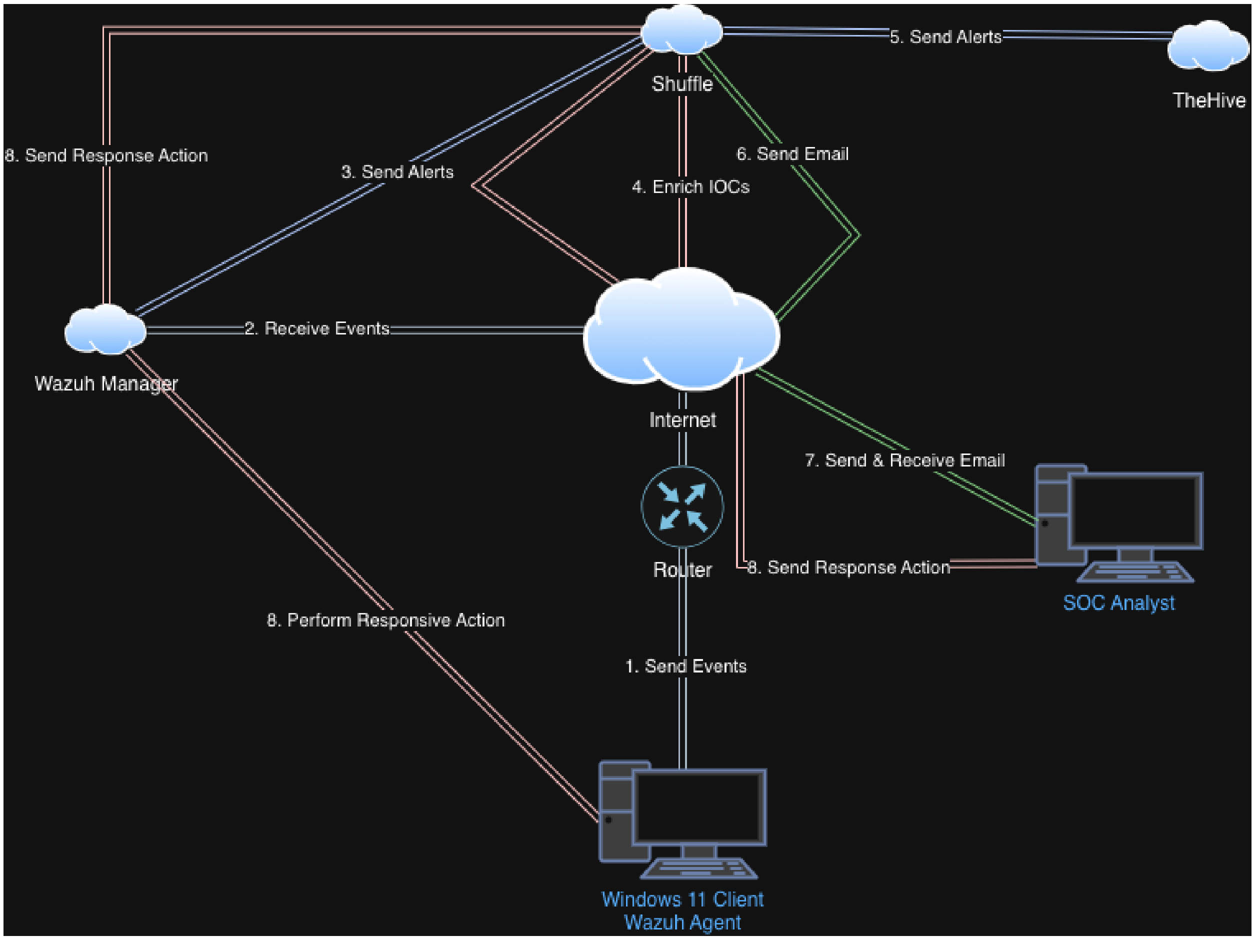
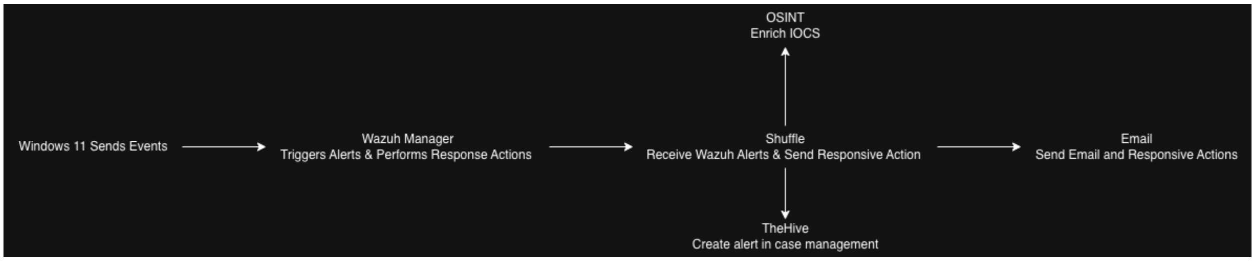
SOC Automation Project: Simulated Mimikatz Credential Dumping

High-Level Architecture Diagram:




OSINT
Enrich IOCS
Windows 11 Sends Events
Wazuh Manager
Triggers Alerts & Performs Response Actions
Shuffle
Receive Wazuh Alerts & Send Responsive Action
Email
Send Email and Responsive Actions
TheHive
Create alert in case management

Tools Used

VirtualBox VM – Client machine running Windows 10

Wazuh – Open Source XDR and SIEM capabilities in onw solution

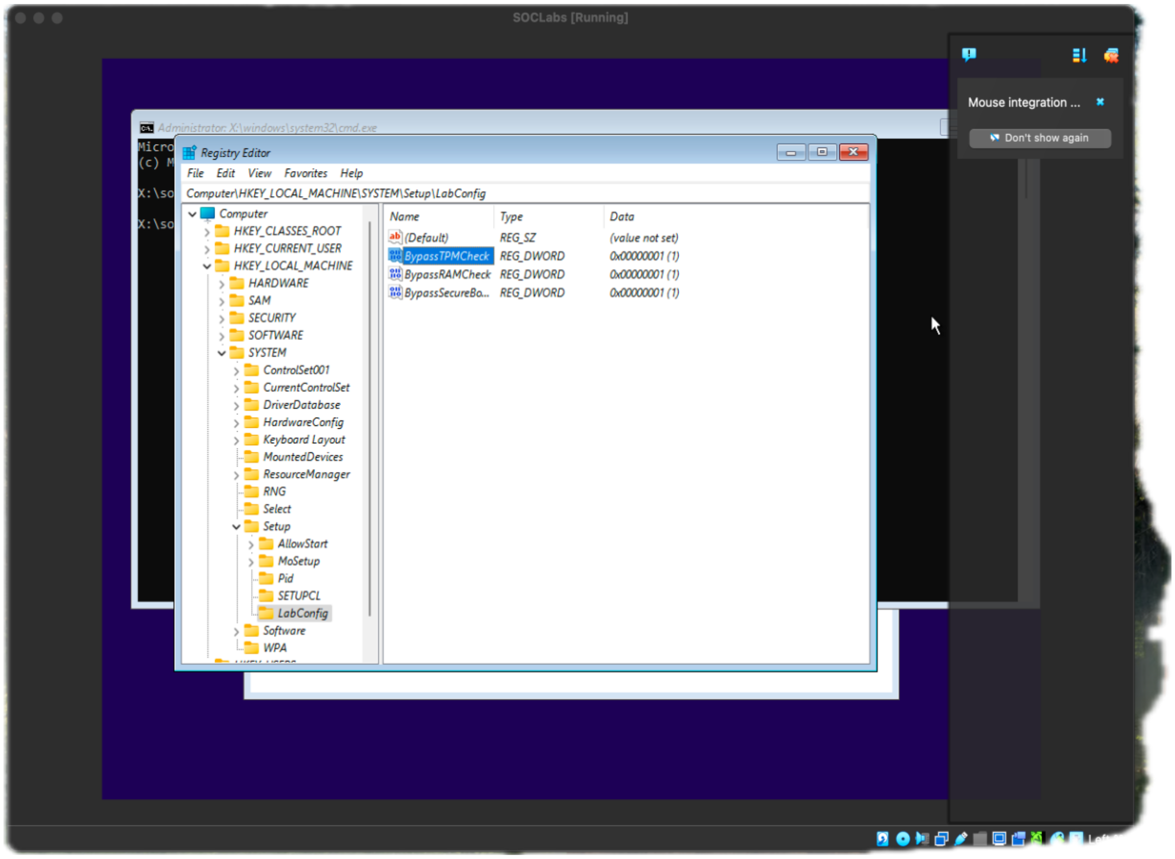
The Hive – Case Management System

Ubuntu 22.04 - Utilized for The Hive and Wazuh

Sysmon (Enhanced Process Monitoring) - Sysmon logs detailed information about process creations, including the parent process, command line arguments, and hashes, allowing for better visibility into potentially malicious activities. Downloaded on the Windows 10 Client.

Shuffle (SOAR) – Used to create automated workflows by integrating webhooks together.

Description: Downloading windows 10 onto client. To bypass TPM and allow installation, configured setup.



SOCLabs [Running]

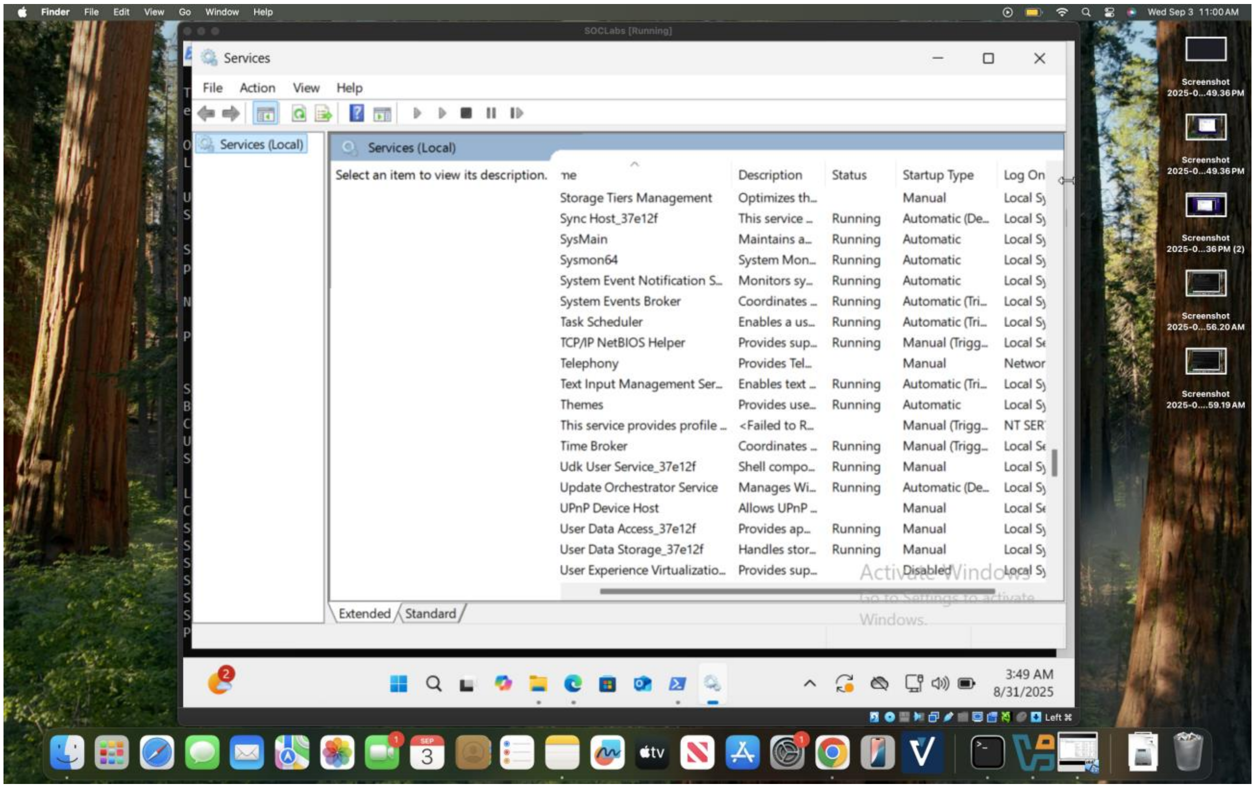
Administrator: X:\windows\system32\cmd.exe

Registry Editor

Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\LabConfig

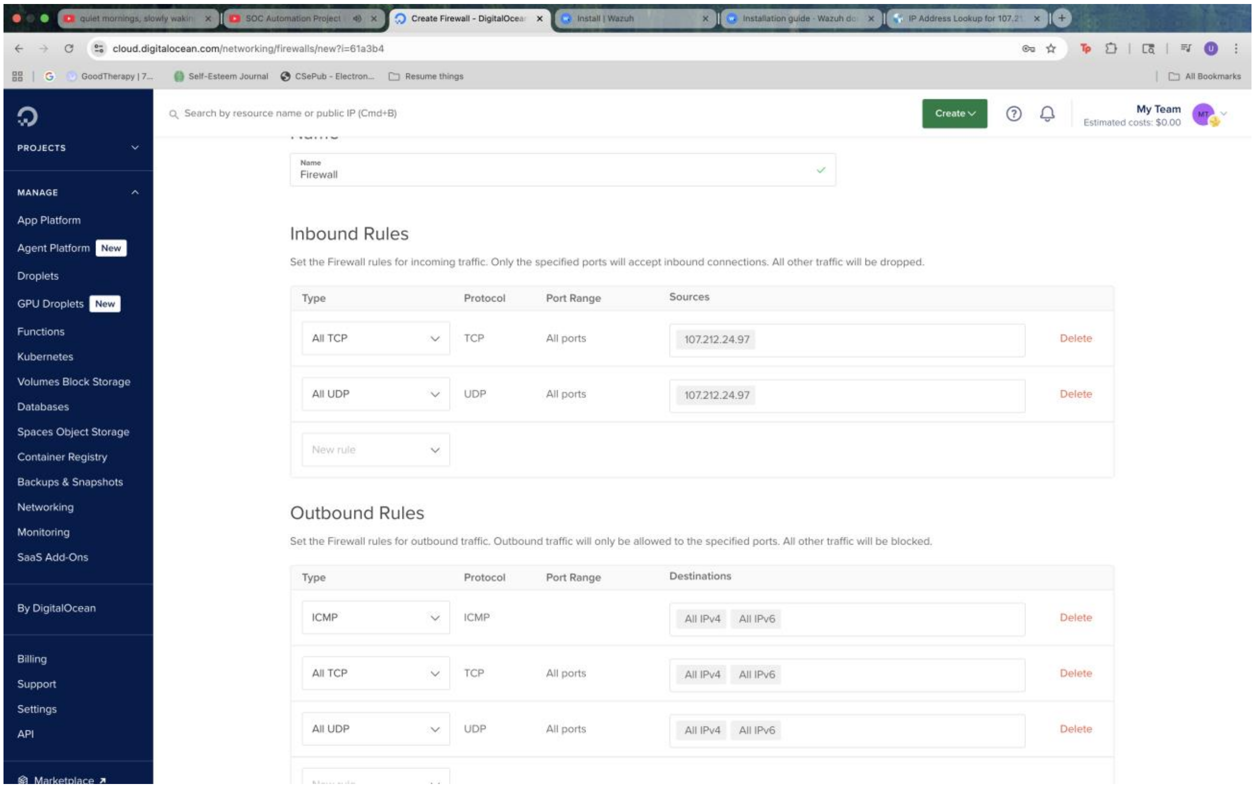
Name	Type	Data
(Default)	REG_SZ	(value not set)
BypassTPMCheck	REG_DWORD	0x00000001 (1)
BypassRAMCheck	REG_DWORD	0x00000001 (1)
BypassSecureBo...	REG_DWORD	0x00000001 (1)

Description: Downloading Sysmon onto client and starting services.


