Policy monitoring

The rootcheck module can be used to enforce and monitor your security policy. This is the process of verifying that all systems conform to a set of predefined rules surrounding configuration settings and approved application usage.

There are several PCI DSS requirements to verify that systems are properly hardened. An example would be:

> **2.2**: Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
> Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), Institute National Institute of Standards Technology (NIST).

Wazuh includes out-of-the-box, CIS baselines for Debian and Red Hat. Other baselines could be created for other systems or applications as well, just by adding the corresponding rootcheck file:

```
<rootcheck>
  <system_audit>/var/ossec/etc/shared/cis_debian_linux_rcl.txt</system_audit>
  <system_audit>/var/ossec/etc/shared/cis_rhel_linux_rcl.txt</system_audit>
  <system_audit>/var/ossec/etc/shared/cis_rhel5_linux_rcl.txt</system_audit>
</rootcheck>
```

Other PCI DSS requirements ask us to check that applications (especially network services) are configured in a secure way. One example is the following control:

> **2.2.4**: Configure system security parameters to prevent misuse.

The following are good examples of rootcheck rules developed to check the configuration of SSH services:

```
[SSH Configuration - Protocol version 1 enabled {PCI_DSS: 2.2.4}] [any]
f:/etc/ssh/sshd_config -> !r:^# && r:Protocol\.+1;

[SSH Configuration - Root login allowed {PCI_DSS: 2.2.4}] [any]
f:/etc/ssh/sshd_config -> !r:^# && r:PermitRootLogin\.+yes;
```

In Wazuh, the rootcheck rules use this syntax in the rootcheck name: **{PCI_DSS: X.Y.Z}**, mapping all rootchecks to their relevant PCI DSS requirement.

Use cases

In order to check SSH security settings and help meet requirement 2.2.4, we have developed the rootchecks `system_audit_ssh`. In our example, when Wazuh runs a rootcheck scan, it is able to detect certain security deficiencies in the SSH configuration.

```
[root@manager ossec]# cat etc/ossec.conf | grep system_audit_ssh -B 4 -A 2
```

```
<rootcheck>
    <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
    <system_audit>/var/ossec/etc/shared/system_audit_rcl.txt<system_audit>
    <system_audit>/var/ossec/etc/shared/ssh/system_audit_ssh.txt<system_audit>
</rootcheck>
```

If enabled, the file `archives.log` stores every log parsed by the Wazuh engine, whether it becomes an alert or not:

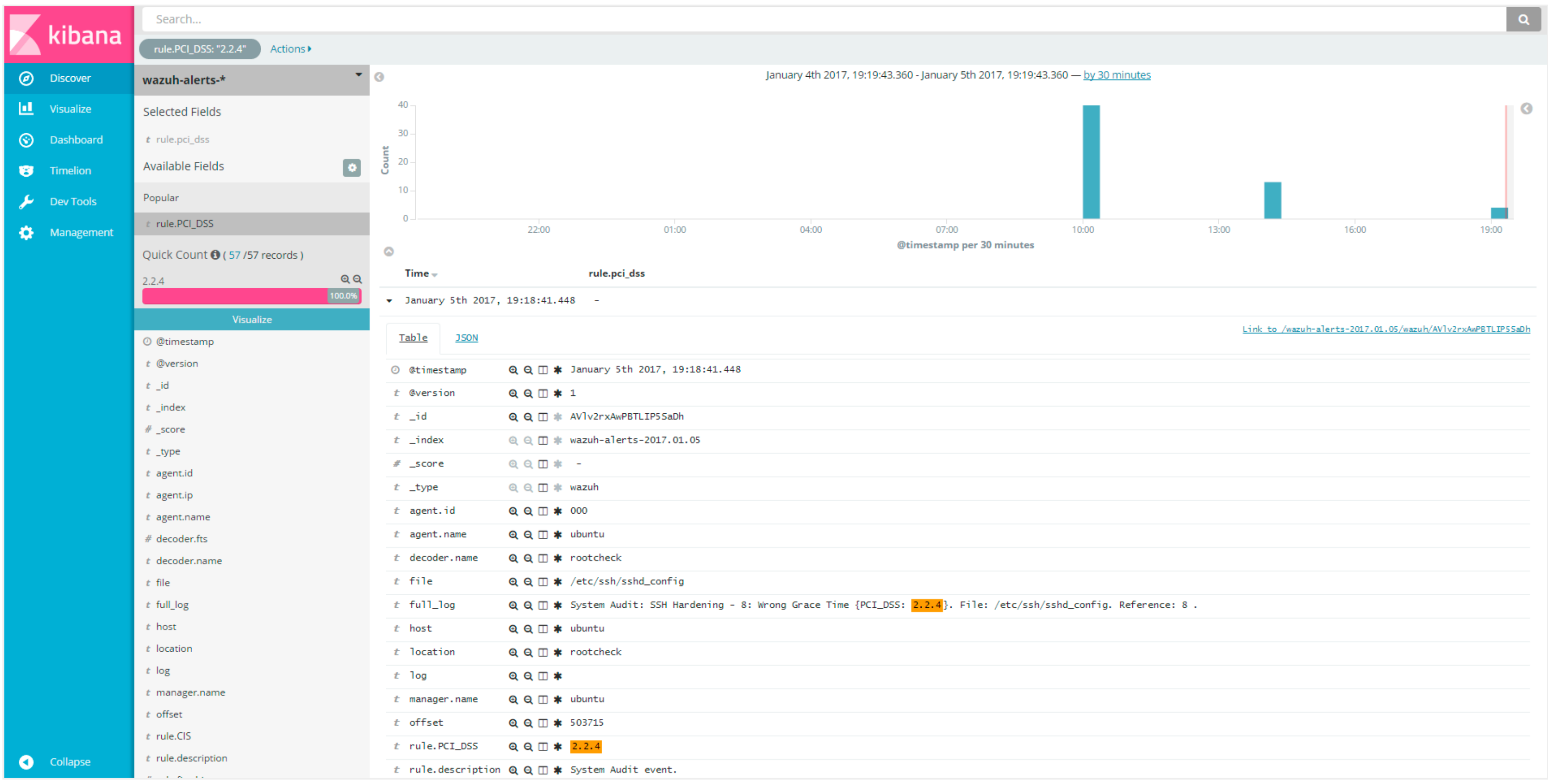
```
[root@manager ossec]# tail -f logs/archives/archives.log
2016 Jan 29 12:58:02 manager->rootcheck Ending rootcheck scan.
2016 Jan 29 13:07:18 manager->ossec-monitord ossec: Ossec started.
2016 Jan 29 13:08:34 manager->rootcheck Starting rootcheck scan.
2016 Jan 29 13:08:36 manager->rootcheck System Audit: SSH Hardening - 3: Root can log in {PCI_DSS: 2.2.4}.
File: /etc/ssh/sshd_config. Reference: 3 .
2016 Jan 29 13:08:36 manager->rootcheck System Audit: SSH Hardening - 4: No Public Key authentication
{PCI_DSS: 2.2.4}. File: /etc/sshd/sshd_config. Reference: 4 .
2016 Jan 29 13:08:36 manager->rootcheck System Audit: SSH Hardening - 5: Password Authentication {PCI_DSS:
2.2.4}. File: /etc/sshd/sshd_config. Reference: 5 .
2016 Jan 29 13:08:36 manager->rootcheck System Audit: SSH Hardening - 6: Empty passwords allowed {PCI_DSS:
2.2.4}. File: /etc/sshd/sshd_config. Reference: 6 .
2016 Jan 29 13:08:36 manager->rootcheck System Audit: SSH Hardening - 7: Rhost or shost used for
authentication {PCI_DSS: 2.2.4}. File: /etc/sshd/sshd_config. Reference: 7 .
2016 Jan 29 13:08:36 manager->rootcheck System Audit: SSH Hardening - 8: Wrong Grace Time {PCI_DSS: 2.2.4}.
File: /etc/sshd/sshd_config. Reference: 8 .
2016 Jan 29 13:08:36 manager->rootcheck System Audit: SSH Hardening - 9: Wrong Maximum number of
authentication attempts {PCI_DSS: 2.2.4}. File: /etc/sshd/sshd_config. Reference: 9 .
```

