Documentation › Using Wazuh for PCI DSS › File integrity monitoring

File integrity monitoring

File integrity monitoring (Syscheck) is performed by comparing the cryptographic checksum and other attributes of a known good file against the checksum and attributes of that file after it has been modified.

First, the Wazuh agent scans the system at an interval you specify, and it sends the checksums of the monitored files and registry keys (for Windows systems) to the Wazuh server. Then, the server stores the checksums and looks for modifications by comparing the newly received checksums against the historical checksum values for those files and/or registry keys. An alert is sent if the checksum (or another file attribute) changes. Wazuh also supports near real-time file integrity checking where this is desired.

Syscheck can be used to meet PCI DSS requirement 11.5:

> **11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Use cases

In this example, we have configured Wazuh to detect changes in the file `/root/credit_cards`.

```
<syscheck>
    <directories check_all="yes" report_changes="yes">/root/credit_cards</directories>
</syscheck>
```

So, when we modify the file, Wazuh generates an alert.

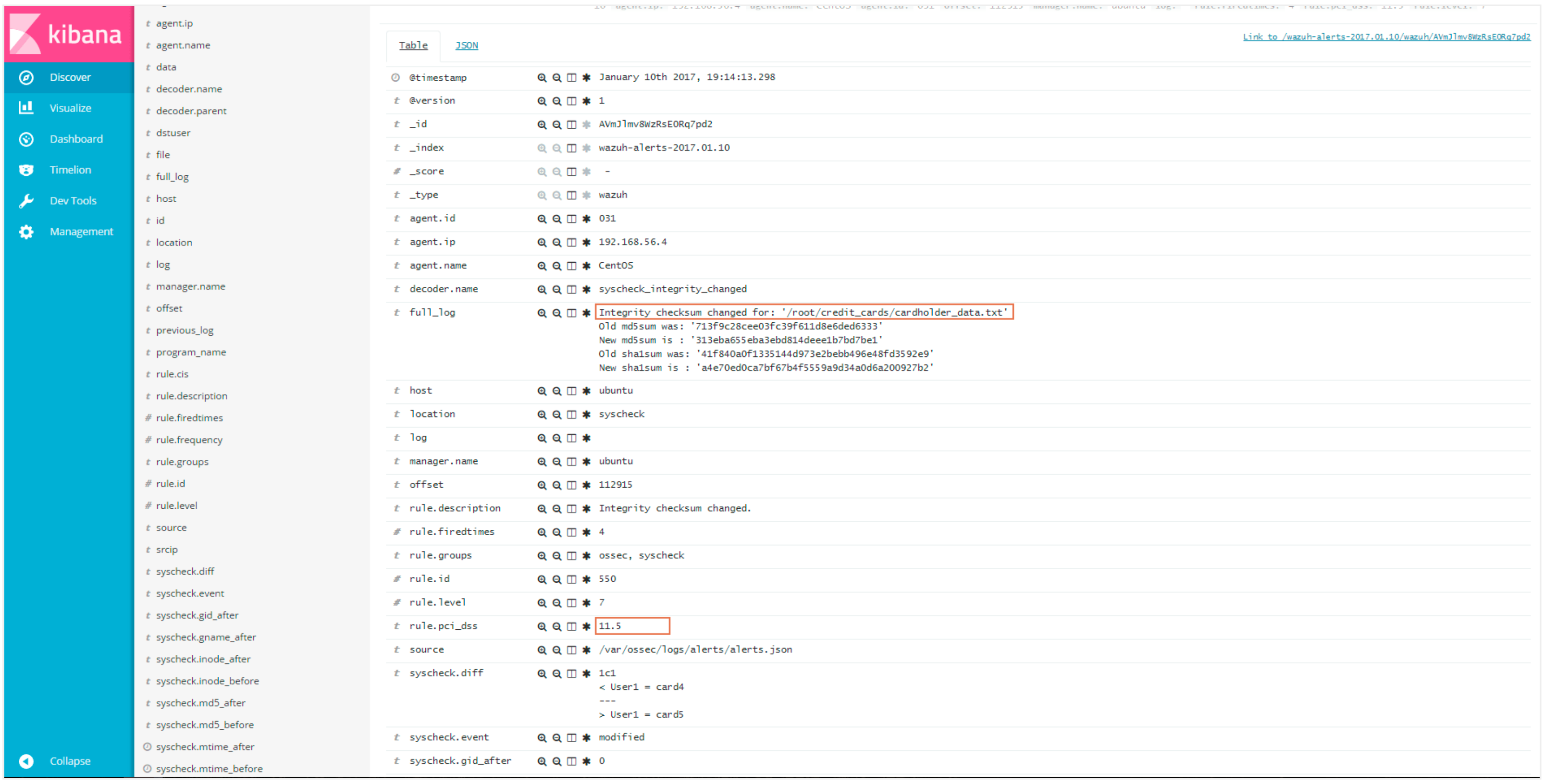
```
[root@centos ~]# ls -l credit_cards
+total 4
-rw-r--r--. 1 root root 14 Jan 10 19:33 cardholder_data.txt
[root@centos ~]# cat credit_cards/cardholder_data.txt
User1 = card4
[root@centos ~]# echo "User1 = card5" > credit_cards/cardholder_data.txt
[root@centos ~]# cat credit_cards/cardholder_data.txt
User1 = card5
```

