Configuration

1. Basic usage
2. Evaluate PCI-DSS compliance on RHEL7
3. Auditing Security Vulnerabilities of Red Hat Products
4. Overwriting the timeout
5. Using profiles
6. Using CPE dictionary
7. Using IDs

Basic usage

To configure the options for OpenSCAP go to ossec.conf, or for more details about specific options, see the OpenSCAP section.

In this example, we configure Wazuh to run OpenSCAP each day, with a timeout of 30 minutes.

```
<wodle name="open-scap">
  <disabled>no</disabled>
  <timeout>1800</timeout>
  <interval>1d</interval>
  <scan-on-start>yes</scan-on-start>

  <content type="xccdf" path="ssg-centos-7-ds.xml">
    <profile>xccdf_org.ssgproject.content_profile_pci-dss</profile>
    <profile>xccdf_org.ssgproject.content_profile_common</profile>
  </content>
</wodle>
```

Evaluate PCI-DSS compliance on RHEL7

This section describes how to evaluate the Payment Card Industry Data Security Standard (PCI-DSS) compliance on Red Hat Enterprise Linux 7 agents.

Step 1: Configure agents

Each agent must be properly identified in order to know which policy and profile to execute.

Agent `ossec.conf`:

```
<client>
  <server-ip>10.0.1.4</server-ip>
  <config-profile>redhat7</config-profile>
</client>
```

Step 2: Configure manager

We want to execute the PCI-DSS profile of the SSG RH7 policy only on Red Hat 7 servers.

Manager `shared/agent.conf`:

```
<agent_config profile="redhat7">

  <wodle name="open-scap">
    <content type="xccdf" path="ssg-rhel7-ds.xml">
      <profile>xccdf_org.ssgproject.content_profile_pci-dss</profile>
    </content>
  </wodle>

</agent_config>
```

Step 3: Restart manager and agents

To apply the new configuration, restart the manager and agents:

```
$ /var/ossec/bin/ossec-control restart
$ /var/ossec/bin/agent_control -R -a
```

If you prefer, you can restart a specific agent with the option `-u <id>` where **id** is the agent's id number.

Step 4: See alerts

When the evaluation is complete you will see the results as OSSEC alerts:

