Wazuh SIEM Lab and Rule Modification

Overview

I wanted to gain experience in Wazuh and Linux by setting up an SIEM lab. This included generating telemetry, rule modification, and lab setup. I used a Ubuntu 22.04 VM on the cloud and a Windows 10 VM with sysmon using VMbox.

What is Wazuh?

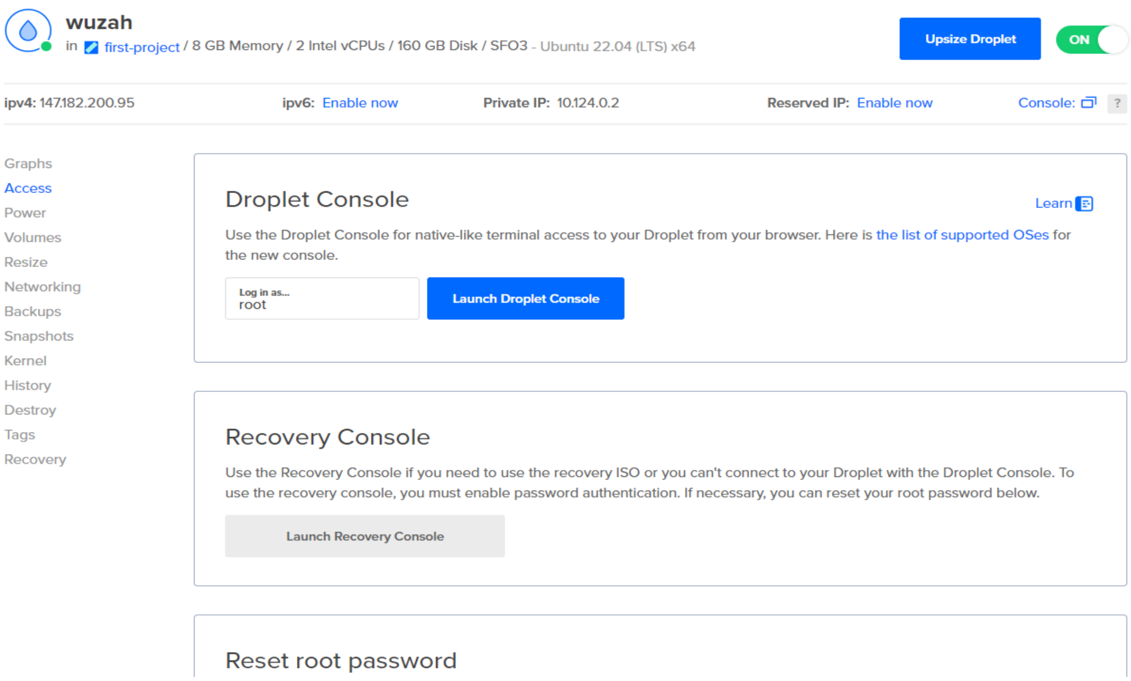
Wazuh is an open-source security platform that covers SIEM and unified XDR for the cloud and endpoints.

How I used Wazuh

I used Wazuh as the platform for the SIEM. From the Wazuh dashboard, I was able to monitor the virtual machine. After generating telemetry, I was able to see the events and the data regarding it. Additionally, I modified the rules of Wazuh to increase detection and my understanding.

Setting Up Wazuh

To set up Wazuh I used a free trial of Digital Ocean to host Ubuntu 22.04. The closest region was San Fransisco and I picked the specs that would be appropriate for this project.



wuzah

in first-project / 8 GB Memory / 2 Intel vCPUs / 160 GB Disk / SFO3 - Ubuntu 22.04 (LTS) x64

ipv4: 147.182.200.95   ipv6: Enable now   Private IP: 10.124.0.2   Reserved IP: Enable now   Console:

Droplet Console

Use the Droplet Console for native-like terminal access to your Droplet from your browser. Here is the list of supported OSes for the new console.

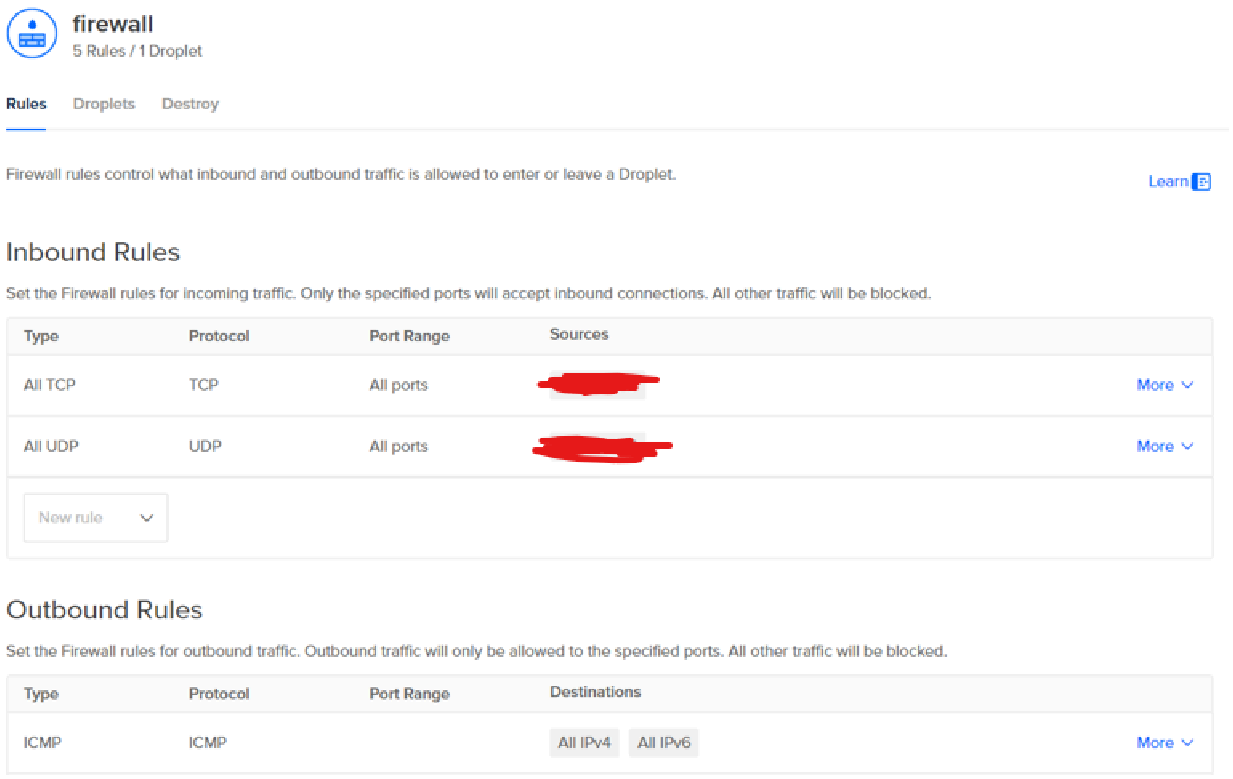
Log in as...
root

Recovery Console

Use the Recovery Console if you need to use the recovery ISO or you can't connect to your Droplet with the Droplet Console. To use the recovery console, you must enable password authentication. If necessary, you can reset your root password below.

Reset root password

I used Digital Ocean again to make a firewall and prevent the machine from being pinged. I set the inbound TCP and UDP to my IP address to prevent this.



firewall
5 Rules / 1 Droplet

Firewall rules control what inbound and outbound traffic is allowed to enter or leave a Droplet.

