CBD Lists

SAMEER HASSAN

Wazuh lab

GitHub-link: GitHub - sameerhassancode/Wazuh-labs

Linkedin: https://www.linkedin.com/in/sameer-hassan-15a428255/

Constant Database - CBD

Constant Database (CDB) lists in Wazuh are a powerful feature designed to organize data and enhance security monitoring. These structured lists are used by various Wazuh modules to streamline threat detection and response.

Purpose

1. **Organized Data Handling**: CDB lists help maintain structured information like IPs, domains, or usernames for security use.
2. **Improved Performance**: They enable fast data lookups, which is key for real-time alerting.
3. **Rule Integration**: They can be linked directly into Wazuh rules, enriching detection logic with context-aware data.

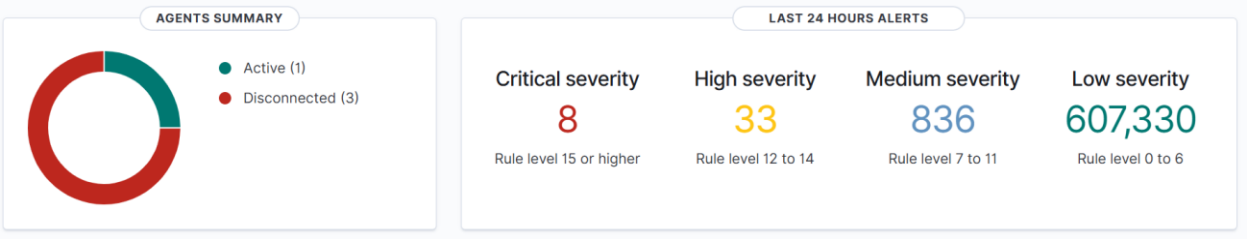
Key Advantages

- **Scalable**: Suited for large datasets in enterprise settings.
- **Customizable**: You can create multiple lists for different types of data.
- **Easy to Manage**: Easily maintained through configuration files.

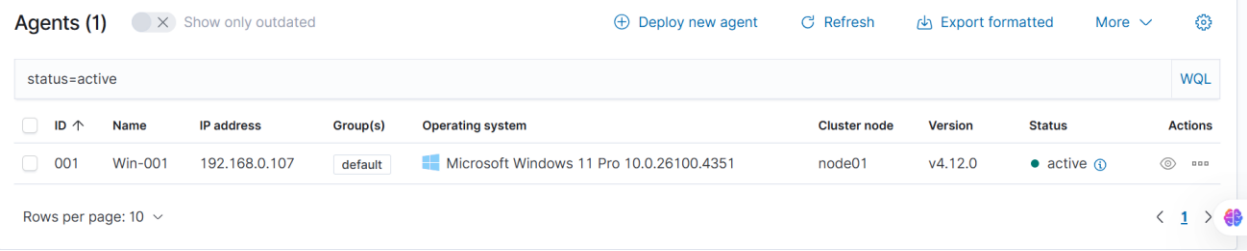
Common Uses

- **IP Blacklists**: Flag known malicious IPs in incoming data.
- **Domain Surveillance**: Detect and respond to traffic involving risky or known bad domains.
- **User Activity Tracking**: Monitor high-risk or privileged users for unusual behavior.

Wazuh-Dashboard:



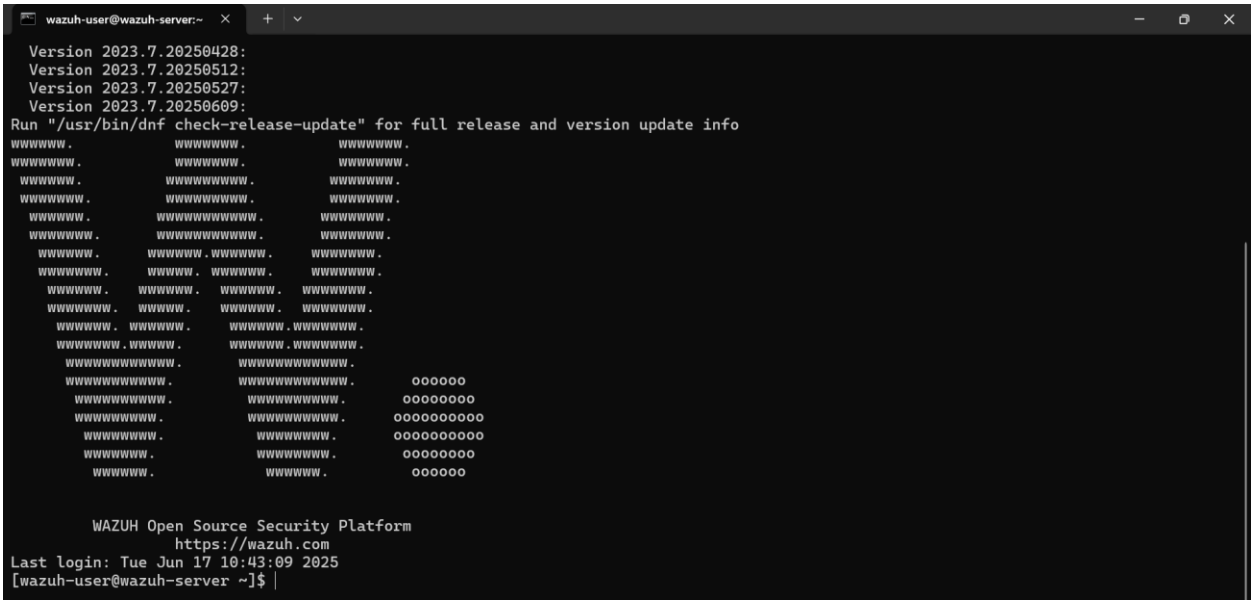
Agent:



SSH Access:

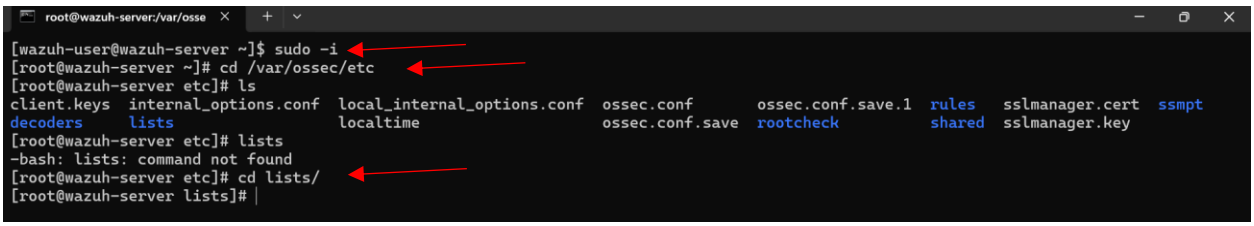
Command:

ssh wazuh-user@192.168.0.111



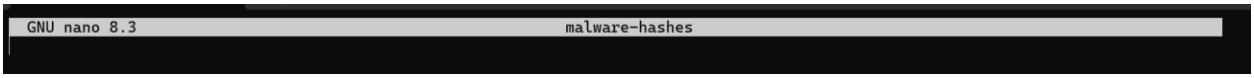
Now We have to Create CBD malware list:

Change directory to
cd /var/ossec/etc and then **lists**



Create New file **“malware-hashes”**

Nano malware-hashes



We will use this file to store malicious hashes of malware to detect.

Let’s configure all other files then we will comeback to this file again for storing malware hashes!