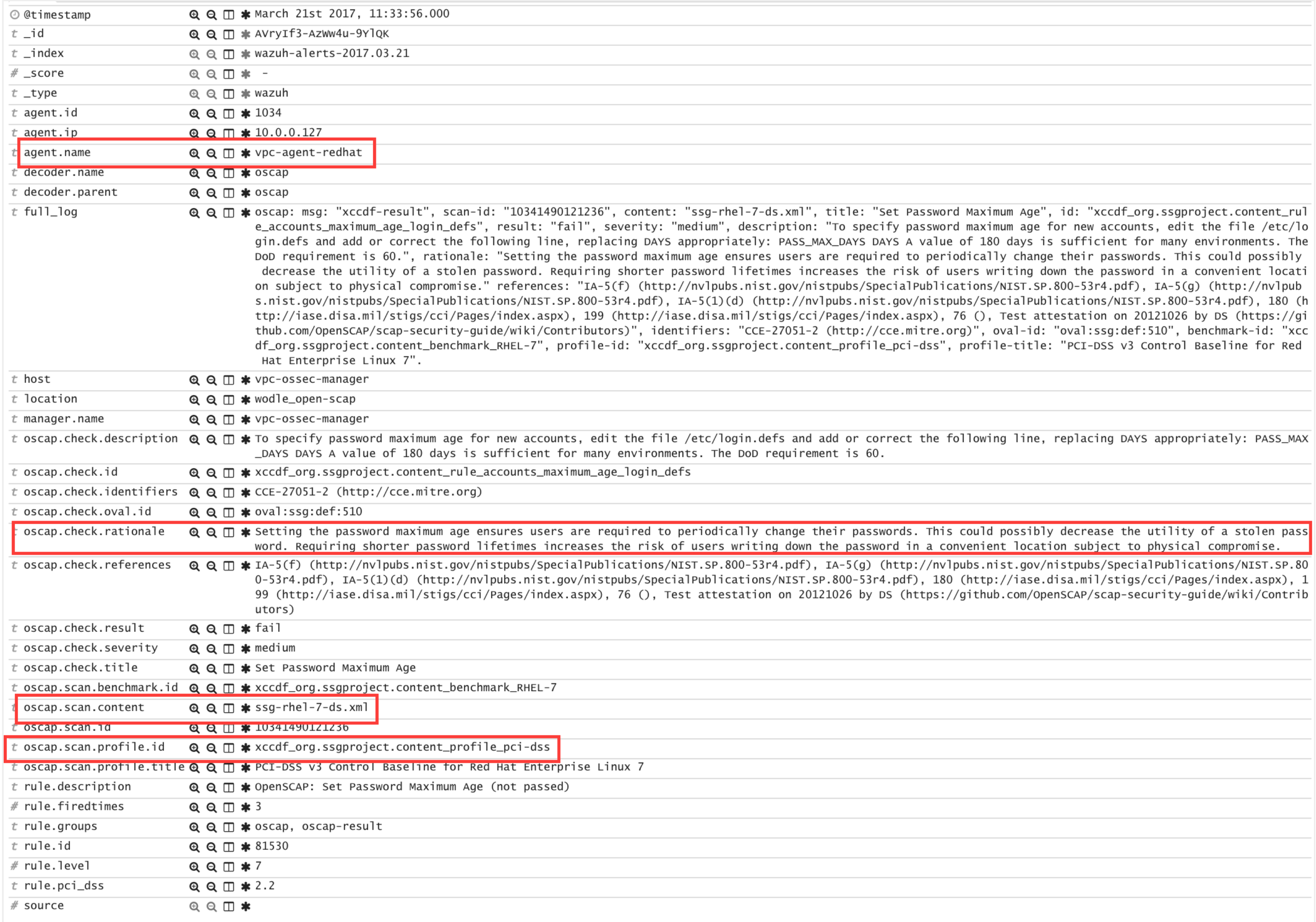
`/var/ossec/logs/alerts/alerts.log`

```
** Alert 1463752181.32768: - oscap,rule-result,pci_dss_2.2,
2016 May 20 13:49:41 (RH_Agent) 10.0.1.7->wodle_open-scap
Rule: 81529 (level 5) -> 'OpenSCAP rule failed (severity low).'
oscap: msg: "rule-result", id: "47T7_Qd08gm4y8TSoD53", policy: "ssg-rhel7-ds.xml", profile:
"xccdf_org.ssgproject.content_profile_pci-dss", rule_id:
"xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout", result: "fail", title: "Set SSH Idle Timeout
Interval", ident: "CCE-26611-4", severity: "low".
```

```
** Alert 1463752181.33254: - oscap,report-overview,pci_dss_2.2,
2016 May 20 13:49:41 (RH_Agent) 10.0.1.7->wodle_open-scap
Rule: 81542 (level 4) -> 'OpenSCAP Report overview: Score less than 80'
oscap: msg: "report-overview", id: "47T7_Qd08gm4y8TSoD53", policy: "ssg-rhel7-ds.xml", profile:
"xccdf_org.ssgproject.content_profile_pci-dss", score: "56.835060" / "100.000000", severity of failed rules:
"high": "1", "medium": "9", "low": "34", "n/a": "0".
```

`Kibana`

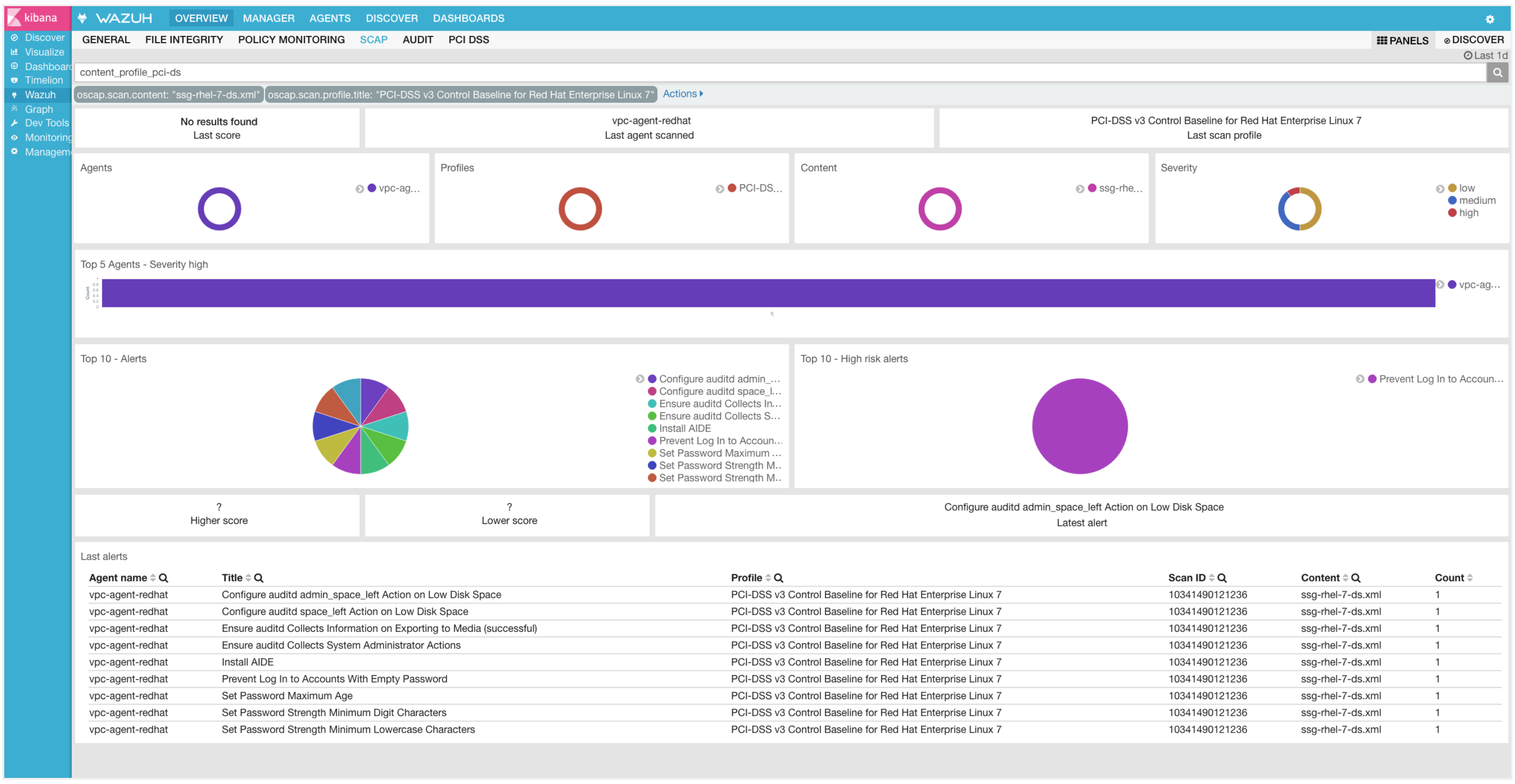
Note that each field is extracted to facilitate searches and analysis.