As you can see, syscheck alerts are tagged with the requirement 11.5.

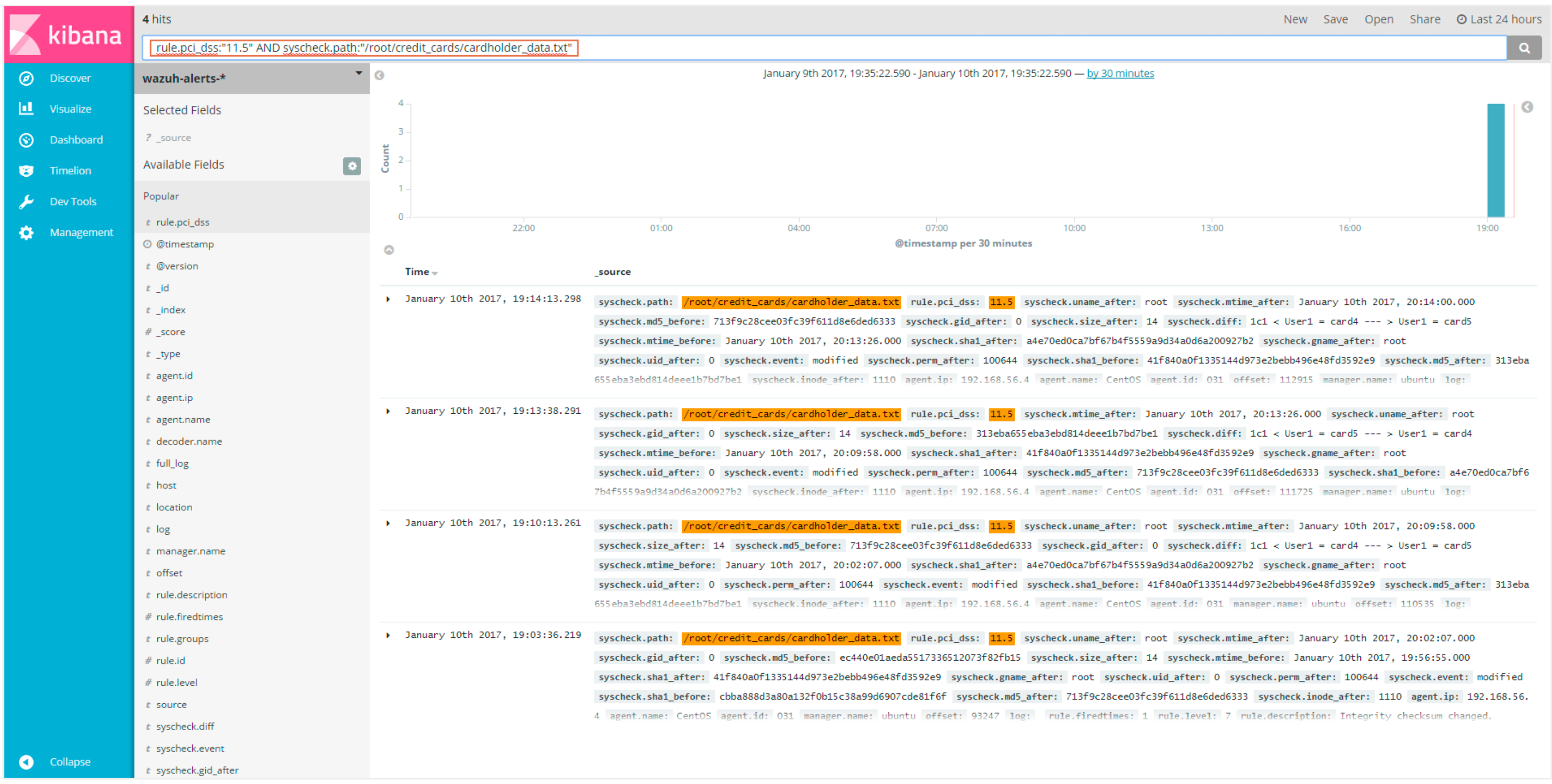
```
root@ubuntu:~# tail -n28 /var/ossec/logs/alerts/alerts.log

** Alert 1484071804.77110: - ossec,syscheck,pci_dss_11.5,
2017 Jan 10 19:10:04 (CentOS) 192.168.56.4->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
Integrity checksum changed for: '/root/credit_cards/cardholder_data.txt'
Old md5sum was: '713f9c28cee03fc39f611d8e6ded6333'
New md5sum is : '313eba655eba3ebd814deee1b7bd7be1'
Old sha1sum was: '41f840a0f1335144d973e2bebb496e48fd3592e9'
New sha1sum is : 'a4e70ed0ca7bf67b4f5559a9d34a0d6a200927b2'

File: /root/credit_cards/cardholder_data.txt
New size: 14
New permissions: 100644
New user: root (0)
New group: root (0)
Old MD5: 713f9c28cee03fc39f611d8e6ded6333
New MD5: 313eba655eba3ebd814deee1b7bd7be1
Old SHA1: 41f840a0f1335144d973e2bebb496e48fd3592e9
New SHA1: a4e70ed0ca7bf67b4f5559a9d34a0d6a200927b2
Old date: Tue Jan 10 19:02:07 2017
New date: Tue Jan 10 19:09:58 2017
New inode: 1110
What changed: 1c1
< User1 = card4
---
> User1 = card5
```



