Use cases

Wazuh is often used to meet compliance requirements (such PCI DSS or HIPAA) and configuration standards (CIS hardening guides). It is also popular among IaaS users (eg. Amazon AWS, Azure or Google cloud), where deploying a host-based IDS in the running instances can be combined with the analysis of the infrastructure events (pulled directly from the cloud provider API).

Here is a list of common use cases:

Signature-based log analysis

Automated log analysis and management accelerate threat detection. There are many cases where evidence of an attack can be found in the logs of your devices, systems, and applications. Wazuh can be used to automatically aggregate and analyze log data.

The Wazuh agent (running on the monitored host) is usually the one in charge of reading operating system and application log messages, forwarding those to the Wazuh server, where the analysis takes place. When no agent is deployed, the server can also receive data via syslog, from network devices or applications.

Wazuh uses decoders to identify the source application of the log message and then analyzes it using application specific rules. Here is an example of a rule used to detect SSH authentication failure events:

```
<rule id="5716" level="5">
  <if_sid>5700</if_sid>
  <match>^Failed|^error: PAM: Authentication</match>
  <description>SSHD authentication failed.</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>
```

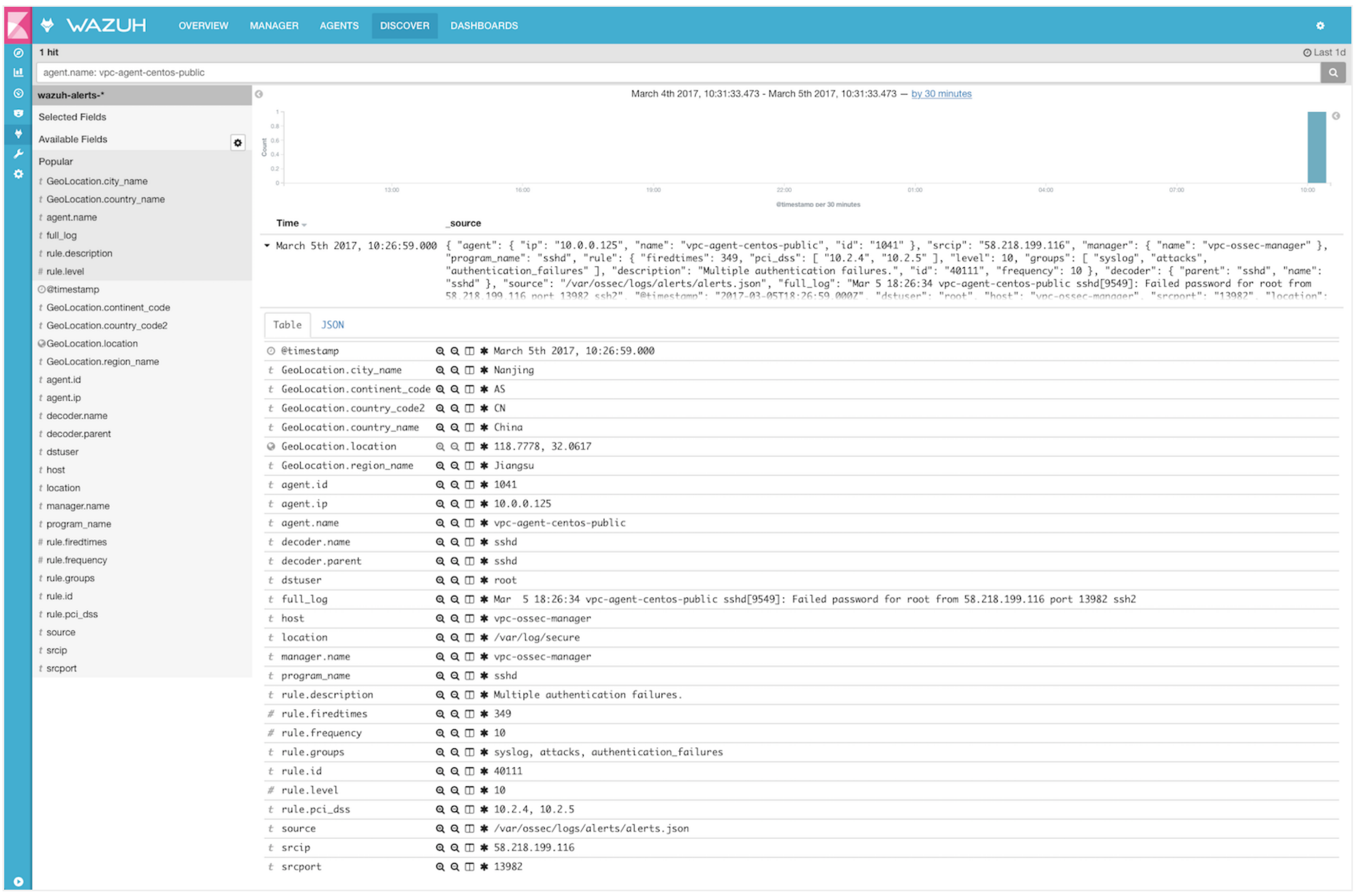
Rules include a `match` field, used to define the pattern the rule is going to be looking for. It also has a `level` field that specifies the resulting alert priority.