Finder File Edit View Go Window Help
Wed Sep 3 11:00 AM
SOCLabs [Running]
Services
File Action View Help
Services (Local)
Services (Local)
Select an item to view its description.
Extended
Standard
Activate Windows
Go to Settings to activate Windows.
3:49 AM
8/31/2025
Screenshot 2025-0...49.36 PM
Screenshot 2025-0...49.36 PM
Screenshot 2025-0...36 PM (2)
Screenshot 2025-0...56.20 AM
Screenshot 2025-0....59.19 AM

ne	Description	Status	Startup Type	Log On
Storage Tiers Management	Optimizes th...		Manual	Local Sy
Sync Host_37e12f	This service ...	Running	Automatic (De...	Local Sy
SysMain	Maintains a...	Running	Automatic	Local Sy
Sysmon64	System Mon...	Running	Automatic	Local Sy
System Event Notification S...	Monitors sy...	Running	Automatic	Local Sy
System Events Broker	Coordinates ...	Running	Automatic (Tri...	Local Sy
Task Scheduler	Enables a us...	Running	Automatic (Tri...	Local Sy
TCP/IP NetBIOS Helper	Provides sup...	Running	Manual (Trigg...	Local Se
Telephony	Provides Tel...		Manual	Networ
Text Input Management Ser...	Enables text ...	Running	Automatic (Tri...	Local Sy
Themes	Provides use...	Running	Automatic	Local Sy
This service provides profile ...	<Failed to R...		Manual (Trigg...	NT SER
Time Broker	Coordinates ...	Running	Manual (Trigg...	Local Se
Udk User Service_37e12f	Shell compo...	Running	Manual	Local Sy
Update Orchestrator Service	Manages Wi...	Running	Automatic (De...	Local Sy
UPnP Device Host	Allows UPnP ...		Manual	Local Se
User Data Access_37e12f	Provides ap...	Running	Manual	Local Sy
User Data Storage_37e12f	Handles stor...	Running	Manual	Local Sy
User Experience Virtualizatio...	Provides sup...		Disabled	Local Sy

Description: Creating Droplets on Digital Ocean and setting up firewall rules for both The Hive and Wazuh.



Name: Firewall

Inbound Rules

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

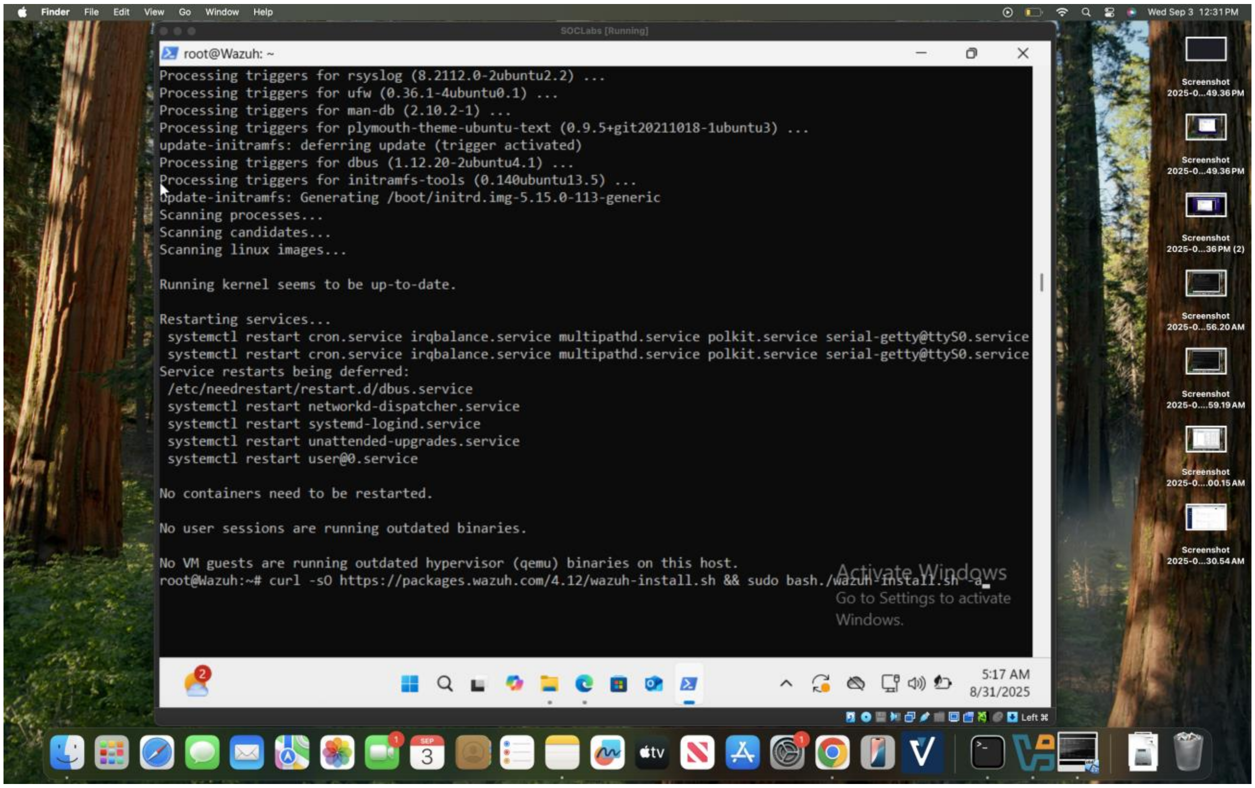
Type	Protocol	Port Range	Sources	
All TCP	TCP	All ports	107.212.24.97	Delete
All UDP	UDP	All ports	107.212.24.97	Delete
New rule				

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.

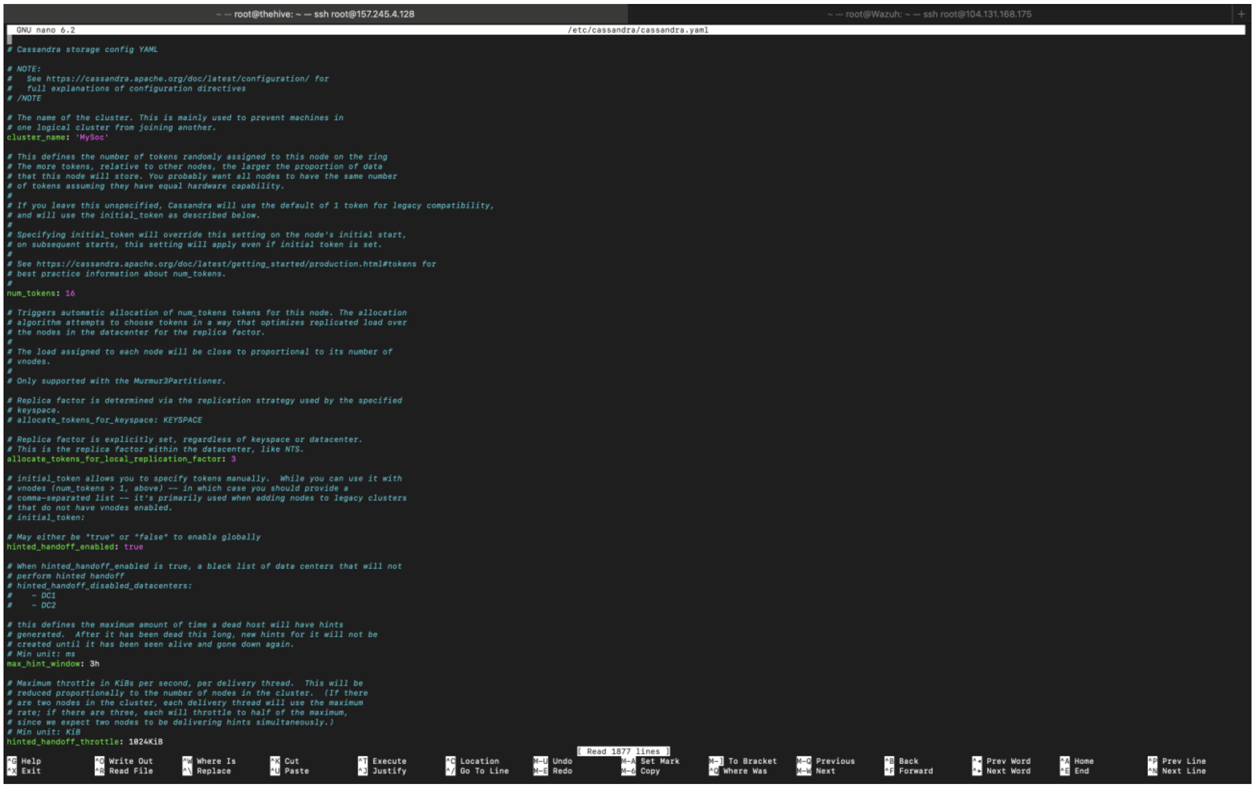
Type	Protocol	Port Range	Destinations	
ICMP	ICMP		All IPv4 All IPv6	Delete
All TCP	TCP	All ports	All IPv4 All IPv6	Delete
All UDP	UDP	All ports	All IPv4 All IPv6	Delete

Description: Installing Wazuh and setting up for The Hive.



```
Processing triggers for rsyslog (8.2112.0-2ubuntu2.2) ...
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for plymouth-theme-ubuntu-text (0.9.5+git20211018-1ubuntu3) ...
update-initramfs: deferring update (trigger activated)
Processing triggers for dbus (1.12.20-2ubuntu4.1) ...
Processing triggers for initramfs-tools (0.140ubuntu13.5) ...
update-initramfs: Generating /boot/initrd.img-5.15.0-113-generic
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
 systemctl restart cron.service irqbalance.service multipathd.service polkit.service serial-getty@ttyS0.service
 systemctl restart cron.service irqbalance.service multipathd.service polkit.service serial-getty@ttyS0.service
Service restarts being deferred:
 /etc/needrestart/restart.d/dbus.service
 systemctl restart networkd-dispatcher.service
 systemctl restart systemd-logind.service
 systemctl restart unattended-upgrades.service
 systemctl restart user@0.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@Wazuh:~# curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash./wazuh-install.sh -a
```

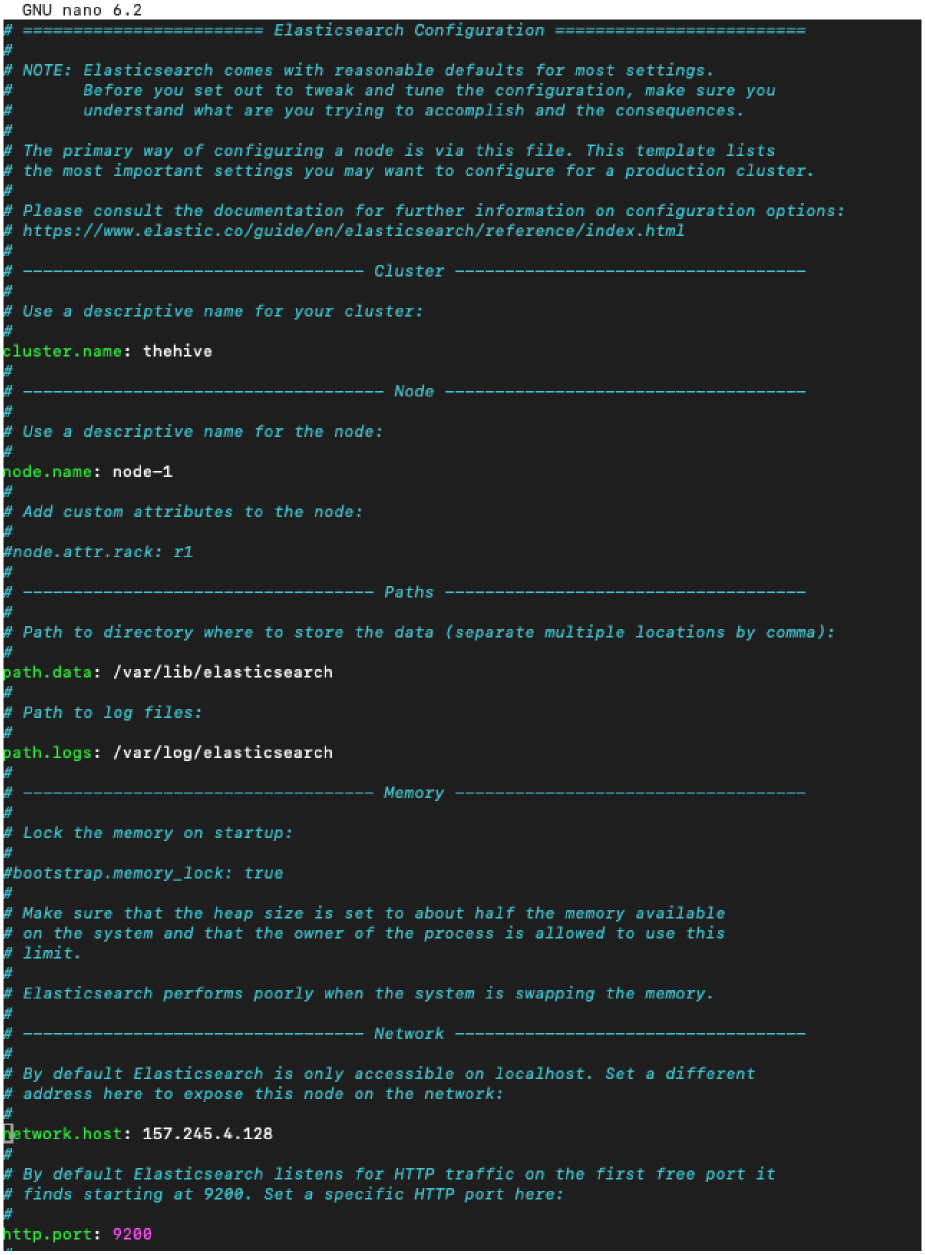
Description: Configuring Cassandra: changing listen, RPC address, and seed address to public IP of The Hive.



~ — root@thehive: ~ — ssh root@157.245.4.128
~ — root@Wazuh: ~ — ssh root@104.131.168.175

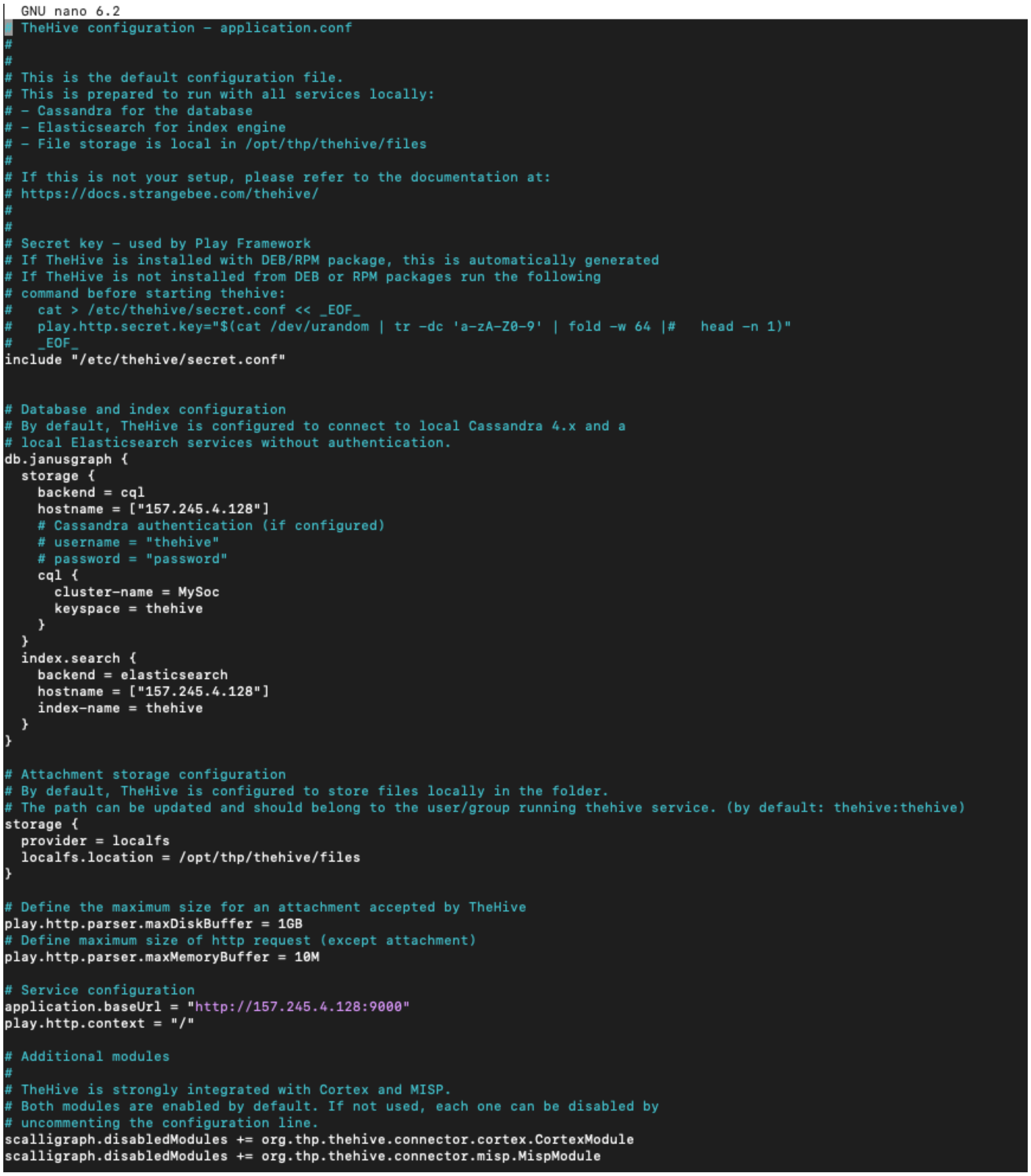
```
  GNU nano 6.2                                   /etc/cassandra/cassandra.yaml

# Cassandra storage config YAML

# NOTE:
#   See https://cassandra.apache.org/doc/latest/configuration/ for
#   full explanations of configuration directives
# /NOTE

# The name of the cluster. This is mainly used to prevent machines in
# one logical cluster from joining another.
cluster_name: 'MySoc'

# This defines the number of tokens randomly assigned to this node on the ring
# The more tokens, relative to other nodes, the larger the proportion of data
# that this node will store. You probably want all nodes to have the same number
# of tokens assuming they have equal hardware capability.
#
# If you leave this unspecified, Cassandra will use the default of 1 token for legacy compatibility,
# and will use the initial_token as described below.
#
# Specifying initial_token will override this setting on the node's initial start,
# on subsequent starts, this setting will apply even if initial token is set.
#
# See https://cassandra.apache.org/doc/latest/getting_started/production.html#tokens for
# best practice information about num_tokens.
#
num_tokens: 16

# Triggers automatic allocation of num_tokens tokens for this node. The allocation
# algorithm attempts to choose tokens in a way that optimizes replicated load over
# the nodes in the datacenter for the replica factor.
#
# The load assigned to each node will be close to proportional to its number of
# vnodes.
#
# Only supported with the Murmur3Partitioner.

# Replica factor is determined via the replication strategy used by the specified
# keyspace.
# allocate_tokens_for_keyspace: KEYSPACE

# Replica factor is explicitly set, regardless of keyspace or datacenter.
# This is the replica factor within the datacenter, like NTS.
allocate_tokens_for_local_replication_factor: 3

# initial_token allows you to specify tokens manually.  While you can use it with
# vnodes (num_tokens > 1, above) -- in which case you should provide a
# comma-separated list -- it's primarily used when adding nodes to legacy clusters
# that do not have vnodes enabled.
# initial_token:

# May either be "true" or "false" to enable globally
hinted_handoff_enabled: true

# When hinted_handoff_enabled is true, a black list of data centers that will not
# perform hinted handoff
# hinted_handoff_disabled_datacenters:
#    - DC1
#    - DC2

# this defines the maximum amount of time a dead host will have hints
# generated.  After it has been dead this long, new hints for it will not be
# created until it has been seen alive and gone down again.
# Min unit: ms
max_hint_window: 3h

# Maximum throttle in KiBs per second, per delivery thread.  This will be
# reduced proportionally to the number of nodes in the cluster.  (If there
# are two nodes in the cluster, each delivery thread will use the maximum
# rate; if there are three, each will throttle to half of the maximum,
# since we expect two nodes to be delivering hints simultaneously.)
# Min unit: KiB
hinted_handoff_throttle: 1024KiB
                                             [ Read 1877 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket M-Q Previous  ^B Back       ^◂ Prev Word  ^A Home       ^P Prev Line
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was  M-W Next      ^F Forward    ^▸ Next Word  ^E End        ^N Next Line
```

