/ossec.conf *
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>
```

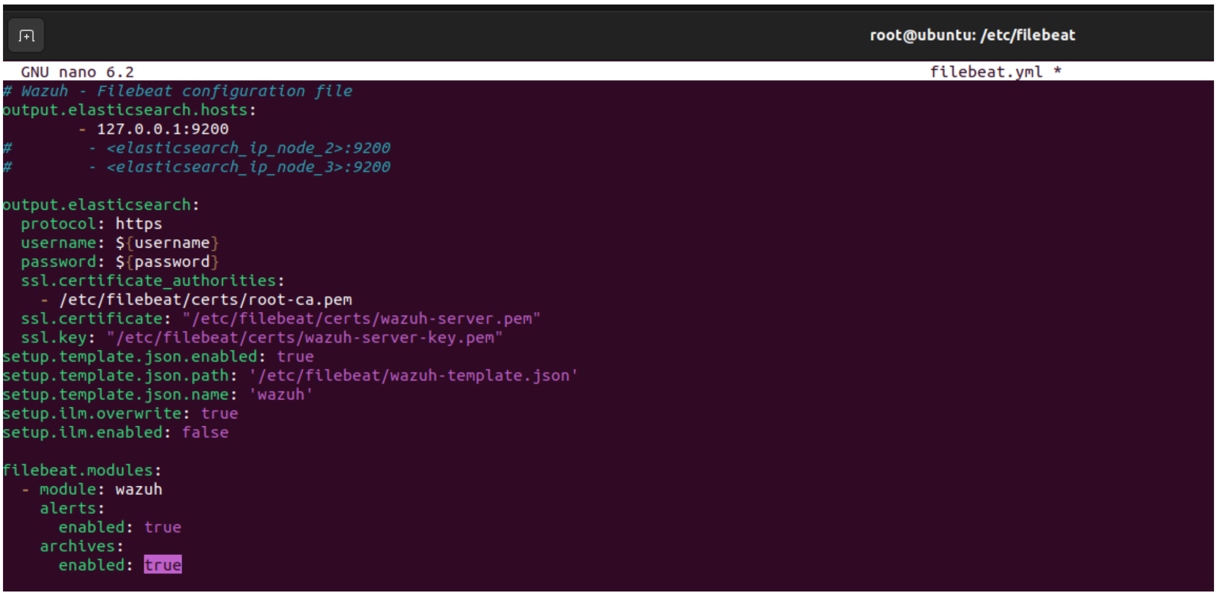
Modify to make it save all logs in a file

- Open /etc/filebeat/filebeat.yml.



```
root@ubuntu:/etc/filebeat# nano filebeat.yml
root@ubuntu:/etc/filebeat#
```

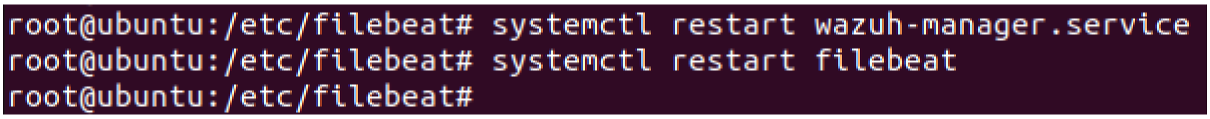
- Set archives.enabled to true.



root@ubuntu: /etc/filebeat

```
  GNU nano 6.2                                                        filebeat.yml *
# Wazuh - Filebeat configuration file
output.elasticsearch.hosts:
        - 127.0.0.1:9200
#         - <elasticsearch_ip_node_2>:9200
#         - <elasticsearch_ip_node_3>:9200

output.elasticsearch:
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/wazuh-server.pem"
  ssl.key: "/etc/filebeat/certs/wazuh-server-key.pem"
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: true
```

- Restart Filebeat service.

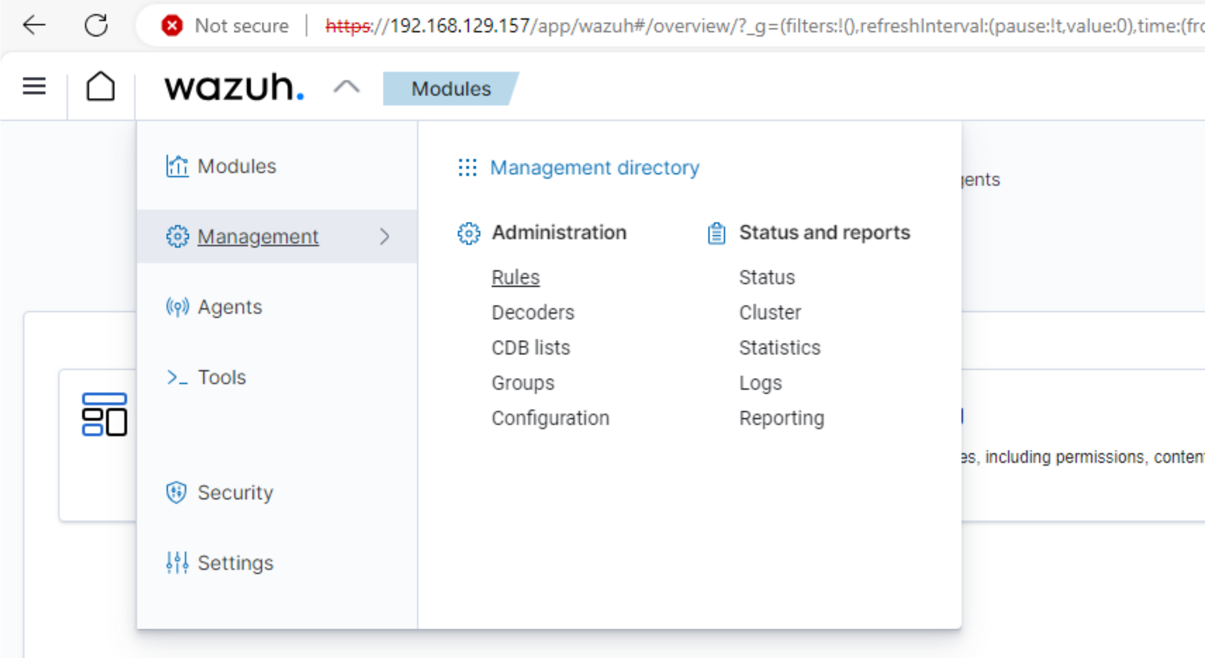


```
root@ubuntu:/etc/filebeat# systemctl restart wazuh-manager.service
root@ubuntu:/etc/filebeat# systemctl restart filebeat
root@ubuntu:/etc/filebeat#
```

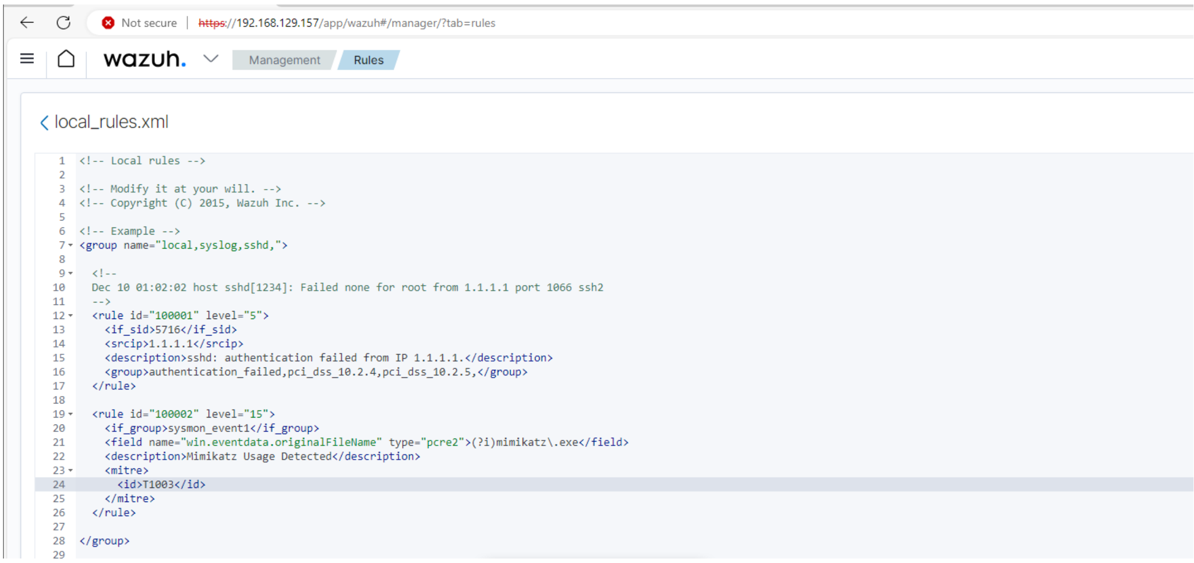
Build a Custom Alert for Mimikatz

Create a Custom Rule for Mimikatz Detection

- Navigate to **Rules** in the Wazuh dashboard → Manage Rule Files → Custom Rules.



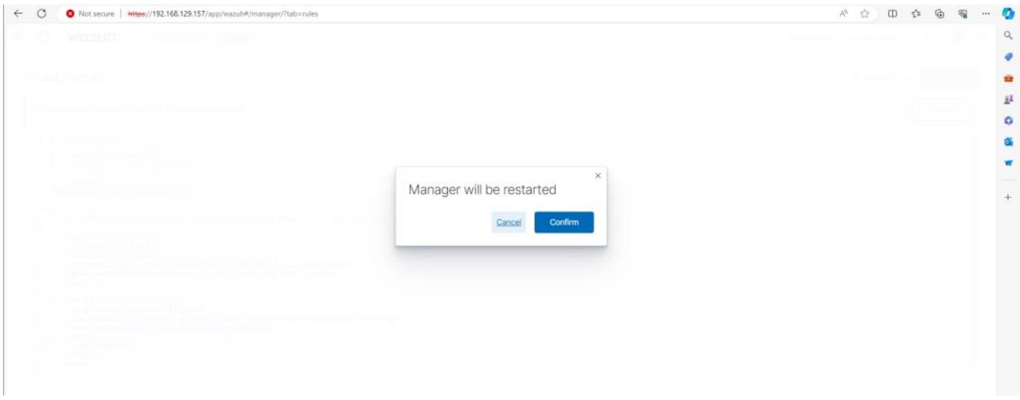
- Copy an existing Sysmon rule and modify:
  - **Rule ID**: Use a number above 100,000.
  - **Field**: Use `original_file_name` to detect Mimikatz regardless of renaming.
  - **Value**: Set to `mimikatz`.
  - **Level**: Set severity level to 15.


Not secure | https://192.168.129.157/app/wazuh#/manager/?tab=rules
wazuh.
Management
Rules
local_rules.xml