The manager will generate an alert every time an event collected by one of the agents (or via syslog) matches a rule (with level higher than zero).

Here is an example found in `/var/ossec/logs/alerts/alerts.json`:

```
{
  "agent": {
      "id": "1041",
      "ip": "10.0.0.125",
      "name": "vpc-agent-centos-public"
  },
  "decoder": {
      "name": "sshd",
      "parent": "sshd"
  },
  "dstuser": "root",
  "full_log": "Mar  5 18:26:34 vpc-agent-centos-public sshd[9549]: Failed password for root from
58.218.199.116 port 13982 ssh2",
  "location": "/var/log/secure",
  "manager": {
      "name": "vpc-ossec-manager"
  },
  "program_name": "sshd",
  "rule": {
      "description": "Multiple authentication failures.",
      "firedtimes": 349,
      "frequency": 10,
      "groups": [
          "syslog",
          "attacks",
          "authentication_failures"
      ],
      "id": "40111",
      "level": 10,
      "pci_dss": [
          "10.2.4",
          "10.2.5"
      ]
  },
  "srcip": "58.218.199.116",
  "srcport": "13982",
  "timestamp": "2017-03-05T10:26:59-0800"
}
```

Once generated by the manager, the alerts are sent to the Elastic Stack component where they are enriched with Geolocation information, stored and indexed. Kibana can be then used to search, analyze and visualize the data. See below an alert as displayed in the interface:



agent.name: vpc-agent-centos-public

Time	_source
March 5th 2017, 10:26:59.000	{ "agent": { "ip": "10.0.0.125", "name": "vpc-agent-centos-public", "id": "1041" }, "srcip": "58.218.199.116", "manager": { "name": "vpc-ossec-manager" }, "program_name": "sshd", "rule": { "firedtimes": 349, "pci_dss": ["10.2.4", "10.2.5"], "level": 10, "groups": ["syslog", "attacks", "authentication_failures"], "description": "Multiple authentication failures.", "id": "40111", "frequency": 10 }, "decoder": { "parent": "sshd", "name": "sshd" }, "source": "/var/ossec/logs/alerts/alerts.json", "full_log": "Mar 5 18:26:34 vpc-agent-centos-public sshd[9549]: Failed password for root from 58.218.199.116 port 13982 ssh2", "@timestamp": "2017-03-05T18:26:59.000Z", "dstuser": "root", "host": "vpc-ossec-manager", "srcport": "13982", "location":

@timestamp	March 5th 2017, 10:26:59.000
GeoLocation.city_name	Nanjing
GeoLocation.continent_code	AS
GeoLocation.country_code2	CN
GeoLocation.country_name	China
GeoLocation.location	118.7778, 32.0617
GeoLocation.region_name	Jiangsu
agent.id	1041
agent.ip	10.0.0.125
agent.name	vpc-agent-centos-public
decoder.name	sshd
decoder.parent	sshd
dstuser	root
full_log	Mar 5 18:26:34 vpc-agent-centos-public sshd[9549]: Failed password for root from 58.218.199.116 port 13982 ssh2
host	vpc-ossec-manager
location	/var/log/secure
manager.name	vpc-ossec-manager
program_name	sshd
rule.description	Multiple authentication failures.
rule.firedtimes	349
rule.frequency	10
rule.groups	syslog, attacks, authentication_failures
rule.id	40111
rule.level	10
rule.pci_dss	10.2.4, 10.2.5
source	/var/ossec/logs/alerts/alerts.json
srcip	58.218.199.116
srcport	13982

Wazuh provides a default ruleset, updated periodically, with over 1,600 rules for different applications.