Change the Directory to ETC:

Change directory to etc and open the ossec.conf file.

```
[root@wazuh-server lists]# cd ..
[root@wazuh-server etc]# ls
client.keys  internal_options.conf  local_internal_options.conf  ossec.conf       ossec.conf.save.1  rules   sslmanager.cert  ssmpt
decoders     lists                  localtime                   ossec.conf.save  rootcheck          shared  sslmanager.key
[root@wazuh-server etc]# nano ossec.conf
```

Now look for lists tags **<lists>**

```
<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <rule_exclude>0215-policy_rules.xml</rule_exclude>
  <list>etc/lists/audit-keys</list>
  <list>etc/lists/amazon/aws-eventnames</list>
  <list>etc/lists/security-eventchannel</list>

  <!-- User-defined ruleset -->
  <decoder_dir>etc/decoders</decoder_dir>
  <rule_dir>etc/rules</rule_dir>

</ruleset>
```

Add the path of malware-hashes file

Command:

<lists>/etc/lists/malware-hashes</lists>

```
<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <rule_exclude>0215-policy_rules.xml</rule_exclude>
  <list>etc/lists/audit-keys</list>
  <list>etc/lists/amazon/aws-eventnames</list>
  <list>etc/lists/security-eventchannel</list>

      <!-- Malware-hashes to store -->
  <list>etc/lists/malware-hashes</list>
```

Configure Local Rules:

Now change directory to rule folder and open **local_rules.xml**

```
[root@wazuh-server etc]# ls
client.keys  internal_options.conf  local_internal_options.conf  ossec.conf       ossec.conf.save.1  rules   sslmanager.cert  ssmpt
decoders     lists                  localtime                   ossec.conf.save  rootcheck          shared  sslmanager.key
[root@wazuh-server etc]# cd rules
[root@wazuh-server rules]# nano local_rules.xml
```

```
 GNU nano 8.3                                          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">
```

Scroll down till the end and add this

```
<group name="malware">

  <rule id="110002" level="13">

    <if_sid>554</if_sid>

    <if_sid>550</if_sid>

    <list field="md5" lookup="match_key">etc/lists/malware-hashes</list>

    <description>Known malware hash is detected</description>

    <mitre>

      <id>T1204.002</id>

    </mitre>

  </rule>

</group>
```

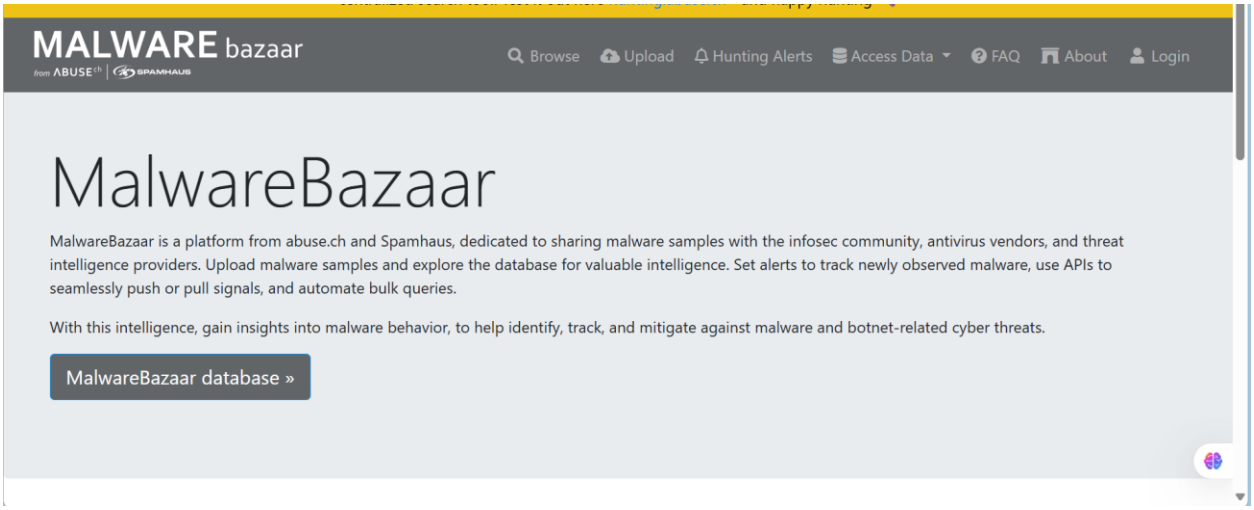
```
<group name="malware">
  <rule id="110002" level="13">
    <if_sid>554</if_sid>
    <if_sid>550</if_sid>
    <list field="md5" lookup="match_key">etc/lists/malware-hashes</list>
    <description>Known malware hash is detected</description>
    <mitre>
      <id>T1204.002</id>
    </mitre>
  </rule>
</group>
```