@timestamp	January 10th 2017, 19:14:13.298
@version	1
_id	AVmJlmv8WzRsE0Rq7pd2
_index	wazuh-alerts-2017.01.10
_score	-
_type	wazuh
agent.id	031
agent.ip	192.168.56.4
agent.name	CentOS
decoder.name	syscheck_integrity_changed
full_log	Integrity checksum changed for: '/root/credit_cards/cardholder_data.txt' Old md5sum was: '713f9c28cee03fc39f611d8e6ded6333' New md5sum is : '313eba655eba3ebd814deee1b7bd7be1' Old sha1sum was: '41f840a0f1335144d973e2bebb496e48fd3592e9' New sha1sum is : 'a4e70ed0ca7bf67b4f5559a9d34a0d6a200927b2'
host	ubuntu
location	syscheck
log	
manager.name	ubuntu
offset	112915
rule.description	Integrity checksum changed.
rule.firedtimes	4
rule.groups	ossec, syscheck
rule.id	550
rule.level	7
rule.pci_dss	11.5
source	/var/ossec/logs/alerts/alerts.json
syscheck.diff	1c1 < User1 = card4 --- > User1 = card5
syscheck.event	modified
syscheck.gid_after	0



4 hits

rule.pci_dss:"11.5" AND syscheck.path:"/root/credit_cards/cardholder_data.txt"