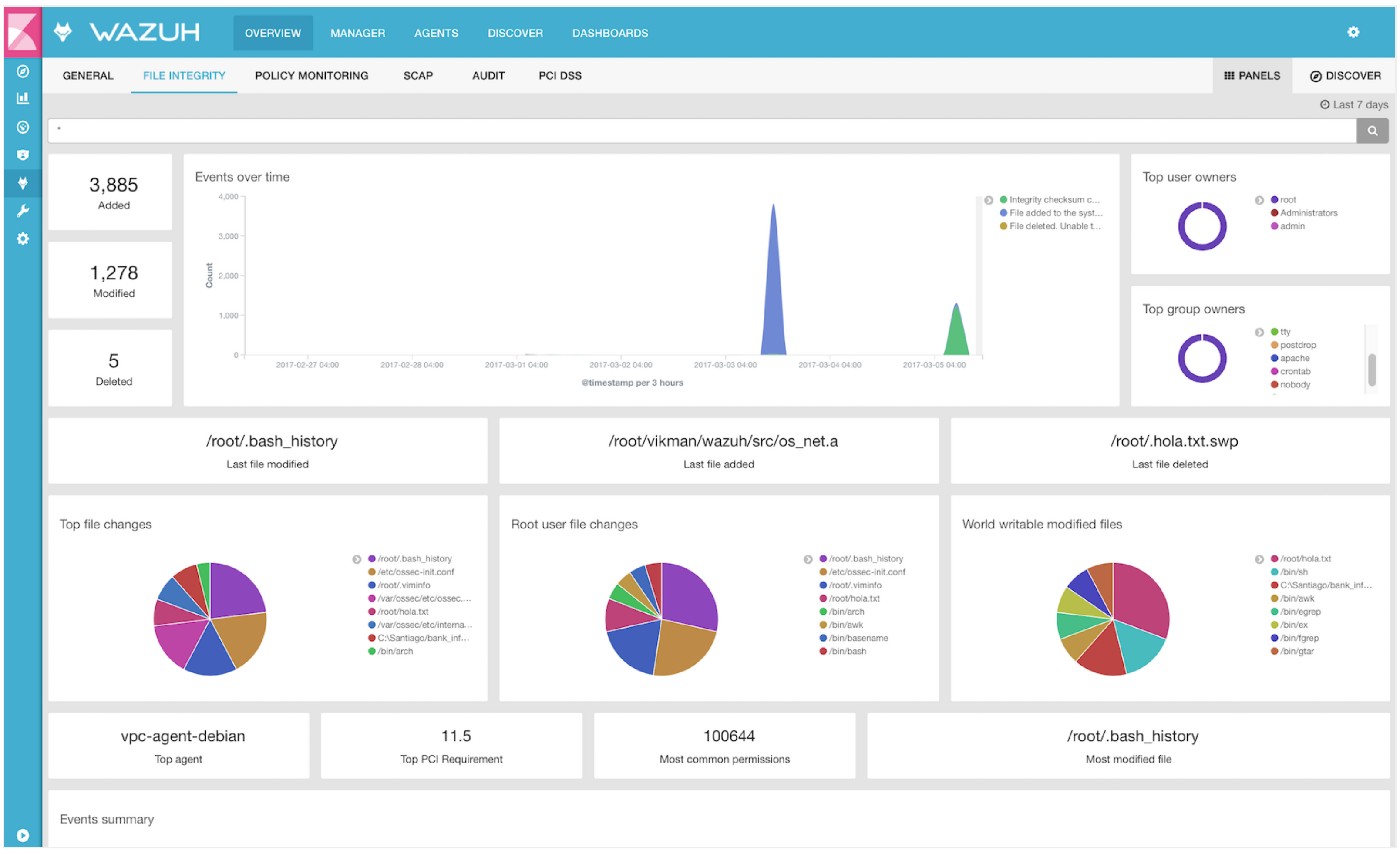
File integrity monitoring

File integrity monitoring (FIM) component detects and alerts when operating system and application files are modified. This capability is often used to detect access or changes to sensitive data. In fact, if your servers are in scope with PCI DSS, the requirement 11.5 states that you must install a file integrity monitoring solution to pass your audit.

