Documentation › Using Wazuh for PCI DSS › Log analysis

Log analysis

Here we will use Wazuh log collection and analysis capabilities to meet the following PCI DSS controls:

10.2.4: Invalid logical access attempts.
10.2.5: Use of and changes to identification and authentication mechanisms —including but not limited to creation of new accounts and escalation of privileges— and all changes, additions, or deletions to accounts with root or administrative privileges.

These controls require us to log invalid logical access attempts, multiple invalid login attempts (possible brute force attacks), privilege escalations, changes to accounts, etc. In order to achieve this, we have added PCI DSS tags to OSSEC log analysis rules, mapping them to the corresponding requirement(s). This makes it easy to analyze and visualize our PCI DSS related alerts.

The syntax used for rule tagging is **pci_dss_** followed by the number of the requirement (e.g., **pci_dss_10.2.4** and **pci_dss_10.2.5**).

Here are some examples of OSSEC rules tagged for PCI requirements 10.2.4 and 10.2.5:

```
<!--apache: access attempt -->
<rule id="30105" level="5">
    <if_sid>30101</if_sid>
    <match>denied by server configuration</match>
    <description>Attempt to access forbidden file or directory.</description>
    <group>access_denied,pci_dss_6.5.8,pci_dss_10.2.4,</group>
</rule>

<!-- syslog-sudo: elevation of privileges -->
<rule id="5401" level="5">
    <if_sid>5400</if_sid>
    <match>incorrect password attempt</match>
    <description>Failed attempt to run sudo</description>
    <group>pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>

<rule id="5402" level="3">
    <if_sid>5400</if_sid>
    <regex> ; USER=root ; COMMAND=| ; USER=root ; TSID=\S+ ; COMMAND=</regex>
    <description>Successful sudo to ROOT executed</description>
    <group>pci_dss_10.2.5,pci_dss_10.2.2,</group>
</rule>

<!-- ssh: identification and authentication mechanisms -->
<rule id="5712" level="10" frequency="6" timeframe="120" ignore="60">
    <if_matched_sid>5710</if_matched_sid>
    <description>SSHD brute force trying to get access to </description>
    <description>the system.</description>
    <same_source_ip />
    <group>authentication_failures,pci_dss_11.4,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>

<rule id="5720" level="10" frequency="6">
    <if_matched_sid>5716</if_matched_sid>
    <same_source_ip />
    <description>Multiple SSHD authentication failures.</description>
    <group>authentication_failures,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_11.4,</group>
</rule>
```

Use cases

In this scenario, we try to open the file `cardholder_data.txt`. Since our current user doesn’t have read access to the file, we run `sudo` to elevate privileges.

```
[agent@centos ~]$ ls -l
total 0
drwxrwxr-x. 2 agent agent  6 Jan  5 18:34 centos
drwxr-x---  2 root  root  33 Jan  5 18:32 credit_cards
drwxrwxr-x. 2 agent agent  6 Jan  5 18:34 user_data
[agent@centos ~]$ sudo cat credit_cards/cardholder_data.txt
Number: 0000-0000-0000-0000
Holder: Mr. John Smith
```

Using the `sudo` log analysis decoder and rules, Wazuh will generate an alert for this particular action and write it to `alerts.log`. Using the rule tags we can see which PCI DSS requirements are specifically related to this alert.