@timestamp	March 21st 2017, 11:33:56.000
_id	AVryIf3-AzWw4u-9YlQK
_index	wazuh-alerts-2017.03.21
_score	-
_type	wazuh
agent.id	1034
agent.ip	10.0.0.127
agent.name	vpc-agent-redhat
decoder.name	oscap
decoder.parent	oscap
full_log	oscap: msg: "xccdf-result", scan-id: "10341490121236", content: "ssg-rhel-7-ds.xml", title: "Set Password Maximum Age", id: "xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs", result: "fail", severity: "medium", description: "To specify password maximum age for new accounts, edit the file /etc/login.defs and add or correct the following line, replacing DAYS appropriately: PASS_MAX_DAYS DAYS A value of 180 days is sufficient for many environments. The DoD requirement is 60.", rationale: "Setting the password maximum age ensures users are required to periodically change their passwords. This could possibly decrease the utility of a stolen password. Requiring shorter password lifetimes increases the risk of users writing down the password in a convenient location subject to physical compromise." references: "IA-5(f) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), IA-5(g) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), IA-5(1)(d) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), 180 (http://iase.disa.mil/stigs/cci/Pages/index.aspx), 199 (http://iase.disa.mil/stigs/cci/Pages/index.aspx), 76 (), Test attestation on 20121026 by DS (https://github.com/OpenSCAP/scap-security-guide/wiki/Contributors)", identifiers: "CCE-27051-2 (http://cce.mitre.org)", oval-id: "oval:ssg:def:510", benchmark-id: "xccdf_org.ssgproject.content_benchmark_RHEL-7", profile-id: "xccdf_org.ssgproject.content_profile_pci-dss", profile-title: "PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7".
host	vpc-ossec-manager
location	wodle_open-scap
manager.name	vpc-ossec-manager
oscap.check.description	To specify password maximum age for new accounts, edit the file /etc/login.defs and add or correct the following line, replacing DAYS appropriately: PASS_MAX_DAYS DAYS A value of 180 days is sufficient for many environments. The DoD requirement is 60.
oscap.check.id	xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs
oscap.check.identifiers	CCE-27051-2 (http://cce.mitre.org)
oscap.check.oval.id	oval:ssg:def:510
oscap.check.rationale	Setting the password maximum age ensures users are required to periodically change their passwords. This could possibly decrease the utility of a stolen password. Requiring shorter password lifetimes increases the risk of users writing down the password in a convenient location subject to physical compromise.
oscap.check.references	IA-5(f) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), IA-5(g) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), IA-5(1)(d) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), 180 (http://iase.disa.mil/stigs/cci/Pages/index.aspx), 199 (http://iase.disa.mil/stigs/cci/Pages/index.aspx), 76 (), Test attestation on 20121026 by DS (https://github.com/OpenSCAP/scap-security-guide/wiki/Contributors)
oscap.check.result	fail
oscap.check.severity	medium
oscap.check.title	Set Password Maximum Age
oscap.scan.benchmark.id	xccdf_org.ssgproject.content_benchmark_RHEL-7
oscap.scan.content	ssg-rhel-7-ds.xml
oscap.scan.id	10341490121236
oscap.scan.profile.id	xccdf_org.ssgproject.content_profile_pci-dss
oscap.scan.profile.title	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
rule.description	OpenSCAP: Set Password Maximum Age (not passed)
rule.firedtimes	3
rule.groups	oscap, oscap-result
rule.id	81530
rule.level	7
rule.pci_dss	2.2
source	