Inbound Rules

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

Type	Protocol	Port Range	Sources	
All TCP	TCP	All ports	[redacted]	More
All UDP	UDP	All ports	[redacted]	More

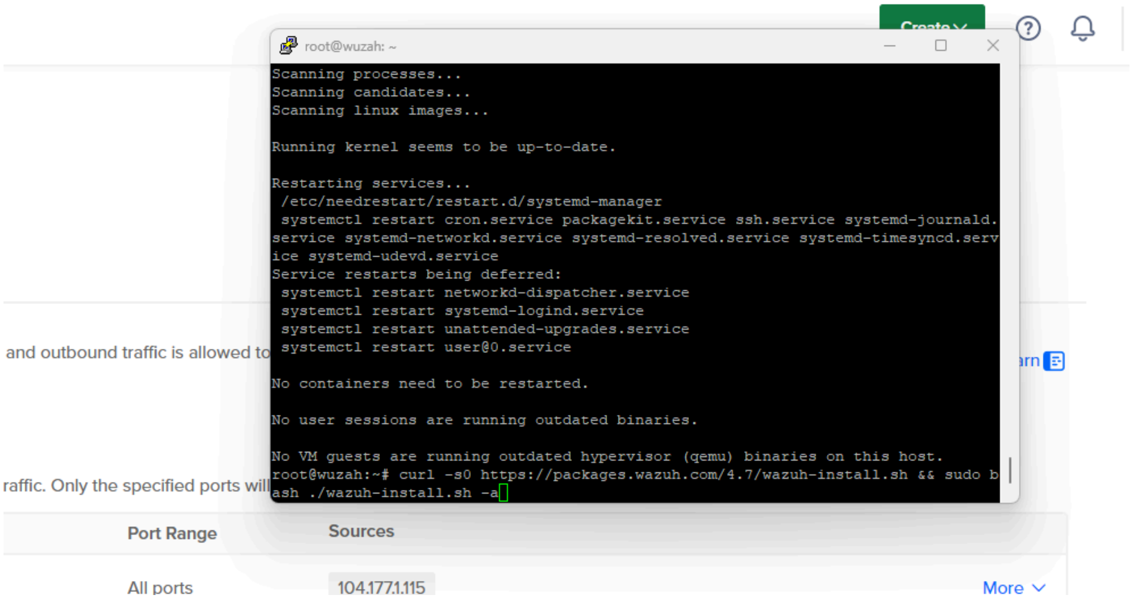
Outbound Rules

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

Type	Protocol	Port Range	Destinations	
ICMP	ICMP		All IPv4 All IPv6	More

Error

I was having trouble connecting to the SSH when using the Digital Ocean launcher. To fix this I download Putty. With Putty, I just inputted my IP for the Wazuh and connected to port 9000.

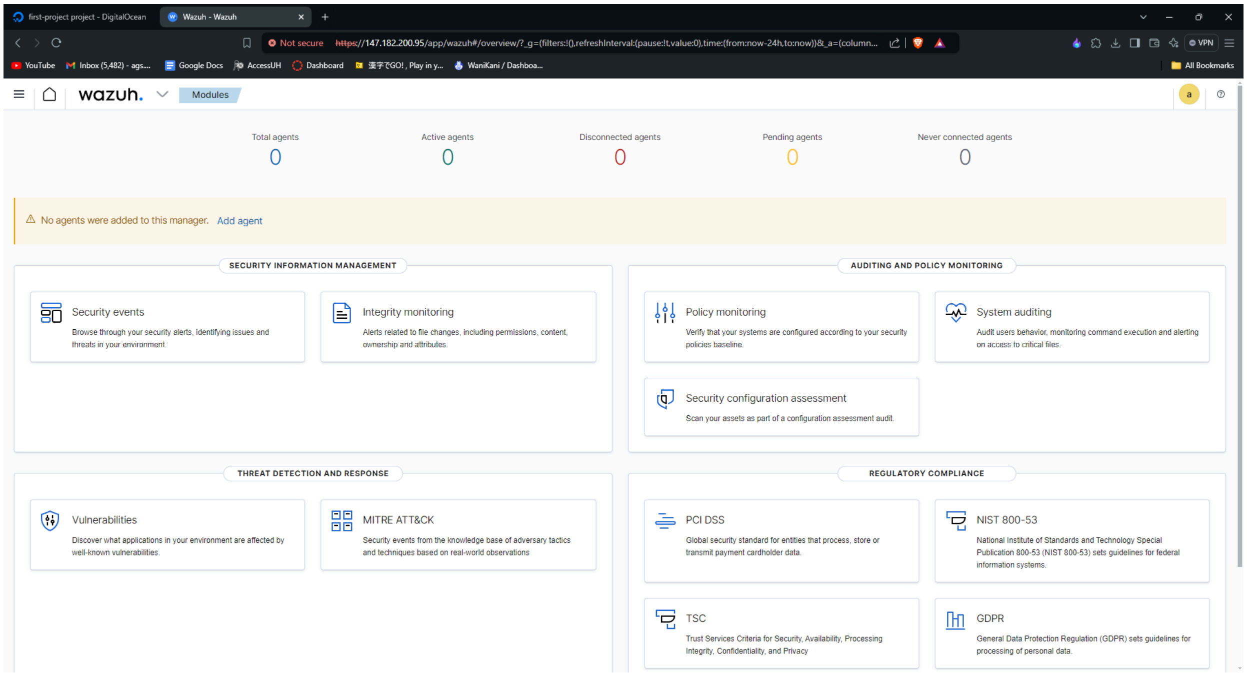


Create
root@wuzah: ~
and outbound traffic is allowed to
rn
raffic. Only the specified ports will
Port Range
Sources
All ports
104.177.1.115
More

```
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
 /etc/needrestart/restart.d/systemd-manager
 systemctl restart cron.service packagekit.service ssh.service systemd-journald.
service systemd-networkd.service systemd-resolved.service systemd-timesyncd.serv
ice systemd-udevd.service
Service restarts being deferred:
 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@wuzah:~# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo b
ash ./wazuh-install.sh -a
```

Installing Wazuh

After stalling Wazuh using the kurl command available on their website and “apt-get update && apt-get upgrade”. I typed in the IP address into my search engine which takes me to my Wazuh login. Wazuh provides login info after the app is installed. Using this info I was able to access the dashboard.



https://147.182.200.95/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(column...

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

⚠ No agents were added to this manager. Add agent

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.

THREAT DETECTION AND RESPONSE

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

MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE

PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.

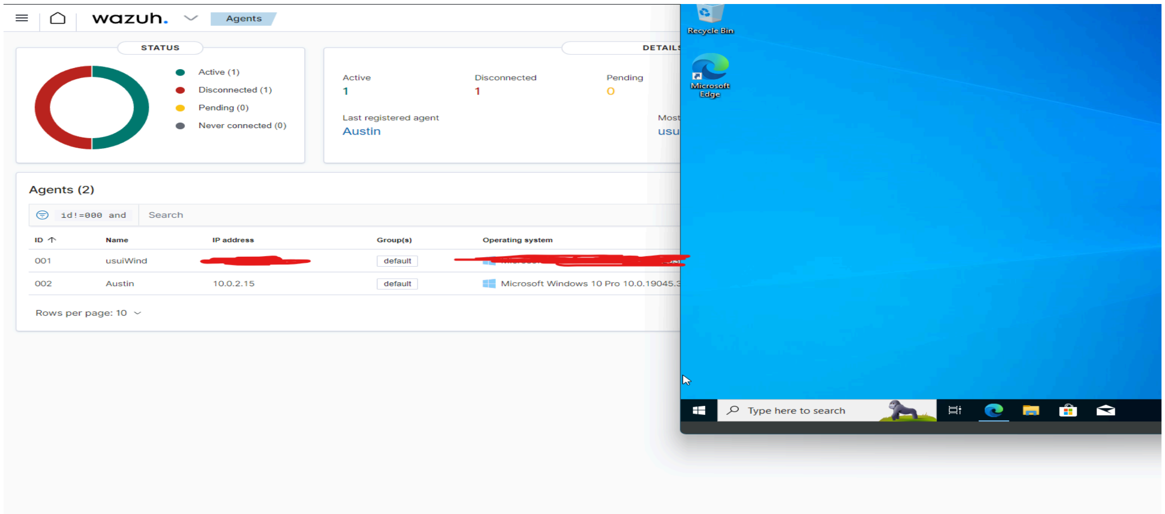
NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC
Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

Wazuh Agent on VM

To get the agent on wazuh. I simply go to the agent's tab from the hamburger menu. After clicking add agent. I will input my IP address since it is shared for the VM. I think copy pasted the commands to add the Wazuh agent. After accidentally adding it to my home computer and the VM. I have Wazuh on the Windows 10 VM.