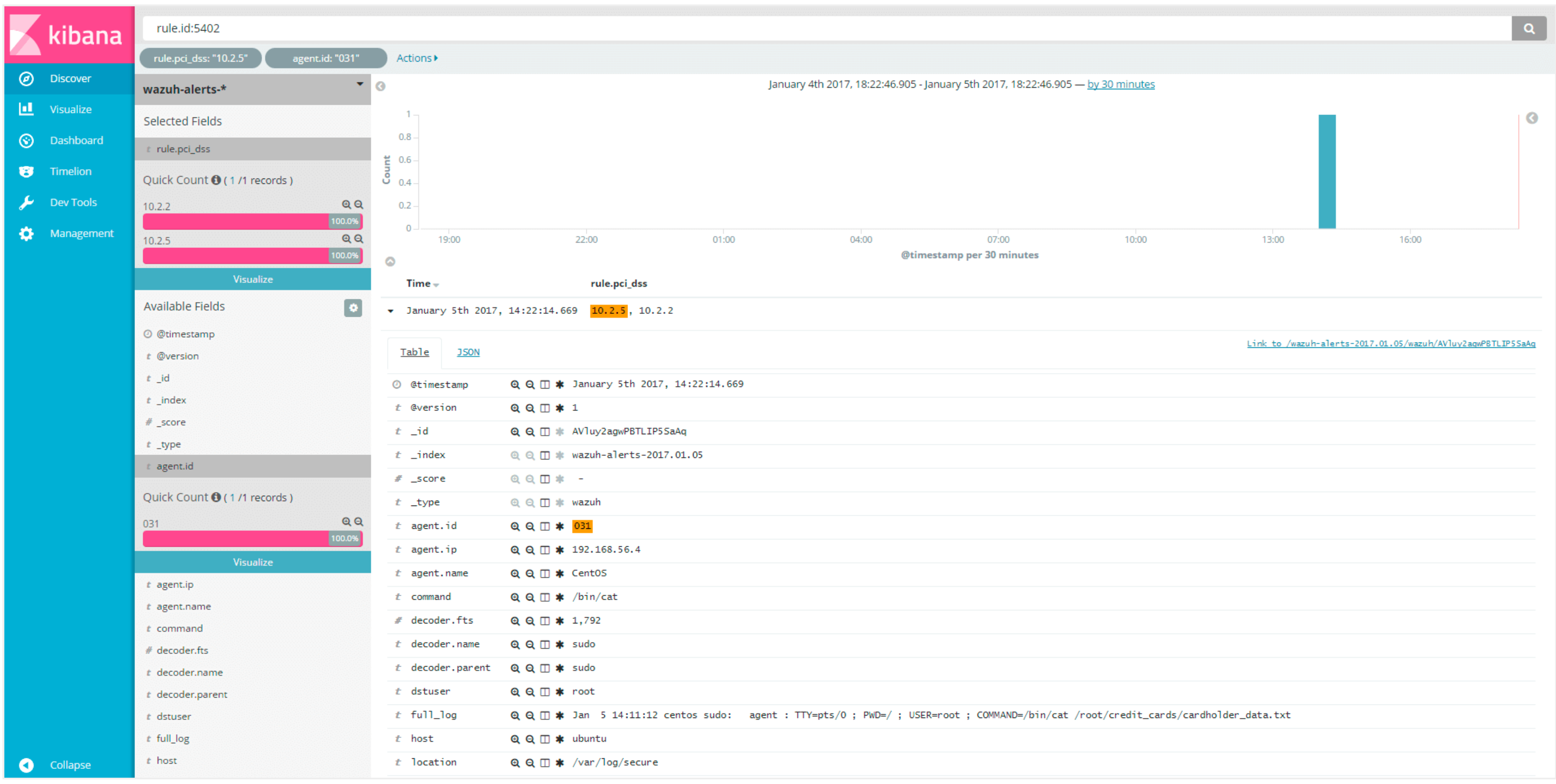
```
root@ubuntu:~# tail -n10 /var/ossec/logs/alerts/alerts.log

** Alert 1483621881.263207: - syslog,sudo,pci_dss_10.2.5,pci_dss_10.2.2,
2017 Jan 05 14:11:21 (CentOS) 192.168.56.4->/var/log/secure
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'
User: root
Jan  5 14:11:12 centos sudo:   agent : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/bin/cat
/root/credit_cards/cardholder_data.txt
tty: pts/0
pwd: /
command: /bin/cat
```

Since we have JSON output enabled, we can also see the alert in `alerts.json`:

```
root@ubuntu:~# tail -n1 /var/ossec/logs/alerts/alerts.json | jq
```

```
{
  "rule": {
    "level": 3,
    "description": "Successful sudo to ROOT executed",
    "id": 5402,
    "firedtimes": 1,
    "groups": [
      "syslog",
      "sudo"
    ],
    "pci_dss": [
      "10.2.5",
      "10.2.2"
    ]
  },
  "agent": {
    "id": "031",
    "name": "CentOS",
    "ip": "192.168.56.4"
  },
  "manager": {
    "name": "ubuntu"
  },
  "srcuser": "agent",
  "dstuser": "root",
  "full_log": "Jan  5 14:11:12 centos sudo:    agent : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/bin/cat
/root/credit_cards/cardholder_data.txt",
  "program_name": "sudo",
  "tty": "pts/0",
  "pwd": "/",
  "command": "/bin/cat",
  "decoder": {
    "fts": 1792,
    "parent": "sudo",
    "name": "sudo"
  },
  "timestamp": "2017 Jan 05 14:11:21",
  "location": "/var/log/secure"
}
```

