



CBD Lists

SAMEER HASSAN

Wazuh lab

GitHub-link: [GitHub - sameerhassancode/Wazuh-labs](https://github.com/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.

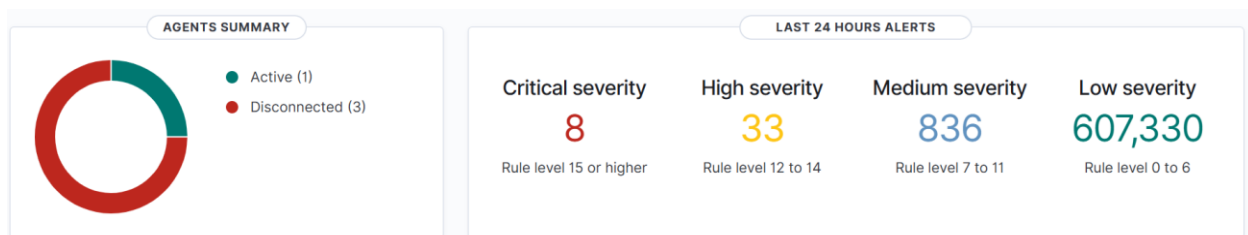
Key Advantages

- **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:

Agents (1) ☐ Show only outdated [Deploy new agent](#) [Refresh](#) [Export formatted](#) [More](#) [Settings](#)

status=active [WQL](#)

<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	001	Win-001	192.168.0.107	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	active info	eye plus

Rows per page: 10 [<](#) [1](#) [>](#) [refresh](#)

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>
```

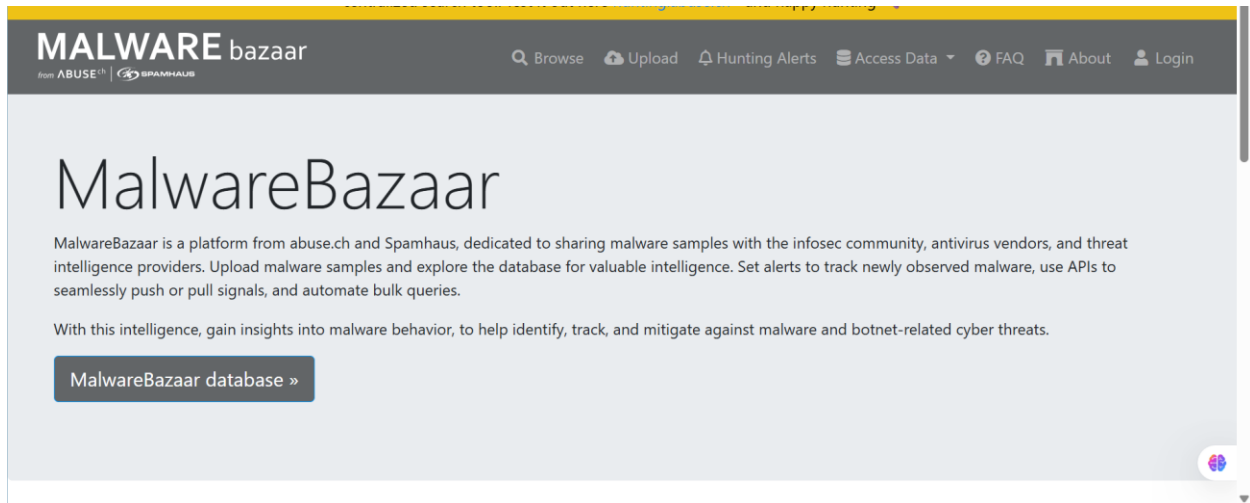
```
<group name="malware">
  <rule id="110002" level="13">
    <if_sid>554</if_sid>
    <if_sid>550</if_sid>
    <list field="md5" lookup="match_key">etc/lists/malware-hashes</list>
    <description>Known malware hash is detected</description>
    <mitre>
      <id>T1204.002</id>
    </mitre>
  </rule>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