Below is an example of an alert, generated when a monitored file is changed. Metadata includes MD5 and SHA1 checksums, file sizes (before and after the change), file permissions, file owner and content changes.

```
{
  "agent": {
      "id": "003",
      "ip": "10.0.0.121",
      "name": "vpc-agent-debian"
  },
  "decoder": {
      "name": "syscheck_integrity_changed"
  },
  "full_log": "Integrity checksum changed for: '/root/hola.txt'\nSize changed from '3089' to '3213'\nOld
md5sum was: '20db2c4c9bdd937975371bc5ca25af92'\nNew md5sum is : '3841e727a28f733e6d34413afd49d607'\nOld
sha1sum was: 'a6c57142a6e6e7e55c58b3174ee52b4f8ec996e3'\nNew sha1sum is :
'99aa4b60467a932c89f32603e410a6c194fb1ac3'\n",
  "location": "syscheck",
  "manager": {
      "name": "vpc-ossec-manager"
  },
  "rule": {
      "description": "Integrity checksum changed.",
      "firedtimes": 8,
      "groups": [
          "ossec",
          "syscheck"
      ],
      "id": "550",
      "level": 7,
      "pci_dss": [
          "11.5"
      ]
  },
  "syscheck": {
      "diff": "0a1,2\n> Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor
incididunt ut labore et dolore magna aliqua\n> \n",
      "event": "modified",
      "gid_after": "0",
      "gname_after": "root",
      "inode_after": 398585,
      "md5_after": "3841e727a28f733e6d34413afd49d607",
      "md5_before": "20db2c4c9bdd937975371bc5ca25af92",
      "mtime_after": "2017-03-05T13:47:32",
      "mtime_before": "2017-03-05T13:44:15",
      "path": "/root/hola.txt",
      "perm_after": "100666",
      "sha1_after": "99aa4b60467a932c89f32603e410a6c194fb1ac3",
      "sha1_before": "a6c57142a6e6e7e55c58b3174ee52b4f8ec996e3",
      "size_after": "3213",
      "size_before": "3089",
      "uid_after": "1000",
      "uname_after": "admin"
  },
  "timestamp": "2017-03-05T13:44:18-0800"
}
```

A good summary of file changes, can be found in the file integrity monitoring dashboard, which provides drill-down capabilities to get all details of the alerts triggered.



Rootkits detection

Wazuh agent periodically scans the monitored system to detect rootkits both at a kernel and user level. This type of malware usually replaces or changes existing operating system components in order to alter the behavior of the system, it can hide other processes, files or network connections like itself.

Wazuh uses different detection mechanisms to look for system anomalies or well-known intrusions. This is done periodically by the *Rootcheck* component:

Action	Detection mechanism	Binary	System call
Detection of hidden processes	Comparing output of system binaries and system calls	ps	setsid()
			getpgid()
			kill()
Detection of hidden files	Comparing output of system binaries and system calls	ls	stat()
			opendir()
			readdir()
	Scanning /dev	ls	opendir()
Detection of hidden ports	Comparing output of system binaries and system calls	netstat	bind()
Detection of known rootkits	Using a malicious file database		stat()
			fopen()
			opendir()
	Inspecting files content using signatures		fopen()
	Detecting file permission and ownership anomalies		stat()

Below is an example of an alert generated when a hidden process is found. In this case, the affected system is running a Linux kernel-level rootkit (named Diamorphine):

```
{
  "agent": {
      "id": "1030",
      "ip": "10.0.0.59",
      "name": "diamorphine-POC"
  },
  "decoder": {
      "name": "rootcheck"
  },
  "full_log": "Process '562' hidden from /proc. Possible kernel level rootkit.",
  "location": "rootcheck",
  "manager": {
      "name": "vpc-ossec-manager"
  },
  "rule": {
      "description": "Host-based anomaly detection event (rootcheck).",
      "firedtimes": 4,
      "groups": [
          "ossec",
          "rootcheck"
      ],
      "id": "510",
      "level": 7
  },
  "timestamp": "2017-03-05T15:13:04-0800",
  "title": "Process '562' hidden from /proc."
}
```

Security policy monitoring

SCAP is a standardized compliance checking solution for enterprise-level infrastructure. It is a line of specifications maintained by the National Institute of Standards and Technology (NIST) with the purpose of maintaining enterprise systems security.