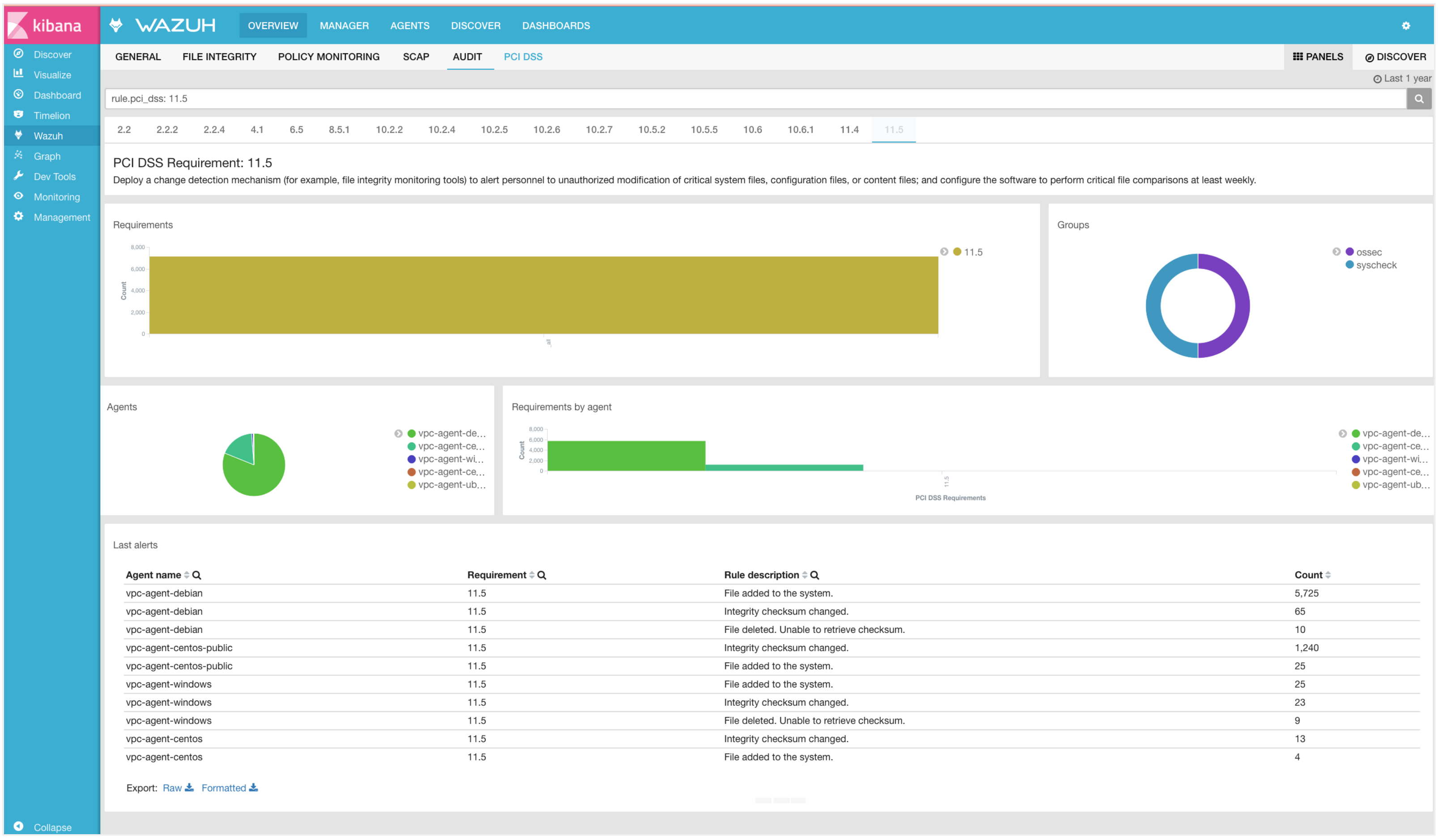
January 9th 2017, 19:35:22.590 - January 10th 2017, 19:35:22.590 — by 30 minutes

```
Time                               _source
January 10th 2017, 19:14:13.298    syscheck.path: /root/credit_cards/cardholder_data.txt rule.pci_dss: 11.5 syscheck.uname_after: root syscheck.mtime_after: January 10th 2017, 20:14:00.000
                                   syscheck.md5_before: 713f9c28cee03fc39f611d8e6ded6333 syscheck.gid_after: 0 syscheck.size_after: 14 syscheck.diff: 1c1 < User1 = card4 --- > User1 = card5
                                   syscheck.mtime_before: January 10th 2017, 20:13:26.000 syscheck.sha1_after: a4e70ed0ca7bf67b4f5559a9d34a0d6a200927b2 syscheck.gname_after: root
                                   syscheck.uid_after: 0 syscheck.event: modified syscheck.perm_after: 100644 syscheck.sha1_before: 41f840a0f1335144d973e2bebb496e48fd3592e9 syscheck.md5_after: 313eba
                                   655eba3ebd814deee1b7bd7be1 syscheck.inode_after: 1110 agent.ip: 192.168.56.4 agent.name: CentOS agent.id: 031 offset: 112915 manager.name: ubuntu log:

January 10th 2017, 19:13:38.291    syscheck.path: /root/credit_cards/cardholder_data.txt rule.pci_dss: 11.5 syscheck.mtime_after: January 10th 2017, 20:13:26.000 syscheck.uname_after: root
                                   syscheck.gid_after: 0 syscheck.size_after: 14 syscheck.md5_before: 313eba655eba3ebd814deee1b7bd7be1 syscheck.diff: 1c1 < User1 = card5 --- > User1 = card4
                                   syscheck.mtime_before: January 10th 2017, 20:09:58.000 syscheck.sha1_after: 41f840a0f1335144d973e2bebb496e48fd3592e9 syscheck.gname_after: root
                                   syscheck.uid_after: 0 syscheck.event: modified syscheck.perm_after: 100644 syscheck.md5_after: 713f9c28cee03fc39f611d8e6ded6333 syscheck.sha1_before: a4e70ed0ca7bf6
                                   7b4f5559a9d34a0d6a200927b2 syscheck.inode_after: 1110 agent.ip: 192.168.56.4 agent.name: CentOS agent.id: 031 offset: 111725 manager.name: ubuntu log:

January 10th 2017, 19:10:13.261    syscheck.path: /root/credit_cards/cardholder_data.txt rule.pci_dss: 11.5 syscheck.uname_after: root syscheck.mtime_after: January 10th 2017, 20:09:58.000
                                   syscheck.size_after: 14 syscheck.md5_before: 713f9c28cee03fc39f611d8e6ded6333 syscheck.gid_after: 0 syscheck.diff: 1c1 < User1 = card4 --- > User1 = card5