In this case, all the logs above are alerts, so we will see an instance of the last alert in JSON:

```
[root@manager ossec]# tail -n 1 logs/alerts/alerts.json | pjson
```

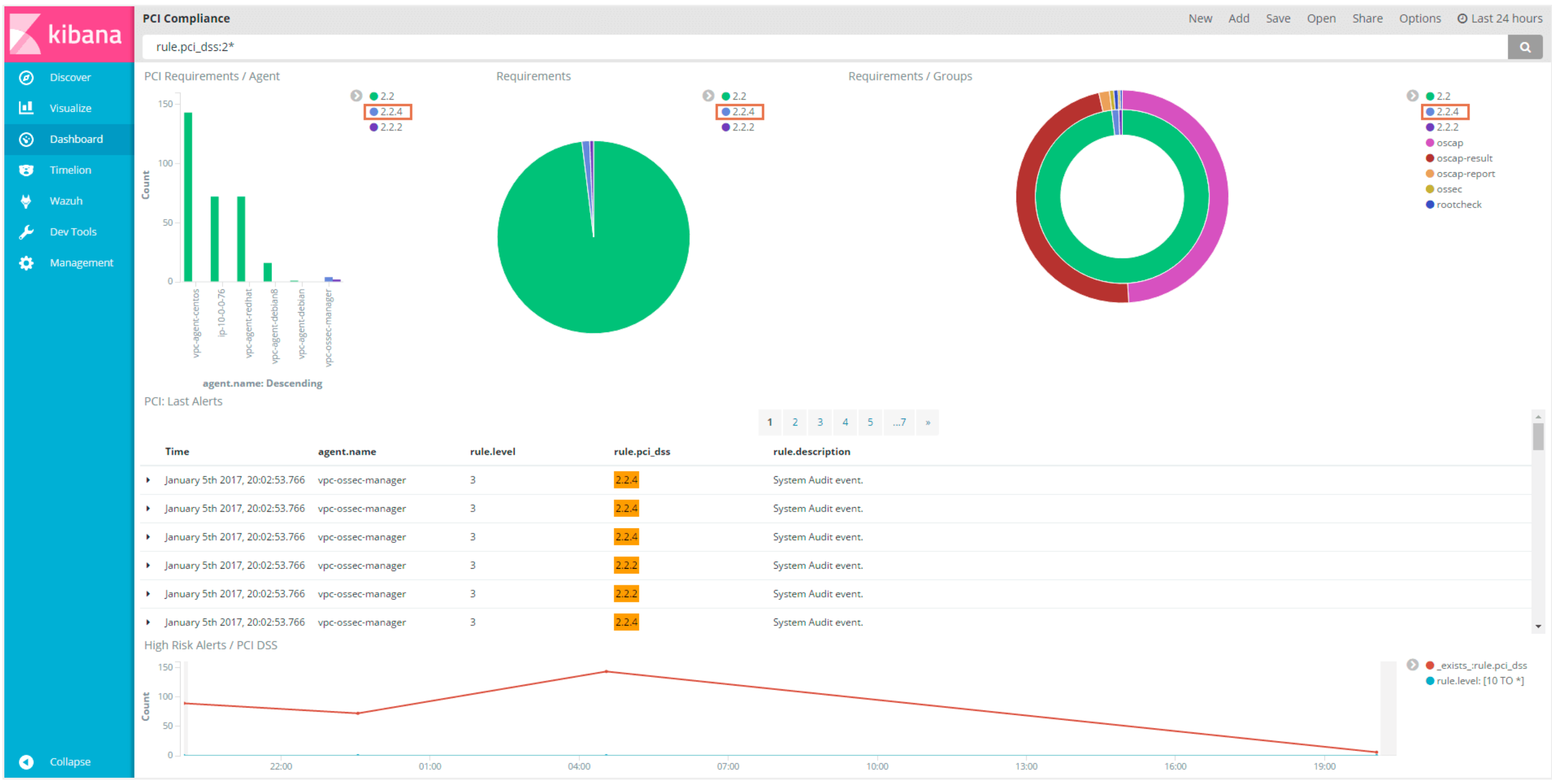
```
{
  "rule": {
    "level": 3,
    "description": "System Audit event.",
    "id": 516,
    "firedtimes": 7,
    "groups": [
      "ossec",
      "rootcheck"
    ],
    "pci_dss": [
      "2.2.4"
    ]
  },
  "agent": {
      "id": "000",
      "name": "manager"
  },
  "manager": {
    "name": "manager"
  },
  "full_log": "System Audit: SSH Hardening - 9: Wrong Maximum number of authentication attempts {PCI_DSS:
2.2.4}. File: /etc/ssh/sshd_config. Reference: 9 .",
  "title": "SSH Hardening - 9: Wrong Maximum number of authentication attempts",
  "file": "/etc/ssh/sshd_config",
  "decoder": {
    "name": "rootcheck"
  },
  "timestamp": "2016 Jan 29 13:08:36",
  "location": "rootcheck"
}
```