Active	Disconnected	Pending
1	1	0

Last registered agent
Austin

Most
usu

Agents (2)

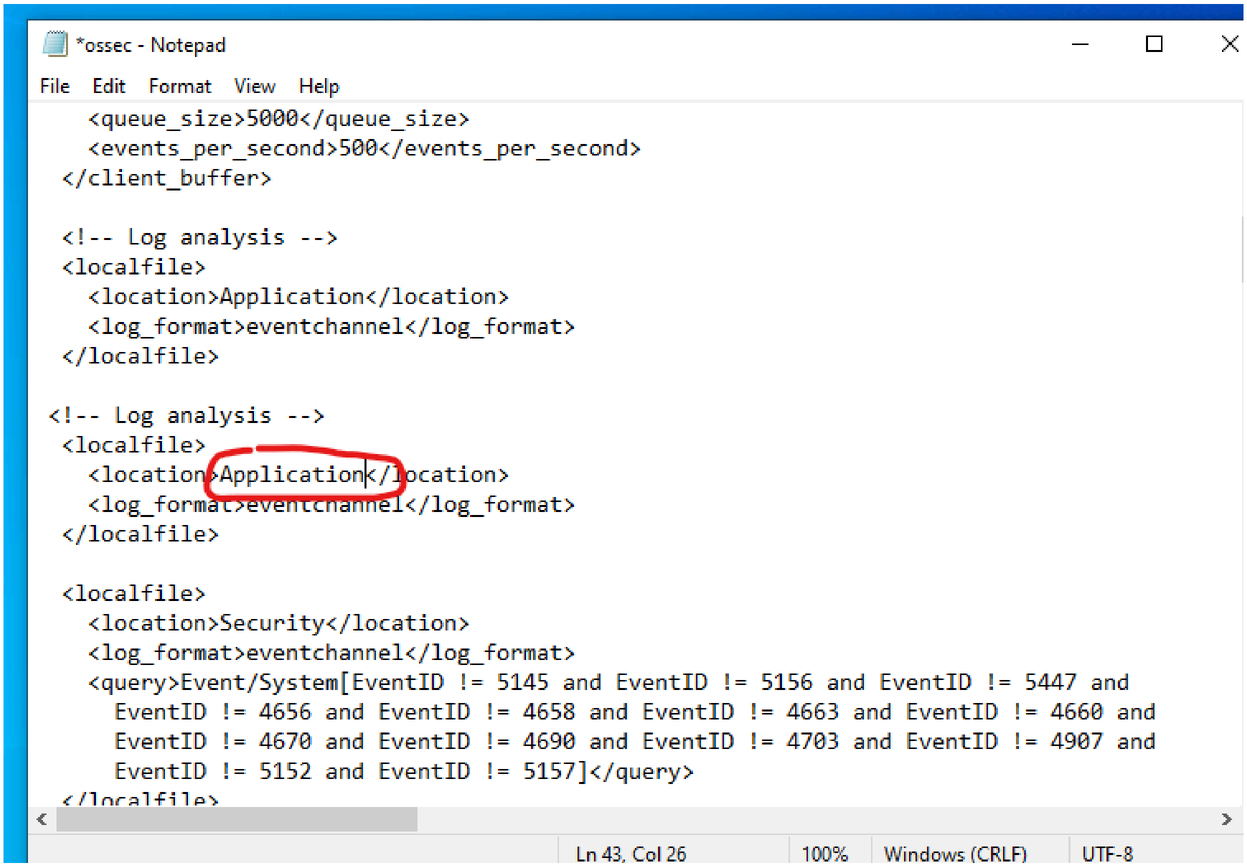
id!=000 and Search

ID ↑	Name	IP address	Group(s)	Operating system
001	usuiWind	[redacted]	default	[redacted]
002	Austin	10.0.2.15	default	Microsoft Windows 10 Pro 10.0.19045.3

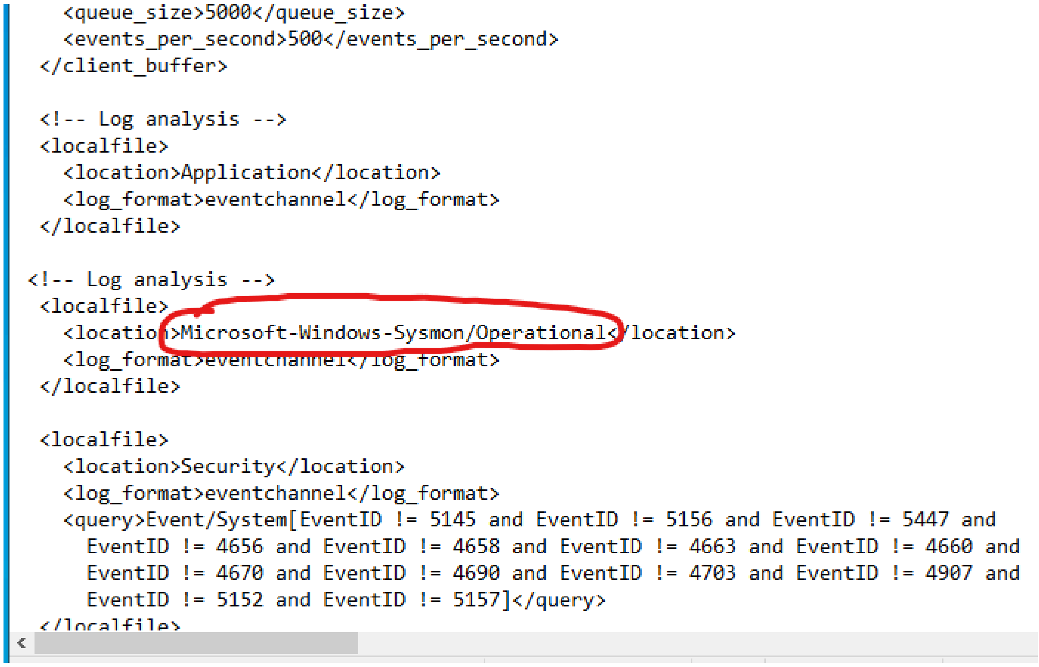
Rows per page: 10

Modifying Wazuh

I modify the Wazuh files to create a log for Sysmon. Replacing ‘application’ for application location for sysmon.

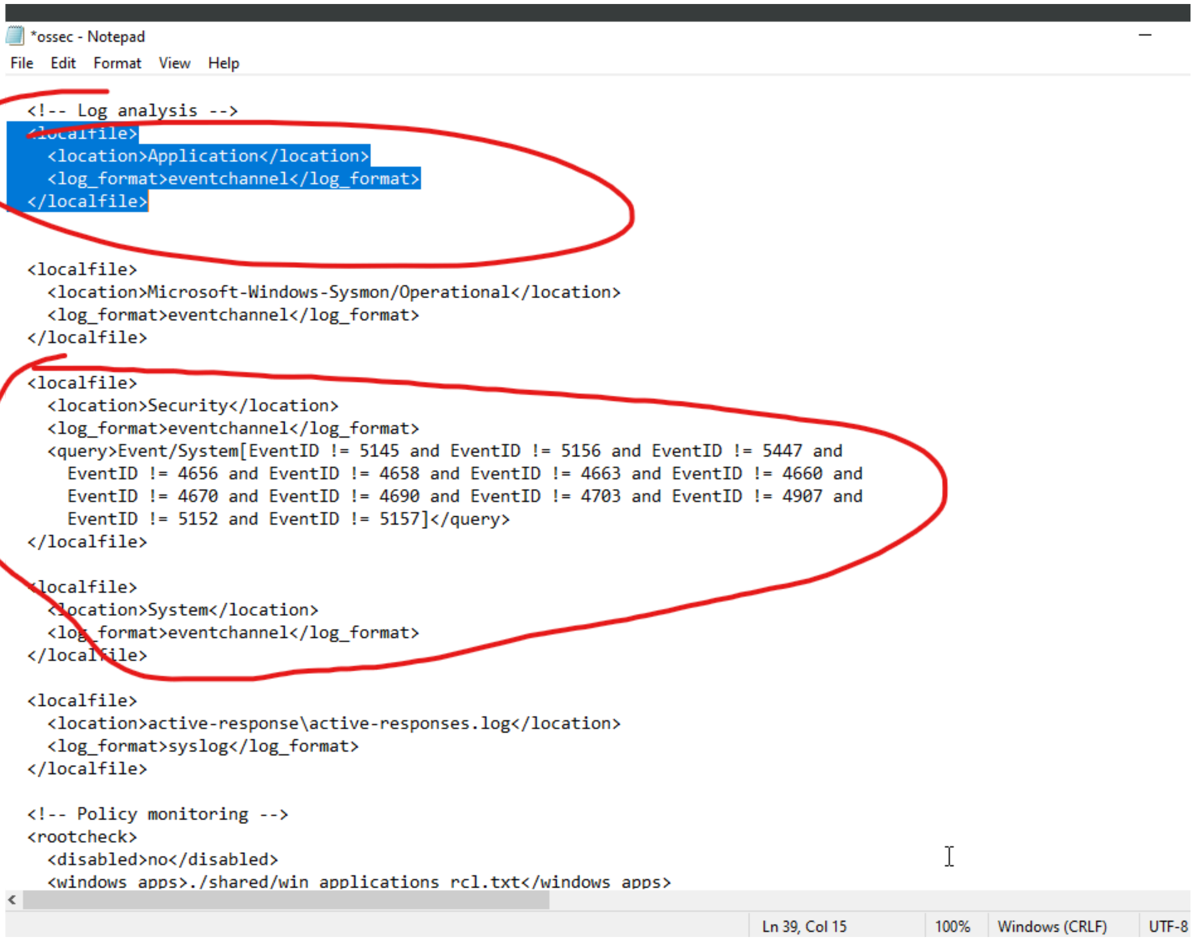


```
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

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

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

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