                                   syscheck.mtime_before: January 10th 2017, 20:02:07.000 syscheck.sha1_after: a4e70ed0ca7bf67b4f5559a9d34a0d6a200927b2 syscheck.gname_after: root
                                   syscheck.uid_after: 0 syscheck.perm_after: 100644 syscheck.event: modified syscheck.sha1_before: 41f840a0f1335144d973e2bebb496e48fd3592e9 syscheck.md5_after: 313eba
                                   655eba3ebd814deee1b7bd7be1 syscheck.inode_after: 1110 agent.ip: 192.168.56.4 agent.name: CentOS agent.id: 031 manager.name: ubuntu offset: 110535 log:

January 10th 2017, 19:03:36.219    syscheck.path: /root/credit_cards/cardholder_data.txt rule.pci_dss: 11.5 syscheck.uname_after: root syscheck.mtime_after: January 10th 2017, 20:02:07.000
                                   syscheck.gid_after: 0 syscheck.md5_before: ec440e01aeda5517336512073f82fb15 syscheck.size_after: 14 syscheck.mtime_before: January 10th 2017, 19:56:55.000
                                   syscheck.sha1_after: 41f840a0f1335144d973e2bebb496e48fd3592e9 syscheck.gname_after: root syscheck.uid_after: 0 syscheck.perm_after: 100644 syscheck.event: modified
                                   syscheck.sha1_before: cbba888d3a80a132f0b15c38a99d6907cde81f6f syscheck.md5_after: 713f9c28cee03fc39f611d8e6ded6333 syscheck.inode_after: 1110 agent.ip: 192.168.56.
                                   4 agent.name: CentOS agent.id: 031 manager.name: ubuntu offset: 93247 log: rule.firedtimes: 1 rule.level: 7 rule.description: Integrity checksum changed.
```



rule.pci_dss: 11.5

PCI DSS Requirement: 11.5

Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Last alerts

Agent name	Requirement	Rule description	Count
vpc-agent-debian	11.5	File added to the system.	5,725
vpc-agent-debian	11.5	Integrity checksum changed.	65
vpc-agent-debian	11.5	File deleted. Unable to retrieve checksum.	10
vpc-agent-centos-public	11.5	Integrity checksum changed.	1,240
vpc-agent-centos-public	11.5	File added to the system.	25
vpc-agent-windows	11.5	File added to the system.	25
vpc-agent-windows	11.5	Integrity checksum changed.	23
vpc-agent-windows	11.5	File deleted. Unable to retrieve checksum.	9
vpc-agent-centos	11.5	Integrity checksum changed.	13
vpc-agent-centos	11.5	File added to the system.	4

Export: Raw Formatted