```
<!-- 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>

</group>

```

Save and Restart Manager

- Save the custom rule and confirm the restart of Wazuh Manager.

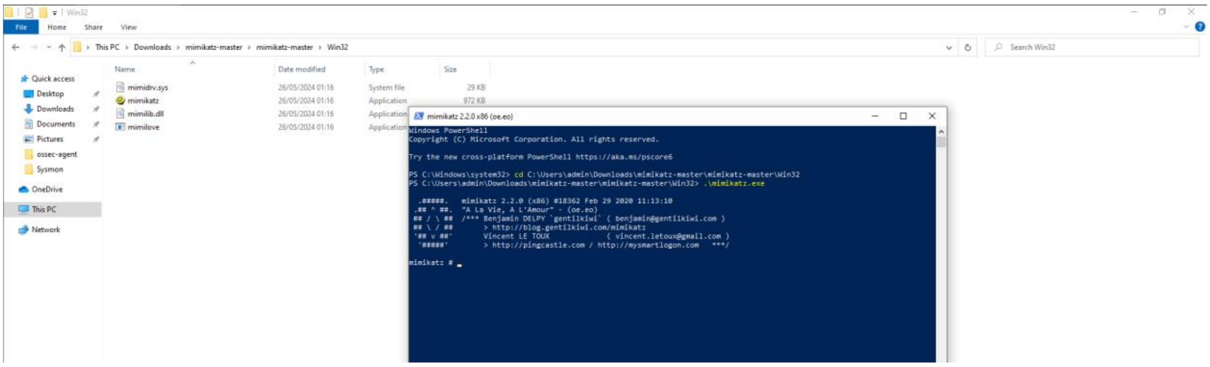


Manager will be restarted

Verify the Alert

Rename Mimikatz and Test

- Rename `mimikatz.exe` to `you_are_awesome.exe`.
- Execute the renamed file from PowerShell.



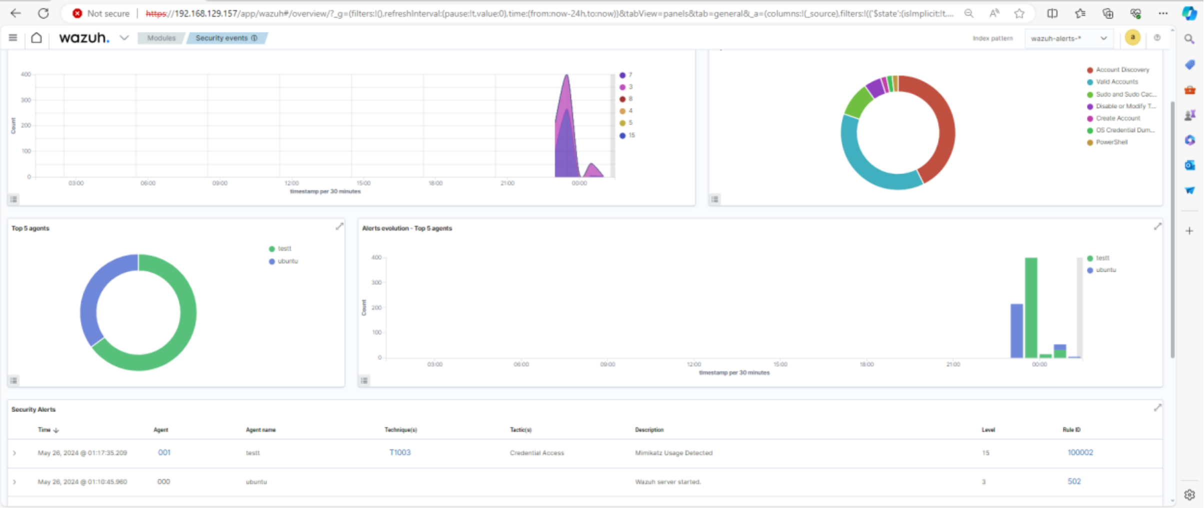
Name	Date modified	Type	Size
mimidrv.sys	26/05/2024 01:16	System file	29 KB
mimikatz	26/05/2024 01:16	Application	972 KB
mimilib.dll	26/05/2024 01:16	Application	
mimilove	26/05/2024 01:16	Application	

mimikatz 2.2.0 x86 (oe.eo)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd C:\Users\admin\Downloads\mimikatz-master\mimikatz-master\Win32
PS C:\Users\admin\Downloads\mimikatz-master\mimikatz-master\Win32> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # _
```

Check Wazuh Dashboard for Alerts

- Search the **archives index** for Mimikatz events.
- Verify alerts triggered on the original file name field.



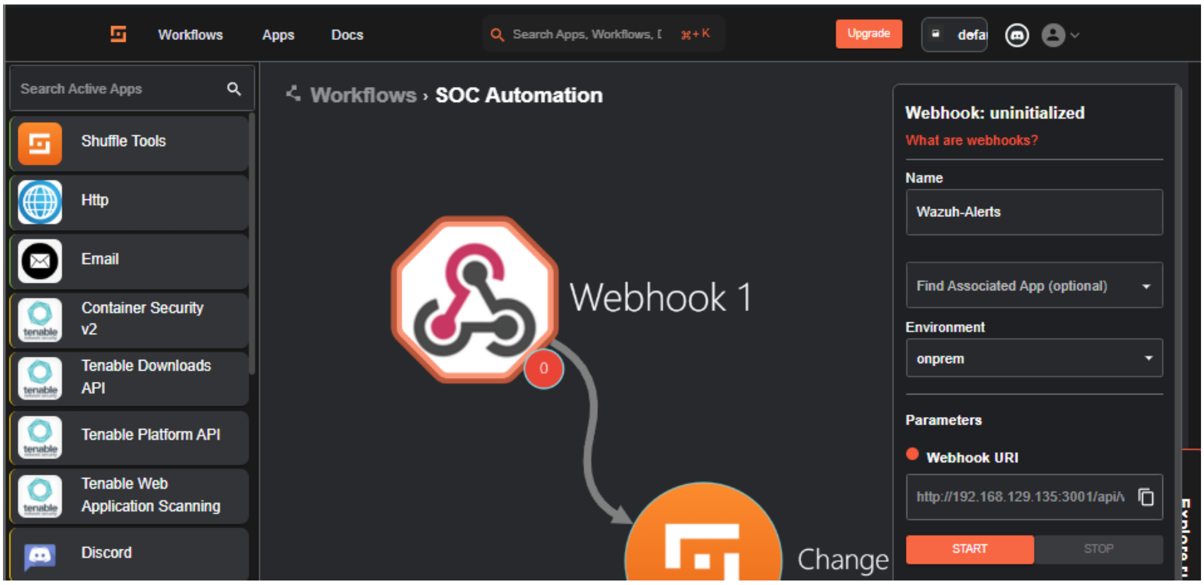
Security Alerts

	Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
›	May 26, 2024 @ 01:17:35.209	001	testt	T1003	Credential Access	Mimikatz Usage Detected	15	100002
›	May 26, 2024 @ 01:10:45.960	000	ubuntu			Wazuh server started.	3	502

Configuring the Environment and Initial Setup

Creating a New Workflow and Setting Up Triggers:

- In the workflow workspace, click on the **Triggers** tab.
- Drag and drop a **Webhook** trigger into the workspace.