After saving the file restart the Wazuh-manager

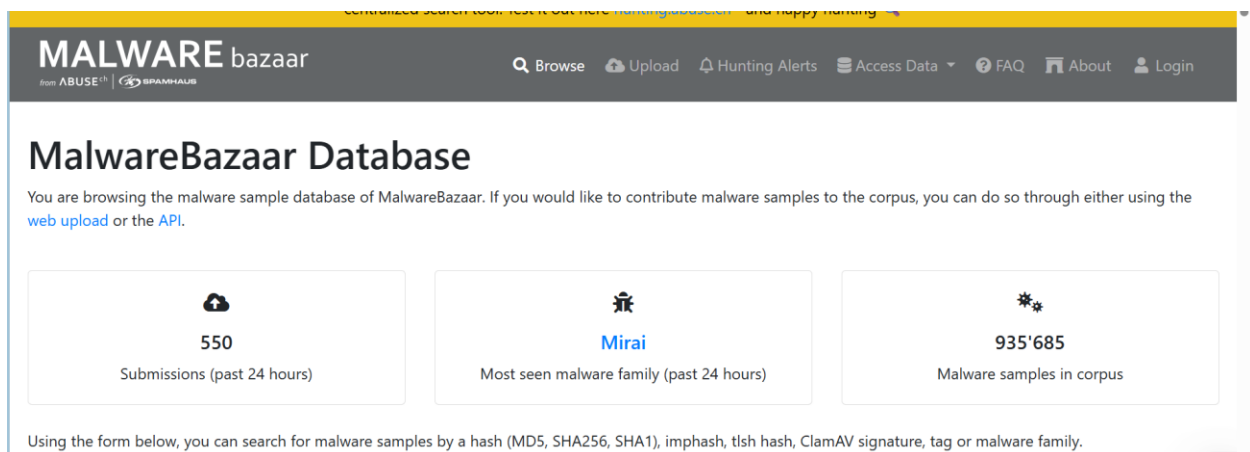
```
[root@wazuh-server rules]# systemctl restart wazuh-manager
```

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:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-06-17 11:45	e09c5d8ea6eb4b7eac7c7...	exe	Smoke Loader	exe Smoke Loader	SecuriteInfoCom	
2025-06-17 11:45	1803fb13ce6c98a85d94c...	exe		exe	SecuriteInfoCom	
2025-06-17 11:45	521dee104e5def4ca798a...	exe		exe	SecuriteInfoCom	
2025-06-17 11:44	fd046b5bd7fe32e1f86a9...	exe		exe	SecuriteInfoCom	
2025-06-17 11:44	adfdb8f3a85d554f98e64...	exe		exe	SecuriteInfoCom	
2025-06-17 11:36	d3de8f202c897add8774f...	elf		elf	abuse_ch	
2025-06-17 11:36	d14e3aabb516476c58b2f...	elf		elf	abuse_ch	

Select any and open it.

MALWARE bazaar
 from ABUSE²⁴ | SPAMHAUS

[Browse](#)
[Upload](#)
[Hunting Alerts](#)
[Access Data](#)
[FAQ](#)
[About](#)
[Login](#)

Intelligence 3	IOCs	YARA 8	File information	Comments	Actions
-----------------------------	------	---------------------	------------------	----------	---------

SHA256 hash:	e09c5d8ea6eb4b7eac7c73e951e3e43d95a62a94fa053fdb4ef64da70fd76361
SHA3-384 hash:	af26460fb484a48f7a7b3218709a84eb660443c1963a12dc21a1f76ce6611e59bbaae98042e86597b325c3f3165ba81c
SHA1 hash:	92dda227fc336cd892931dad8598a906f9c2f269
MD5 hash:	5a2574ff6f213f9e477be5dbf093a93b
humanhash:	sweet-carolina-music-mexico
File name:	SecuritelInfo.com.Win32.MalwareX-gen.8670.21364
Download:	download sample
Signature	Smoke Loader Alert
File size:	577'544 bytes
First seen:	2025-06-17 11:45:00 UTC