```
    <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>

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

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

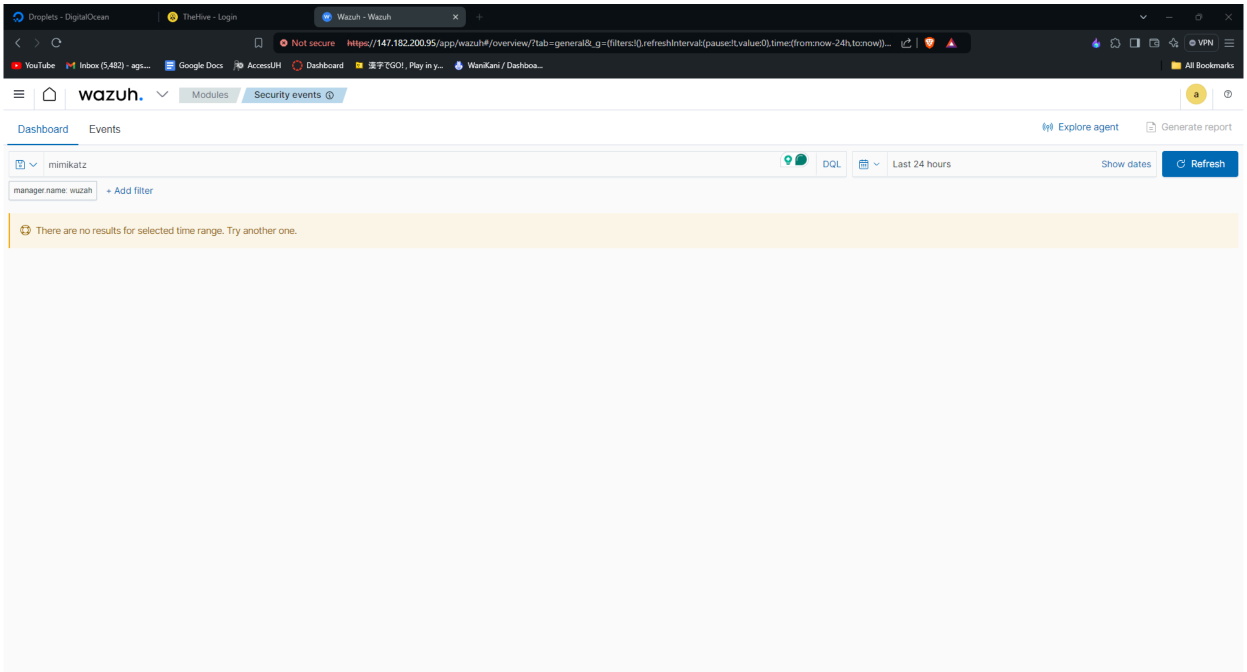
I then delete all these parts of the Wazuh so only sysmon events are stored.



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

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

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

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

<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>
```

Data Problem

There are no events on mimikatz or sysmon. This is because there are no rules for mimikatz and Wazuh does not log everything. Consequently, I changed Wazuh to log all. Additionally, I changed the filebeat to ingest all of the logs.

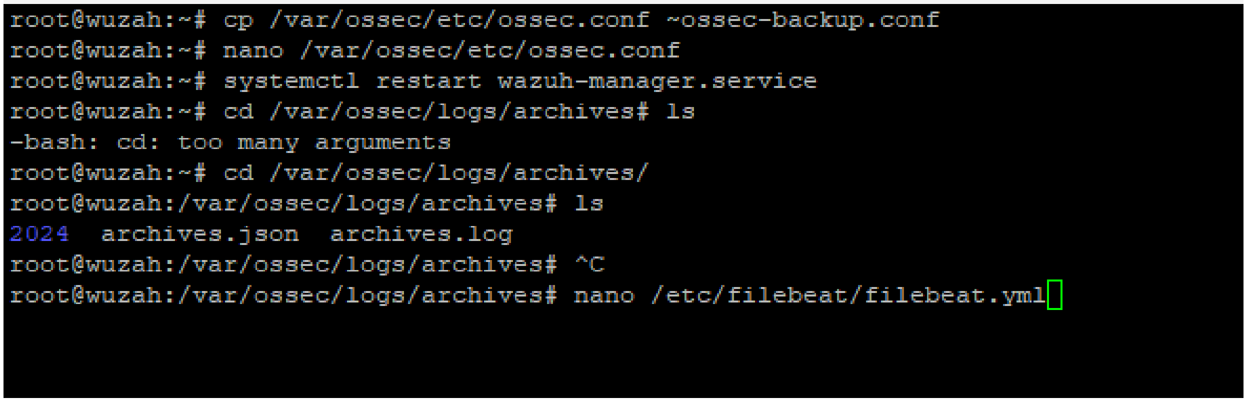


mimikatz

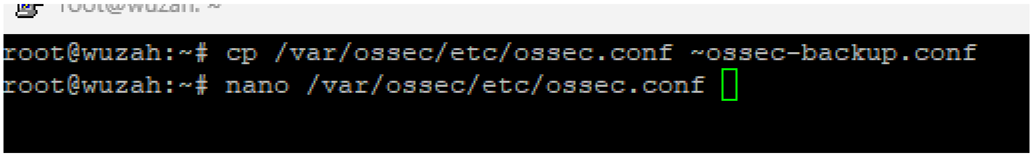
Last 24 hours

manager.name: wuzah

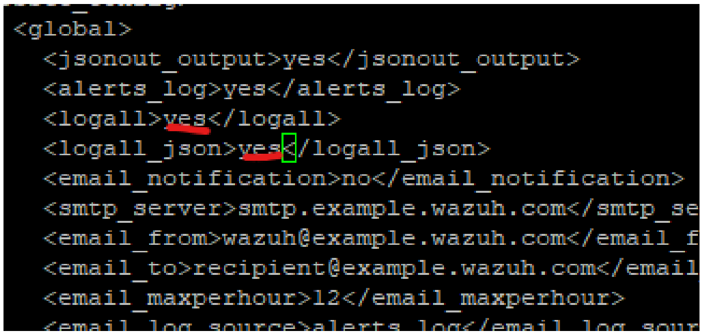
There are no results for selected time range. Try another one.



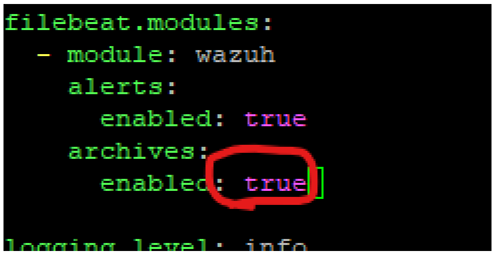
```
root@wuzah:~# cp /var/ossec/etc/ossec.conf ~ossec-backup.conf
root@wuzah:~# nano /var/ossec/etc/ossec.conf
root@wuzah:~# systemctl restart wazuh-manager.service
root@wuzah:~# cd /var/ossec/logs/archives# ls
-bash: cd: too many arguments
root@wuzah:~# cd /var/ossec/logs/archives/
root@wuzah:/var/ossec/logs/archives# ls
2024  archives.json  archives.log
root@wuzah:/var/ossec/logs/archives# ^C
root@wuzah:/var/ossec/logs/archives# nano /etc/filebeat/filebeat.yml
```