OpenSCAP is an auditing tool that utilizes the Extensible Configuration Checklist Description Format (XCCDF). XCCDF is a standard way of expressing checklist content and defines security checklists. It also combines with other specifications such as CPE, CVE, CCE, and OVAL, to create SCAP-expressed checklist that can be processed by SCAP-validated products.

Wazuh agent uses OpenSCAP internally to verify that systems conform to CIS hardening standards. Below is an example of an SCAP rule used to check if SSH daemon is configured to allow empty passwords:

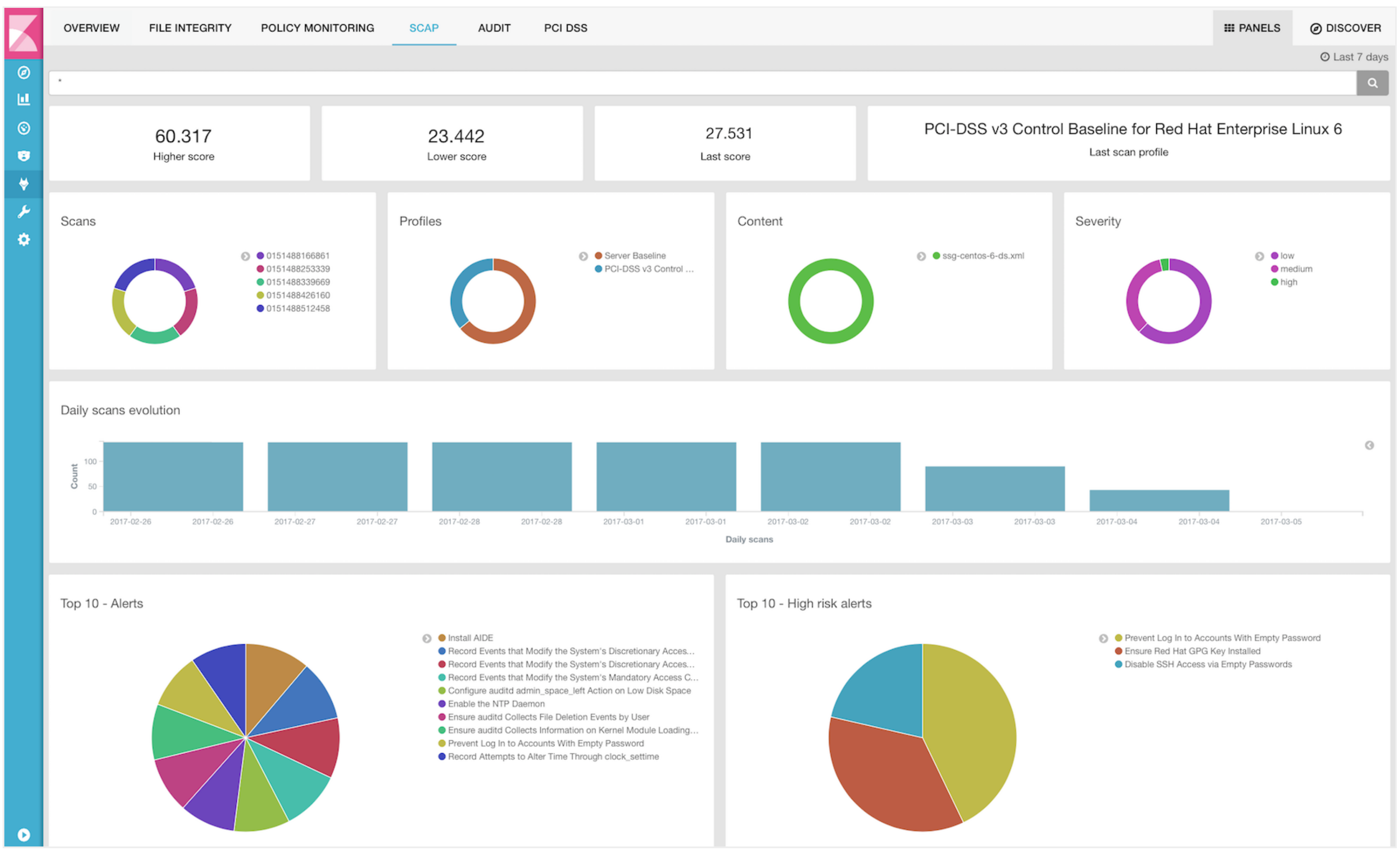
```
<ns10:Rule id="xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords" selected="false"
severity="high">
  <ns10:title xml:lang="en-US">Disable SSH Access via Empty Passwords</ns10:title>
  <ns10:description xml:lang="en-US">To explicitly disallow remote login from accounts with empty passwords,
add or correct the following line in <html:code>/etc/ssh/sshd_config</html:code>:
<html:pre>PermitEmptyPasswords no</html:pre> Any accounts with empty passwords should be disabled
immediately, and PAM configuration should prevent users from being able to assign themselves empty passwords.
  </ns10:description>
  <ns10:reference href="http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf">AC-
3</ns10:reference>
  <ns10:reference href="http://iase.disa.mil/stigs/cci/Pages/index.aspx">765</ns10:reference>
  <ns10:reference href="http://iase.disa.mil/stigs/cci/Pages/index.aspx">766</ns10:reference>
  <ns10:rationale xml:lang="en-US">Configuring this setting for the SSH daemon provides additional assurance
that remote login via SSH will require a password, even in the event of misconfiguration elsewhere.
</ns10:rationale>
  <ns10:fix complexity="low" disruption="low" id="sshd_disable_empty_passwords" reboot="false"
strategy="enable" system="urn:xccdf:fix:script:sh">grep -q ^PermitEmptyPasswords /etc/ssh/sshd_config
&amp;&amp; \ sed -i "s/PermitEmptyPasswords.*/PermitEmptyPasswords no/g" /etc/ssh/sshd_config; if ! [ $? -eq
0 ]; then; echo "PermitEmptyPasswords no" &gt;&gt; /etc/ssh/sshd_config; fi
  </ns10:fix>
  <ns10:check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <ns10:check-content-ref href="ssg-rhel6-oval.xml" name="oval:ssg-sshd_disable_empty_passwords:def:1" />
  </ns10:check>
  <ns10:check system="http://scap.nist.gov/schema/ocil/2">
    <ns10:check-content-ref href="ssg-rhel6-ocil.xml" name="ocil:ssg-
sshd_disable_empty_passwords_ocil:questionnaire:1" />
  </ns10:check>
</ns10:Rule>
```