Description: Updating Elasticsearch configuration by changing the network host to the Hive IP address, uncommenting and configuring the HTTP port, setting cluster.initial_master_nodes to node-1, and defining discovery seed hosts to support cluster scaling. Starting Elasticsearch and verifying that the service is running and accessible.



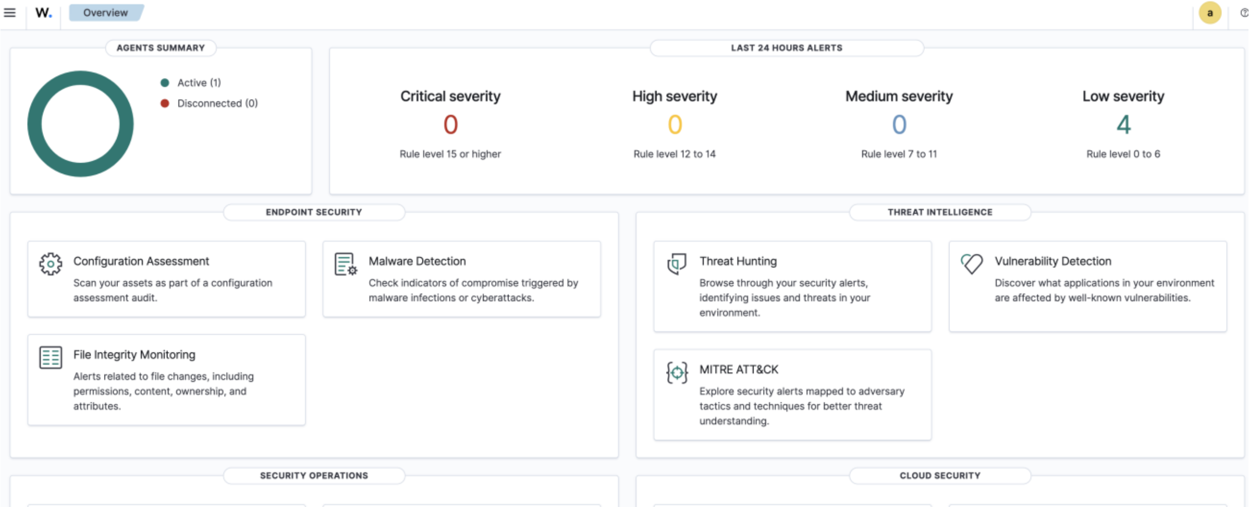
```
  GNU nano 6.2
# ======================== Elasticsearch Configuration =========================
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
#       Before you set out to tweak and tune the configuration, make sure you
#       understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluster.
#
# Please consult the documentation for further information on configuration options:
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: thehive
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
# ----------------------------------- Paths ------------------------------------
#
# Path to directory where to store the data (separate multiple locations by comma):
#
path.data: /var/lib/elasticsearch
#
# Path to log files:
#
path.logs: /var/log/elasticsearch
#
# ----------------------------------- Memory -----------------------------------
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 157.245.4.128
#
# 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
```

Description: Configuring TheHive by updating application.conf, changing the hostname to the Hive public IP address, updating the cluster name from Cassandra, setting the application base URL to the Hive public IP, and starting and enabling TheHive service.



```
  GNU nano 6.2
# TheHive configuration - application.conf
#
#
# This is the default configuration file.
# This is prepared to run with all services locally:
# - Cassandra for the database
# - Elasticsearch for index engine
# - File storage is local in /opt/thp/thehive/files
#
# If this is not your setup, please refer to the documentation at:
# https://docs.strangebee.com/thehive/
#
#
# Secret key - used by Play Framework
# If TheHive is installed with DEB/RPM package, this is automatically generated
# If TheHive is not installed from DEB or RPM packages run the following
# command before starting thehive:
#   cat > /etc/thehive/secret.conf << _EOF_
#   play.http.secret.key="$(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 64 |#   head -n 1)"
#   _EOF_
include "/etc/thehive/secret.conf"


# Database and index configuration
# 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 = ["157.245.4.128"]
    # Cassandra authentication (if configured)
    # username = "thehive"
    # password = "password"
    cql {
      cluster-name = MySoc
      keyspace = thehive
    }
  }
  index.search {
    backend = elasticsearch
    hostname = ["157.245.4.128"]
    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 default: thehive:thehive)
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://157.245.4.128:9000"
play.http.context = "/"

# Additional modules
#
# TheHive is strongly integrated with Cortex and MISP.
# Both modules are enabled by default. If not used, each one can be disabled by
# uncommenting the configuration line.
scalligraph.disabledModules += org.thp.thehive.connector.cortex.CortexModule
scalligraph.disabledModules += org.thp.thehive.connector.misp.MispModule
```

Description: Configuring Wazuh and integrating it with the virtual machine.



W. Overview

AGENTS SUMMARY

● Active (1)
● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	0	4
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

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

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

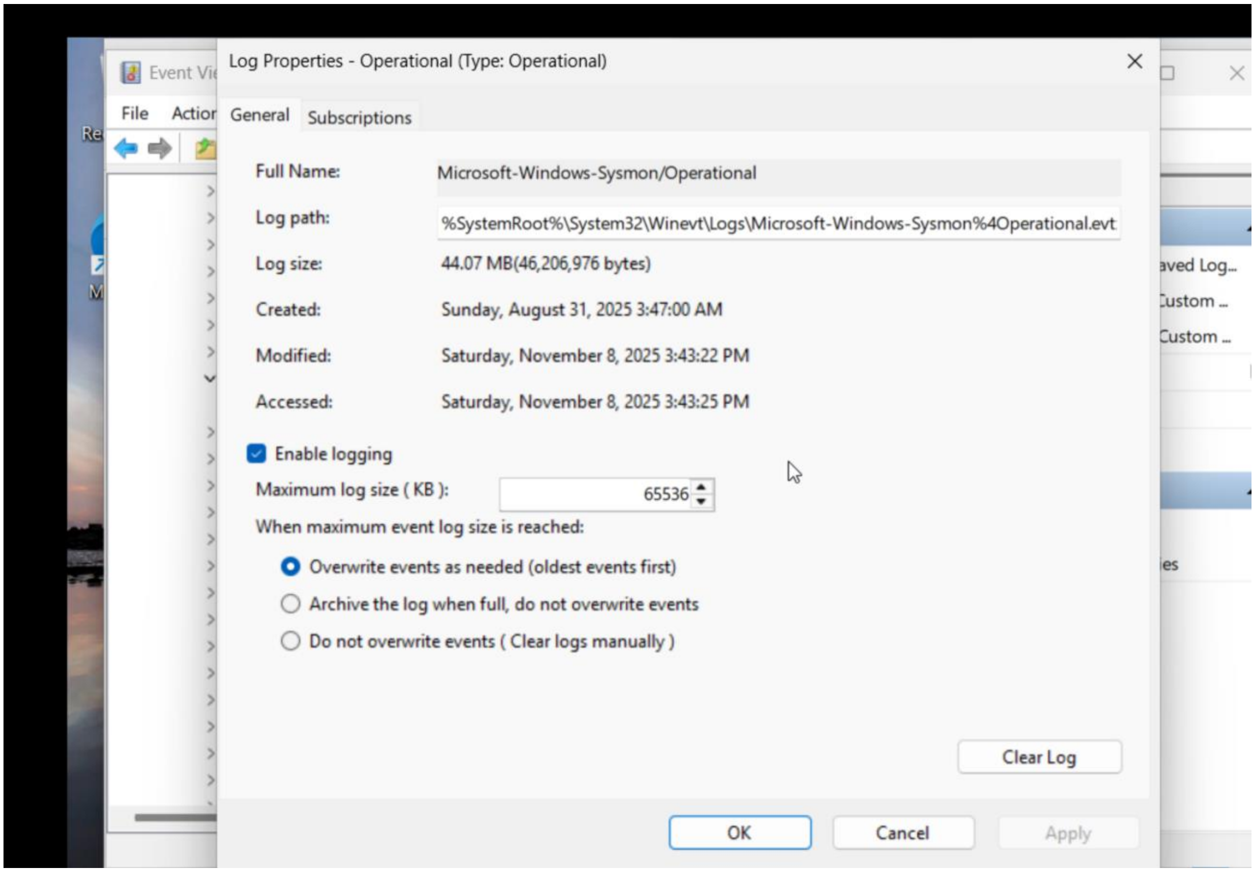
Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

CLOUD SECURITY

Description: Finding Sysmon event properties in Event Viewer to correctly map and name Event IDs in the OSSEC configuration file.



Log Properties - Operational (Type: Operational)

Full Name: Microsoft-Windows-Sysmon/Operational

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

Log size: 44.07 MB(46,206,976 bytes)

Created: Sunday, August 31, 2025 3:47:00 AM

Modified: Saturday, November 8, 2025 3:43:22 PM

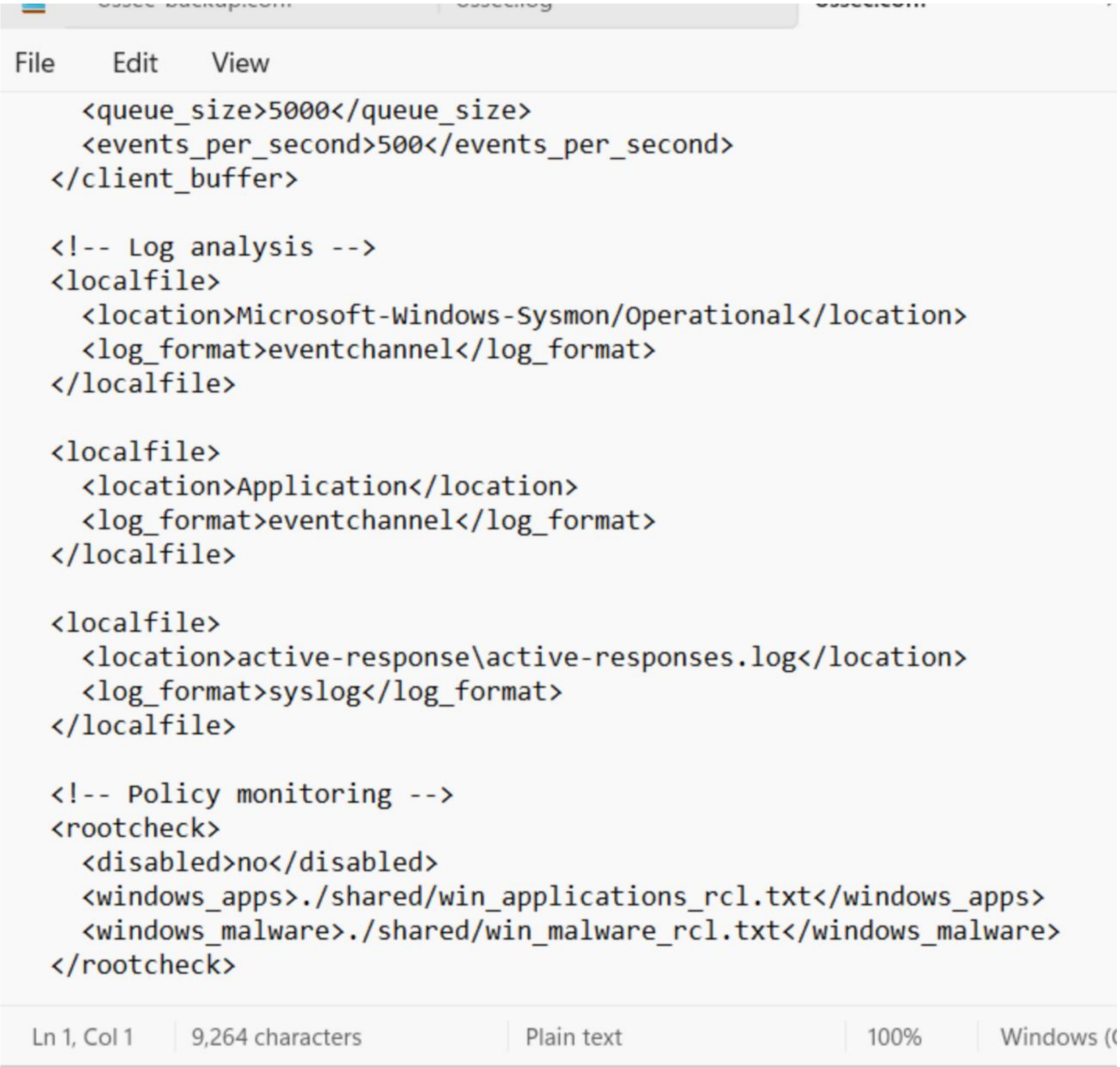
Accessed: Saturday, November 8, 2025 3:43:25 PM