Webhook: uninitialized

What are webhooks?

Name: Wazuh-Alerts

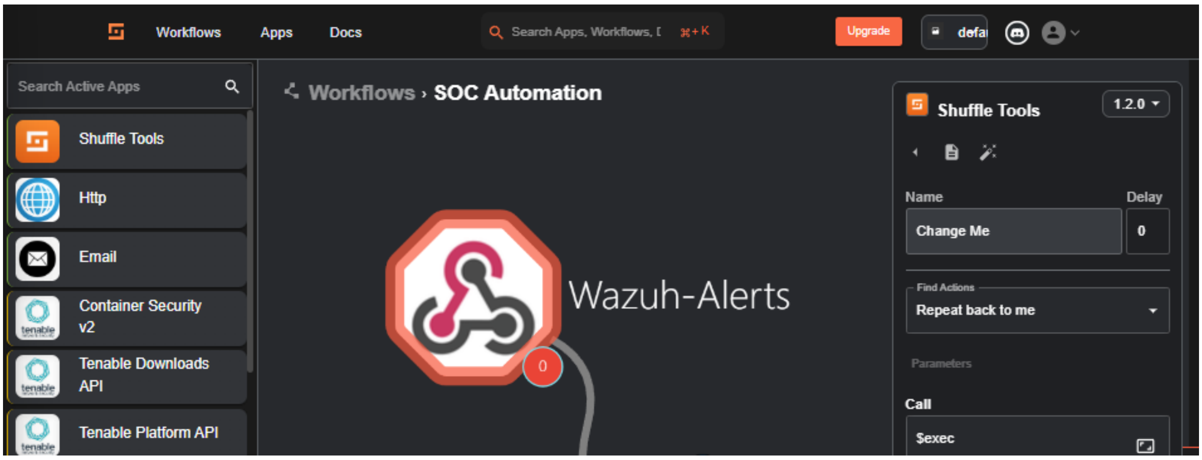
Find Associated App (optional)

Environment: onprem

Parameters

Webhook URI: http://192.168.129.135:3001/api/\

- Name the webhook (e.g., "Wazuh Alerts") and copy the webhook URI for future use.



Shuffle Tools 1.2.0

Name: Change Me

Delay: 0

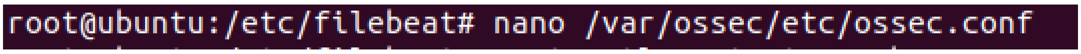
Find Actions: Repeat back to me

Parameters

Call: $exec

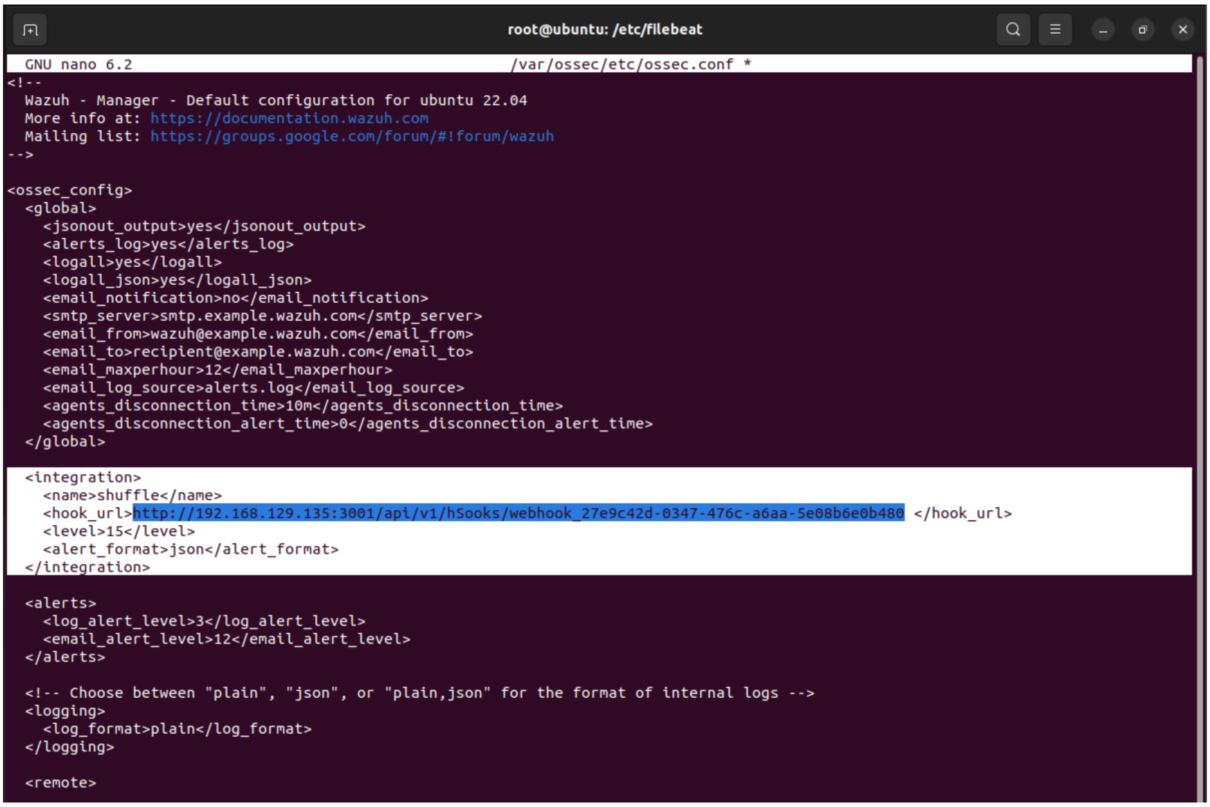
Configuring Wazuh Manager:

- Access the Wazuh Manager CLI and locate the configuration file at `/var/ossec/etc/ossec.conf`.



```
root@ubuntu:/etc/filebeat# nano /var/ossec/etc/ossec.conf
```

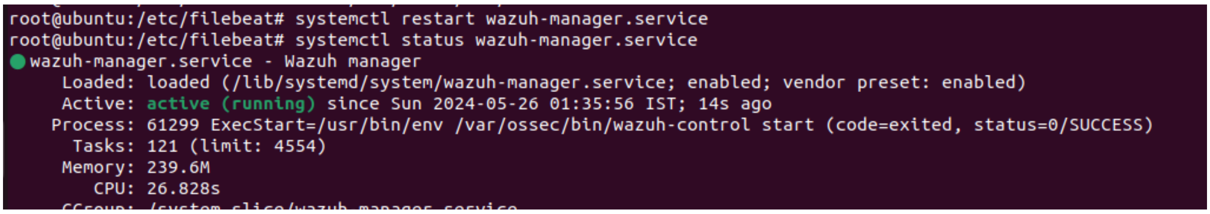
- Insert the integration tag within the global tag section while maintaining proper indentation.
- Replace the placeholder Shuffle URL with the copied webhook URL, ensuring it is formatted correctly.
- Change the default alert level from 3 to a specific rule ID (e.g., `100,2`) to filter alerts.



```
  GNU nano 6.2                                               /var/ossec/etc/ossec.conf *
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <integration>
    <name>shuffle</name>
    <hook_url>http://192.168.129.135:3001/api/v1/hSooks/webhook_27e9c42d-0347-476c-a6aa-5e08b6e0b480 </hook_url>
    <level>15</level>
    <alert_format>json</alert_format>
  </integration>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
  <logging>
    <log_format>plain</log_format>
  </logging>

  <remote>
```