```
root@wuzah:~# cp /var/ossec/etc/ossec.conf ~ossec-backup.conf
root@wuzah:~# nano /var/ossec/etc/ossec.conf
```



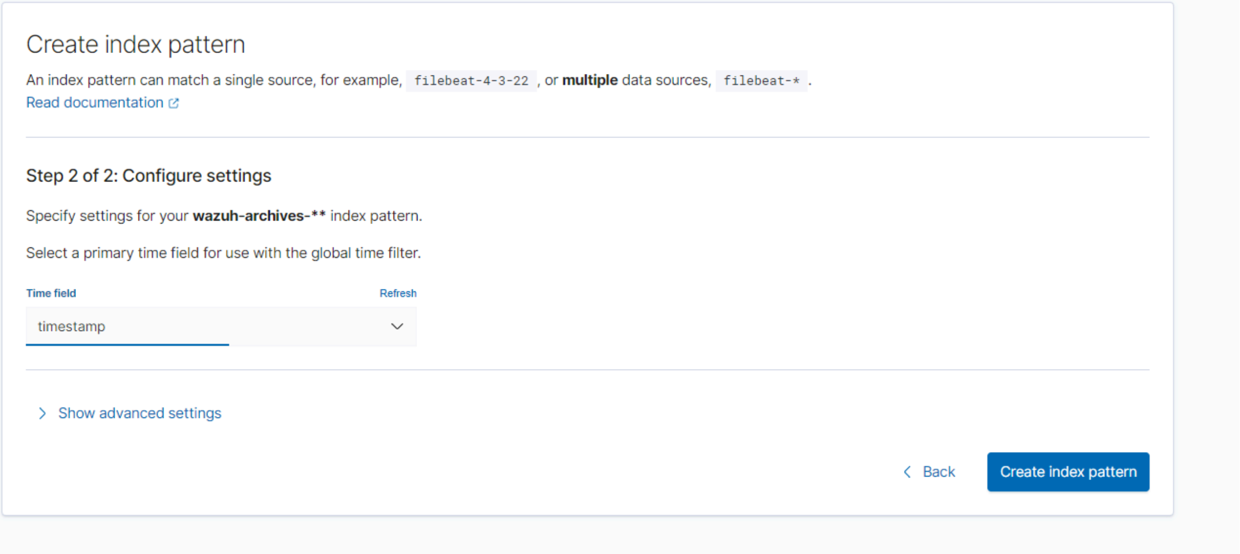
```
<global>
  <jsonout_output>yes</jsonout_output>
  <alerts_log>yes</alerts_log>
  <logall>yes</logall>
  <logall_json>yes</logall_json>
  <email_notification>no</email_notification>
  <smtp_server>smtp.example.wazuh.com</smtp_se
  <email_from>wazuh@example.wazuh.com</email_f
  <email_to>recipient@example.wazuh.com</email
  <email_maxperhour>12</email_maxperhour>
  <email_log_source>alerts_log</email_log_sour
```



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

logging.level: info
```

Index Creation:

Next I created an index for all the logs.Then execute bash commands to see that mimikatz is in the output of the archives (mimikatz in the red).



Create index pattern

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

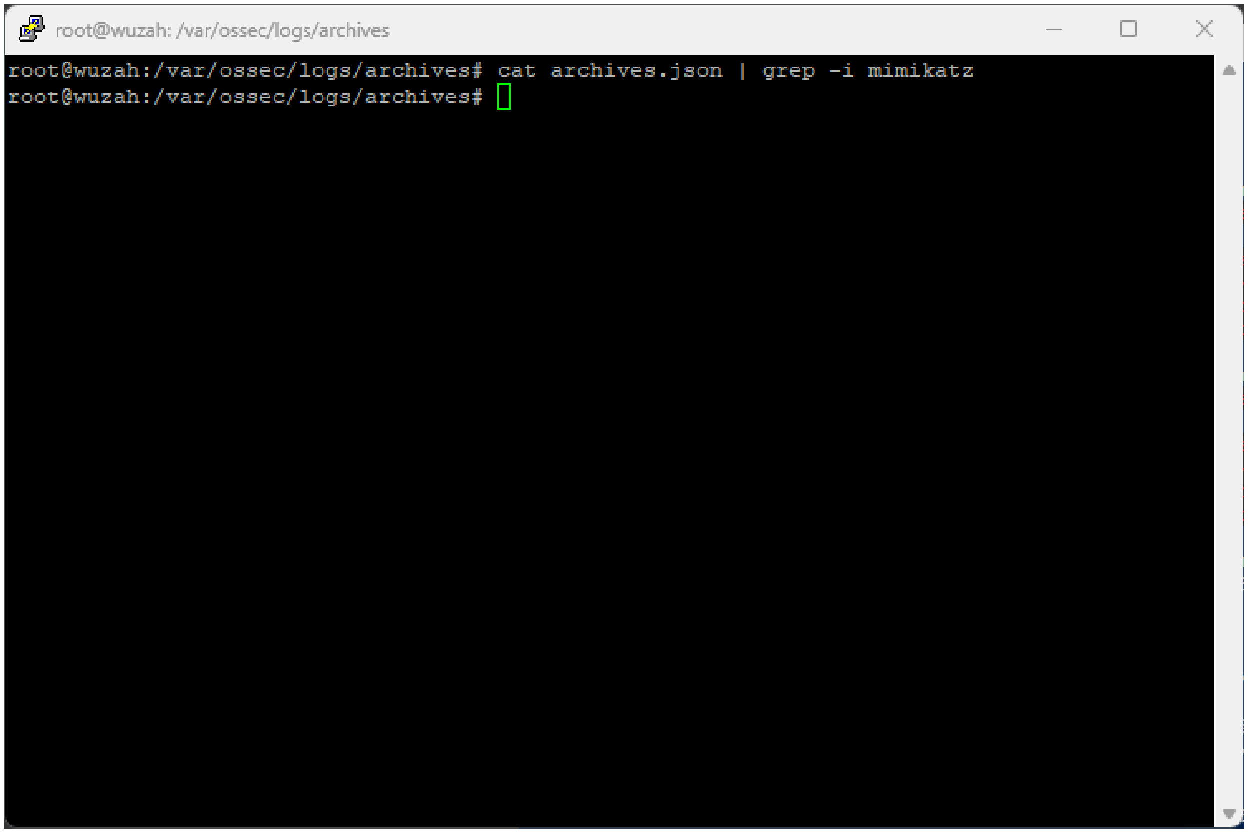
Read documentation

Step 2 of 2: Configure settings

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

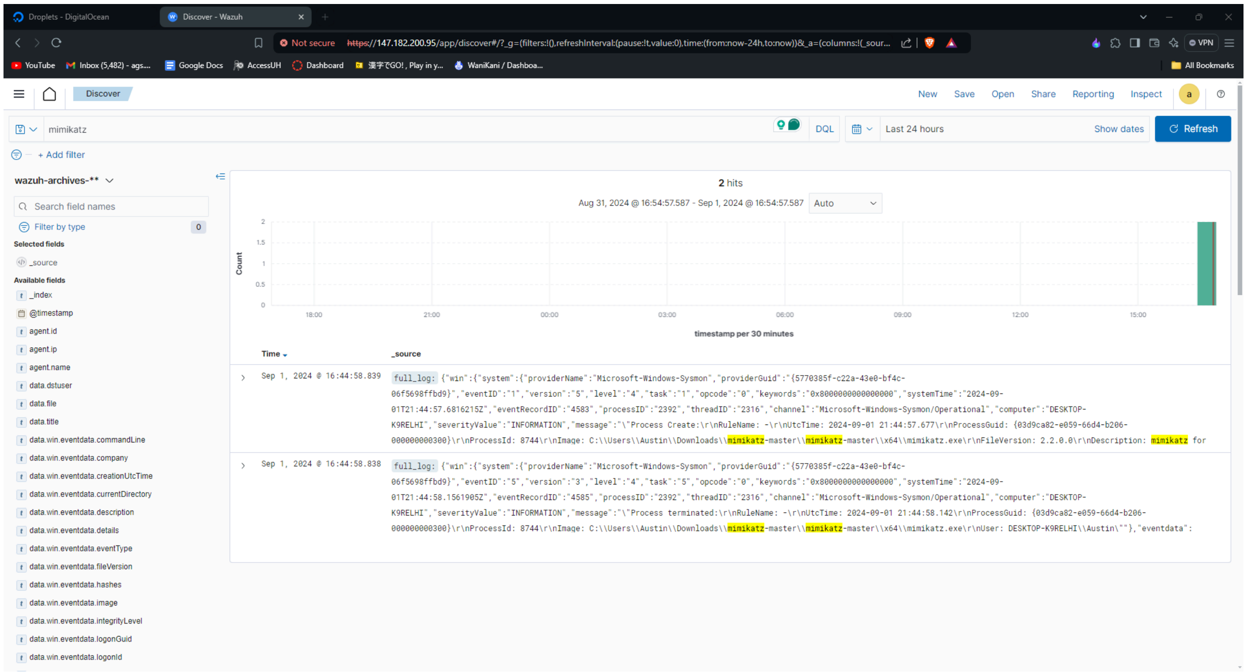
Select a primary time field for use with the global time filter.