☑ Enable logging

Maximum log size (KB): 65536

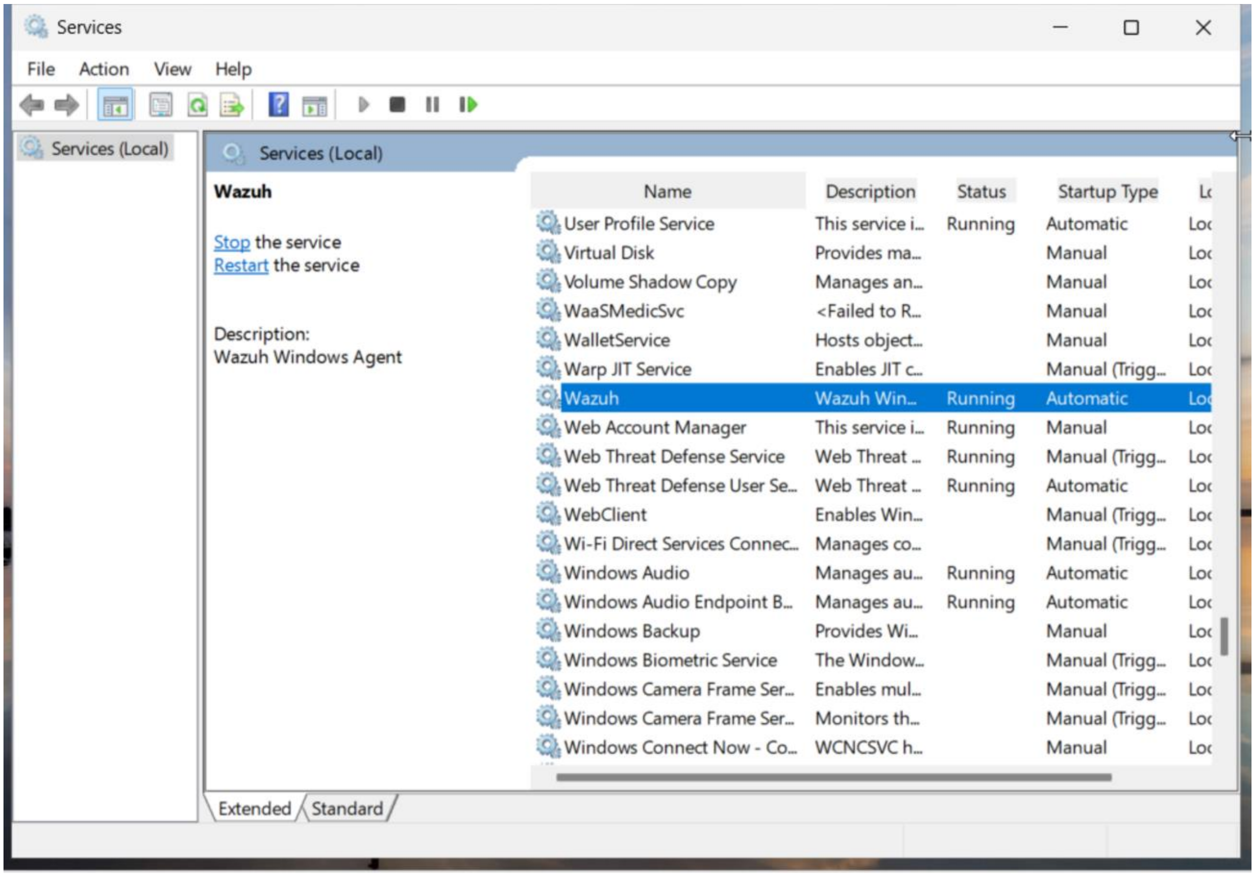
When maximum event log size is reached:

- ● Overwrite events as needed (oldest events first)
- ○ Archive the log when full, do not overwrite events
- ○ Do not overwrite events (Clear logs manually)



```
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

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

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

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

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
    <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
  </rootcheck>
```

Description: Restarting Wazuh services.



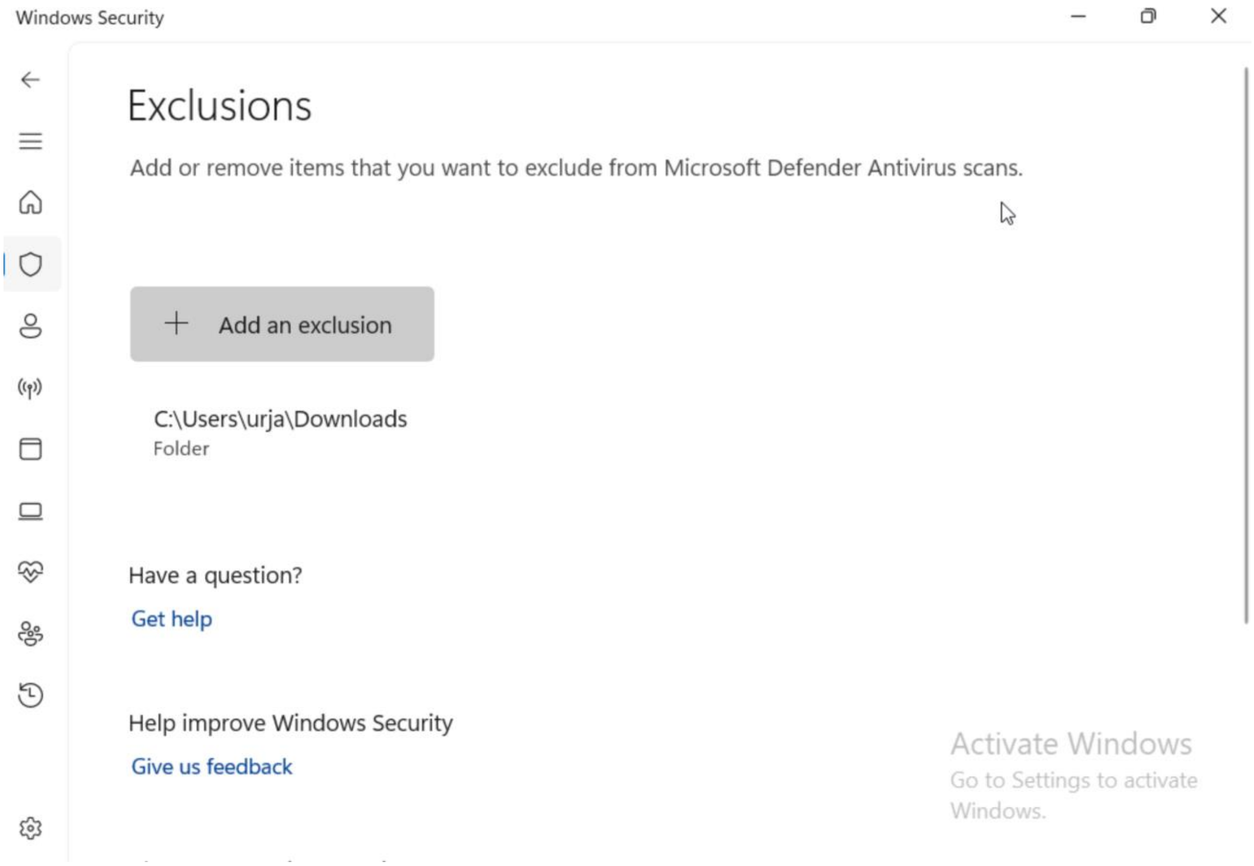
Wazuh

Stop the service
Restart the service

Description:
Wazuh Windows Agent

Name	Description	Status	Startup Type	Lo
User Profile Service	This service i...	Running	Automatic	Loc
Virtual Disk	Provides ma...		Manual	Loc
Volume Shadow Copy	Manages an...		Manual	Loc
WaaSMedicSvc	<Failed to R...		Manual	Loc
WalletService	Hosts object...		Manual	Loc
Warp JIT Service	Enables JIT c...		Manual (Trigg...	Loc
Wazuh	Wazuh Win...	Running	Automatic	Loc
Web Account Manager	This service i...	Running	Manual	Loc
Web Threat Defense Service	Web Threat ...	Running	Manual (Trigg...	Loc
Web Threat Defense User Se...	Web Threat ...	Running	Automatic	Loc
WebClient	Enables Win...		Manual (Trigg...	Loc
Wi-Fi Direct Services Connec...	Manages co...		Manual (Trigg...	Loc
Windows Audio	Manages au...	Running	Automatic	Loc
Windows Audio Endpoint B...	Manages au...	Running	Automatic	Loc
Windows Backup	Provides Wi...		Manual	Loc
Windows Biometric Service	The Window...		Manual (Trigg...	Loc
Windows Camera Frame Ser...	Enables mul...		Manual (Trigg...	Loc
Windows Camera Frame Ser...	Monitors th...		Manual (Trigg...	Loc
Windows Connect Now - Co...	WCNCSVC h...		Manual	Loc

Description: Excluding downloads folder in exclusions on security settings of VM to be able to download Mimikatz.



Windows Security

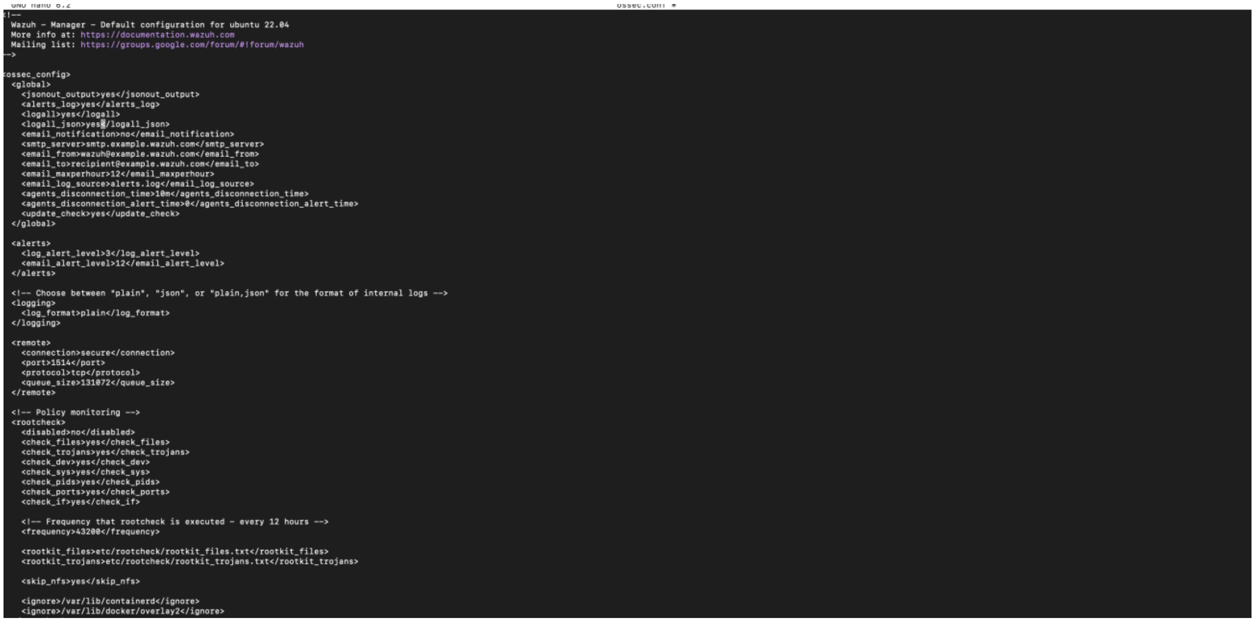
Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

C:\Users\urja\Downloads
Folder

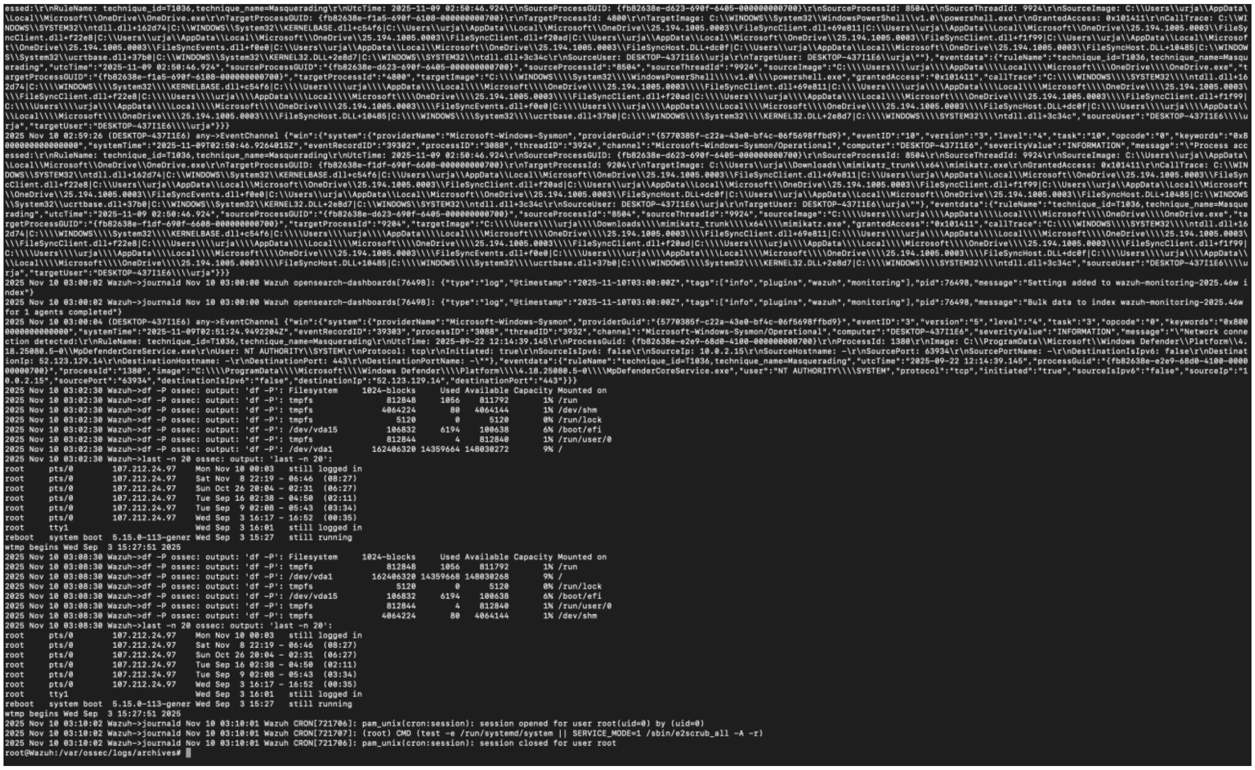
Have a question?
Get help
Help improve Windows Security
Give us feedback
Activate Windows
Go to Settings to activate Windows.

Description: Configuring the Wazuh manager by updating the OSSEC configuration file, setting logall to yes, and restarting services. Enabling logall capabilities is allowing Wazuh to log all events under the archive.



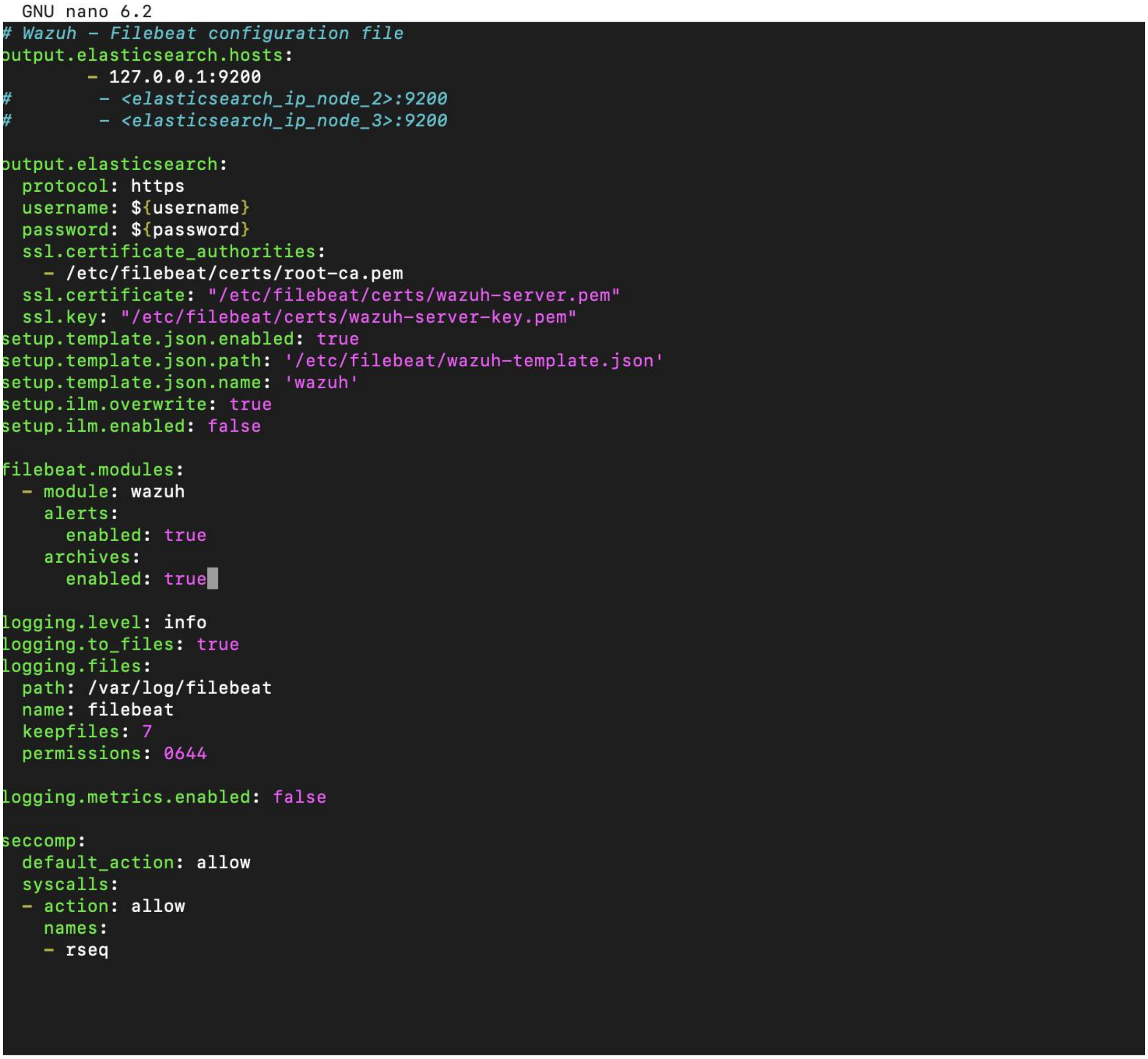
```
  GNU nano 6.2                                                                                    ossec.conf *
<!--
  Wazuh - Manager - Default configuration for ubuntu 22.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<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>
    <update_check>yes</update_check>
  </global>

  <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>
    <connection>secure</connection>
    <port>1514</port>
    <protocol>tcp</protocol>
    <queue_size>131072</queue_size>
  </remote>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_dev>yes</check_dev>
    <check_sys>yes</check_sys>
    <check_pids>yes</check_pids>
    <check_ports>yes</check_ports>
    <check_if>yes</check_if>

    <!-- Frequency that rootcheck is executed - every 12 hours -->
    <frequency>43200</frequency>

    <rootkit_files>etc/rootcheck/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>etc/rootcheck/rootkit_trojans.txt</rootkit_trojans>

    <skip_nfs>yes</skip_nfs>

    <ignore>/var/lib/containerd</ignore>
    <ignore>/var/lib/docker/overlay2</ignore>
```

Description: Viewing archive.log in /var/ossec/logs/archives using cat to verify that Wazuh is logging events under the archive.