After saving the file restart the Wazuh-manager

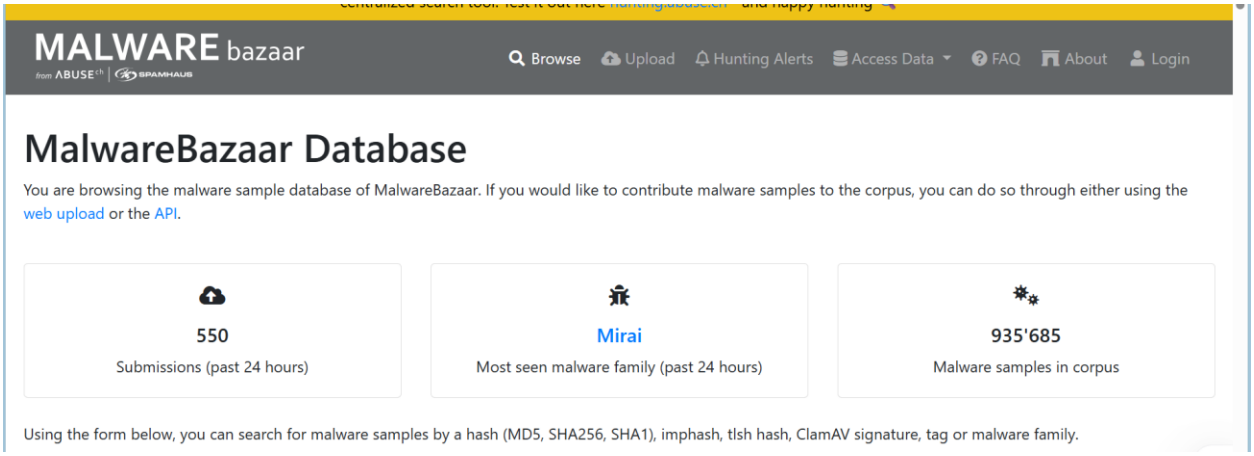
```
[root@wazuh-server rules]# systemctl restart wazuh-manager
```

Note: I added the download folder path in FIM (file integrity monitoring) please check your path and save malware file there.

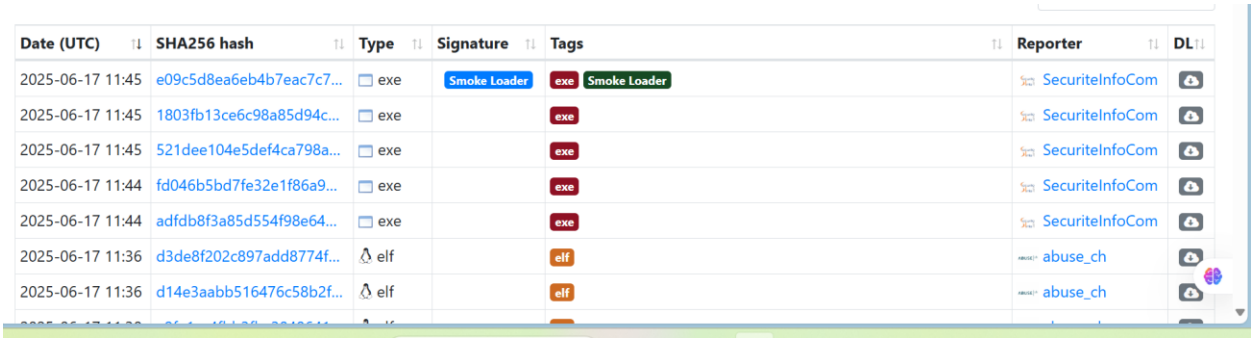
Now open Malware Bazar Site and copy some Malware hashes.