Time field: timestamp

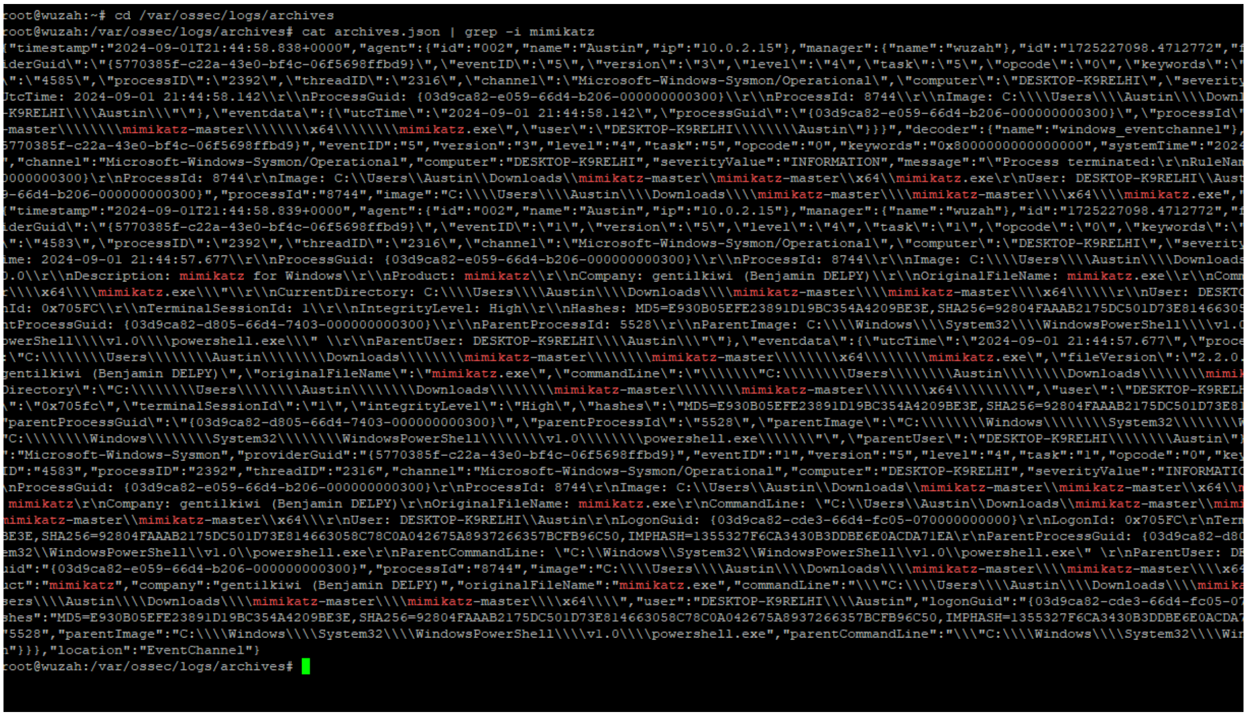


root@wuzah: /var/ossec/logs/archives

```
root@wuzah:/var/ossec/logs/archives# cat archives.json | grep -i mimikatz
root@wuzah:/var/ossec/logs/archives#
```


Droplets - DigitalOcean
Discover - Wazuh
Not secure
https://147.182.200.95/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_sour...
Discover
New
Save
Open
Share
Reporting
Inspect
DQL
Show dates
Refresh
+ Add filter
wazuh-archives-**
Search field names
Filter by type
Selected fields
_source
Available fields
_index
@timestamp
agent.id
agent.ip
agent.name
data.dstuser
data.file
data.title
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.hashes
data.win.eventdata.image
data.win.eventdata.integrityLevel
data.win.eventdata.logonGuid
data.win.eventdata.logonId
Count
timestamp per 30 minutes
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00