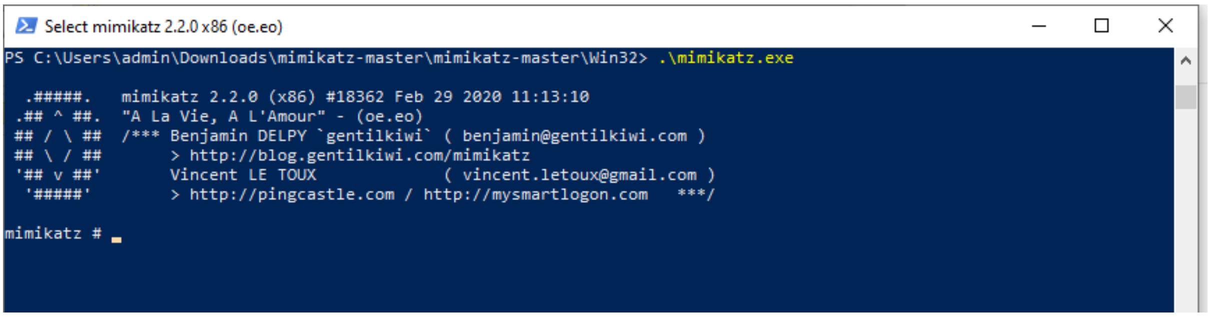
Testing the Integration:

- Restart the Wazuh Manager service.



```
root@ubuntu:/etc/filebeat# systemctl restart wazuh-manager.service
root@ubuntu:/etc/filebeat# systemctl status wazuh-manager.service
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-05-26 01:35:56 IST; 14s ago
    Process: 61299 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 121 (limit: 4554)
     Memory: 239.6M
        CPU: 26.828s
     CGroup: /system.slice/wazuh-manager.service
```

- Generate test alerts using the Mimikatz tool on the client machine.

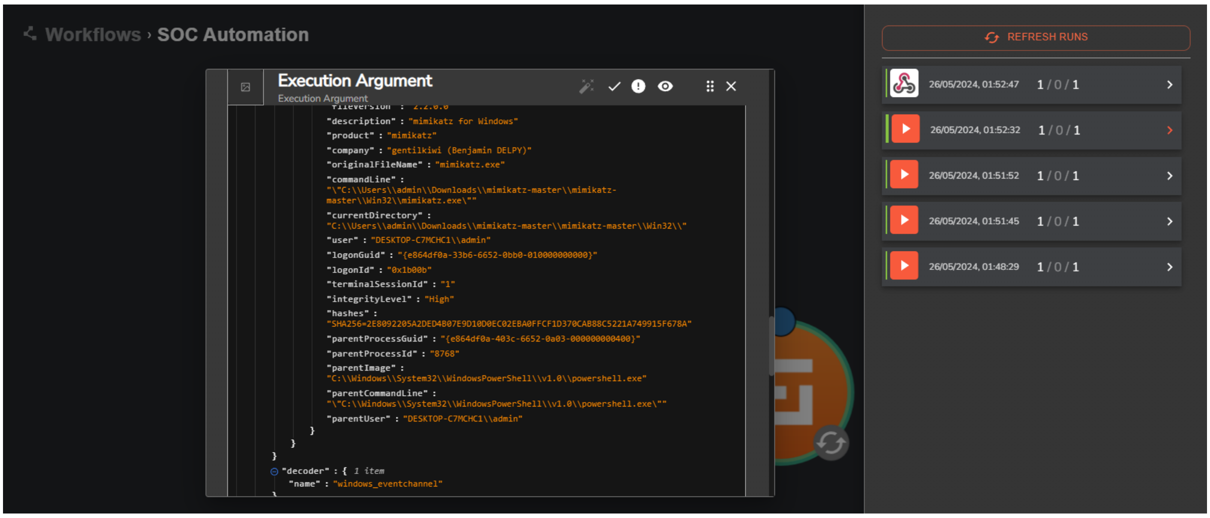


```
PS C:\Users\admin\Downloads\mimikatz-master\mimikatz-master\Win32> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # _
```

- Verify that alerts appear in Shuffle and check execution arguments.

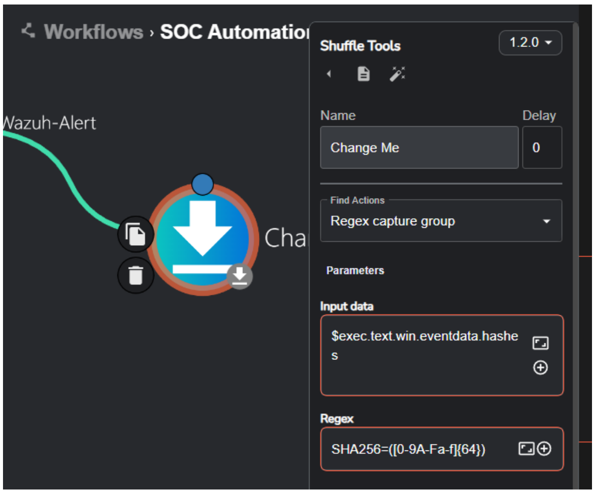
Parsing Hash Values:

- Modify the workflow to parse the SHA-256 hash value from alerts.
- Use Regex (Rex) to extract the hash. If unsure, ask AI tools like ChatGPT for help with writing the Regex.



```
            "fileVersion" : "2.2.0.0"
            "description" : "mimikatz for Windows"
            "product" : "mimikatz"
            "company" : "gentilkiwi (Benjamin DELPY)"
            "originalFileName" : "mimikatz.exe"
            "commandLine" :
            "\"C:\\Users\\admin\\Downloads\\mimikatz-master\\mimikatz-
            master\\Win32\\mimikatz.exe\""
            "currentDirectory" :
            "C:\\Users\\admin\\Downloads\\mimikatz-master\\mimikatz-master\\Win32\\"
            "user" : "DESKTOP-C7MCHC1\\admin"
            "logonGuid" : "{e864df0a-33b6-6652-0bb0-010000000000}"
            "logonId" : "0x1b00b"
            "terminalSessionId" : "1"
            "integrityLevel" : "High"
            "hashes" :
            "SHA256=2E8092205A2DED4B07E9D10D0EC02EBA0FFCF1D370CAB88C5221A749915F678A"
            "parentProcessGuid" : "{e864df0a-403c-6652-0a03-000000000400}"
            "parentProcessId" : "8768"
            "parentImage" :
            "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
            "parentCommandLine" :
            "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\""
            "parentUser" : "DESKTOP-C7MCHC1\\admin"
         }
      }
   }
"decoder" : { 1 item
   "name" : "windows_eventchannel"
```

- Paste the Regex into Shuffle and save the workflow.



Name: Change Me

Delay: 0

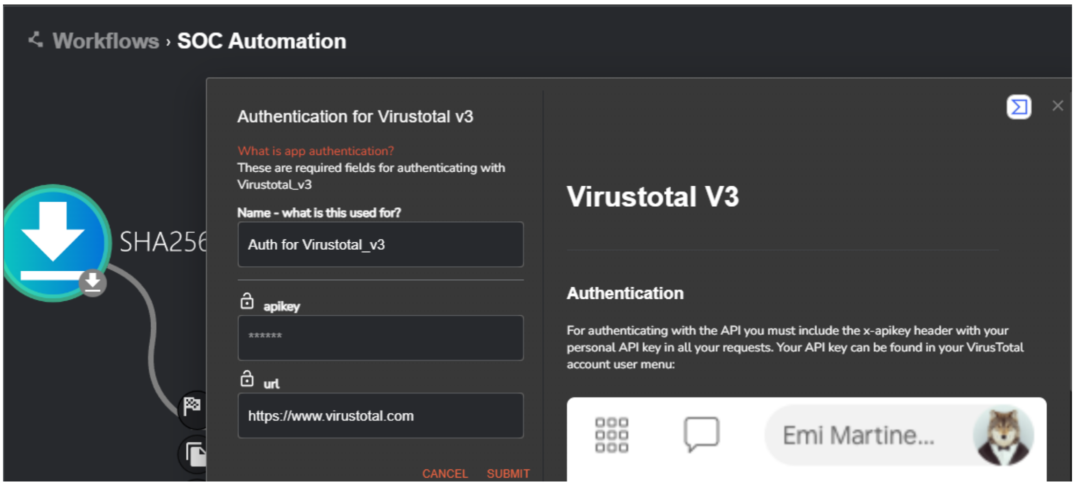
Find Actions: Regex capture group

Input data: $exec.text.win.eventdata.hashes

Regex: SHA256=([0-9A-Fa-f]{64})

Integrating VirusTotal:

- Create an account on VirusTotal and copy your API key.
- In Shuffle, add the VirusTotal app and configure it to look for hash reports instead of IP addresses.
- Authenticate with your API key.



Authentication for Virustotal v3

What is app authentication?