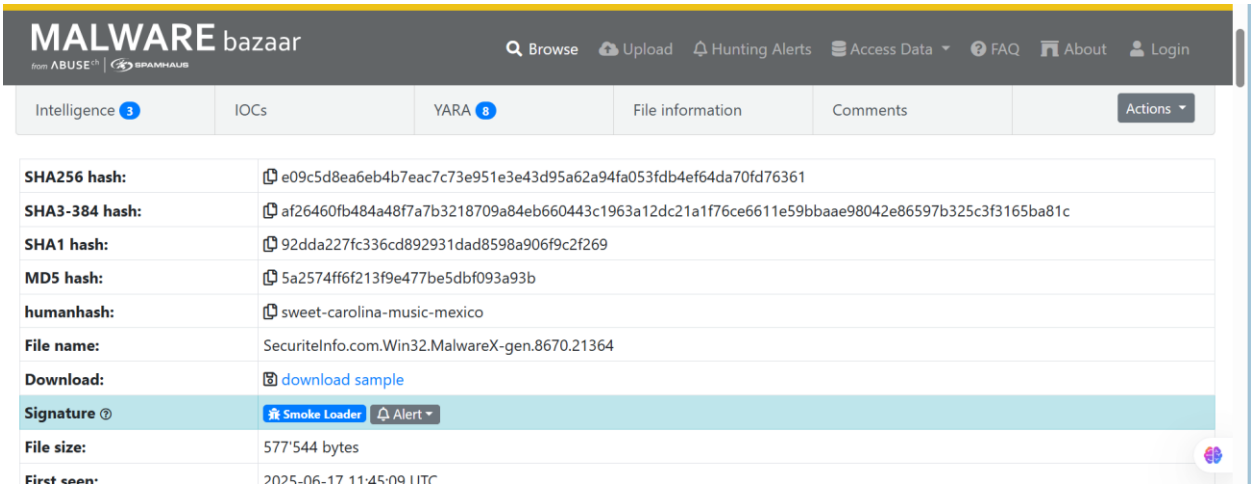
Click on malwareBazar database



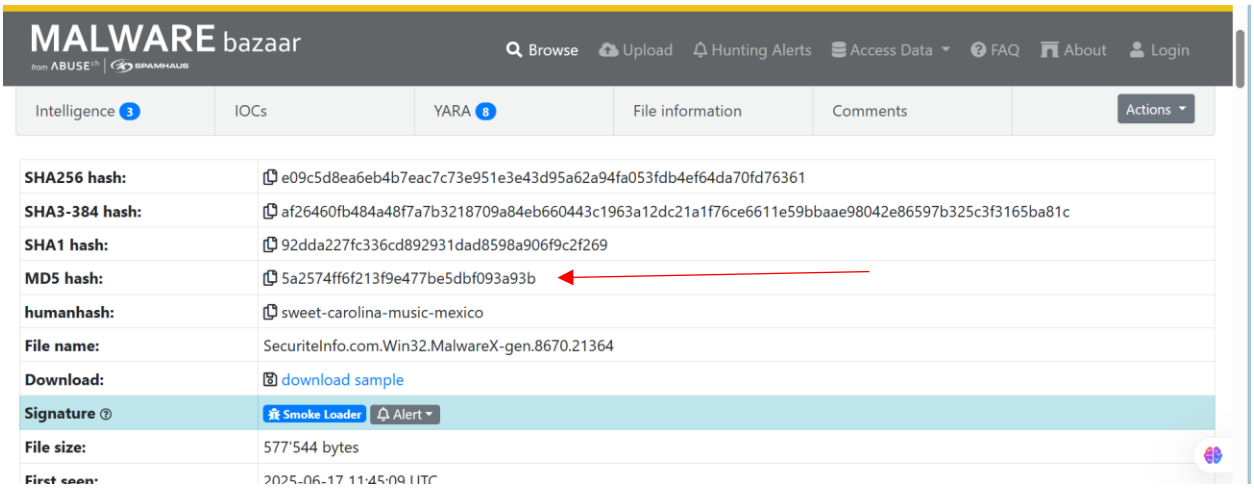
Scroll down and you will so many malware samples:



Select any and open it.

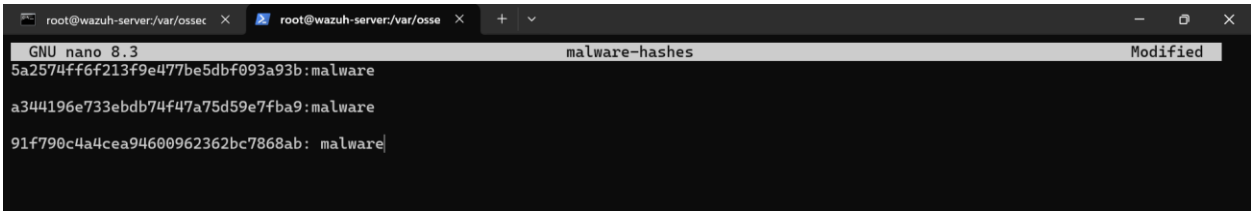


Copy the md5 of this malware:

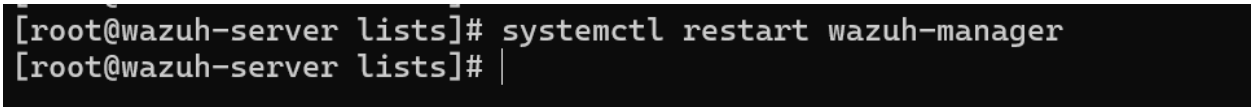


Paste this md5 hash in the malware-hash file.

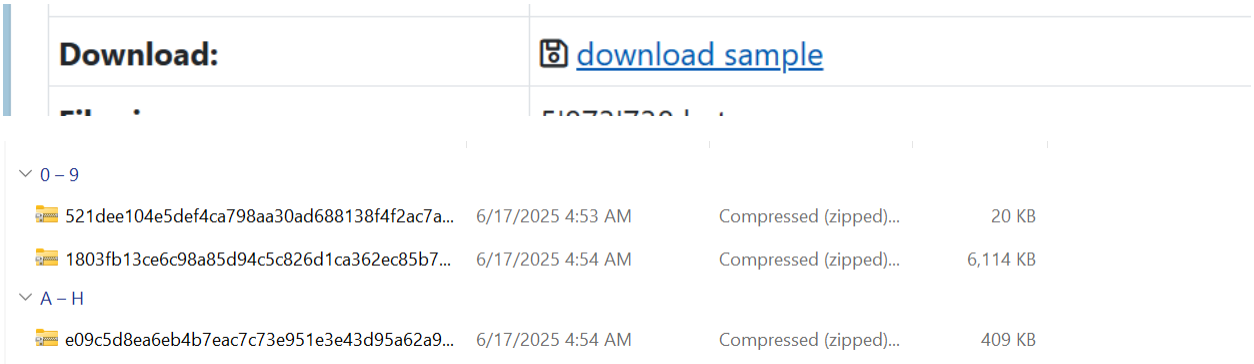
Add some more Malware hashes for better result.



Now save the file and restart Wazuh-manager!