Step 5: Dashboards

Finally, you can explore all results using the OpenSCAP dashboards for Kibana.



content_profile_pci-ds

oscap.scan.content: "ssg-rhel-7-ds.xml" oscap.scan.profile.title: "PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7"

No results found
Last score

vpc-agent-redhat
Last agent scanned

PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
Last scan profile

?
Higher score

?
Lower score

Configure auditd admin_space_left Action on Low Disk Space
Latest alert

Last alerts

Agent name	Title	Profile	Scan ID	Content	Count
vpc-agent-redhat	Configure auditd admin_space_left Action on Low Disk Space	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Configure auditd space_left Action on Low Disk Space	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Ensure auditd Collects Information on Exporting to Media (successful)	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Ensure auditd Collects System Administrator Actions	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Install AIDE	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Prevent Log In to Accounts With Empty Password	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Set Password Maximum Age	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Set Password Strength Minimum Digit Characters	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1
vpc-agent-redhat	Set Password Strength Minimum Lowercase Characters	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7	10341490121236	ssg-rhel-7-ds.xml	1

Auditing Security Vulnerabilities of Red Hat Products

The Red Hat Security Response Team provides OVAL definitions for all vulnerabilities (identified by CVE name) that affect Red Hat Enterprise Linux 3, 4, 5, 6 and 7. This enables users to perform a vulnerability scan and diagnose whether a system is vulnerable or not.

Step 1: Configure agents

Each agent must be properly identified in order to know which policy and profile to execute.

Agent `ossec.conf`:

```
<client>
  <server-ip>10.0.1.4</server-ip>
  <config-profile>redhat7</config-profile>
</client>
```

Step 2: Configure manager

We want to execute the RedHat security policy only on Red Hat 7 servers.

Manager `shared/agent.conf`:

```
<agent_config profile="redhat7">

  <wodle name="open-scap">
    <content type="xccdf" path="com.redhat.rhsa-RHEL7.ds.xml"/>
  </wodle>

</agent_config>
```

Step 3: Restart manager and agents

To apply the new configuration, restart the manager and agents:

```
$ /var/ossec/bin/ossec-control restart
$ /var/ossec/bin/agent_control -R -a
```

If you prefer, you can restart a specific agent with option `-u <id>`.

Step 4: See alerts

When the evaluation is completed you will see the results as OSSEC alerts:

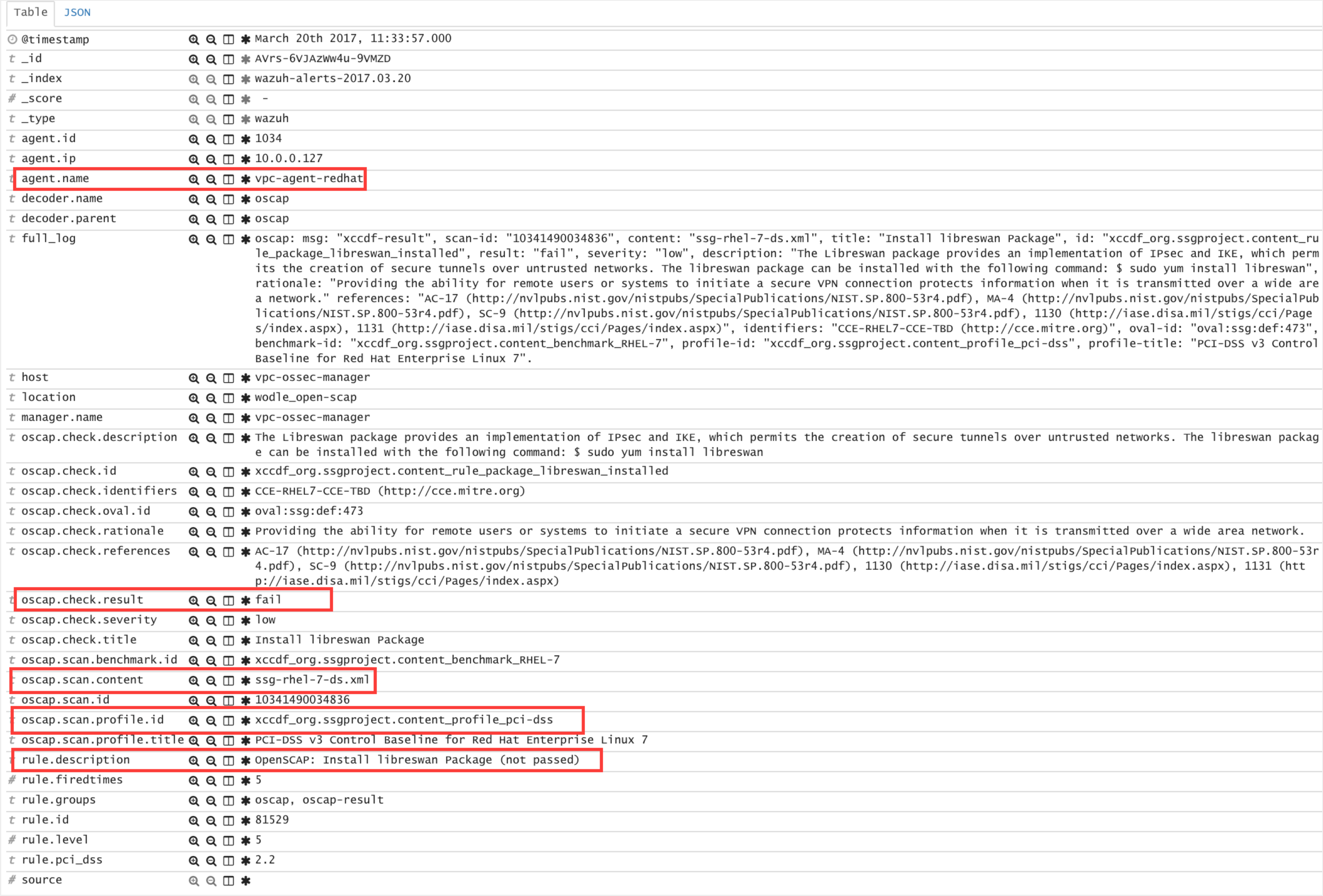
`/var/ossec/logs/alerts/alerts.log`

```
** Alert 1463757700.70731: mail  - oscap,rule-result,pci_dss_2.2,
2016 May 20 15:21:40 (RH_Agent) 10.0.1.7->wodle_open-scap
Rule: 81531 (level 9) -> 'OpenSCAP rule failed (severity high).'
oscap: msg: "rule-result", id: "I0iLEGFi4iTkxjnL9LWQ", policy: "com.redhat.rhsa-RHEL7.ds.xml", profile: "no-profiles", rule_id: "xccdf_com.redhat.rhsa_rule_oval-com.redhat.rhsa-def-20160722", result: "fail", title: "RHSA-2016:0722: openssl security update (Important)", ident: "RHSA-2016-0722, CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842", severity: "high".
```