These are required fields for authenticating with Virustotal_v3

Name - what is this used for?: Auth for Virustotal_v3

apikey: ******

url: https://www.virustotal.com

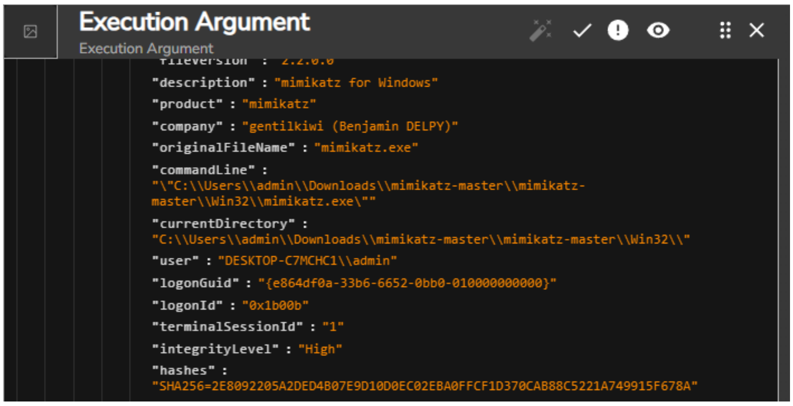
Virustotal V3

Authentication

For authenticating with the API you must include the x-apikey header with your personal API key in all your requests. Your API key can be found in your VirusTotal account user menu:

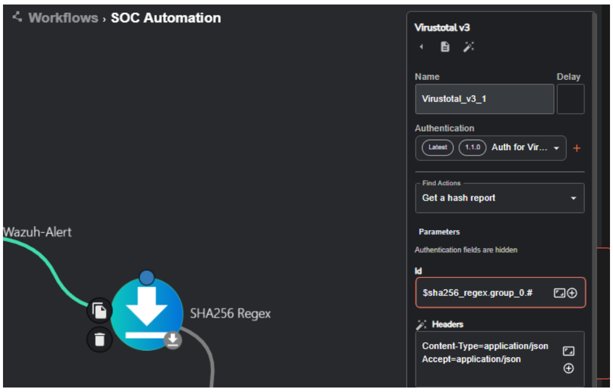
Extracting File Hashes

- Use Regex to extract the SHA-256 hash from the output.



```
"fileVersion" : "2.2.0.0"
"description" : "mimikatz for Windows"
"product" : "mimikatz"
"company" : "gentilkiwi (Benjamin DELPY)"
"originalFileName" : "mimikatz.exe"
"commandLine" :
"\"C:\\Users\\admin\\Downloads\\mimikatz-master\\mimikatz-
master\\Win32\\mimikatz.exe\""
"currentDirectory" :
"C:\\Users\\admin\\Downloads\\mimikatz-master\\mimikatz-master\\Win32\\"
"user" : "DESKTOP-C7MCHC1\\admin"
"logonGuid" : "{e864df0a-33b6-6652-0bb0-010000000000}"
"logonId" : "0x1b00b"
"terminalSessionId" : "1"
"integrityLevel" : "High"
"hashes" :
"SHA256=2E8092205A2DED4B07E9D10D0EC02EBA0FFCF1D370CAB88C5221A749915F678A"
```

- Rename the previous step to "SHA-256 Regex" and save.
- Make sure the workflow uses the extracted hash value for API calls.



Name: Virustotal_v3_1

Delay:

Authentication: Latest 1.1.0 Auth for Vir...

Find Actions: Get a hash report

Parameters

Authentication fields are hidden

Id: $sha256_regex.group_0.#

Headers:
Content-Type=application/json
Accept=application/json

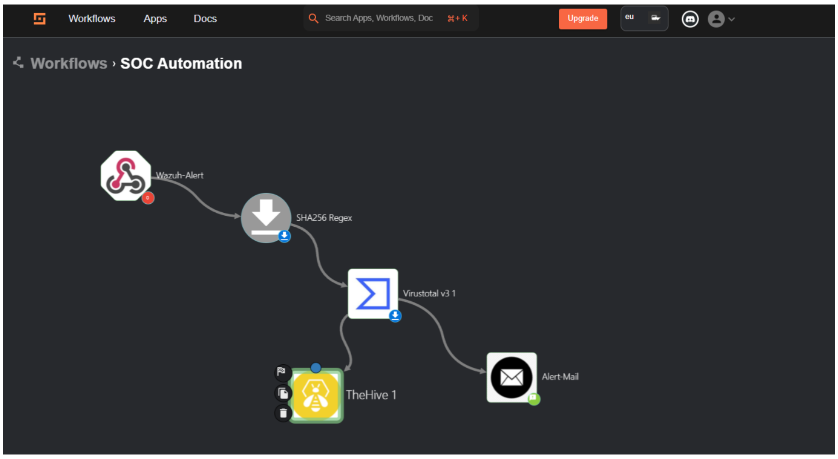
The Hive Integration with Shuffle

Access The Hive in Shuffle:

- Go to the application tab in Shuffle.
- Search for "The Hive" and drag "The Hive Five" into your workflow.

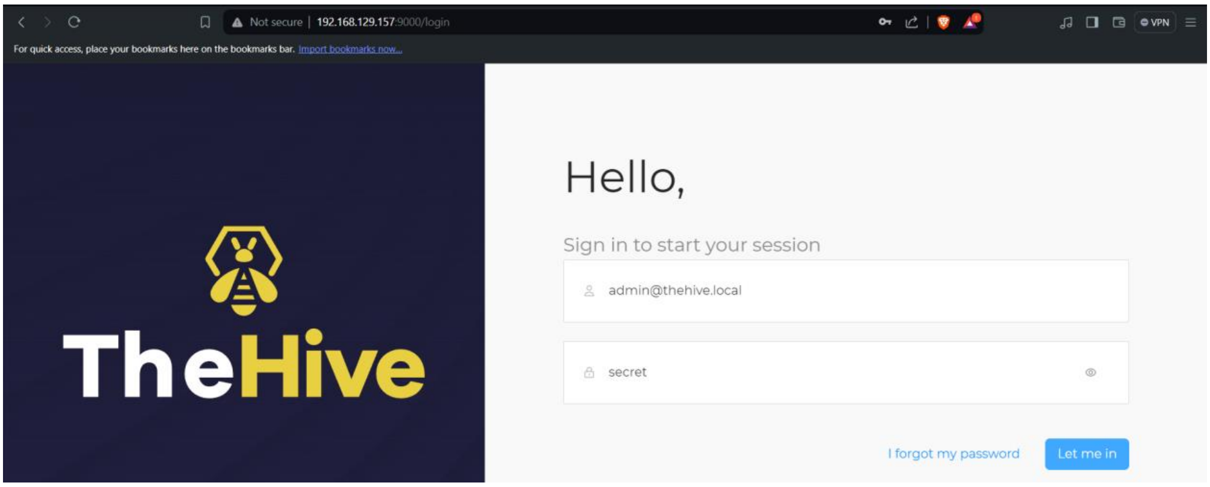
Refresh Workflow Actions:

- If only one action appears, refresh the workflow to load additional actions.



Log into The Hive using default credentials:

- Username: `admin`
- Password: `Secret`



Not secure | 192.168.129.157:9000/login
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
TheHive