SCAP checks are run periodically (default is once a day), and results are set to the Wazuh server where they are processed through OpenSCAP decoders and rules. Below is an example of an alert, generated when Linux audit policies (auditd) are not configured to monitor user actions:

```
{
  "agent": {
      "id": "1040",
      "ip": "10.0.0.76",
      "name": "ip-10-0-0-76"
  },
  "decoder": {
      "name": "oscap",
      "parent": "oscap"
  },
  "full_log": "oscap: msg: \"xccdf-result\", scan-id: \"10401488754797\", content: \"ssg-centos-7-ds.xml\",
title: \"Ensure auditd Collects System Administrator Actions\", id:
\"xccdf_org.ssgproject.content_rule_audit_rules_sysadmin_actions\", result: \"fail\", severity: \"low\",
description: \"At a minimum the audit system should collect administrator actions for all users and root. If
the auditd daemon is configured to use the augenrules program to read audit rules during daemon startup (the
default), add the following line to a file with suffix .rules in the directory /etc/audit/rules.d: -w
/etc/sudoers -p wa -k actions If the auditd daemon is configured to use the auditctl utility to read audit
rules during daemon startup, add the following line to /etc/audit/audit.rules file: -w /etc/sudoers -p wa -k
actions\", rationale: \"The actions taken by system administrators should be audited to keep a record of what
was executed on the system, as well as, for accountability purposes.\" references: \"AC-2(7)(b)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AC-17(7)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-1(b)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-2(a)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-2(c)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-2(d)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-12(a)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-12(c)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), IR-5
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), 126
(http://iase.disa.mil/stigs/cci/Pages/index.aspx), Test attestation on 20121024 by DS
(https://github.com/OpenSCAP/scap-security-guide/wiki/Contributors)\", identifiers: \"CCE-RHEL7-CCE-TBD
(http://cce.mitre.org)\", oval-id: \"oval:ssg:def:370\", benchmark-id:
\"xccdf_org.ssgproject.content_benchmark_RHEL-7\", profile-id:
\"xccdf_org.ssgproject.content_profile_common\", profile-title: \"Common Profile for General-Purpose
Systems\".",
  "location": "wodle_open-scap",
  "manager": {
      "name": "vpc-ossec-manager"
  },
  "oscap": {
      "check": {
          "description": "At a minimum the audit system should collect administrator actions for all users
and root. If the auditd daemon is configured to use the augenrules program to read audit rules during daemon
startup (the default), add the following line to a file with suffix .rules in the directory
/etc/audit/rules.d: -w /etc/sudoers -p wa -k actions If the auditd daemon is configured to use the auditctl
utility to read audit rules during daemon startup, add the following line to /etc/audit/audit.rules file: -w
/etc/sudoers -p wa -k actions",
          "id": "xccdf_org.ssgproject.content_rule_audit_rules_sysadmin_actions",
          "identifiers": "CCE-RHEL7-CCE-TBD (http://cce.mitre.org)",
          "oval": {
              "id": "oval:ssg:def:370"
          },
          "rationale": "The actions taken by system administrators should be audited to keep a record of what
was executed on the system, as well as, for accountability purposes.",
          "references": "AC-2(7)(b) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-
53r4.pdf), AC-17(7) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-1(b)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-2(a)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-2(c)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-2(d)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-12(a)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), AU-12(c)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), IR-5
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), 126
(http://iase.disa.mil/stigs/cci/Pages/index.aspx), Test attestation on 20121024 by DS
(https://github.com/OpenSCAP/scap-security-guide/wiki/Contributors)",
          "result": "fail",
          "severity": "low",
          "title": "Ensure auditd Collects System Administrator Actions"
```

```
        },
        "scan": {
            "benchmark": {
                "id": "xccdf_org.ssgproject.content_benchmark_RHEL-7"
            },
            "content": "ssg-centos-7-ds.xml",
            "id": "10401488754797",
            "profile": {
                "id": "xccdf_org.ssgproject.content_profile_common",
                "title": "Common Profile for General-Purpose Systems"
            }
        }
    },
    "rule": {
        "description": "OpenSCAP: Ensure auditd Collects System Administrator Actions (not passed)",
        "firedtimes": 3,
        "groups": [
            "oscap",
            "oscap-result"
        ],
        "id": "81529",
        "level": 5,
        "pci_dss": [
            "2.2"
        ]
    },
    "timestamp": "2017-03-05T15:00:03-0800"
}
```