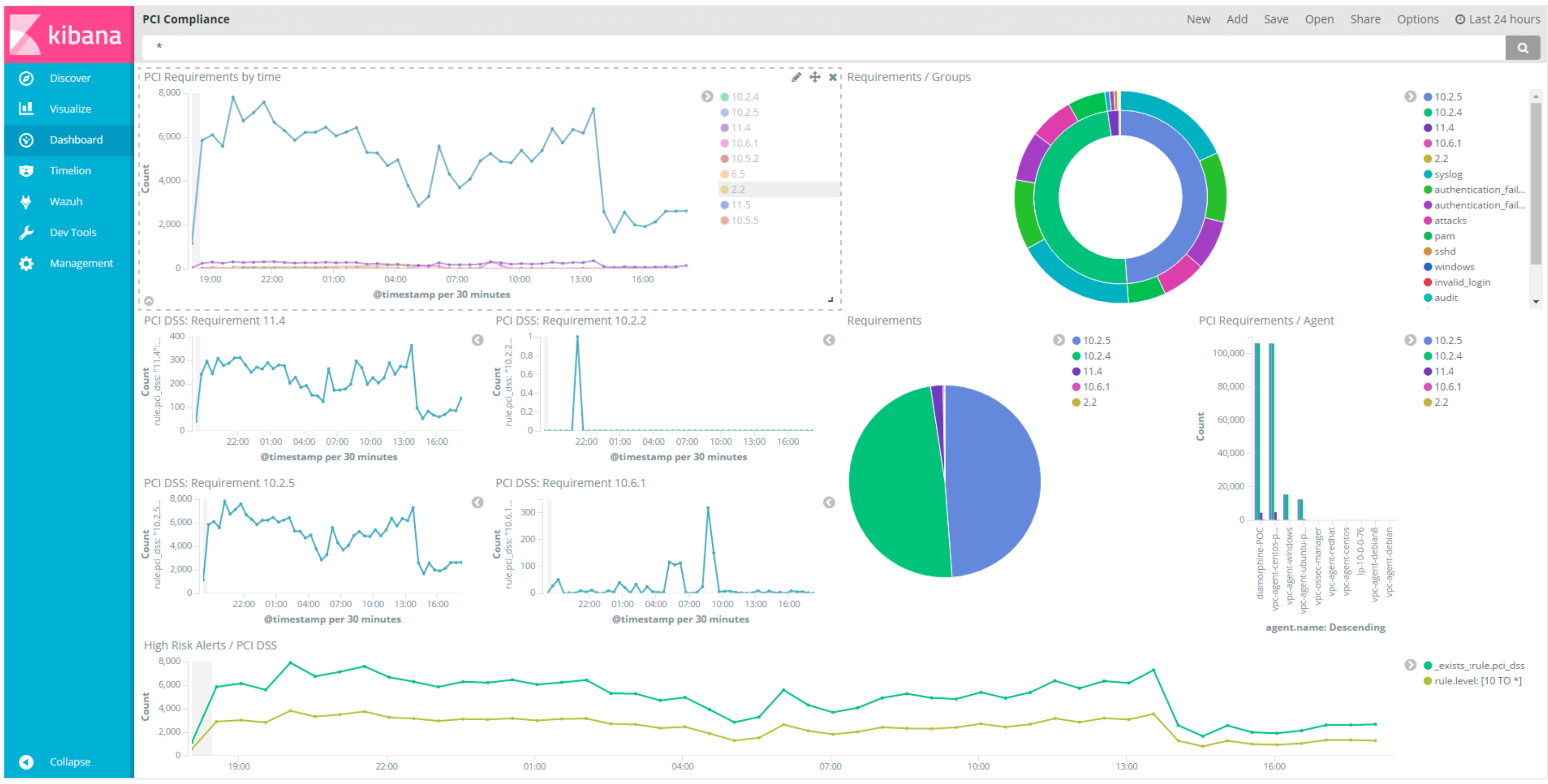
Kibana displays information in an organized way, allowing filtering by different types of alert fields, including compliance controls. We have also developed a couple of PCI DSS dashboards for convenient viewing of relevant alerts.