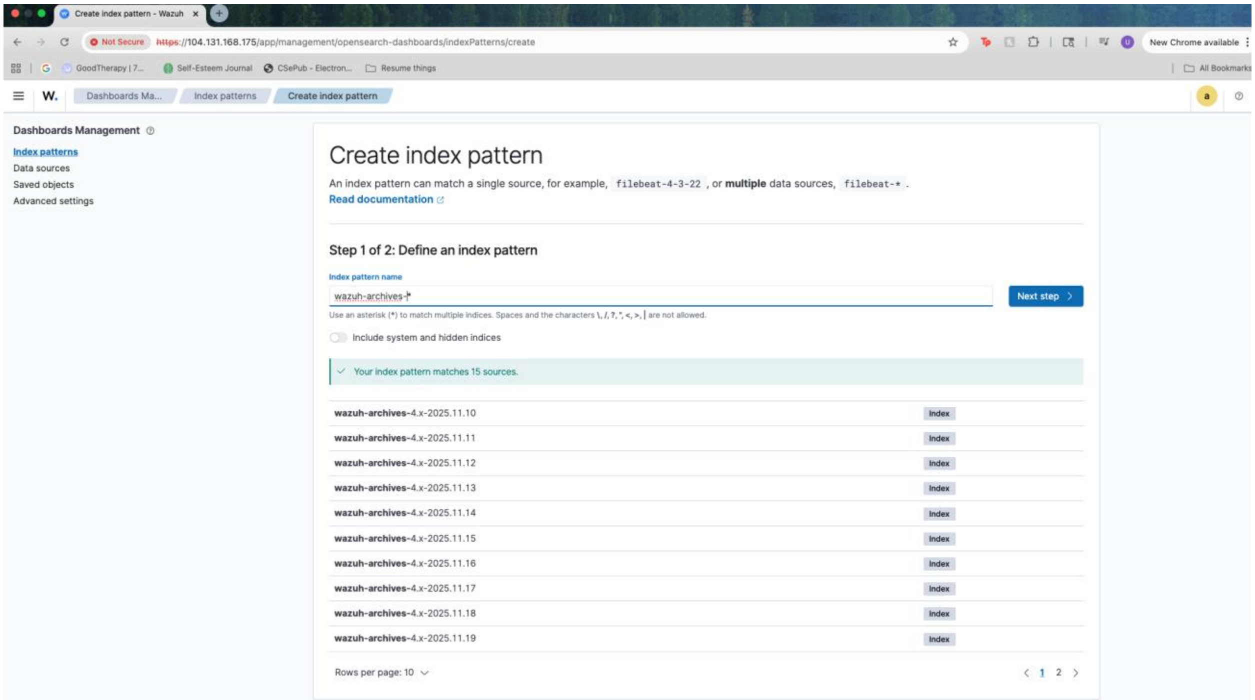
```
essed:\r\nRuleName: technique_id=T1036,technique_name=Masquerading\r\nUtcTime: 2025-11-09 02:50:46.924\r\nSourceProcessGUID: {fb82638e-d623-690f-6405-000000000700}\r\nSourceProcessId: 8504\r\nSourceThreadId: 9924\r\nSourceImage: C:\\Users\\urja\\AppData\
\Local\\Microsoft\\OneDrive\\OneDrive.exe\r\nTargetProcessGUID: {fb82638e-f1a5-690f-6108-000000000700}\r\nTargetProcessId: 4800\r\nTargetImage: C:\\WINDOWS\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\r\nGrantedAccess: 0x101411\r\nCallTrace: C:\\WI
NDOWS\\SYSTEM32\\ntdll.dll+162d74|C:\\WINDOWS\\System32\\KERNELBASE.dll+c54f6|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncClient.dll+69e811|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSy
ncClient.dll+f22e8|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncClient.dll+f20ad|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncClient.dll+f1f99|C:\\Users\\urja\\AppData\\Local\\Microsof
t\\OneDrive\\25.194.1005.0003\\FileSyncEvents.dll+f0e0|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncHost.DLL+dc0f|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncHost.DLL+10485|C:\\WINDOW
S\\System32\\ucrtbase.dll+37b0|C:\\WINDOWS\\System32\\KERNEL32.DLL+2e8d7|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+3c34c\r\nSourceUser: DESKTOP-437I1E6\\urja\r\nTargetUser: DESKTOP-437I1E6\\urja\""},"eventdata":{"ruleName":"technique_id=T1036,technique_name=Masqu
erading","utcTime":"2025-11-09 02:50:46.924","sourceProcessGUID":"{fb82638e-d623-690f-6405-000000000700}","sourceProcessId":"8504","sourceThreadId":"9924","sourceImage":"C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\OneDrive.exe","t
argetProcessGUID":"{fb82638e-f1a5-690f-6108-000000000700}","targetProcessId":"4800","targetImage":"C:\\\\WINDOWS\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\powershell.exe","grantedAccess":"0x101411","callTrace":"C:\\\\WINDOWS\\\\SYSTEM32\\\\ntdll.dll+16
2d74|C:\\\\WINDOWS\\\\System32\\\\KERNELBASE.dll+c54f6|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncClient.dll+69e811|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\
\\\FileSyncClient.dll+f22e8|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncClient.dll+f20ad|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncClient.dll+f1f99|
C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncEvents.dll+f0e0|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncHost.DLL+dc0f|C:\\\\Users\\\\urja\\\\AppData\\
\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncHost.DLL+10485|C:\\\\WINDOWS\\\\System32\\\\ucrtbase.dll+37b0|C:\\\\WINDOWS\\\\System32\\\\KERNEL32.DLL+2e8d7|C:\\\\WINDOWS\\\\SYSTEM32\\\\ntdll.dll+3c34c","sourceUser":"DESKTOP-437I1E6\\\\u
rja","targetUser":"DESKTOP-437I1E6\\\\urja"}}}
2025 Nov 10 02:59:26 (DESKTOP-437I1E6) any->EventChannel {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"10","version":"3","level":"4","task":"10","opcode":"0","keywords":"0x8
000000000000000","systemTime":"2025-11-09T02:50:46.9264015Z","eventRecordID":"39302","processID":"3088","threadID":"3924","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-437I1E6","severityValue":"INFORMATION","message":"\"Process acc
essed:\r\nRuleName: technique_id=T1036,technique_name=Masquerading\r\nUtcTime: 2025-11-09 02:50:46.924\r\nSourceProcessGUID: {fb82638e-d623-690f-6405-000000000700}\r\nSourceProcessId: 8504\r\nSourceThreadId: 9924\r\nSourceImage: C:\\Users\\urja\\AppData\
\Local\\Microsoft\\OneDrive\\OneDrive.exe\r\nTargetProcessGUID: {fb82638e-f1df-690f-6608-000000000700}\r\nTargetProcessId: 9204\r\nTargetImage: C:\\Users\\urja\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\r\nGrantedAccess: 0x101411\r\nCallTrace: C:\\WIN
DOWS\\SYSTEM32\\ntdll.dll+162d74|C:\\WINDOWS\\System32\\KERNELBASE.dll+c54f6|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncClient.dll+69e811|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyn
cClient.dll+f22e8|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncClient.dll+f20ad|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncClient.dll+f1f99|C:\\Users\\urja\\AppData\\Local\\Microsoft
\\OneDrive\\25.194.1005.0003\\FileSyncEvents.dll+f0e0|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncHost.DLL+dc0f|C:\\Users\\urja\\AppData\\Local\\Microsoft\\OneDrive\\25.194.1005.0003\\FileSyncHost.DLL+10485|C:\\WINDOWS
\\System32\\ucrtbase.dll+37b0|C:\\WINDOWS\\System32\\KERNEL32.DLL+2e8d7|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+3c34c\r\nSourceUser: DESKTOP-437I1E6\\urja\r\nTargetUser: DESKTOP-437I1E6\\urja\""},"eventdata":{"ruleName":"technique_id=T1036,technique_name=Masque
rading","utcTime":"2025-11-09 02:50:46.924","sourceProcessGUID":"{fb82638e-d623-690f-6405-000000000700}","sourceProcessId":"8504","sourceThreadId":"9924","sourceImage":"C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\OneDrive.exe","ta
rgetProcessGUID":"{fb82638e-f1df-690f-6608-000000000700}","targetProcessId":"9204","targetImage":"C:\\\\Users\\\\urja\\\\Downloads\\\\mimikatz_trunk\\\\x64\\\\mimikatz.exe","grantedAccess":"0x101411","callTrace":"C:\\\\WINDOWS\\\\SYSTEM32\\\\ntdll.dll+16
2d74|C:\\\\WINDOWS\\\\System32\\\\KERNELBASE.dll+c54f6|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncClient.dll+69e811|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\
\\\FileSyncClient.dll+f22e8|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncClient.dll+f20ad|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncClient.dll+f1f99|
C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncEvents.dll+f0e0|C:\\\\Users\\\\urja\\\\AppData\\\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncHost.DLL+dc0f|C:\\\\Users\\\\urja\\\\AppData\\
\\Local\\\\Microsoft\\\\OneDrive\\\\25.194.1005.0003\\\\FileSyncHost.DLL+10485|C:\\\\WINDOWS\\\\System32\\\\ucrtbase.dll+37b0|C:\\\\WINDOWS\\\\System32\\\\KERNEL32.DLL+2e8d7|C:\\\\WINDOWS\\\\SYSTEM32\\\\ntdll.dll+3c34c","sourceUser":"DESKTOP-437I1E6\\\\u
rja","targetUser":"DESKTOP-437I1E6\\\\urja"}}}
2025 Nov 10 03:00:02 Wazuh->journald Nov 10 03:00:00 Wazuh opensearch-dashboards[76498]: {"type":"log","@timestamp":"2025-11-10T03:00:00Z","tags":["info","plugins","wazuh","monitoring"],"pid":76498,"message":"Settings added to wazuh-monitoring-2025.46w i
ndex"}
2025 Nov 10 03:00:02 Wazuh->journald Nov 10 03:00:00 Wazuh opensearch-dashboards[76498]: {"type":"log","@timestamp":"2025-11-10T03:00:00Z","tags":["info","plugins","wazuh","monitoring"],"pid":76498,"message":"Bulk data to index wazuh-monitoring-2025.46w
for 1 agents completed"}
2025 Nov 10 03:00:04 (DESKTOP-437I1E6) any->EventChannel {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"3","version":"5","level":"4","task":"3","opcode":"0","keywords":"0x800
0000000000000","systemTime":"2025-11-09T02:51:24.9492204Z","eventRecordID":"39303","processID":"3088","threadID":"3932","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-437I1E6","severityValue":"INFORMATION","message":"\"Network conne
ction detected:\r\nRuleName: technique_id=T1036,technique_name=Masquerading\r\nUtcTime: 2025-09-22 12:14:39.145\r\nProcessGuid: {fb82638e-e2e9-68d0-4100-000000000700}\r\nProcessId: 1380\r\nImage: C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.
18.25080.5-0\\MpDefenderCoreService.exe\r\nUser: NT AUTHORITY\\SYSTEM\r\nProtocol: tcp\r\nInitiated: true\r\nSourceIsIpv6: false\r\nSourceIp: 10.0.2.15\r\nSourceHostname: -\r\nSourcePort: 63934\r\nSourcePortName: -\r\nDestinationIsIpv6: false\r\nDestinat
ionIp: 52.123.129.14\r\nDestinationHostname: -\r\nDestinationPort: 443\r\nDestinationPortName: -\""},"eventdata":{"ruleName":"technique_id=T1036,technique_name=Masquerading","utcTime":"2025-09-22 12:14:39.145","processGuid":"{fb82638e-e2e9-68d0-4100-0000
00000700}","processId":"1380","image":"C:\\\\ProgramData\\\\Microsoft\\\\Windows Defender\\\\Platform\\\\4.18.25080.5-0\\\\MpDefenderCoreService.exe","user":"NT AUTHORITY\\\\SYSTEM","protocol":"tcp","initiated":"true","sourceIsIpv6":"false","sourceIp":"1
0.0.2.15","sourcePort":"63934","destinationIsIpv6":"false","destinationIp":"52.123.129.14","destinationPort":"443"}}}
2025 Nov 10 03:02:30 Wazuh->df -P ossec: output: 'df -P': Filesystem     1024-blocks     Used Available Capacity Mounted on
2025 Nov 10 03:02:30 Wazuh->df -P ossec: output: 'df -P': tmpfs               812848     1056    811792       1% /run
2025 Nov 10 03:02:30 Wazuh->df -P ossec: output: 'df -P': tmpfs              4064224       80   4064144       1% /dev/shm
2025 Nov 10 03:02:30 Wazuh->df -P ossec: output: 'df -P': tmpfs                 5120        0      5120       0% /run/lock
2025 Nov 10 03:02:30 Wazuh->df -P ossec: output: 'df -P': /dev/vda15          106832     6194    100638       6% /boot/efi
2025 Nov 10 03:02:30 Wazuh->df -P ossec: output: 'df -P': tmpfs               812844        4    812840       1% /run/user/0
2025 Nov 10 03:02:30 Wazuh->df -P ossec: output: 'df -P': /dev/vda1        162406320 14359664 148030272       9% /
2025 Nov 10 03:02:30 Wazuh->last -n 20 ossec: output: 'last -n 20':
root     pts/0        107.212.24.97    Mon Nov 10 00:03   still logged in
root     pts/0        107.212.24.97    Sat Nov  8 22:19 - 06:46  (08:27)
root     pts/0        107.212.24.97    Sun Oct 26 20:04 - 02:31  (06:27)
root     pts/0        107.212.24.97    Tue Sep 16 02:38 - 04:50  (02:11)
root     pts/0        107.212.24.97    Tue Sep  9 02:08 - 05:43  (03:34)
root     pts/0        107.212.24.97    Wed Sep  3 16:17 - 16:52  (00:35)
root     tty1                          Wed Sep  3 16:01   still logged in
reboot   system boot  5.15.0-113-gener Wed Sep  3 15:27   still running
wtmp begins Wed Sep  3 15:27:51 2025
2025 Nov 10 03:08:30 Wazuh->df -P ossec: output: 'df -P': Filesystem     1024-blocks     Used Available Capacity Mounted on
2025 Nov 10 03:08:30 Wazuh->df -P ossec: output: 'df -P': tmpfs               812848     1056    811792       1% /run
2025 Nov 10 03:08:30 Wazuh->df -P ossec: output: 'df -P': /dev/vda1        162406320 14359668 148030268       9% /
2025 Nov 10 03:08:30 Wazuh->df -P ossec: output: 'df -P': tmpfs                 5120        0      5120       0% /run/lock
2025 Nov 10 03:08:30 Wazuh->df -P ossec: output: 'df -P': /dev/vda15          106832     6194    100638       6% /boot/efi
2025 Nov 10 03:08:30 Wazuh->df -P ossec: output: 'df -P': tmpfs               812844        4    812840       1% /run/user/0
2025 Nov 10 03:08:30 Wazuh->df -P ossec: output: 'df -P': tmpfs              4064224       80   4064144       1% /dev/shm
2025 Nov 10 03:08:30 Wazuh->last -n 20 ossec: output: 'last -n 20':
root     pts/0        107.212.24.97    Mon Nov 10 00:03   still logged in
root     pts/0        107.212.24.97    Sat Nov  8 22:19 - 06:46  (08:27)
root     pts/0        107.212.24.97    Sun Oct 26 20:04 - 02:31  (06:27)
root     pts/0        107.212.24.97    Tue Sep 16 02:38 - 04:50  (02:11)
root     pts/0        107.212.24.97    Tue Sep  9 02:08 - 05:43  (03:34)
root     pts/0        107.212.24.97    Wed Sep  3 16:17 - 16:52  (00:35)
root     tty1                          Wed Sep  3 16:01   still logged in
reboot   system boot  5.15.0-113-gener Wed Sep  3 15:27   still running
wtmp begins Wed Sep  3 15:27:51 2025
2025 Nov 10 03:10:02 Wazuh->journald Nov 10 03:10:01 Wazuh CRON[721706]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2025 Nov 10 03:10:02 Wazuh->journald Nov 10 03:10:01 Wazuh CRON[721707]: (root) CMD (test -e /run/systemd/system || SERVICE_MODE=1 /sbin/e2scrub_all -A -r)
2025 Nov 10 03:10:02 Wazuh->journald Nov 10 03:10:01 Wazuh CRON[721706]: pam_unix(cron:session): session closed for user root
root@Wazuh:/var/ossec/logs/archives# 
```

Description: Modifying the Filebeat configuration by enabling archive and alerts to true and restarting the Filebeat service.



```
  GNU nano 6.2
# 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

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
  permissions: 0644

logging.metrics.enabled: false

seccomp:
  default_action: allow
  syscalls:
  - action: allow
    names:
    - rseq
```

Description: Defining an index pattern in Dashboard Management for indexing and searching logs.