Hello,

Sign in to start your session

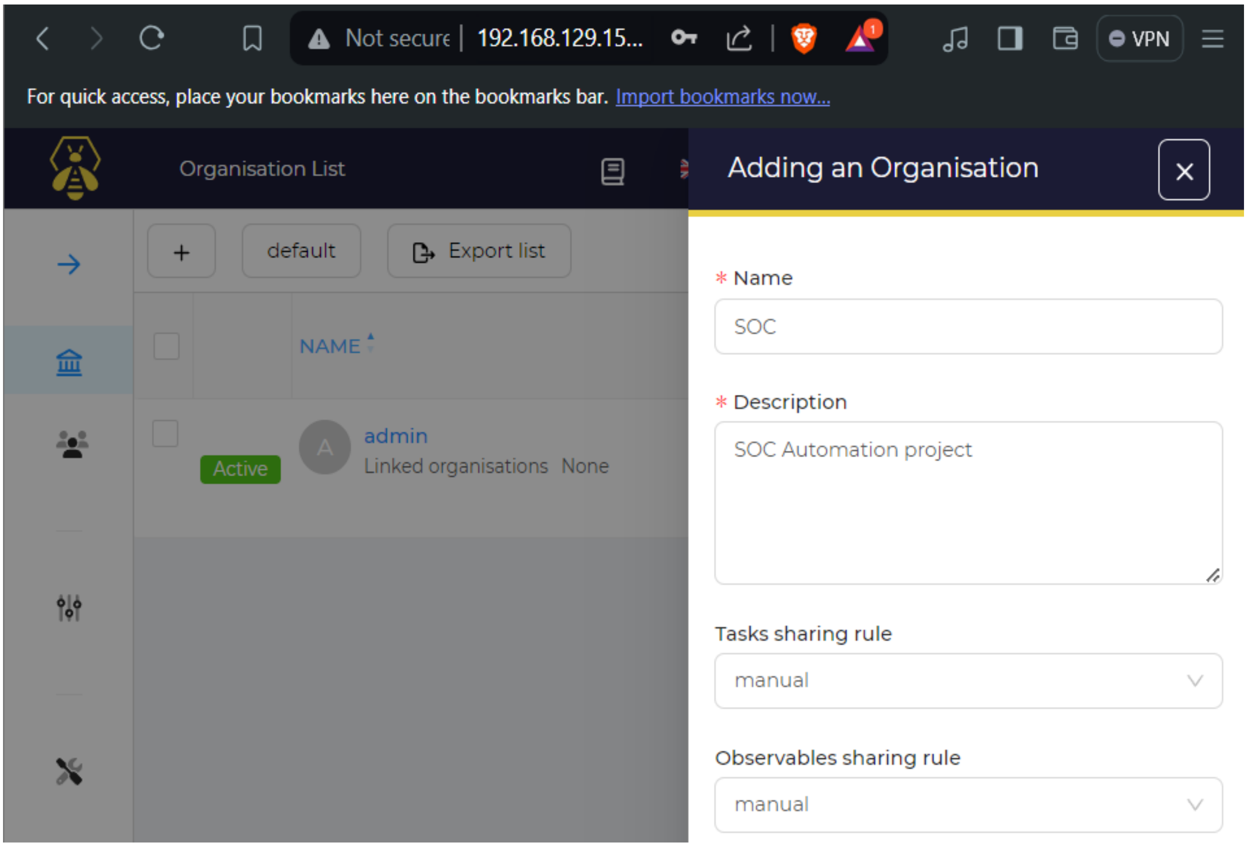
admin@thehive.local

secret

I forgot my password
Let me in

Create a New Organization:

- Click the plus (+) button at the top left corner.
- Enter:
  - Organization Name: `SOC`
  - Description: `SOC Automation Project`
- Confirm the creation of the organization.



Not secure | 192.168.129.15...
VPN
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Organisation List
+
default
Export list
NAME
Active
A
admin
Linked organisations None

Adding an Organisation

* Name

SOC

* Description

SOC Automation project

Tasks sharing rule

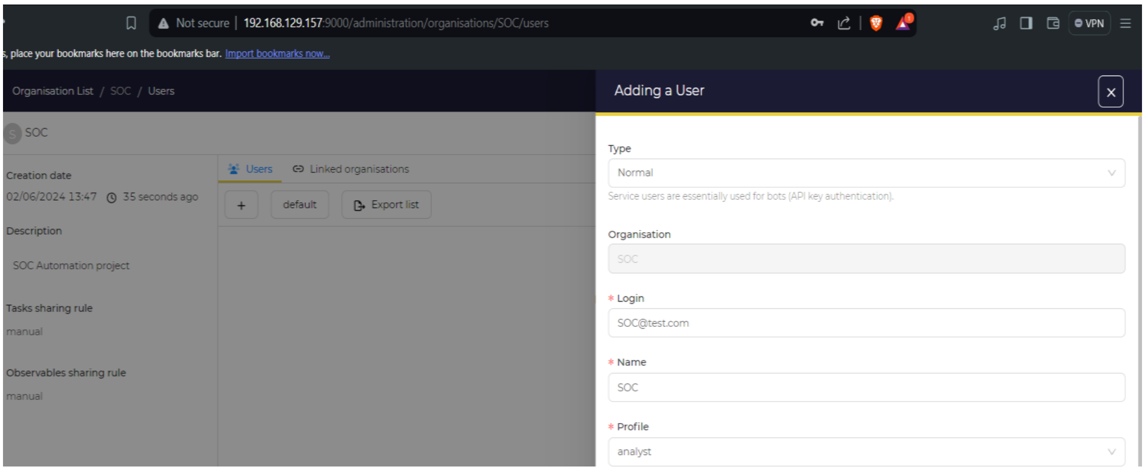
manual

Observables sharing rule

manual

Add Users to the Organization:

- Click into the new organization (SOC).
- Since it shows "no users found," proceed to add users:
  - **User 1:**
    - Type: Normal
    - Login: SOCtest.com
    - Name: SOC
    - Profile: Analyst
    - Save the user.



Not secure | 192.168.129.157:9000/administration/organisations/SOC/users

s, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Organisation List / SOC / Users

SOC

Creation date
02/06/2024 13:47 35 seconds ago

Description
SOC Automation project

Tasks sharing rule
manual

Observables sharing rule
manual

Adding a User

Type
Normal
Service users are essentially used for bots (API key authentication).

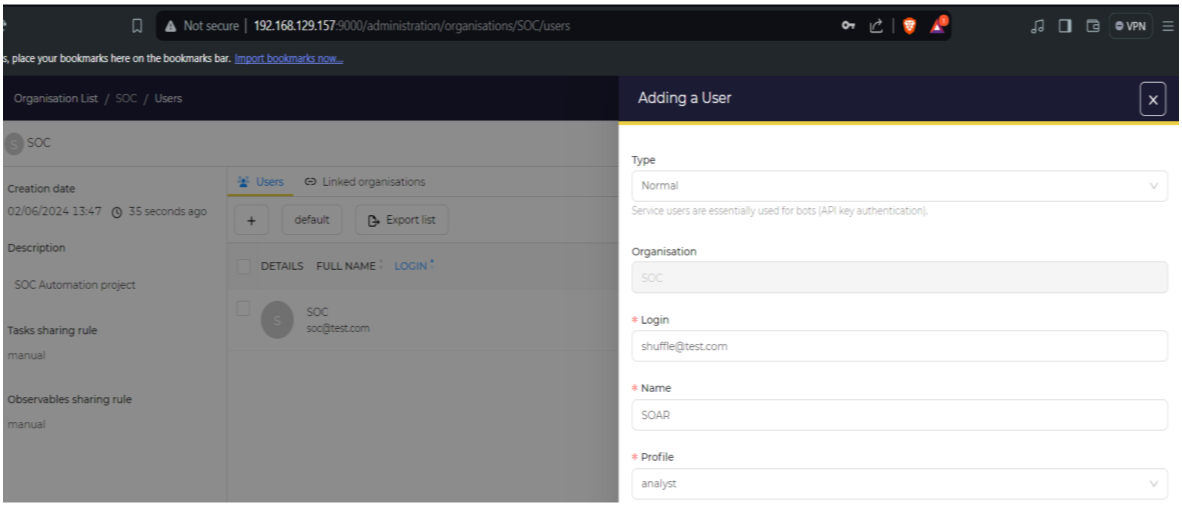
Organisation
SOC

* Login
SOC@test.com

* Name
SOC

* Profile
analyst

  - **User 2:**
    - Type: Normal
    - Login: shuffle@test.com
    - Name: SOAR
    - Profile: Analyst (for demo purposes).
    - Confirm the user.



Not secure | 192.168.129.157:9000/administration/organisations/SOC/users

s, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Organisation List / SOC / Users

SOC

Creation date
02/06/2024 13:47 35 seconds ago

Description
SOC Automation project

Tasks sharing rule
manual

Observables sharing rule
manual

DETAILS	FULL NAME	LOGIN
	SOC soc@test.com	

Adding a User

Type
Normal
Service users are essentially used for bots (API key authentication).