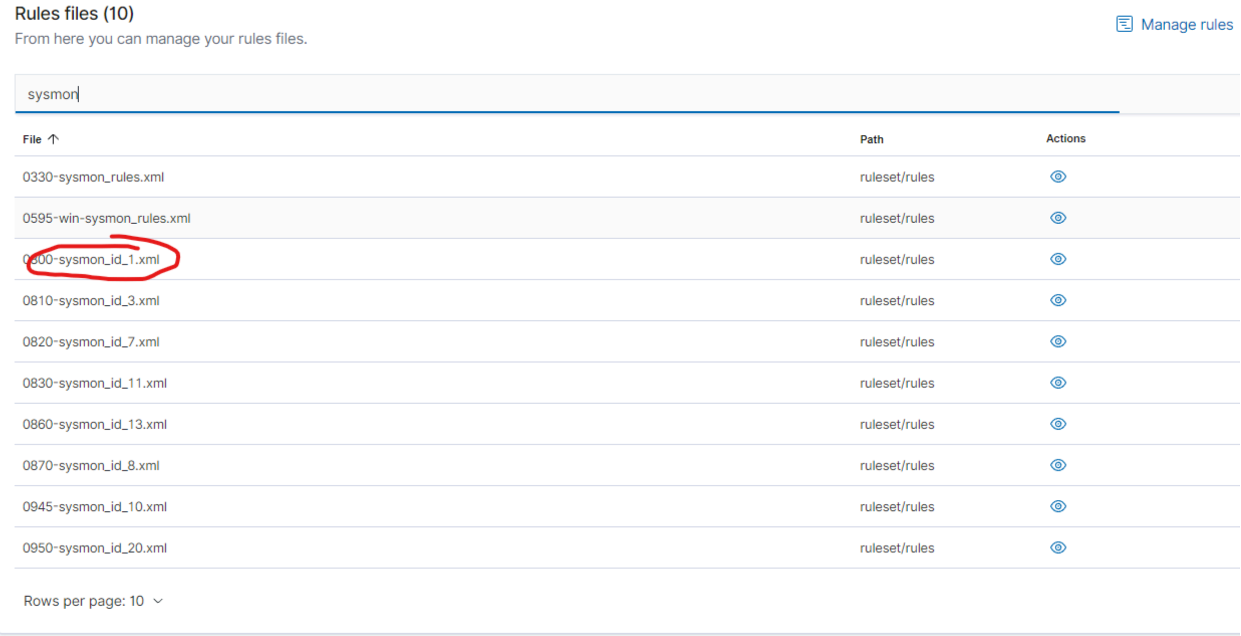
```
mimikatz
Last 24 hours
2 hits
Aug 31, 2024 @ 16:54:57.587 - Sep 1, 2024 @ 16:54:57.587   Auto

Time                          _source
Sep 1, 2024 @ 16:44:58.839    full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"1","version":"5","level":"4","task":"1","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024-09-01T21:44:57.6816215Z","eventRecordID":"4583","processID":"2392","threadID":"2316","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-K9RELHI","severityValue":"INFORMATION","message":"\"Process Create:\r\nRuleName: -\r\nUtcTime: 2024-09-01 21:44:57.677\r\nProcessGuid: {03d9ca82-e059-66d4-b206-000000000300}\r\nProcessId: 8744\r\nImage: C:\\Users\\Austin\\Downloads\\mimikatz-master\\mimikatz-master\\x64\\mimikatz.exe\r\nFileVersion: 2.2.0.0\r\nDescription: mimikatz for
Sep 1, 2024 @ 16:44:58.838    full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"5","version":"3","level":"4","task":"5","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024-09-01T21:44:58.1561905Z","eventRecordID":"4585","processID":"2392","threadID":"2316","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-K9RELHI","severityValue":"INFORMATION","message":"\"Process terminated:\r\nRuleName: -\r\nUtcTime: 2024-09-01 21:44:58.142\r\nProcessGuid: {03d9ca82-e059-66d4-b206-000000000300}\r\nProcessId: 8744\r\nImage: C:\\Users\\Austin\\Downloads\\mimikatz-master\\mimikatz-master\\x64\\mimikatz.exe\r\nUser: DESKTOP-K9RELHI\\Austin\""},"eventdata":
```



```
root@wuzah:~# cd /var/ossec/logs/archives
root@wuzah:/var/ossec/logs/archives# cat archives.json | grep -i mimikatz
{"timestamp":"2024-09-01T21:44:58.838+0000","agent":{"id":"002","name":"Austin","ip":"10.0.2.15"},"manager":{"name":"wuzah"},"id":"1725227098.4712772","f
iderGuid\":\"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}\",\"eventID\":\"5\",\"version\":\"3\",\"level\":\"4\",\"task\":\"5\",\"opcode\":\"0\",\"keywords\":\"
\":\"4585\",\"processID\":\"2392\",\"threadID\":\"2316\",\"channel\":\"Microsoft-Windows-Sysmon/Operational\",\"computer\":\"DESKTOP-K9RELHI\",\"severity
UtcTime: 2024-09-01 21:44:58.142\\r\\nProcessGuid: {03d9ca82-e059-66d4-b206-000000000300}\\r\\nProcessId: 8744\\r\\nImage: C:\\\\Users\\\\Austin\\\\Downl
-K9RELHI\\\\Austin\\\"\"},\"eventdata\":{\"utcTime\":\"2024-09-01 21:44:58.142\",\"processGuid\":\"{03d9ca82-e059-66d4-b206-000000000300}\",\"processId\"
-master\\\\\\\\mimikatz-master\\\\\\\\x64\\\\\\\\mimikatz.exe\",\"user\":\"DESKTOP-K9RELHI\\\\\\\\Austin\"}}}","decoder":{"name":"windows_eventchannel"},
5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"5","version":"3","level":"4","task":"5","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024
","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-K9RELHI","severityValue":"INFORMATION","message":"\"Process terminated:\r\nRuleNam
0000000300}\r\nProcessId: 8744\r\nImage: C:\\Users\\Austin\\Downloads\\mimikatz-master\\mimikatz-master\\x64\\mimikatz.exe\r\nUser: DESKTOP-K9RELHI\\Aust
9-66d4-b206-000000000300}","processId":"8744","image":"C:\\\\Users\\\\Austin\\\\Downloads\\\\mimikatz-master\\\\mimikatz-master\\\\x64\\\\mimikatz.exe","
{"timestamp":"2024-09-01T21:44:58.839+0000","agent":{"id":"002","name":"Austin","ip":"10.0.2.15"},"manager":{"name":"wuzah"},"id":"1725227098.4712772","f
iderGuid\":\"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}\",\"eventID\":\"1\",\"version\":\"5\",\"level\":\"4\",\"task\":\"1\",\"opcode\":\"0\",\"keywords\":\"
\":\"4583\",\"processID\":\"2392\",\"threadID\":\"2316\",\"channel\":\"Microsoft-Windows-Sysmon/Operational\",\"computer\":\"DESKTOP-K9RELHI\",\"severity
ime: 2024-09-01 21:44:57.677\\r\\nProcessGuid: {03d9ca82-e059-66d4-b206-000000000300}\\r\\nProcessId: 8744\\r\\nImage: C:\\\\Users\\\\Austin\\\\Downloads
0.0\\r\\nDescription: mimikatz for Windows\\r\\nProduct: mimikatz\\r\\nCompany: gentilkiwi (Benjamin DELPY)\\r\\nOriginalFileName: mimikatz.exe\\r\\nComm
r\\\\x64\\\\mimikatz.exe\\\"\\r\\nCurrentDirectory: C:\\\\Users\\\\Austin\\\\Downloads\\\\mimikatz-master\\\\mimikatz-master\\\\x64\\\\\\r\\nUser: DESKTO
nId: 0x705FC\\r\\nTerminalSessionId: 1\\r\\nIntegrityLevel: High\\r\\nHashes: MD5=E930B05EFE23891D19BC354A4209BE3E,SHA256=92804FAAAB2175DC501D73E8146630
ntProcessGuid: {03d9ca82-d805-66d4-7403-000000000300}\\r\\nParentProcessId: 5528\\r\\nParentImage: C:\\\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0
owerShell\\\\v1.0\\\\powershell.exe\\\" \\r\\nParentUser: DESKTOP-K9RELHI\\\\Austin\\\"\"},\"eventdata\":{\"utcTime\":\"2024-09-01 21:44:57.677\",\"proce
:\"C:\\\\\\\\Users\\\\\\\\Austin\\\\\\\\Downloads\\\\\\\\mimikatz-master\\\\\\\\mimikatz-master\\\\\\\\x64\\\\\\\\mimikatz.exe\",\"fileVersion\":\"2.2.0.
gentilkiwi (Benjamin DELPY)\",\"originalFileName\":\"mimikatz.exe\",\"commandLine\":\"\\\\\\\"C:\\\\\\\\Users\\\\\\\\Austin\\\\\\\\Downloads\\\\\\\\mimik
Directory\":\"C:\\\\\\\\Users\\\\\\\\Austin\\\\\\\\Downloads\\\\\\\\mimikatz-master\\\\\\\\mimikatz-master\\\\\\\\x64\\\\\\\\\",\"user\":\"DESKTOP-K9RELH
\":\"0x705fc\",\"terminalSessionId\":\"1\",\"integrityLevel\":\"High\",\"hashes\":\"MD5=E930B05EFE23891D19BC354A4209BE3E,SHA256=92804FAAAB2175DC501D73E8
"parentProcessGuid\":\"{03d9ca82-d805-66d4-7403-000000000300}\",\"parentProcessId\":\"5528\",\"parentImage\":\"C:\\\\\\\\Windows\\\\\\\\System32\\\\\\\\W
"C:\\\\\\\\Windows\\\\\\\\System32\\\\\\\\WindowsPowerShell\\\\\\\\v1.0\\\\\\\\powershell.exe\\\\\\\"\",\"parentUser\":\"DESKTOP-K9RELHI\\\\\\\\Austin\"}
":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"1","version":"5","level":"4","task":"1","opcode":"0","key
ID":"4583","processID":"2392","threadID":"2316","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-K9RELHI","severityValue":"INFORMATIC
\nProcessGuid: {03d9ca82-e059-66d4-b206-000000000300}\r\nProcessId: 8744\r\nImage: C:\\Users\\Austin\\Downloads\\mimikatz-master\\mimikatz-master\\x64\\m
 mimikatz\r\nCompany: gentilkiwi (Benjamin DELPY)\r\nOriginalFileName: mimikatz.exe\r\nCommandLine: \"C:\\Users\\Austin\\Downloads\\mimikatz-master\\mimi
mimikatz-master\\mimikatz-master\\x64\\\r\nUser: DESKTOP-K9RELHI\\Austin\r\nLogonGuid: {03d9ca82-cde3-66d4-fc05-070000000000}\r\nLogonId: 0x705FC\r\nTerm
BE3E,SHA256=92804FAAAB2175DC501D73E814663058C78C0A042675A8937266357BCFB96C50,IMPHASH=1355327F6CA3430B3DDBE6E0ACDA71EA\r\nParentProcessGuid: {03d9ca82-d80
em32\\WindowsPowerShell\\v1.0\\powershell.exe\r\nParentCommandLine: \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \r\nParentUser: DE
uid":"{03d9ca82-e059-66d4-b206-000000000300}","processId":"8744","image":"C:\\\\Users\\\\Austin\\\\Downloads\\\\mimikatz-master\\\\mimikatz-master\\\\x64
uct":"mimikatz","company":"gentilkiwi (Benjamin DELPY)","originalFileName":"mimikatz.exe","commandLine":"\\\"C:\\\\Users\\\\Austin\\\\Downloads\\\\mimika
sers\\\\Austin\\\\Downloads\\\\mimikatz-master\\\\mimikatz-master\\\\x64\\\\","user":"DESKTOP-K9RELHI\\\\Austin","logonGuid":"{03d9ca82-cde3-66d4-fc05-07
shes":"MD5=E930B05EFE23891D19BC354A4209BE3E,SHA256=92804FAAAB2175DC501D73E814663058C78C0A042675A8937266357BCFB96C50,IMPHASH=1355327F6CA3430B3DDBE6E0ACDA7
"5528","parentImage":"C:\\\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\powershell.exe","parentCommandLine":"\\\"C:\\\\Windows\\\\System32\\\\Wir
h"}}},"location":"EventChannel"}
root@wuzah:/var/ossec/logs/archives#
```

Rule creation:

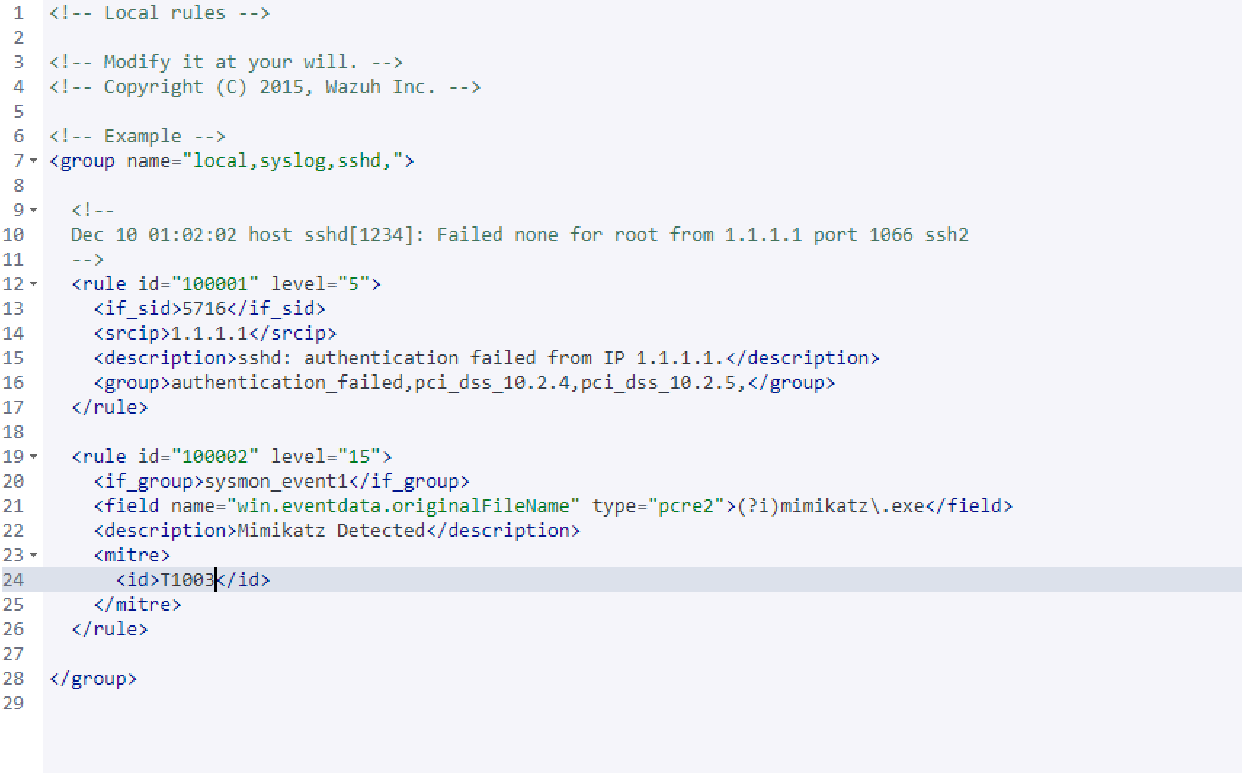
Next is the rule creation. Copying an existing sysmon rule then changing the rule id, field name, description, and id gave me a custom rule to detect mimikatz. Then after running mimikatz after changing the name of the file still yielded results showing our rule was a success.



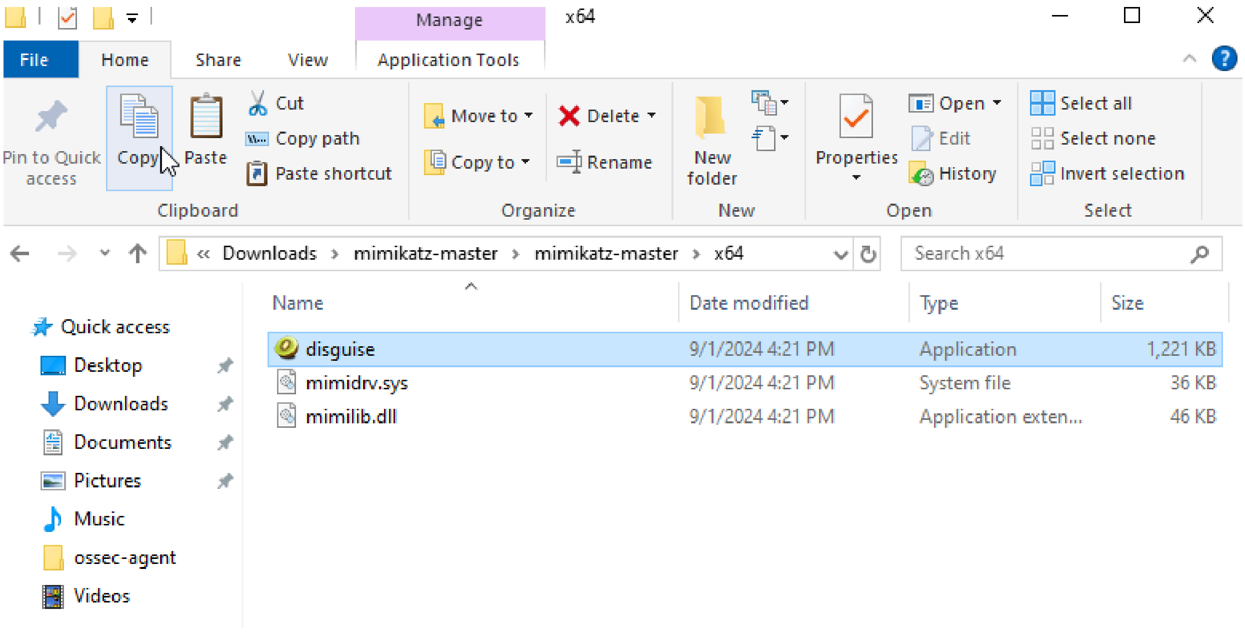
Rules files (10)

From here you can manage your rules files.

File ↑	Path	Actions
0330-sysmon_rules.xml	ruleset/rules	👁
0595-win-sysmon_rules.xml	ruleset/rules	👁
0800-sysmon_id_1.xml	ruleset/rules	👁
0810-sysmon_id_3.xml	ruleset/rules	👁
0820-sysmon_id_7.xml	ruleset/rules	👁
0830-sysmon_id_11.xml	ruleset/rules	👁
0860-sysmon_id_13.xml	ruleset/rules	👁
0870-sysmon_id_8.xml	ruleset/rules	👁
0945-sysmon_id_10.xml	ruleset/rules	👁
0950-sysmon_id_20.xml	ruleset/rules	👁

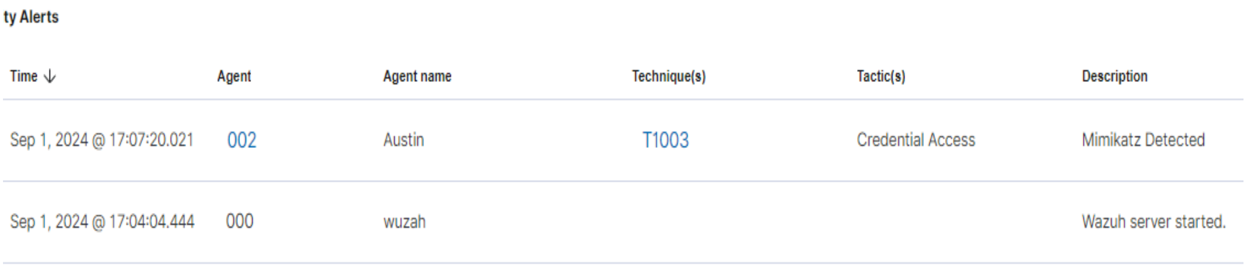


```xml
<!-- Local rules -->

<!-- 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 Detected</description>
    <mitre>
      <id>T1003</id>
    </mitre>
  </rule>

</group>
```



« Downloads › mimikatz-master › mimikatz-master › x64

Name	Date modified	Type	Size
disguise	9/1/2024 4:21 PM	Application	1,221 KB
mimidrv.sys	9/1/2024 4:21 PM	System file	36 KB
mimilib.dll	9/1/2024 4:21 PM	Application exten...	46 KB



ty Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description
Sep 1, 2024 @ 17:07:20.021	002	Austin	T1003	Credential Access	Mimikatz Detected
Sep 1, 2024 @ 17:04:04.444	000	wuzah			Wazuh server started.