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .

Read documentation

Step 1 of 2: Define an index pattern

Index pattern name: wazuh-archives-*

Next step

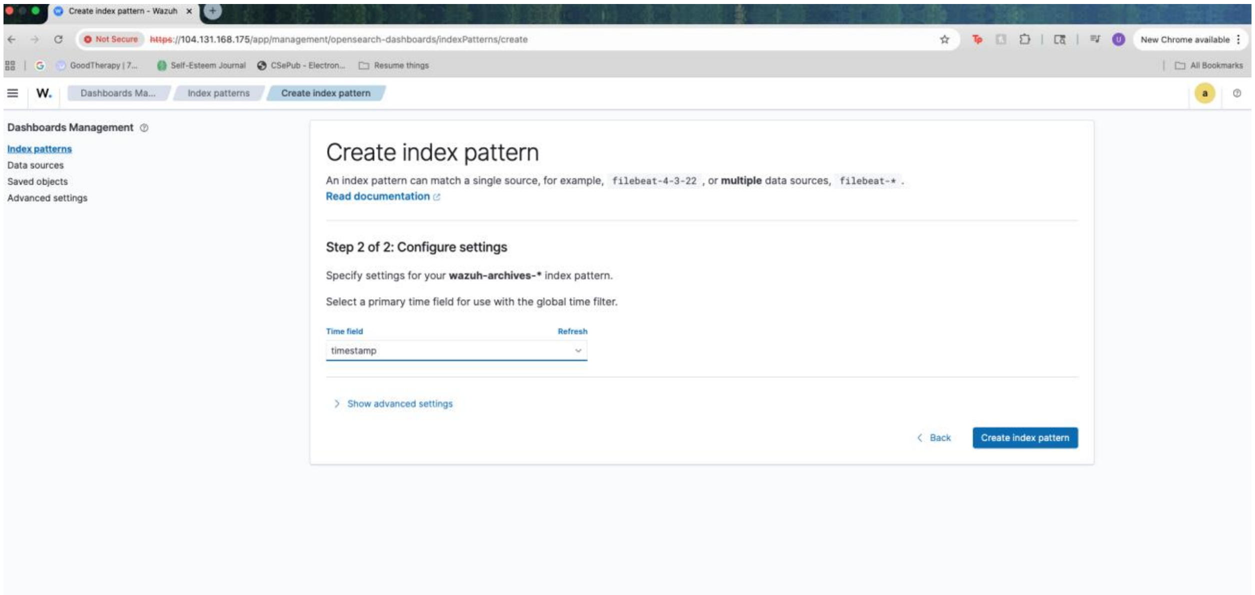
Use an asterisk (*) to match multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.

Include system and hidden indices

✓ Your index pattern matches 15 sources.

wazuh-archives-4.x-2025.11.10	Index
wazuh-archives-4.x-2025.11.11	Index
wazuh-archives-4.x-2025.11.12	Index
wazuh-archives-4.x-2025.11.13	Index
wazuh-archives-4.x-2025.11.14	Index
wazuh-archives-4.x-2025.11.15	Index
wazuh-archives-4.x-2025.11.16	Index
wazuh-archives-4.x-2025.11.17	Index
wazuh-archives-4.x-2025.11.18	Index
wazuh-archives-4.x-2025.11.19	Index

Rows per page: 10



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .

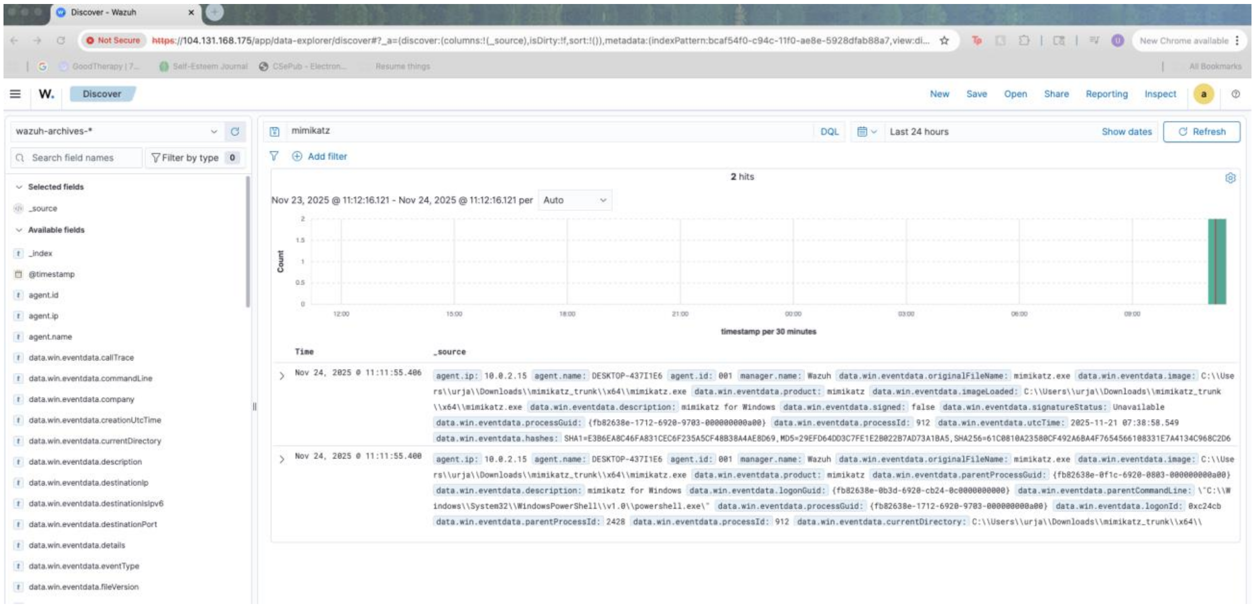
Read documentation

Step 2 of 2: Configure settings

Specify settings for your **wazuh-archives-*** index pattern.

Select a primary time field for use with the global time filter.

Time field: timestamp



```
https://104.131.168.175/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty:!f,sort:!()),metadata:(indexPattern:bcaf54f0-c94c-11f0-ae8e-5928dfab88a7,view:di...
```

wazuh-archives-*

mimikatz

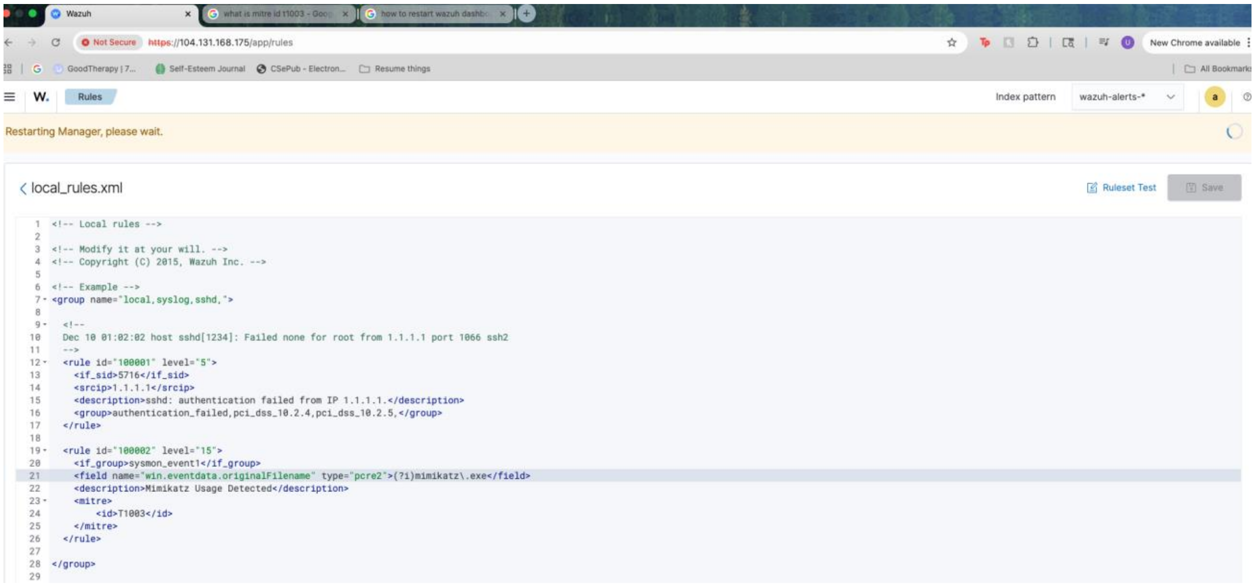
Last 24 hours

2 hits

Nov 23, 2025 @ 11:12:16.121 - Nov 24, 2025 @ 11:12:16.121 per Auto

```
Time                          _source
Nov 24, 2025 @ 11:11:55.406   agent.ip: 10.0.2.15 agent.name: DESKTOP-437I1E6 agent.id: 001 manager.name: Wazuh data.win.eventdata.originalFileName: mimikatz.exe data.win.eventdata.image: C:\\Use
                              rs\\urja\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe data.win.eventdata.product: mimikatz data.win.eventdata.imageLoaded: C:\\Users\\urja\\Downloads\\mimikatz_trunk
                              \\x64\\mimikatz.exe data.win.eventdata.description: mimikatz for Windows data.win.eventdata.signed: false data.win.eventdata.signatureStatus: Unavailable
                              data.win.eventdata.processGuid: {fb82638e-1712-6920-9703-000000000a00} data.win.eventdata.processId: 912 data.win.eventdata.utcTime: 2025-11-21 07:38:58.549
                              data.win.eventdata.hashes: SHA1=E3B6EA8C46FA831CEC6F235A5CF48B38A4AE8D69,MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5,SHA256=61C0810A23580CF492A6BA4F7654566108331E7A4134C968C2D6
Nov 24, 2025 @ 11:11:55.400   agent.ip: 10.0.2.15 agent.name: DESKTOP-437I1E6 agent.id: 001 manager.name: Wazuh data.win.eventdata.originalFileName: mimikatz.exe data.win.eventdata.image: C:\\Use
                              rs\\urja\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe data.win.eventdata.product: mimikatz data.win.eventdata.parentProcessGuid: {fb82638e-0f1c-6920-0803-000000000a00}
                              data.win.eventdata.description: mimikatz for Windows data.win.eventdata.logonGuid: {fb82638e-0b3d-6920-cb24-0c0000000000} data.win.eventdata.parentCommandLine: \"C:\\W
                              indows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" data.win.eventdata.processGuid: {fb82638e-1712-6920-9703-000000000a00} data.win.eventdata.logonId: 0xc24cb
                              data.win.eventdata.parentProcessId: 2428 data.win.eventdata.processId: 912 data.win.eventdata.currentDirectory: C:\\Users\\urja\\Downloads\\mimikatz_trunk\\x64\\
```

Description: Editing local rules to add a detection for Mimikatz. Triggering the rule when the original file name for Mimikatz appears in Sysmon Event ID 1 (process creation). Mapping the detection to the MITRE ATT&CK framework under T1003 – OS Credential Dumping.

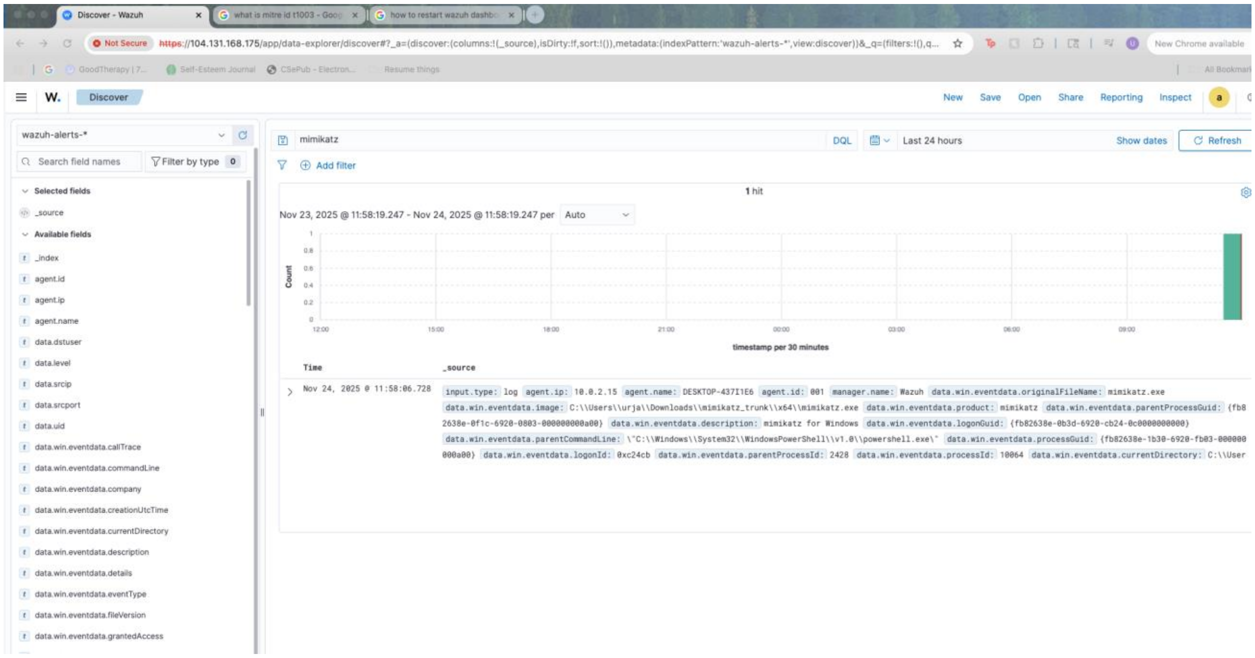


Restarting Manager, please wait.