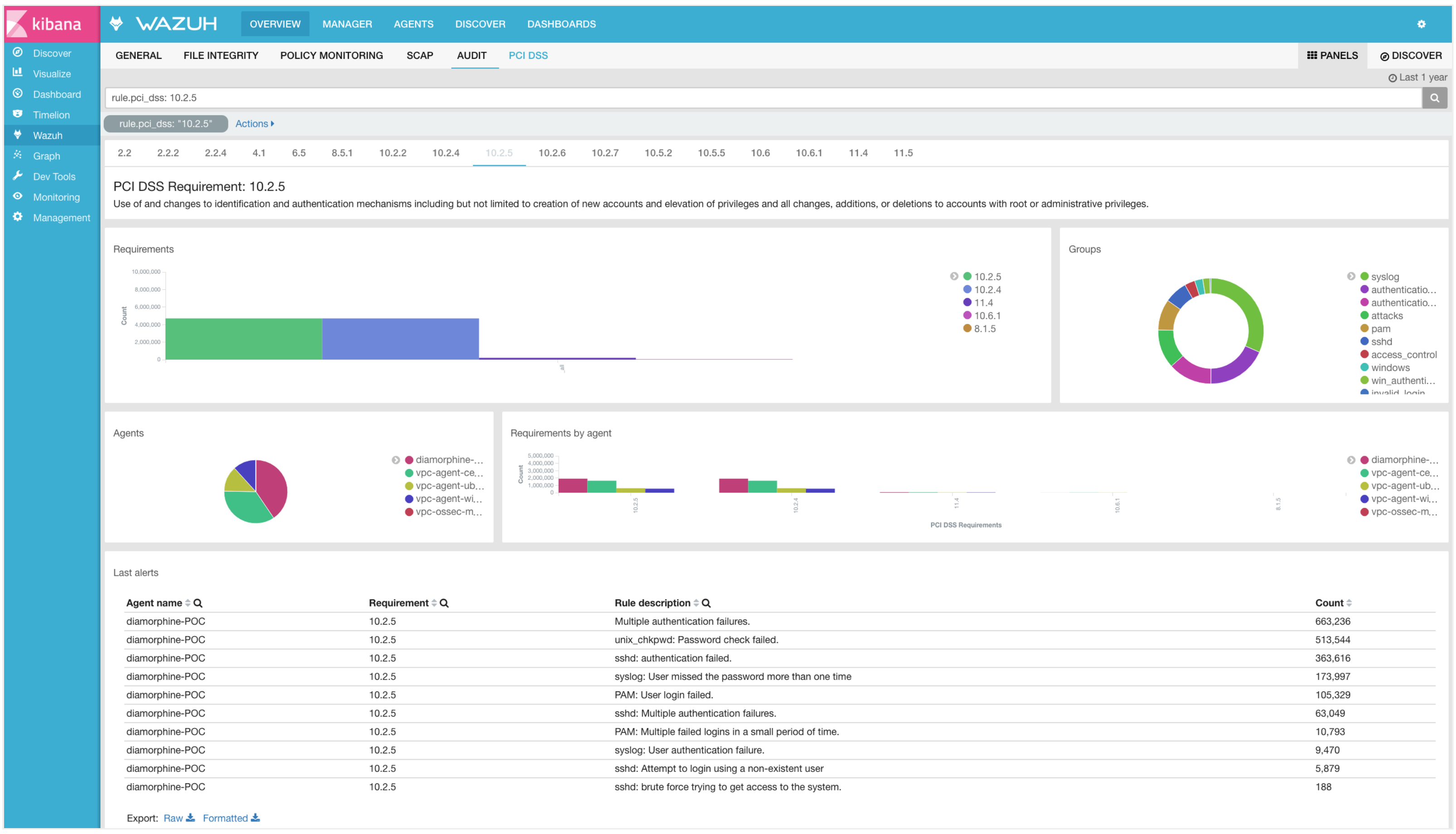


Time	rule.pci_dss
January 5th 2017, 14:22:14.669	10.2.5, 10.2.2

Link to /wazuh-alerts-2017.01.05/wazuh/AVluy2agwPBTLIP5SaAq

@timestamp	January 5th 2017, 14:22:14.669
@version	1
_id	AVluy2agwPBTLIP5SaAq
_index	wazuh-alerts-2017.01.05
_score	-
_type	wazuh
agent.id	031
agent.ip	192.168.56.4
agent.name	CentOS
command	/bin/cat
decoder.fts	1,792
decoder.name	sudo
decoder.parent	sudo
dstuser	root
full_log	Jan 5 14:11:12 centos sudo: agent : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/bin/cat /root/credit_cards/cardholder_data.txt
host	ubuntu
location	/var/log/secure





PCI DSS Requirement: 10.2.5

Use of and changes to identification and authentication mechanisms including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges.

Last alerts

Agent name	Requirement	Rule description	Count
diamorphine-POC	10.2.5	Multiple authentication failures.	663,236
diamorphine-POC	10.2.5	unix_chkpwd: Password check failed.	513,544
diamorphine-POC	10.2.5	sshd: authentication failed.	363,616
diamorphine-POC	10.2.5	syslog: User missed the password more than one time	173,997
diamorphine-POC	10.2.5	PAM: User login failed.	105,329
diamorphine-POC	10.2.5	sshd: Multiple authentication failures.	63,049
diamorphine-POC	10.2.5	PAM: Multiple failed logins in a small period of time.	10,793
diamorphine-POC	10.2.5	syslog: User authentication failure.	9,470
diamorphine-POC	10.2.5	sshd: Attempt to login using a non-existent user	5,879
diamorphine-POC	10.2.5	sshd: brute force trying to get access to the system.	188

Export: Raw Formatted