info@wazuh.com
https://wazuh.com

PCI DSS report

Global security standard for entities that process, store or transmit payment cardholder data.

2024-04-16T17:36:15 to 2024-05-16T17:36:15

rule.pci_dss: * AND cluster.name: wazuh

Most common PCI DSS requirements alerts found

Requirement 10.2.4

Invalid logical access attempts

Top rules for 10.2.4 requirement

Rule ID	Description
30306	Apache: Attempt to access forbidden directory index.
5710	sshd: Attempt to login using a non-existent user
5712	sshd: brute force trying to get access to the system.

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.

Top rules for 10.2.5 requirement

Rule ID	Description
5710	sshd: Attempt to login using a non-existent user
5712	sshd: brute force trying to get access to the system.
5557	unix_chkpwd: Password check failed.

Requirement 11.2.1

Top rules for 11.2.1 requirement

Rule ID	Description

Rule ID	Description
23503	CVE-2013-4235 affects login
23505	CVE-2018-1000035 affects unzip
23505	CVE-2020-1747 affects python3-yaml

Requirement 11.4

Use intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up to date.

Top rules for 11.4 requirement

Rule ID	Description
31151	Multiple web server 400 error codes from same source ip.
31101	Web server 400 error code.
5702	sshd: Reverse lookup error (bad ISP or attack).

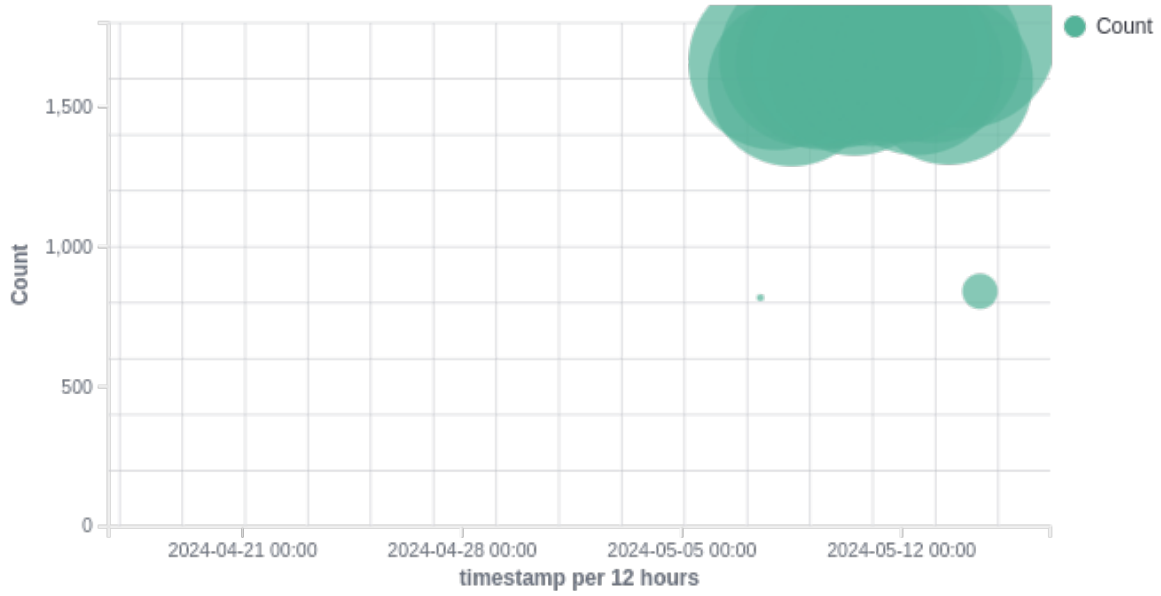
Requirement 11.5

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.