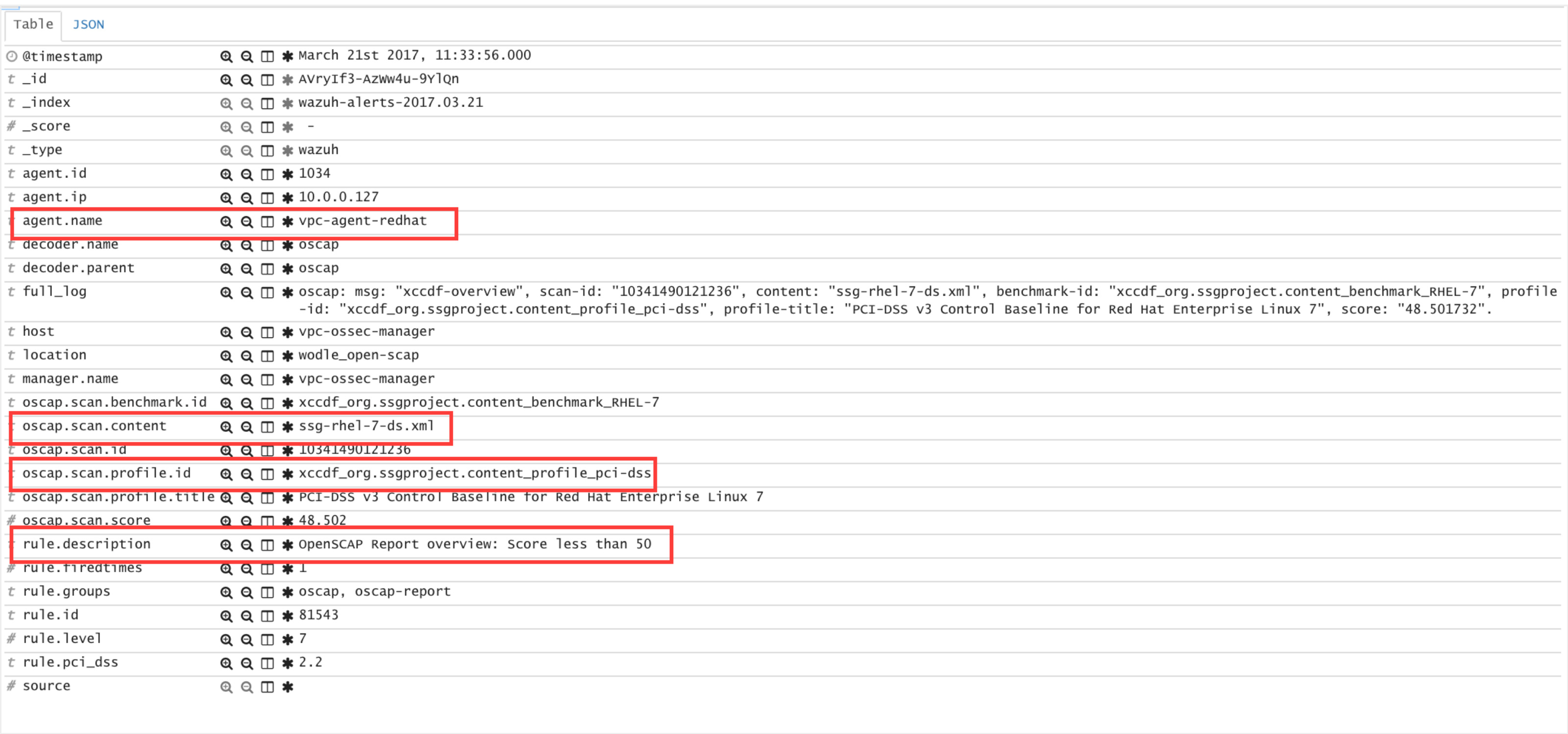
```
** Alert 1463757700.71339: - oscap,report-overview,pci_dss_2.2,
2016 May 20 15:21:40 (RH_Agent) 10.0.1.7->wodle_open-scap
Rule: 81540 (level 1) -> 'OpenSCAP Report overview.'
oscap: msg: "report-overview", id: "I0iLEGFi4iTkxjnL9LWQ", policy: "com.redhat.rhsa-RHEL7.ds.xml", profile: "no-profiles", score: "92.617447" / "100.000000", severity of failed rules: "high": "8", "medium": "14", "low": "0", "n/a": "0".
```

`Kibana`

Note that each field is extracted to facilitate searches and analysis.