Kibana shows the full information about the alert:

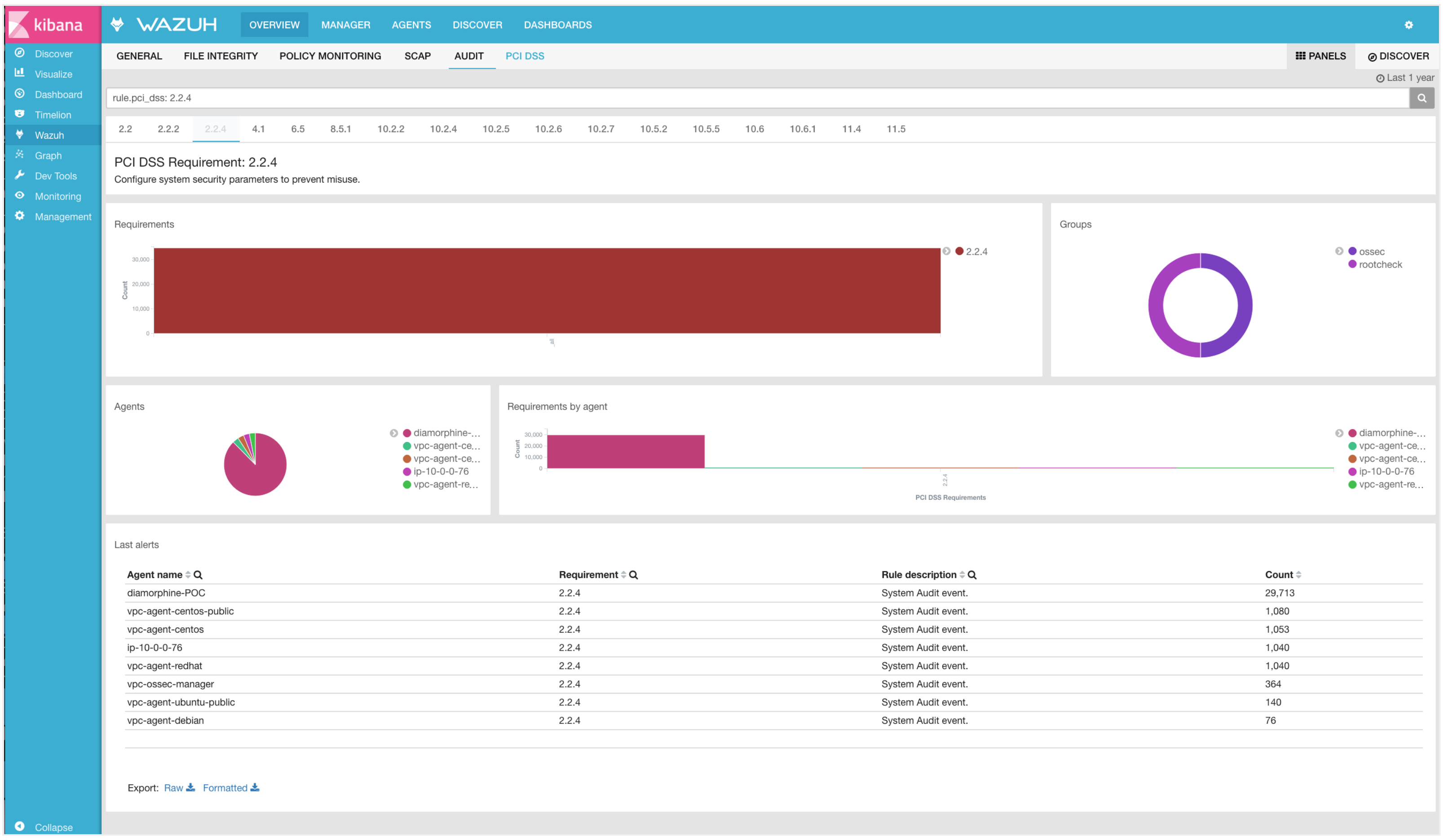


Time	rule.pci_dss
January 5th 2017, 19:18:41.448	-

```
@timestamp        January 5th 2017, 19:18:41.448
@version          1
_id               AVlv2rxAwPBTLIP5SaDh
_index            wazuh-alerts-2017.01.05
_score            -
_type             wazuh
agent.id          000
agent.name        ubuntu
decoder.name      rootcheck
file              /etc/ssh/sshd_config
full_log          System Audit: SSH Hardening - 8: Wrong Grace Time {PCI_DSS: 2.2.4}. File: /etc/ssh/sshd_config. Reference: 8 .
host              ubuntu
location          rootcheck
log
manager.name      ubuntu
offset            503715
rule.PCI_DSS      2.2.4
rule.description  System Audit event.
```



Time	agent.name	rule.level	rule.pci_dss	rule.description
January 5th 2017, 20:02:53.766	vpc-ossec-manager	3	2.2.4	System Audit event.
January 5th 2017, 20:02:53.766	vpc-ossec-manager	3	2.2.4	System Audit event.
January 5th 2017, 20:02:53.766	vpc-ossec-manager	3	2.2.4	System Audit event.
January 5th 2017, 20:02:53.766	vpc-ossec-manager	3	2.2.2	System Audit event.
January 5th 2017, 20:02:53.766	vpc-ossec-manager	3	2.2.2	System Audit event.
January 5th 2017, 20:02:53.766	vpc-ossec-manager	3	2.2.4	System Audit event.



PCI DSS Requirement: 2.2.4

Configure system security parameters to prevent misuse.

Last alerts

Agent name	Requirement	Rule description	Count
diamorphine-POC	2.2.4	System Audit event.	29,713
vpc-agent-centos-public	2.2.4	System Audit event.	1,080
vpc-agent-centos	2.2.4	System Audit event.	1,053
ip-10-0-0-76	2.2.4	System Audit event.	1,040
vpc-agent-redhat	2.2.4	System Audit event.	1,040
vpc-ossec-manager	2.2.4	System Audit event.	364
vpc-agent-ubuntu-public	2.2.4	System Audit event.	140
vpc-agent-debian	2.2.4	System Audit event.	76

Export: Raw Formatted