Organisation
SOC

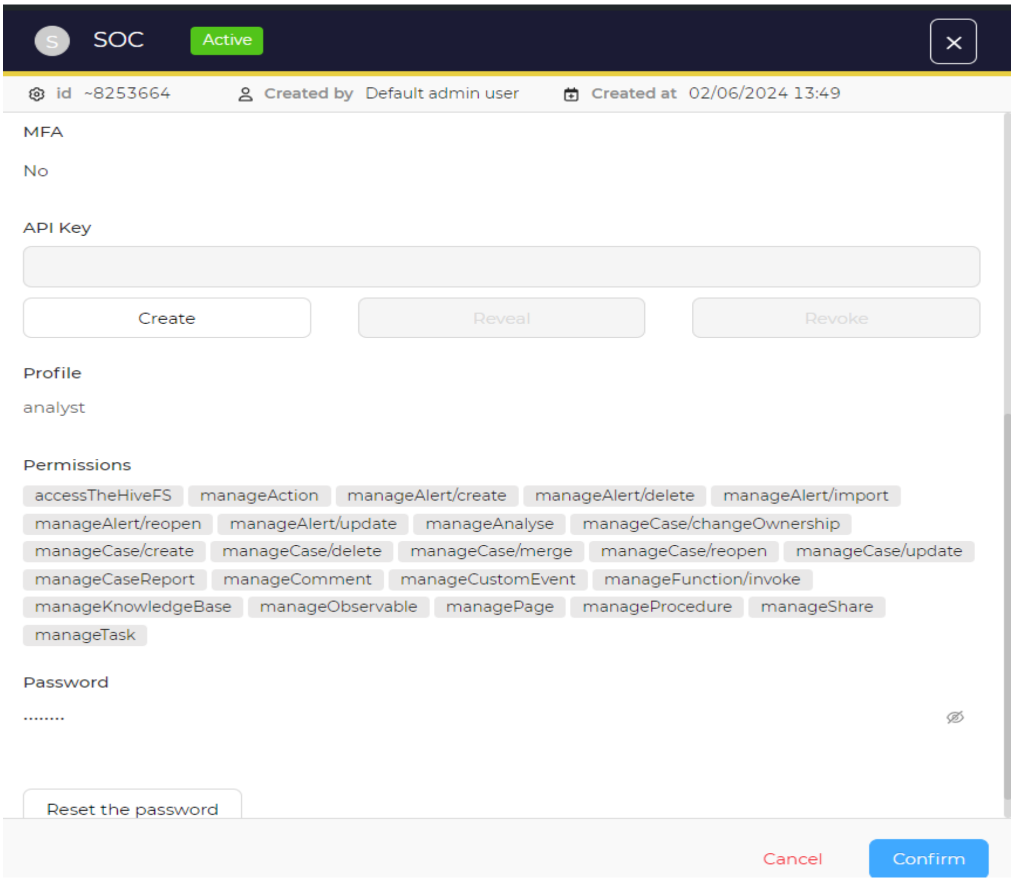
* Login
shuffle@test.com

* Name
SOAR

* Profile
analyst

Set Passwords and Generate API Key:

- For SOC, highlight the account, select preview, scroll down, set a new password, and hit confirm.



MFA

No

API Key

Profile

analyst

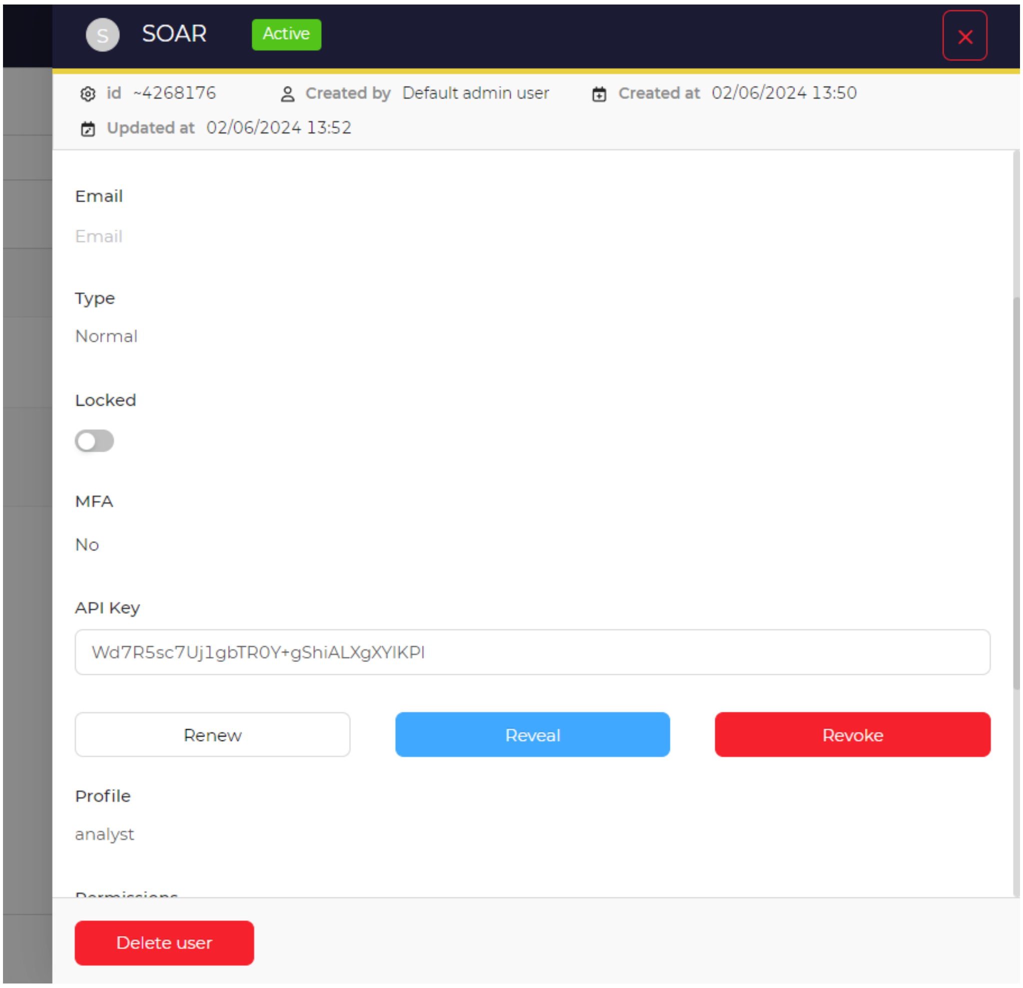
Permissions

accessTheHiveFS, manageAction, manageAlert/create, manageAlert/delete, manageAlert/import, manageAlert/reopen, manageAlert/update, manageAnalyse, manageCase/changeOwnership, manageCase/create, manageCase/delete, manageCase/merge, manageCase/reopen, manageCase/update, manageCaseReport, manageComment, manageCustomEvent, manageFunction/invoke, manageKnowledgeBase, manageObservable, managePage, manageProcedure, manageShare, manageTask

Password

········

- For the SOAR user, select preview and create an API key.



SOAR Active

id ~4268176 Created by Default admin user Created at 02/06/2024 13:50

Updated at 02/06/2024 13:52

Email

Email

Type

Normal

Locked

MFA

No

API Key

Wd7R5sc7Uj1gbTR0Y+gShiALXgXYIKPl

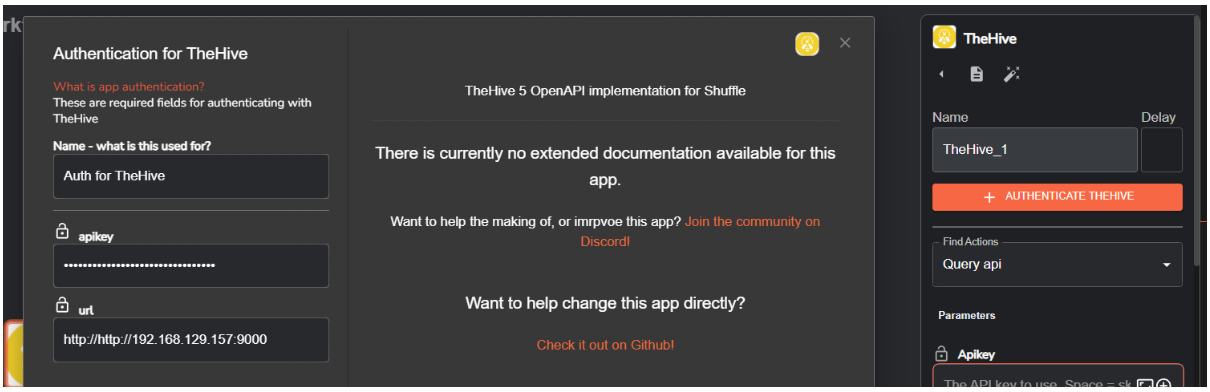
Profile

analyst

- Important: Copy the API key and store it securely for future use.

Authenticate The Hive in Shuffle:

- In Shuffle, click the plus (+) button next to authenticate.
- Paste the API key into the Hive authentication field.
- Enter the public IP of your Hive instance and the port number (e.g., 191.168.129.157:9000).
- Hit submit.



Authentication for TheHive

What is app authentication?
These are required fields for authenticating with TheHive

Name - what is this used for?
Auth for TheHive

apikey
••••••••••••••••••••••••••••••••

url
http://http://192.168.129.157:9000

TheHive 5 OpenAPI implementation for Shuffle

There is currently no extended documentation available for this app.

Want to help the making of, or imrpvoe this app? Join the community on Discord!

Want to help change this app directly?

Check it out on Github!