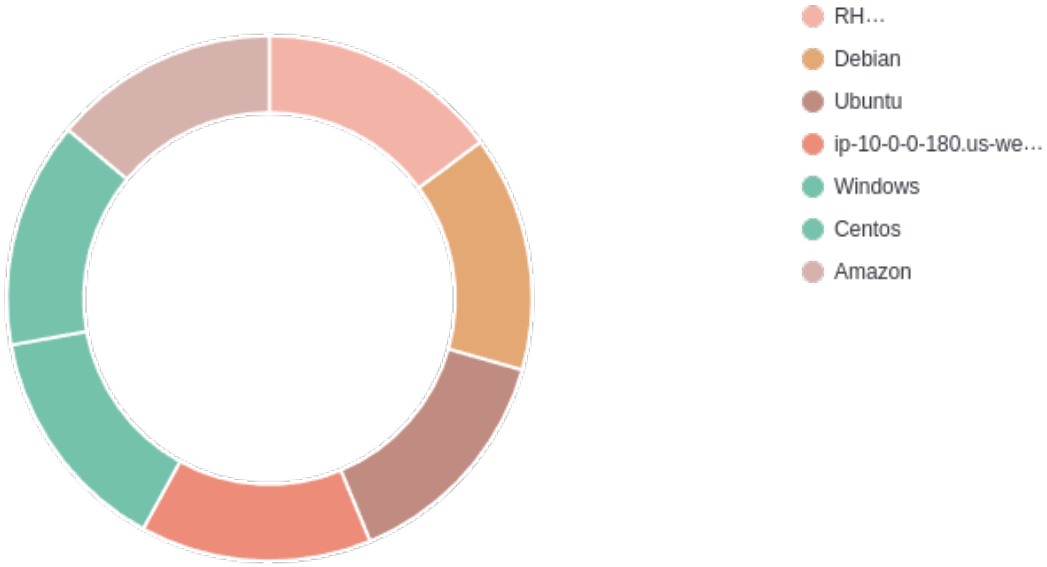
Top rules for 11.5 requirement

Rule ID	Description
550	Integrity checksum changed.
554	File added to the system.
553	File deleted.