Copy the md5 of this malware:

MALWARE bazaar
 from ABUSE²⁴ | SPAMHAUS

[Browse](#)
[Upload](#)
[Hunting Alerts](#)
[Access Data](#)
[FAQ](#)
[About](#)
[Login](#)

Intelligence 3	IOCs	YARA 8	File information	Comments	Actions
-----------------------------	------	---------------------	------------------	----------	---------

SHA256 hash:	e09c5d8ea6eb4b7eac7c73e951e3e43d95a62a94fa053fdb4ef64da70fd76361
SHA3-384 hash:	af26460fb484a48f7a7b3218709a84eb660443c1963a12dc21a1f76ce6611e59bbaae98042e86597b325c3f3165ba81c
SHA1 hash:	92dda227fc336cd892931dad8598a906f9c2f269
MD5 hash:	5a2574ff6f213f9e477be5dbf093a93b
humanhash:	sweet-carolina-music-mexico
File name:	SecuritelInfo.com.Win32.MalwareX-gen.8670.21364
Download:	download sample
Signature	Smoke Loader Alert
File size:	577'544 bytes
First seen:	2025-06-17 11:45:00 UTC

Paste this md5 hash in the malware-hash file.

```

root@wazuh-server:/var/ossec  root@wazuh-server:/var/osse  +  v
GNU nano 8.3                  malware-hashes
5a2574ff6f213f9e477be5dbf093a93b:malware
  
```

Add some more Malware hashes for better result.

```
root@wazuh-server:/var/ossec X root@wazuh-server:/var/osse X + v
GNU nano 8.3 malware-hashes Modified
5a2574ff6f213f9e477be5dbf093a93b:malware
a344196e733ebdb74f47a75d59e7fba9:malware
91f790c4a4cea94600962362bc7868ab: malware
```

Now save the file and restart Wazuh-manager!

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

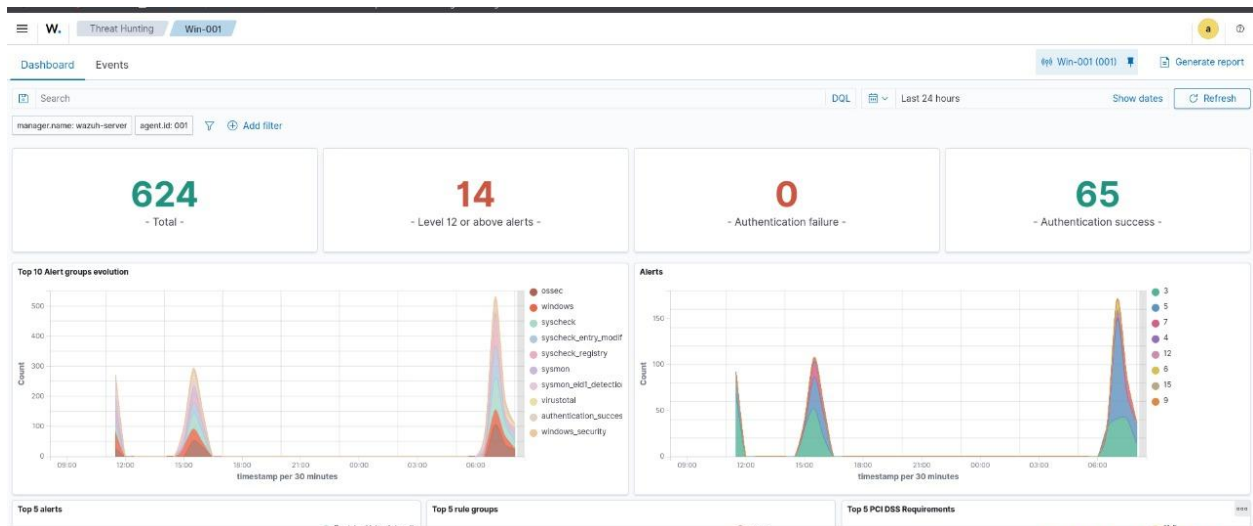
After saving and restarting the hashes download the malware samples