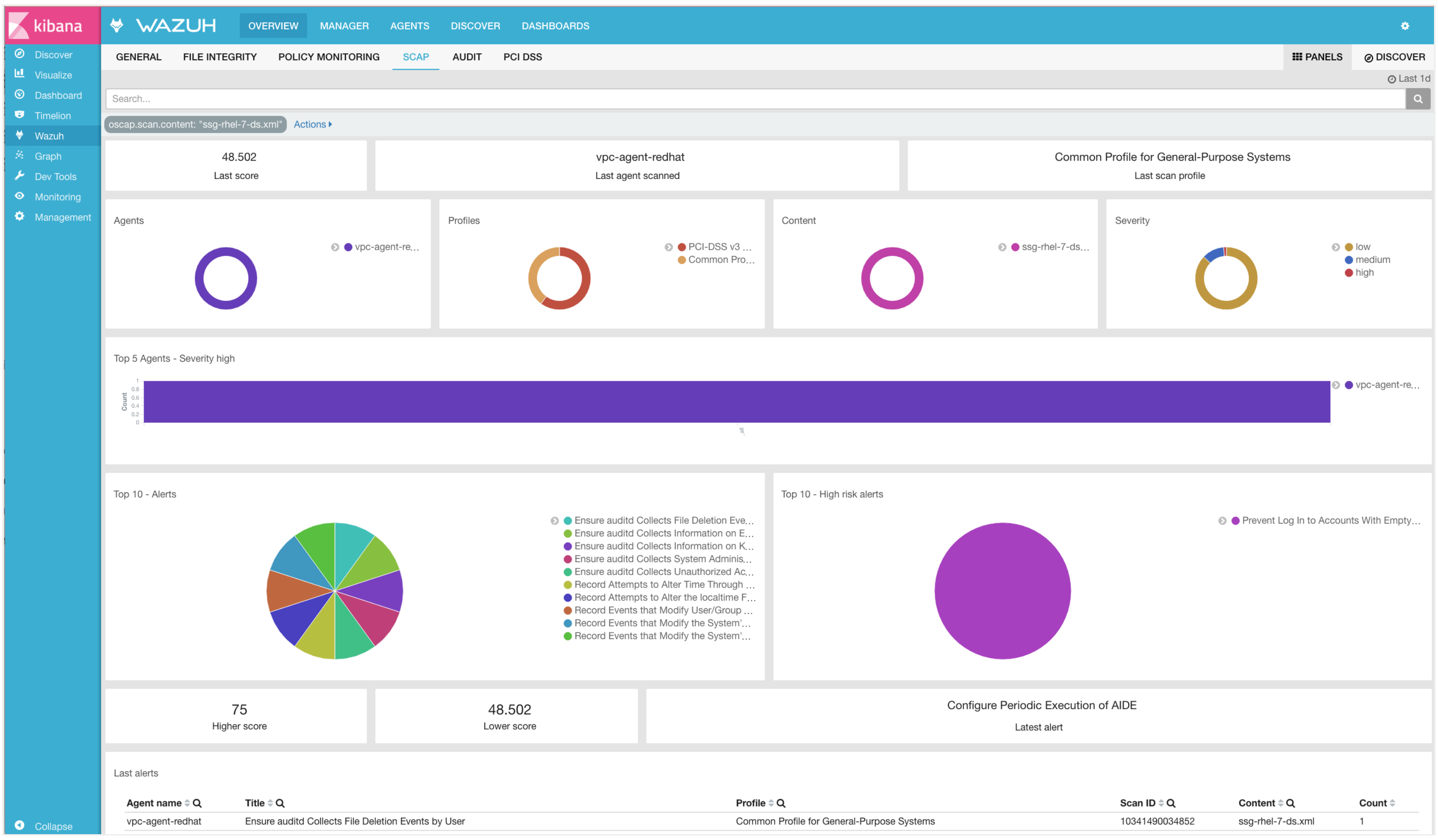
@timestamp	March 20th 2017, 11:33:57.000
_id	AVrs-6VJAzWw4u-9VMZD
_index	wazuh-alerts-2017.03.20
_score	-
_type	wazuh
agent.id	1034
agent.ip	10.0.0.127
agent.name	vpc-agent-redhat
decoder.name	oscap
decoder.parent	oscap
full_log	oscap: msg: "xccdf-result", scan-id: "10341490034836", content: "ssg-rhel-7-ds.xml", title: "Install libreswan Package", id: "xccdf_org.ssgproject.content_rule_package_libreswan_installed", result: "fail", severity: "low", description: "The Libreswan package provides an implementation of IPsec and IKE, which permits the creation of secure tunnels over untrusted networks. The libreswan package can be installed with the following command: $ sudo yum install libreswan", rationale: "Providing the ability for remote users or systems to initiate a secure VPN connection protects information when it is transmitted over a wide area network." references: "AC-17 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), MA-4 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), SC-9 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), 1130 (http://iase.disa.mil/stigs/cci/Pages/index.aspx), 1131 (http://iase.disa.mil/stigs/cci/Pages/index.aspx)", identifiers: "CCE-RHEL7-CCE-TBD (http://cce.mitre.org)", oval-id: "oval:ssg:def:473", benchmark-id: "xccdf_org.ssgproject.content_benchmark_RHEL-7", profile-id: "xccdf_org.ssgproject.content_profile_pci-dss", profile-title: "PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7".
host	vpc-ossec-manager
location	wodle_open-scap
manager.name	vpc-ossec-manager
oscap.check.description	The Libreswan package provides an implementation of IPsec and IKE, which permits the creation of secure tunnels over untrusted networks. The libreswan package can be installed with the following command: $ sudo yum install libreswan
oscap.check.id	xccdf_org.ssgproject.content_rule_package_libreswan_installed
oscap.check.identifiers	CCE-RHEL7-CCE-TBD (http://cce.mitre.org)
oscap.check.oval.id	oval:ssg:def:473
oscap.check.rationale	Providing the ability for remote users or systems to initiate a secure VPN connection protects information when it is transmitted over a wide area network.
oscap.check.references	AC-17 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), MA-4 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), SC-9 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), 1130 (http://iase.disa.mil/stigs/cci/Pages/index.aspx), 1131 (http://iase.disa.mil/stigs/cci/Pages/index.aspx)
oscap.check.result	fail
oscap.check.severity	low
oscap.check.title	Install libreswan Package
oscap.scan.benchmark.id	xccdf_org.ssgproject.content_benchmark_RHEL-7
oscap.scan.content	ssg-rhel-7-ds.xml
oscap.scan.id	10341490034836
oscap.scan.profile.id	xccdf_org.ssgproject.content_profile_pci-dss
oscap.scan.profile.title	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
rule.description	OpenSCAP: Install libreswan Package (not passed)
rule.firedtimes	5
rule.groups	oscap, oscap-result
rule.id	81529
rule.level	5
rule.pci_dss	2.2
source	