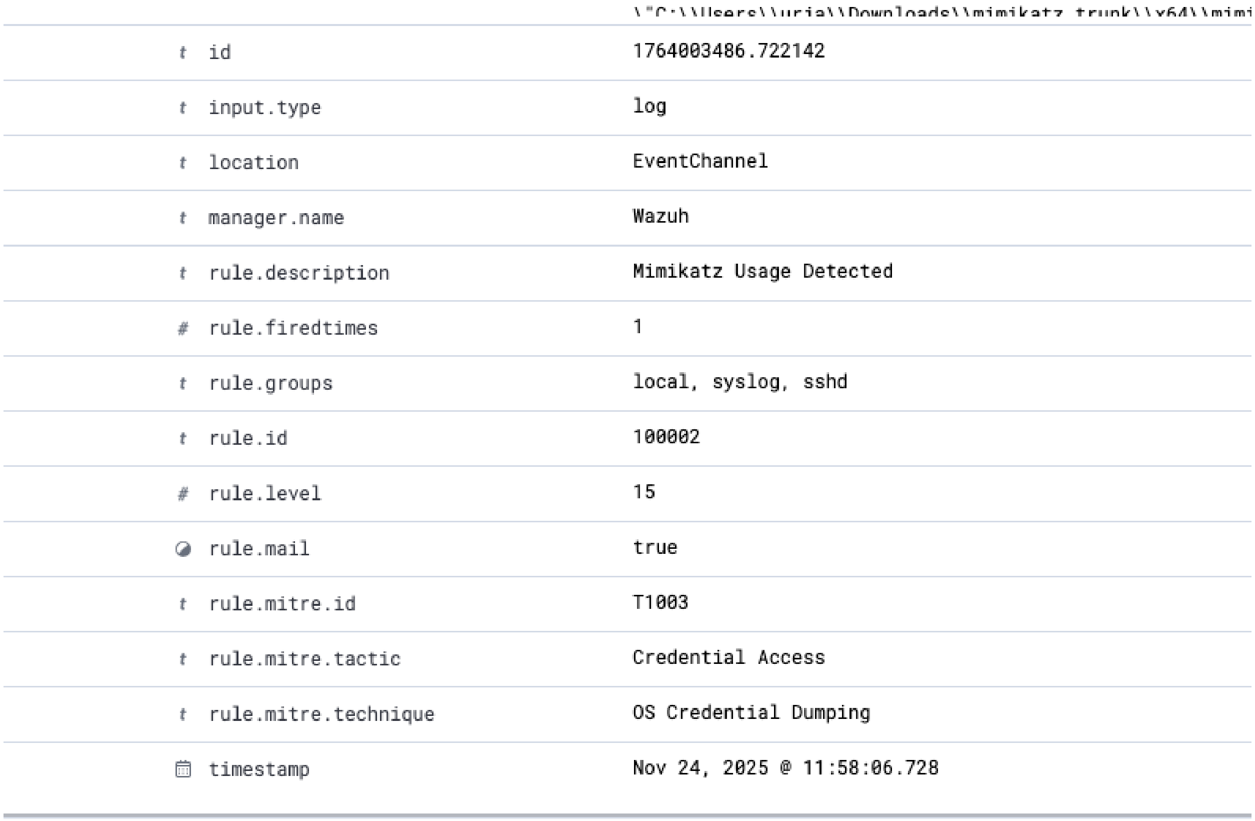
local_rules.xml

```
<!-- 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>

```

Description: Restarting the Wazuh dashboard and executing Mimikatz again on the Windows machine. Using the Discover function to verify that the Mimikatz detection rule is generated.


Discover - Wazuh
what is mitre id t1003 - Goog
how to restart wazuh dashb
Not Secure
https://104.131.168.175/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty:!f,sort:!()),metadata:(indexPattern:'wazuh-alerts-*',view:discover))&_q=(filters:!(),q...
New Chrome available
Discover
New
Save
Open
Share
Reporting
Inspect
wazuh-alerts-*
Search field names
Filter by type 0
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.dstuser
data.level
data.srcip
data.srcport
data.uid
data.win.eventdata.callTrace
data.win.eventdata.commandLine
data.win.eventdata.company
data.win.eventdata.creationUtcTime
data.win.eventdata.currentDirectory
data.win.eventdata.description
data.win.eventdata.details
data.win.eventdata.eventType
data.win.eventdata.fileVersion
data.win.eventdata.grantedAccess
mimikatz
DQL
Last 24 hours
Show dates
Refresh
Add filter
1 hit
Nov 23, 2025 @ 11:58:19.247 - Nov 24, 2025 @ 11:58:19.247 per
Auto
Count
1
0.8
0.6
0.4
0.2
0
12:00
15:00
18:00
21:00
00:00
03:00
06:00
09:00
timestamp per 30 minutes

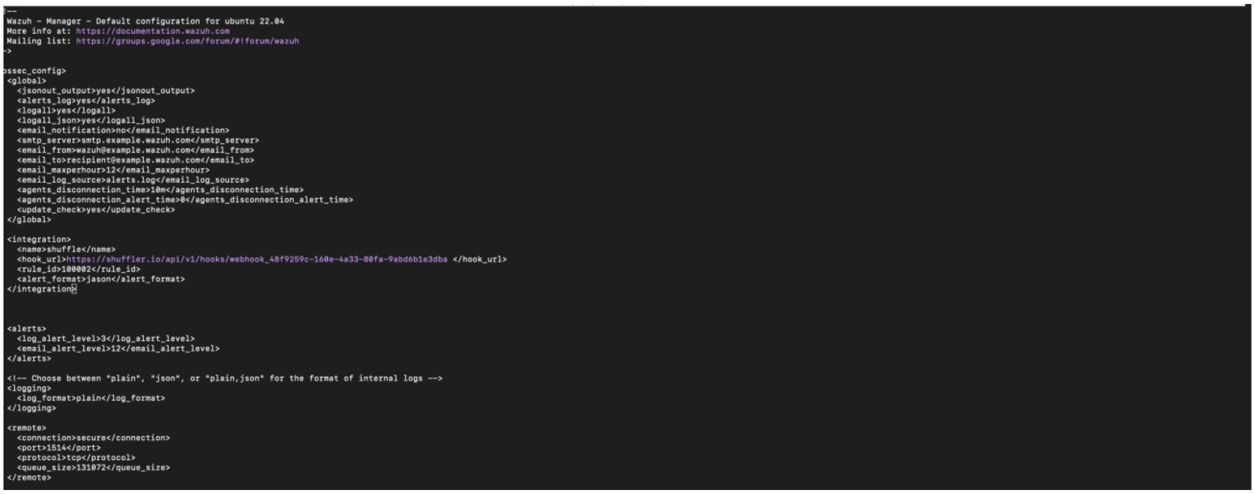
```
Time                       _source
Nov 24, 2025 @ 11:58:06.728  input.type: log agent.ip: 10.0.2.15 agent.name: DESKTOP-437I1E6 agent.id: 001 manager.name: Wazuh data.win.eventdata.originalFileName: mimikatz.exe
                           data.win.eventdata.image: C:\\Users\\urja\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe data.win.eventdata.product: mimikatz data.win.eventdata.parentProcessGuid: {fb8
                           2638e-0f1c-6920-0803-000000000a00} data.win.eventdata.description: mimikatz for Windows data.win.eventdata.logonGuid: {fb82638e-0b3d-6920-cb24-0c0000000000}
                           data.win.eventdata.parentCommandLine: \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" data.win.eventdata.processGuid: {fb82638e-1b30-6920-fb03-000000
                           000a00} data.win.eventdata.logonId: 0xc24cb data.win.eventdata.parentProcessId: 2428 data.win.eventdata.processId: 10064 data.win.eventdata.currentDirectory: C:\\User
```



\"C:\\Users\\urja\\Downloads\\mimikatz_trunk\\x64\\mimi

t	id	1764003486.722142
t	input.type	log
t	location	EventChannel
t	manager.name	Wazuh
t	rule.description	Mimikatz Usage Detected
#	rule.firedtimes	1
t	rule.groups	local, syslog, sshd
t	rule.id	100002
#	rule.level	15
◐	rule.mail	true
t	rule.mitre.id	T1003
t	rule.mitre.tactic	Credential Access
t	rule.mitre.technique	OS Credential Dumping
📅	timestamp	Nov 24, 2025 @ 11:58:06.728

Description: Adding the Shuffle integration to the OSSEC configuration file and restarting the Wazuh manager.

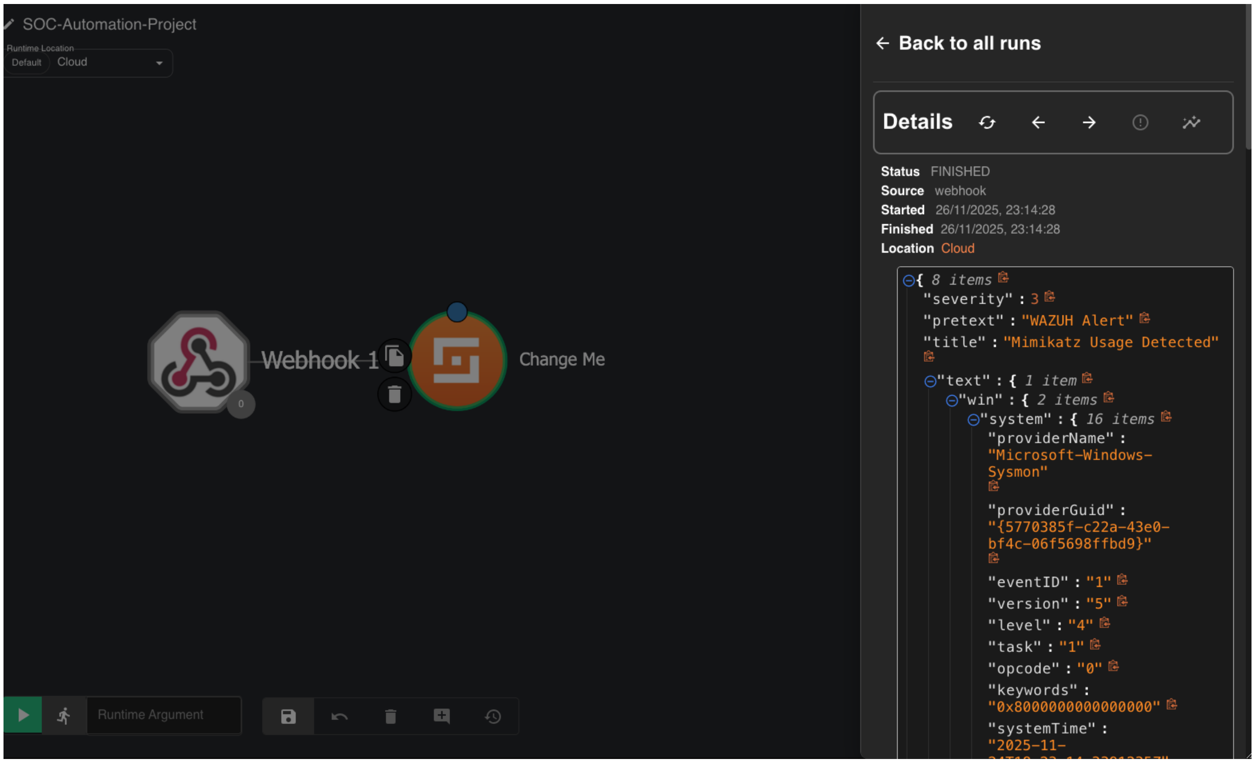


```
!--
 Wazuh - Manager - Default configuration for ubuntu 22.04
 More info at: https://documentation.wazuh.com
 Mailing list: https://groups.google.com/forum/#!forum/wazuh
->

ssec_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>
   <update_check>yes</update_check>
 </global>

 <integration>
   <name>shuffle</name>
   <hook_url>https://shuffler.io/api/v1/hooks/webhook_48f9259c-160e-4a33-80fa-9abd6b1e3dba </hook_url>
   <rule_id>100002</rule_id>
   <alert_format>jason</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>
   <connection>secure</connection>
   <port>1514</port>
   <protocol>tcp</protocol>
   <queue_size>131072</queue_size>
 </remote>
```

Description: Build workflow in shuffle soar using webhooks:

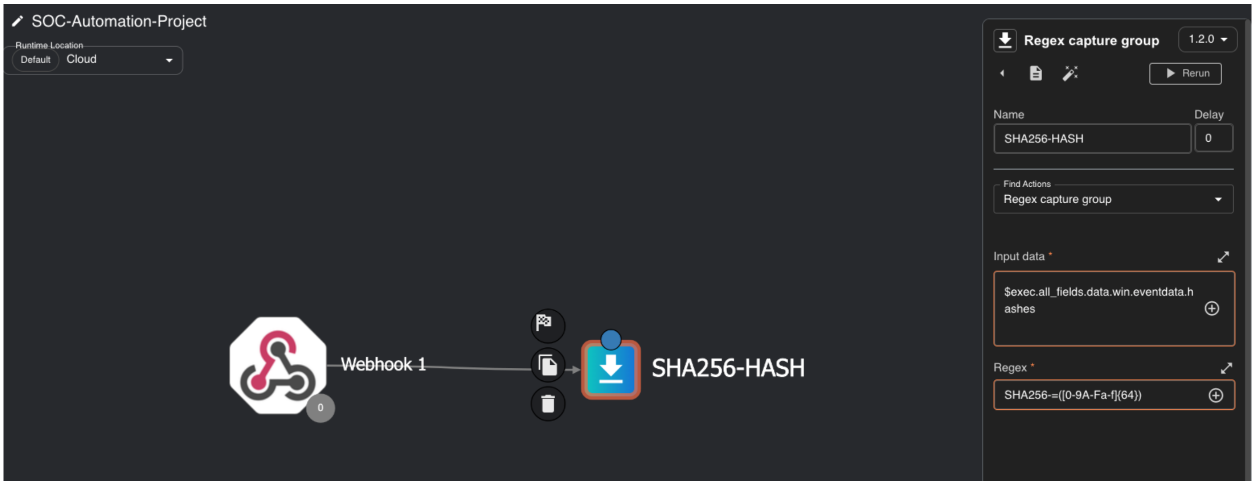
1. Mimikatz Alert Sent to Shuffle
2. Shuffle Receives Mimikatz Alert – Extracting SHA256 Hash From File

3. Check Reputation Score with Virus total
4. Send details to Hive to create alert
5. Send email to SOC Analyst to begin Investigation

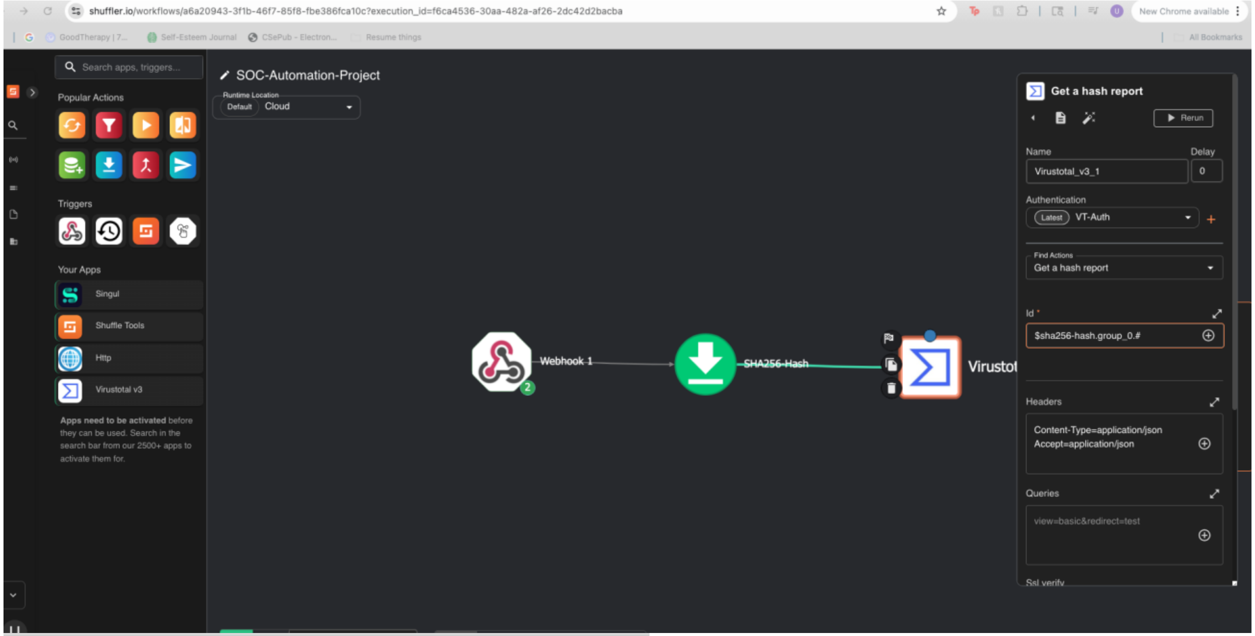


Status FINISHED
Source webhook
Started 26/11/2025, 23:14:28
Finished 26/11/2025, 23:14:28
Location Cloud

```
{ 8 items
  "severity" : 3
  "pretext" : "WAZUH Alert"
  "title" : "Mimikatz Usage Detected"
  "text" : { 1 item
    "win" : { 2 items
      "system" : { 16 items
        "providerName" :
        "Microsoft-Windows-
        Sysmon"
        "providerGuid" :
        "{5770385f-c22a-43e0-
        bf4c-06f5698ffbd9}"
        "eventID" : "1"
        "version" : "5"
        "level" : "4"
        "task" : "1"
        "opcode" : "0"
        "keywords" :
        "0x8000000000000000"
        "systemTime" :
        "2025-11-
```



Name: SHA256-HASH
Delay: 0
Find Actions: Regex capture group
Input data *: $exec.all_fields.data.win.eventdata.hashes
Regex *: SHA256-=([0-9A-Fa-f]{64})



shuffler.io/workflows/a6a20943-3f1b-46f7-85f8-fbe386fca10c?execution_id=f6ca4536-30aa-482a-af26-2dc42d2bacba