Download: [download sample](#)

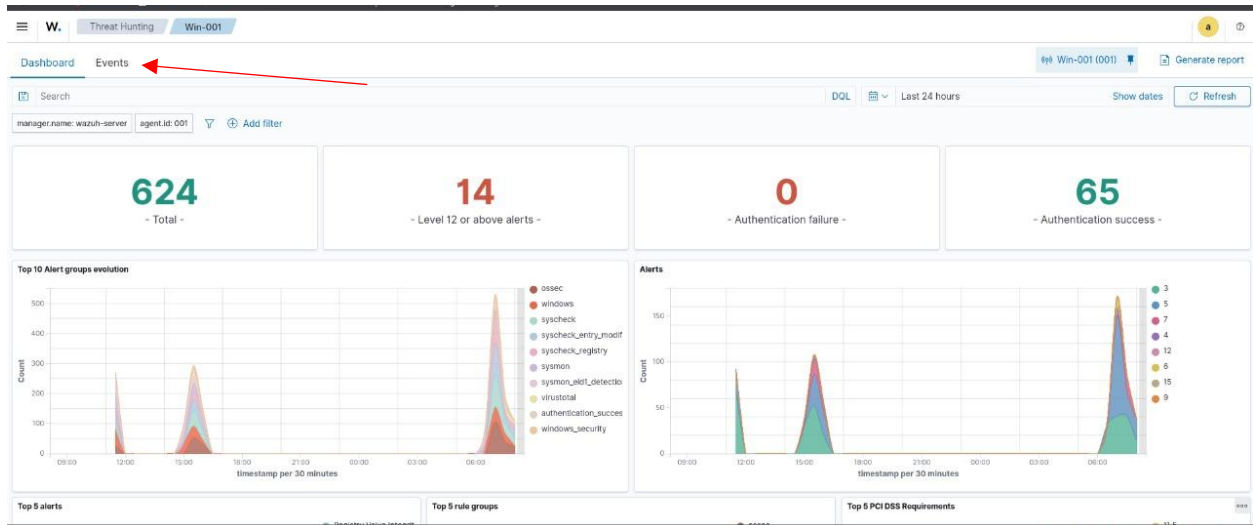
0 - 9			
	521dee104e5def4ca798aa30ad688138f4f2ac7a...	6/17/2025 4:53 AM	Compressed (zipped)... 20 KB
	1803fb13ce6c98a85d94c5c826d1ca362ec85b7...	6/17/2025 4:54 AM	Compressed (zipped)... 6,114 KB
A - H			
	e09c5d8ea6eb4b7eac7c73e951e3e43d95a62a9...	6/17/2025 4:54 AM	Compressed (zipped)... 409 KB

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\52afcc5f-a383-415e-a966-d162d1c56d81.tmp	deleted	File deleted.	7	553
Jun 17, 2025 @ 08:19:05.357	c:\users\shifat\downloads\52afcc5f-a383-415e-a966-d162d1c56d81.tmp	added	File added to the system.	5	554
Jun 17, 2025 @ 08:17:20.157	c:\users\shifat\downloads\1803fb13ce6c98a85d94c5c826d1ca362ec85b78417954f9e8c9a2b4c6dc...	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",
    "agent.id": "001",
    "agent.ip": "192.168.100.32",
    "agent.name": "Windows11",
    "decoder.name": "syscheck_new_entry",
    "full_log": "File 'c:\\users\\windows11\\downloads\\malware.exe' added\nMode: realtime",
    "id": "1716060692.82931444",
    "input.type": "log",
    "location": "syscheck",
    "manager.name": "wazuh-server",
    "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