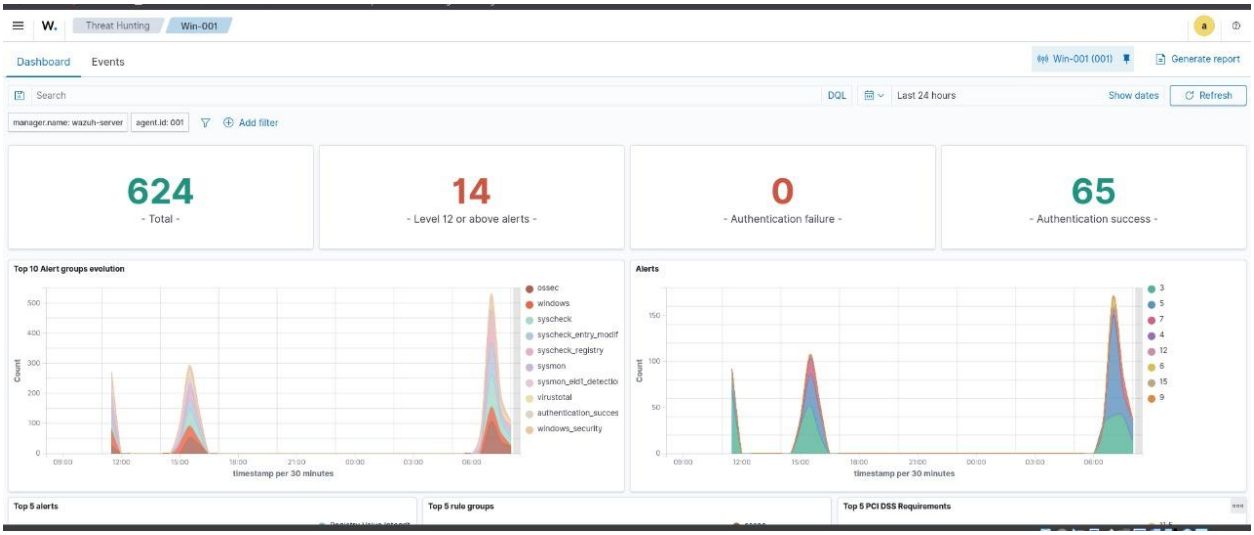


After saving and restarting the hashes download the malware samples

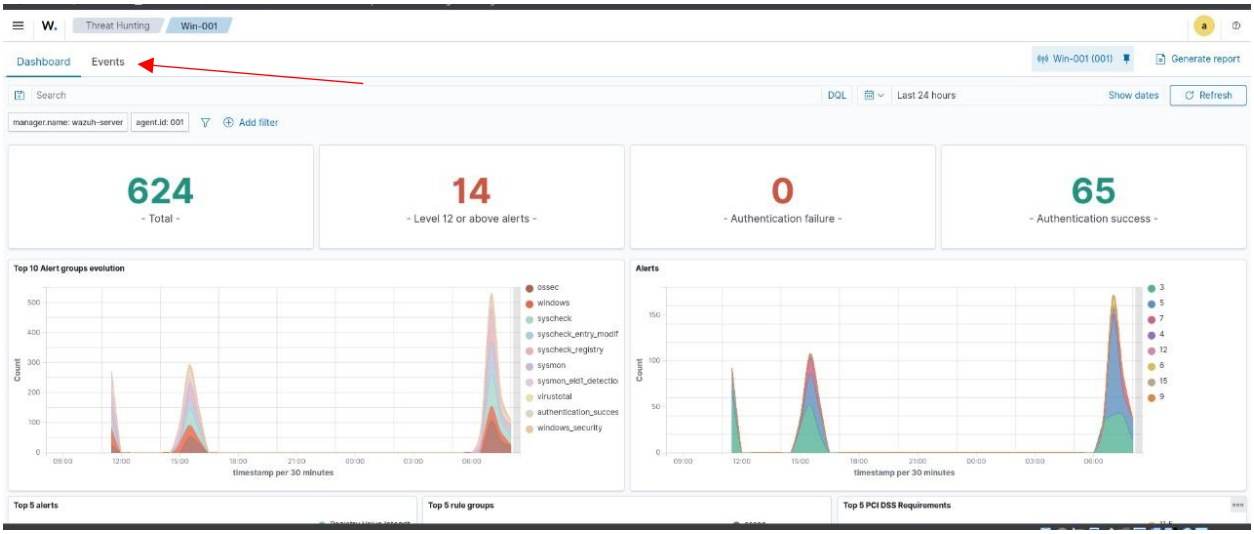


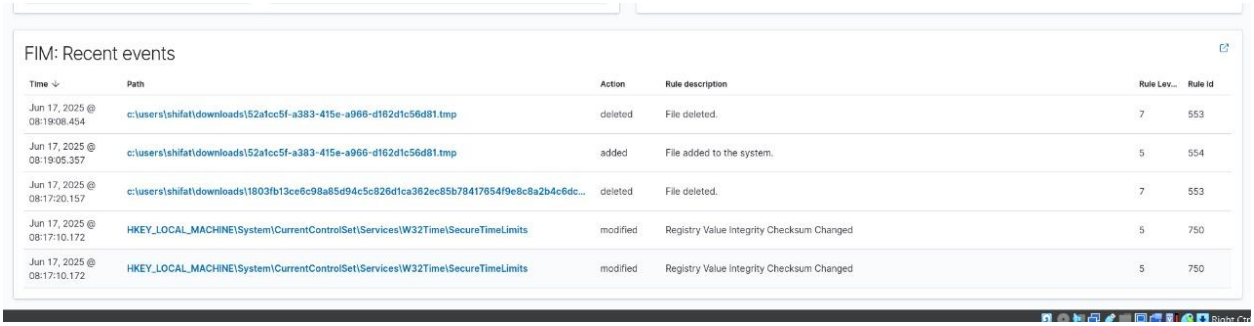
Now extract this with password: infected

After open Wazuh dashboard and go to threat hunting section:



Now click on Events:





FIM: Recent events

Time	Path	Action	Rule description	Rule Lev...	Rule id
Jun 17, 2025 @ 08:19:08.454	c:\users\shifat\downloads\52a1cc5f-a383-415e-a966-d162d1c56d81.tmp	deleted	File deleted.	7	553
Jun 17, 2025 @ 08:19:05.357	c:\users\shifat\downloads\52a1cc5f-a383-415e-a966-d162d1c56d81.tmp	added	File added to the system.	5	554
Jun 17, 2025 @ 08:17:20.157	c:\users\shifat\downloads\1803fb13ce6c98a85d94c5c826d1ca362ec85b78417654f9e8c8a2b4c6dc...	deleted	File deleted.	7	553
Jun 17, 2025 @ 08:17:10.172	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750
Jun 17, 2025 @ 08:17:10.172	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750

Table JSON

t	_index	wazuh-alerts-4.x-2024.05.18
t	agent.id	001
t	agent.ip	192.168.100.32
t	agent.name	Windows11
t	decoder.name	syscheck_new_entry
t	full_log	File 'c:\users\windows11\downloads\malware.exe' added Mode: realtime
t	id	1716060692.82931444
t	input.type	log
t	location	syscheck
t	manager.name	wazuh-server
t	rule.description	Known Malware File Hash is detected in Moizuddin Rafay Computer System: c:\users\windows11\downloads\malware.exe
#	rule.firedtimes	4

Summary:

CDB lists in Wazuh play a critical role in strengthening security monitoring. By organizing structured data efficiently, they support faster and more accurate threat detection. This makes them a valuable asset for security operations teams aiming to improve threat response and overall security posture.

Need training on Wazuh ?

Contact number: +923355345678

Email: sameeerishassan@gmail.com

LinkedIn: https://pk.linkedin.com/in/sameer-hassan-15a428255

Other SIEM

1. IBM Qradar

2. Splunk

3. Azure Sentinel