SOC-Automation-Project

Runtime Location: Default Cloud

Get a hash report

Name: Virustotal_v3_1

Delay: 0

Authentication: Latest VT-Auth

Find Actions: Get a hash report

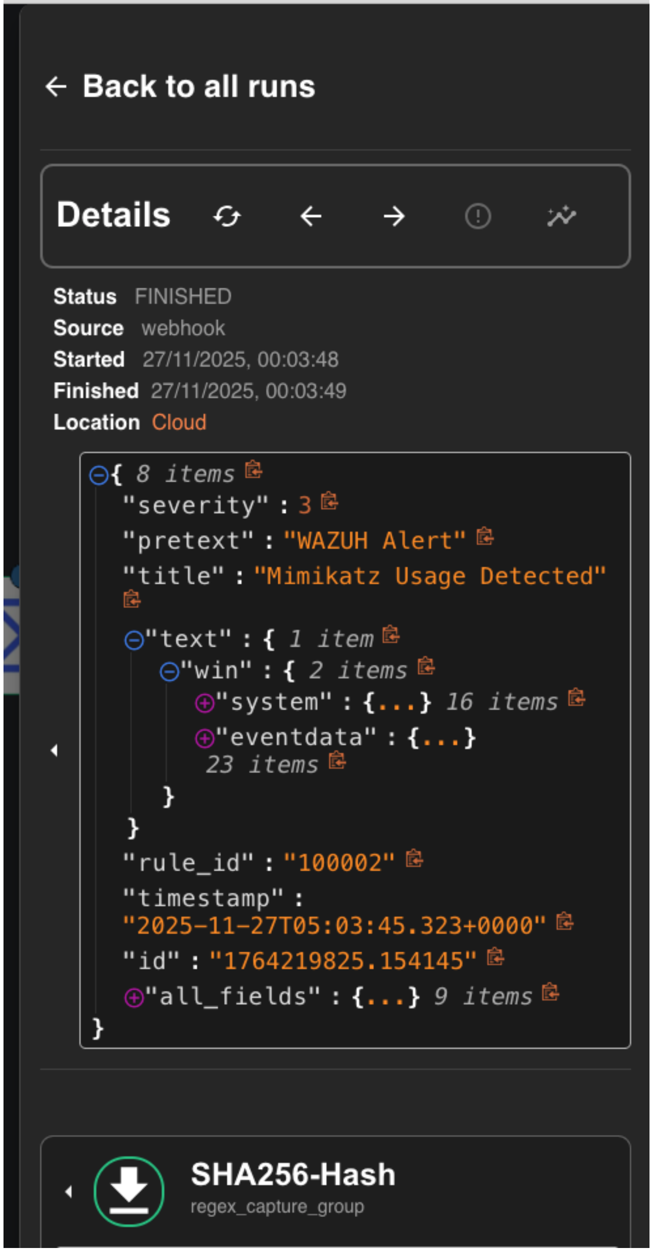
Id *: $sha256-hash.group_0.#

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

Queries: view=basic&redirect=test

Ssl verify

Apps need to be activated before they can be used. Search in the search bar from our 2500+ apps to activate them for.



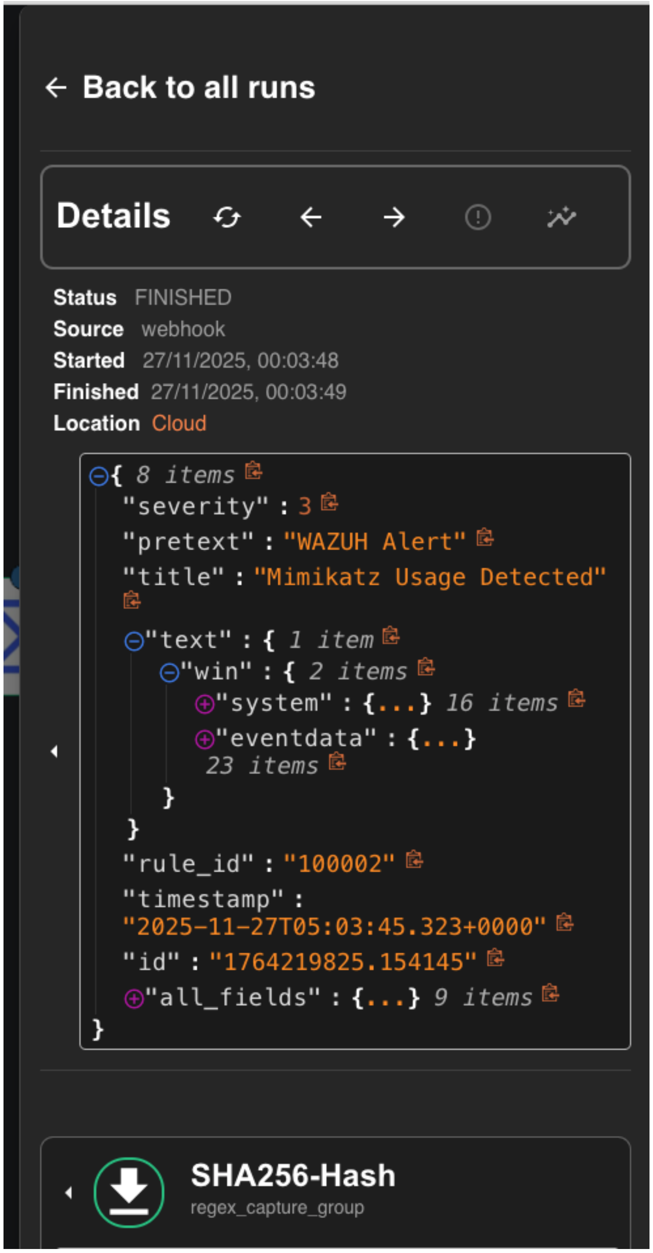
Back to all runs

Details

Status FINISHED
Source webhook
Started 27/11/2025, 00:03:48
Finished 27/11/2025, 00:03:49
Location Cloud

```
{ 8 items
  "severity" : 3
  "pretext" : "WAZUH Alert"
  "title" : "Mimikatz Usage Detected"
  "text" : { 1 item
    "win" : { 2 items
      "system" : {...} 16 items
      "eventdata" : {...} 23 items
    }
  }
  "rule_id" : "100002"
  "timestamp" : "2025-11-27T05:03:45.323+0000"
  "id" : "1764219825.154145"
  "all_fields" : {...} 9 items
}
```

SHA256-Hash
regex_capture_group



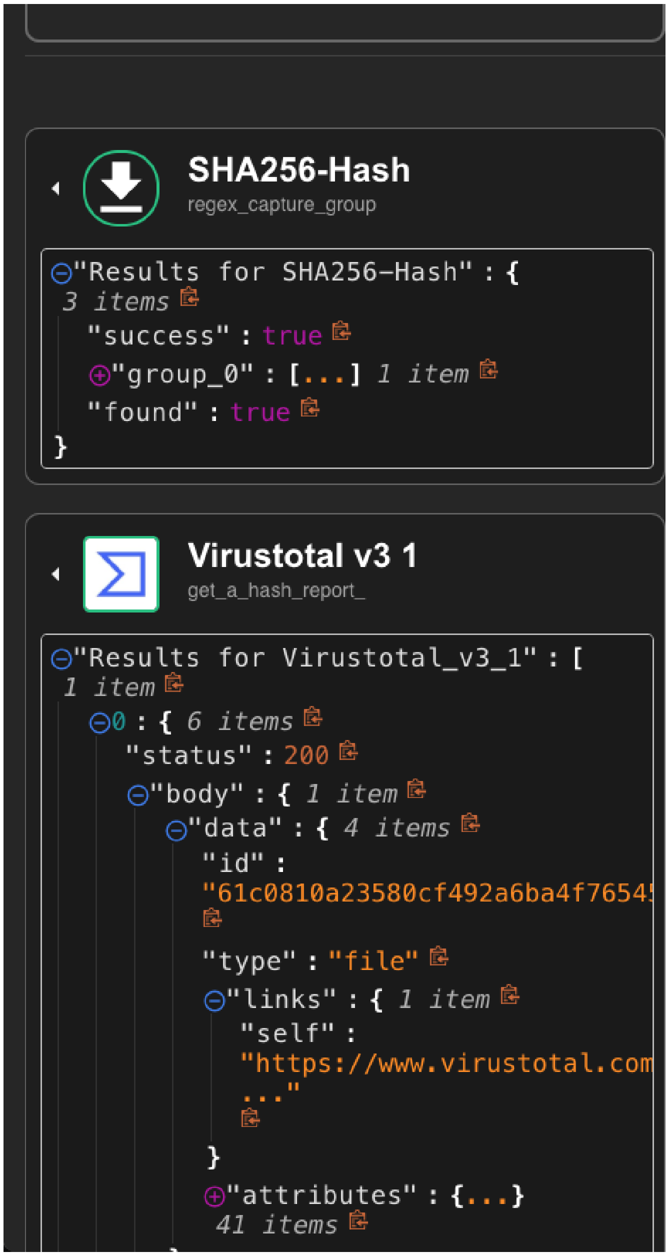
← Back to all runs

Details

Status FINISHED
Source webhook
Started 27/11/2025, 00:03:48
Finished 27/11/2025, 00:03:49
Location Cloud

```
⊖{ 8 items
  "severity" : 3
  "pretext" : "WAZUH Alert"
  "title" : "Mimikatz Usage Detected"
  ⊖"text" : { 1 item
    ⊖"win" : { 2 items
      ⊕"system" : {...} 16 items
      ⊕"eventdata" : {...}
       23 items
    }
  }
  "rule_id" : "100002"
  "timestamp" :
  "2025-11-27T05:03:45.323+0000"
  "id" : "1764219825.154145"
  ⊕"all_fields" : {...} 9 items
}
```

SHA256-Hash
regex_capture_group



SHA256-Hash

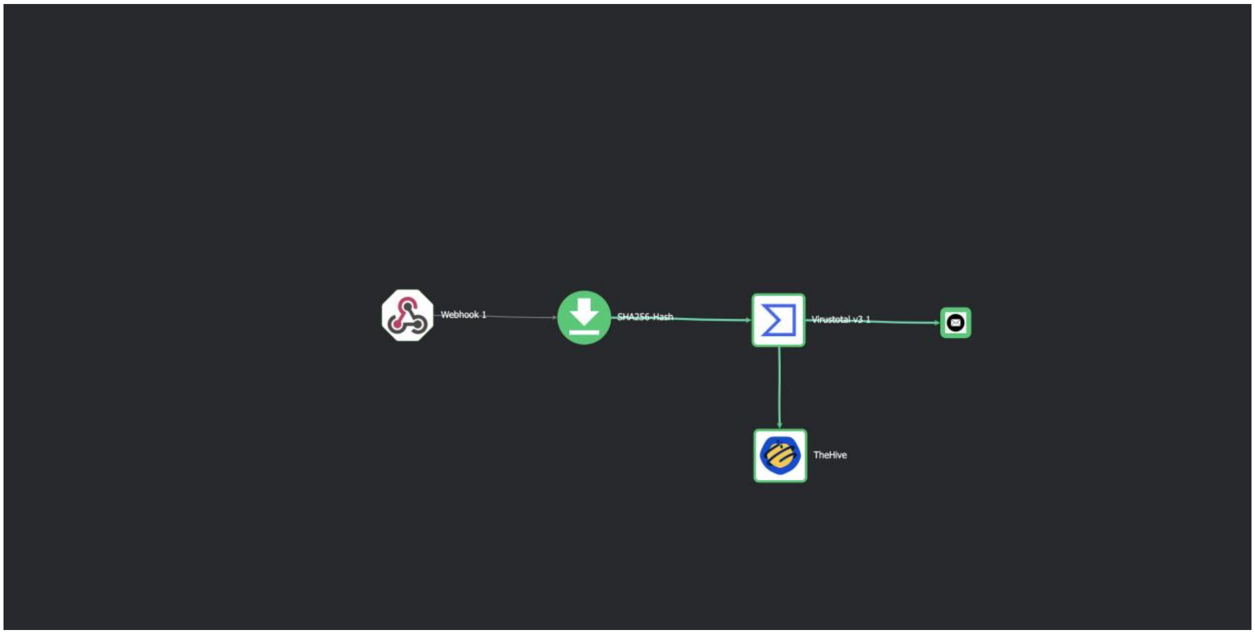
regex_capture_group

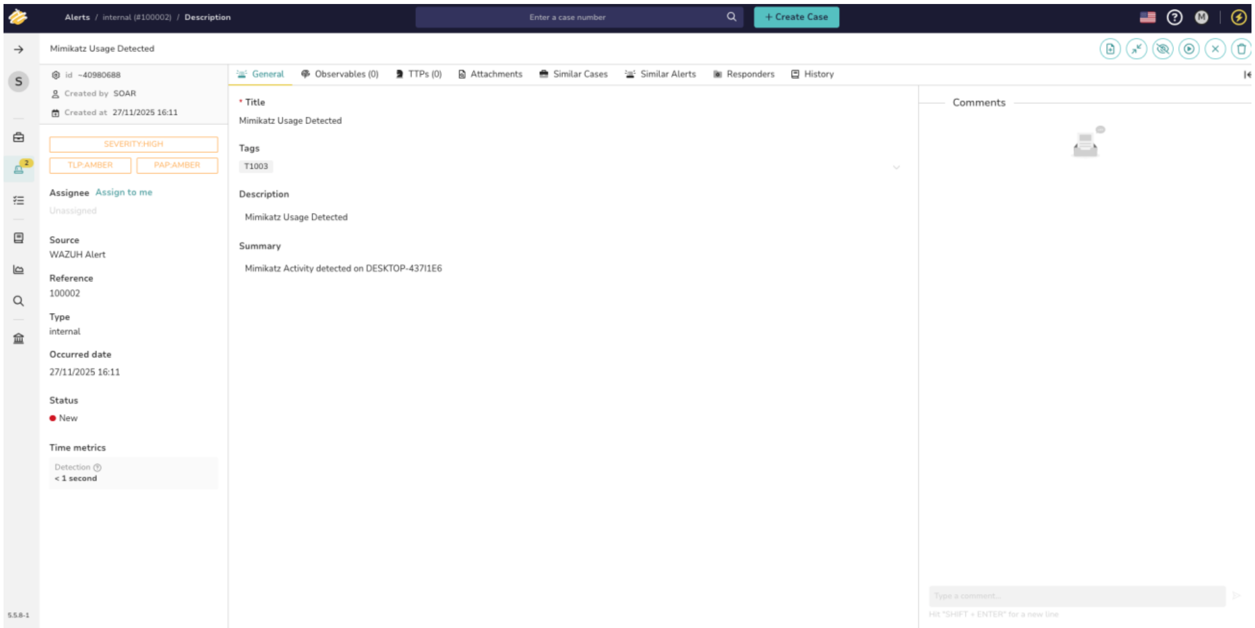
```
⊖"Results for SHA256-Hash" : {
 3 items
   "success" : true
  ⊕"group_0" : [...] 1 item
   "found" : true
}
```

Virustotal v3 1

get_a_hash_report_

```
⊖"Results for Virustotal_v3_1" : [
 1 item
  ⊖0 : { 6 items
    "status" : 200
   ⊖"body" : { 1 item
     ⊖"data" : { 4 items
        "id" :
        "61c0810a23580cf492a6ba4f7654

        "type" : "file"
       ⊖"links" : { 1 item
          "self" :
          "https://www.virustotal.com
          ..."

        }
       ⊕"attributes" : {...}
        41 items
```





Mimikatz Usage Detected

id ~40980688
Created by SOAR
Created at 27/11/2025 16:11

SEVERITY:HIGH
TLP:AMBER PAP:AMBER

Assignee Assign to me
Unassigned

Source
WAZUH Alert

Reference
100002

Type
internal

Occurred date
27/11/2025 16:11

Status
● New

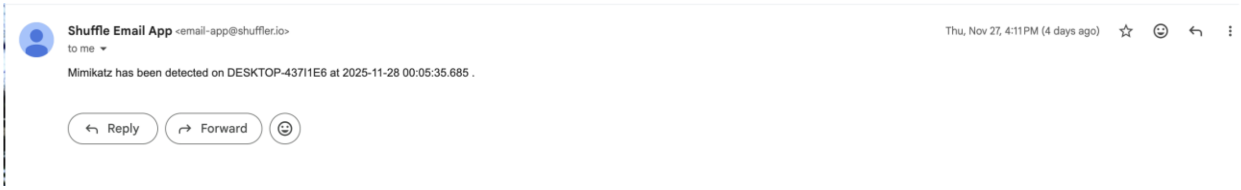
Time metrics
Detection
< 1 second

* Title
Mimikatz Usage Detected

Tags
T1003

Description
Mimikatz Usage Detected

Summary
Mimikatz Activity detected on DESKTOP-437I1E6



Shuffle Email App <email-app@shuffler.io>
to me

Thu, Nov 27, 4:11 PM (4 days ago)

Mimikatz has been detected on DESKTOP-437I1E6 at 2025-11-28 00:05:35.685 .