@timestamp	March 21st 2017, 11:33:56.000
_id	AVryIf3-AzWw4u-9YlQn
_index	wazuh-alerts-2017.03.21
_score	-
_type	wazuh
agent.id	1034
agent.ip	10.0.0.127
agent.name	vpc-agent-redhat
decoder.name	oscap
decoder.parent	oscap
full_log	oscap: msg: "xccdf-overview", scan-id: "10341490121236", content: "ssg-rhel-7-ds.xml", benchmark-id: "xccdf_org.ssgproject.content_benchmark_RHEL-7", profile-id: "xccdf_org.ssgproject.content_profile_pci-dss", profile-title: "PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7", score: "48.501732".
host	vpc-ossec-manager
location	wodle_open-scap
manager.name	vpc-ossec-manager
oscap.scan.benchmark.id	xccdf_org.ssgproject.content_benchmark_RHEL-7
oscap.scan.content	ssg-rhel-7-ds.xml
oscap.scan.id	10341490121236
oscap.scan.profile.id	xccdf_org.ssgproject.content_profile_pci-dss
oscap.scan.profile.title	PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
oscap.scan.score	48.502
rule.description	OpenSCAP Report overview: Score less than 50
rule.firedtimes	1
rule.groups	oscap, oscap-report
rule.id	81543
rule.level	7
rule.pci_dss	2.2
source	

Step 5: Dashboards

Finally, you can explore all scan results using the OpenSCAP dashboards for Kibana.


kibana
Discover
Visualize
Dashboard
Timelion
Wazuh
Graph
Dev Tools
Monitoring
Management
Collapse
WAZUH
OVERVIEW
MANAGER
AGENTS
DISCOVER
DASHBOARDS
GENERAL
FILE INTEGRITY
POLICY MONITORING
SCAP
AUDIT
PCI DSS
PANELS
DISCOVER
Last 1d
Search...
Actions
Agents
vpc-agent-re...
Profiles
PCI-DSS v3 ...
Common Pro...
Content
ssg-rhel-7-ds...
Severity
low
medium
high
Top 5 Agents - Severity high
Count
1
0.8
0.6
0.4
0.2
0
vpc-agent-re...
Top 10 - Alerts
Ensure auditd Collects File Deletion Eve...
Ensure auditd Collects Information on E...
Ensure auditd Collects Information on K...
Ensure auditd Collects System Adminis...
Ensure auditd Collects Unauthorized Ac...
Record Attempts to Alter Time Through ...
Record Attempts to Alter the localtime F...
Record Events that Modify User/Group ...
Record Events that Modify the System'...
Record Events that Modify the System'...
Top 10 - High risk alerts
Prevent Log In to Accounts With Empty...

oscap.scan.content: "ssg-rhel-7-ds.xml"

48.502
Last score

vpc-agent-redhat
Last agent scanned

Common Profile for General-Purpose Systems
Last scan profile

75
Higher score

48.502
Lower score

Configure Periodic Execution of AIDE
Latest alert

Last alerts

Agent name	Title	Profile	Scan ID	Content	Count
vpc-agent-redhat	Ensure auditd Collects File Deletion Events by User	Common Profile for General-Purpose Systems	10341490034852	ssg-rhel-7-ds.xml	1

Overwriting the timeout

It is possible to overwrite the timeout for a specific evaluation:

```
<wodle name="open-scap">

    <timeout>1800</timeout>

    <content type="xccdf" path="ssg-centos7-ds.xml">
        <timeout>120</timeout>
    </content>

    <content type="xccdf" path="ssg-centos6-ds.xml"/>

</wodle>
```

Using profiles

We can limit the evaluation to only specific profiles of a policy:

```
<wodle name="open-scap">

    <content type="xccdf" path="ssg-centos7-ds.xml">
        <profile>xccdf_org.ssgproject.content_profile_standard</profile>
        <profile>xccdf_org.ssgproject.content_profile_pci-dss</profile>
    </content>

    <content type="xccdf" path="ssg-centos6-ds.xml"/>

</wodle>
```

Using CPE dictionary

You can also optionally specify the CPE dictionary file, which is used to determine which checks are relevant to specific platforms.

```
<wodle name="open-scap">

    <content type="xccdf" path=policy="ssg-centos7-ds.xml">
        <cpe>file.xml</cpe>
    </content>

    <content type="xccdf" path="ssg-centos6-ds.xml" />

</wodle>
```

Using IDs

You can select a specific ID of the datastream file:

```
<wodle name="open-scap">

    <content type="xccdf" path="ssg-centos7-ds.xml">
        <datastream-id>id</datastream-id>
        <xccdf-id>id</xccdf-id>
    </content>

    <content type="xccdf" path="ssg-centos6-ds.xml" />

</wodle>
```