TheHive

Name: TheHive_1

Delay

Find Actions: Query api

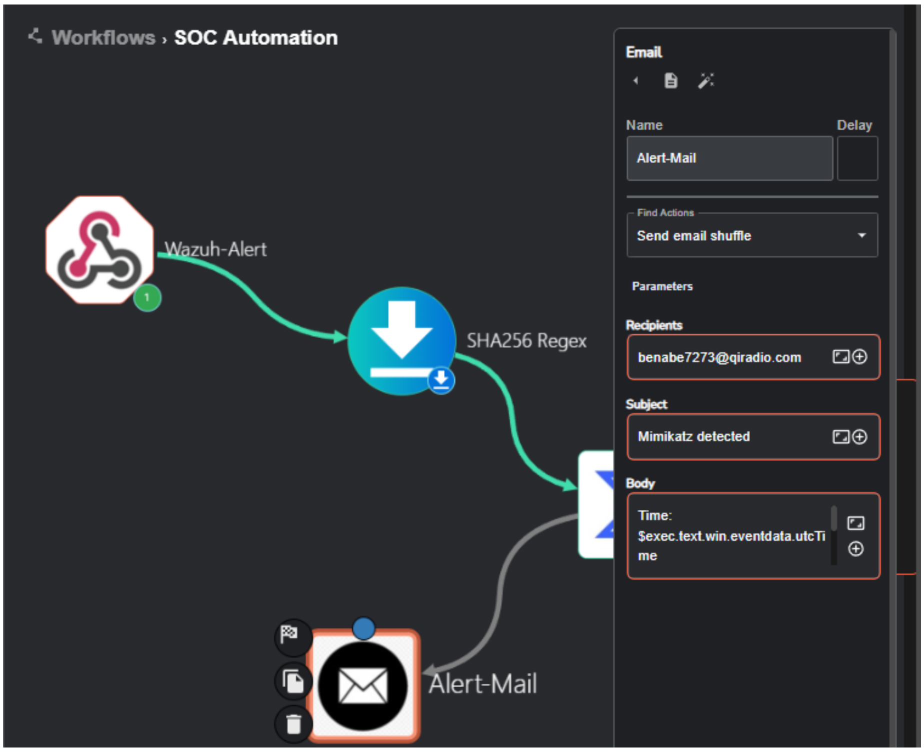
Parameters

Apikey

The API key to use. Space = sk

Send Email to Analyst

- In Shuffle, click on "Apps" at the bottom left and drag the email application into your workflow.
- Connect the VirusTotal node over to the email application.
- Configure the email:
    - Recipient: Enter your disposable email from SquareX.
    - Subject: Set to "Mimikatz detected."
    - Body: Add relevant details like the time, title, and host where the detection occurred.



Name: Alert-Mail

Delay:

Find Actions: Send email shuffle

Parameters

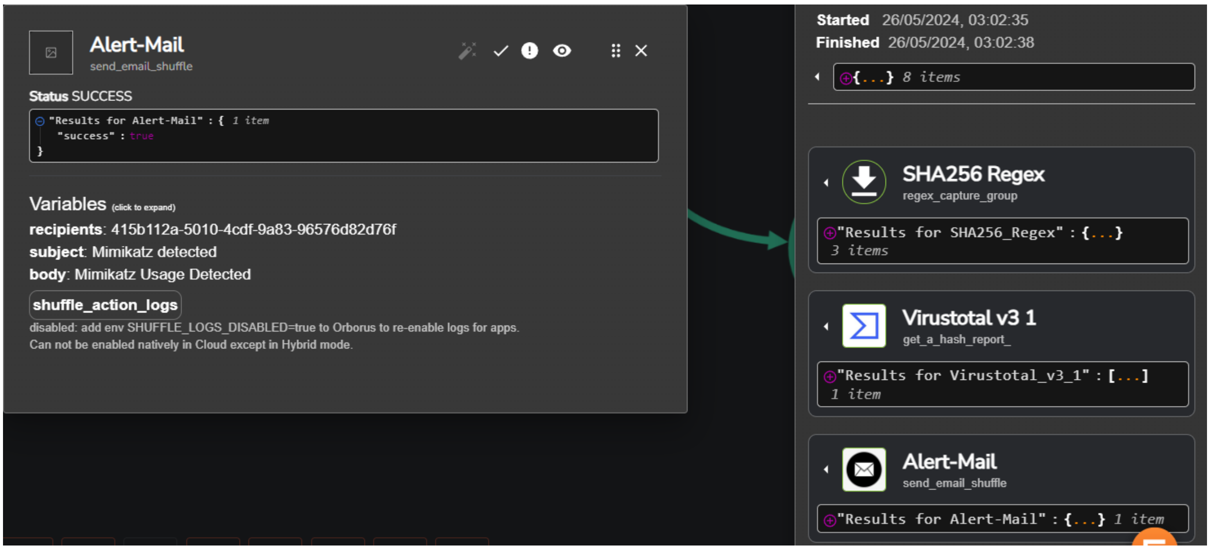
Recipients: benabe7273@qiradio.com

Subject: Mimikatz detected

Body: Time: $exec.text.win.eventdata.utcTime

Verifying Working of flowchart:

Run the flowchart process and then click on email to see if the email was sent successfully or not to the security analyst.



Alert-Mail
send_email_shuffle

Status SUCCESS

```
"Results for Alert-Mail" : { 1 item
  "success" : true
}
```

Variables (click to expand)

recipients: 415b112a-5010-4cdf-9a83-96576d82d76f

subject: Mimikatz detected

body: Mimikatz Usage Detected

shuffle_action_logs

disabled: add env SHUFFLE_LOGS_DISABLED=true to Orborus to re-enable logs for apps.
Can not be enabled natively in Cloud except in Hybrid mode.

Started 26/05/2024, 03:02:35
Finished 26/05/2024, 03:02:38

```
{...} 8 items
```

SHA256 Regex
regex_capture_group

```
"Results for SHA256_Regex" : {...}
3 items
```

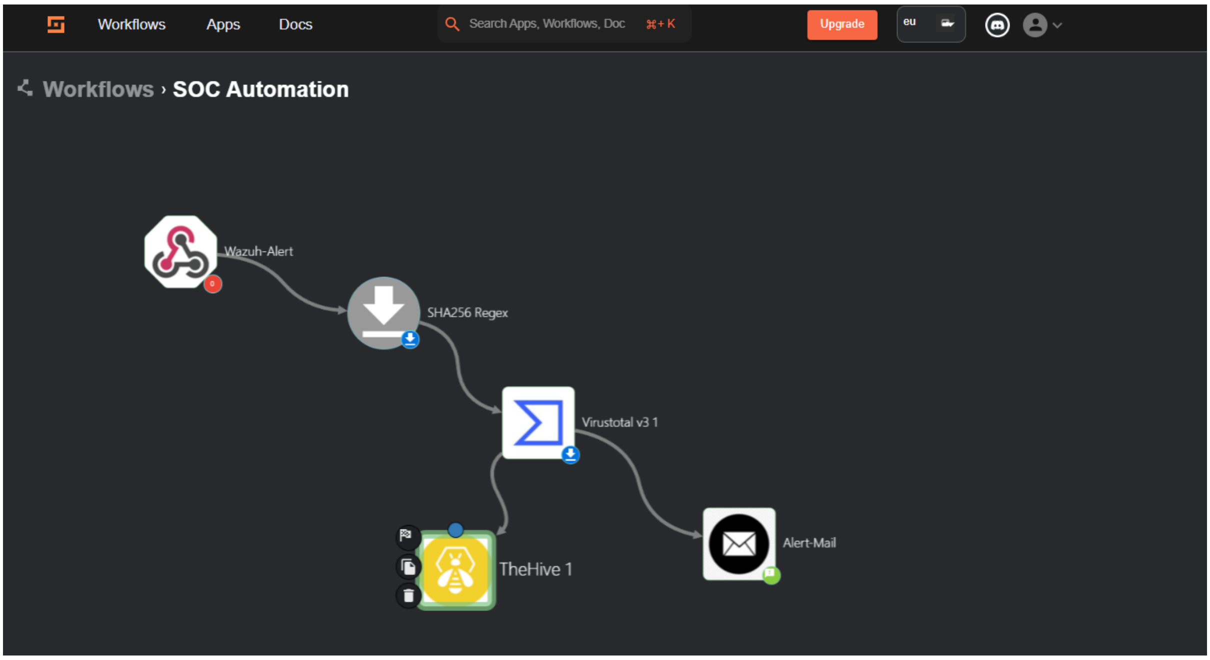
Virustotal v3 1
get_a_hash_report_

```
"Results for Virustotal_v3_1" : [...]
1 item
```

Alert-Mail
send_email_shuffle

```
"Results for Alert-Mail" : {...} 1 item
```

Final Flowchart:



Workflows
Apps
Docs
Search Apps, Workflows, Doc
⌘+K
Upgrade
eu
Workflows › SOC Automation
Wazuh-Alert
SHA256 Regex
Virustotal v3 1
TheHive 1
Alert-Mail