In addition, Wazuh WUI can be used to visualize and analyze policy monitoring scan results. For example, here is a screenshot of data collected from a CentOS system when scanning it using `Server baseline` and `PCI DSS v3` pre-defined profiles:


OVERVIEW
FILE INTEGRITY
POLICY MONITORING
SCAP
AUDIT
PCI DSS
PANELS
DISCOVER
Last 7 days
60.317
Higher score
23.442
Lower score
27.531
Last score
PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 6
Last scan profile
Scans
0151488166861
0151488253339
0151488339669
0151488426160
0151488512458
Profiles
Server Baseline
PCI-DSS v3 Control ...
Content
ssg-centos-6-ds.xml
Severity
low
medium
high
Daily scans evolution
Count
Daily scans
Top 10 - Alerts
Install AIDE
Record Events that Modify the System's Discretionary Acces...
Record Events that Modify the System's Discretionary Acces...
Record Events that Modify the System's Mandatory Access C...
Configure auditd admin_space_left Action on Low Disk Space
Enable the NTP Daemon
Ensure auditd Collects File Deletion Events by User
Ensure auditd Collects Information on Kernel Module Loading...
Prevent Log In to Accounts With Empty Password
Record Attempts to Alter Time Through clock_settime
Top 10 - High risk alerts
Prevent Log In to Accounts With Empty Password
Ensure Red Hat GPG Key Installed
Disable SSH Access via Empty Passwords