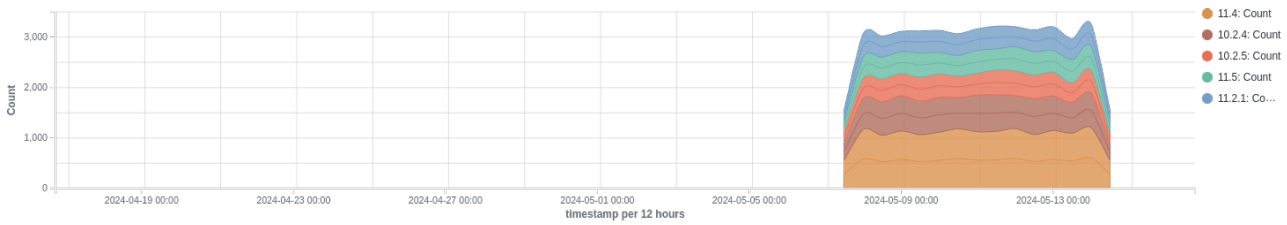
Top 10 PCI DSS requirements



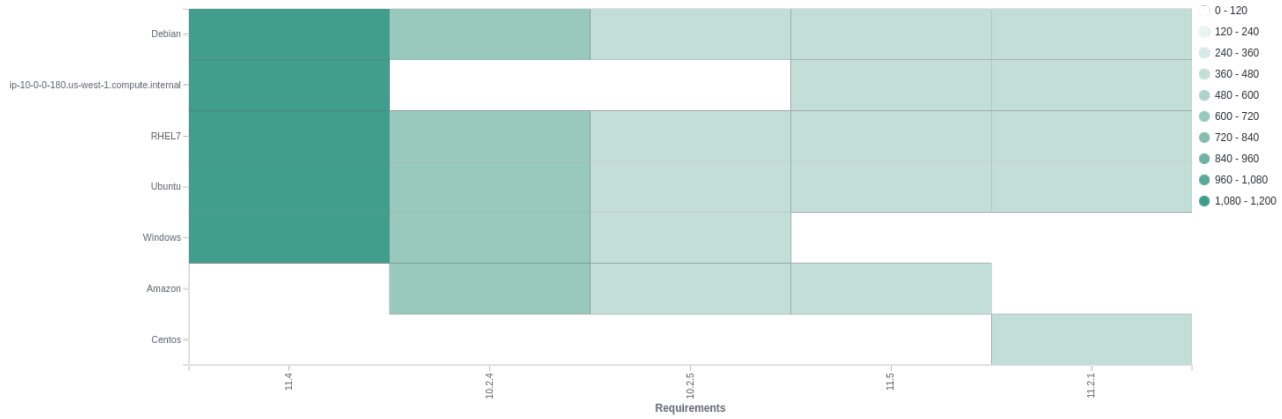
Top 10 agents by alerts count



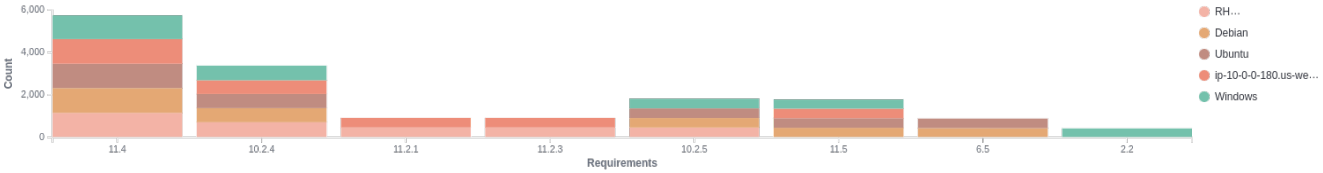
Top requirements over time



Last alerts



Requirements by agent



Alerts summary

Agent name	Requirement	Description	Count
RHEL7	10.2.4	Apache: Attempt to access forbidden directory index.	311
RHEL7	11.4	Web server 400 error code.	230
RHEL7	11.4	Multiple web server 400 error codes from same source ip.	222
RHEL7	11.4	sshd: Reverse lookup error (bad ISP or attack).	125
RHEL7	11.4	sshd: Possible breakin attempt (high number of reverse lookup errors).	109
RHEL7	11.4	sshd: insecure connection attempt (scan).	108
RHEL7	11.4	sshd: Possible attack on the ssh server (or version gathering).	98
RHEL7	10.2.4	sshd: Attempt to login using a non-existent user	86
RHEL7	10.2.5	sshd: Attempt to login using a non-existent user	86
RHEL7	10.2.4	Logon Failure - Unknown user or bad password	54
RHEL7	10.2.5	Logon Failure - Unknown user or bad password	54
RHEL7	10.2.4	unix_chkpwd: Password check failed.	49
RHEL7	10.2.5	unix_chkpwd: Password check failed.	49
RHEL7	11.4	sshd: Multiple authentication failures.	42
RHEL7	10.2.4	sshd: Multiple authentication failures.	42
RHEL7	10.2.5	sshd: Multiple authentication failures.	42
RHEL7	11.4	sshd: brute force trying to get access to the system.	39
RHEL7	10.2.4	sshd: brute force trying to get access to the system.	39
RHEL7	10.2.5	sshd: brute force trying to get access to the system.	39
RHEL7	10.2.4	sshd: authentication failed.	37
RHEL7	10.2.5	sshd: authentication failed.	37
RHEL7	10.2.4	PAM: User login failed.	33
RHEL7	10.2.5	PAM: User login failed.	33
RHEL7	11.2.1	CVE-2018-1000035 affects unzip	21
RHEL7	11.2.3	CVE-2018-1000035 affects unzip	21
RHEL7	11.2.1	CVE-2013-4235 affects login	19
RHEL7	11.2.3	CVE-2013-4235 affects login	19
RHEL7	11.2.1	CVE-2018-6485 affects libc-bin	14
RHEL7	11.2.1	CVE-2020-1747 affects python3-yaml	14
RHEL7	11.2.3	CVE-2018-6485 affects libc-bin	14
RHEL7	11.2.3	CVE-2020-1747 affects python3-yaml	14
RHEL7	11.2.1	CVE-2018-20482 affects tar	13
RHEL7	11.2.3	CVE-2018-20482 affects tar	13
RHEL7	11.2.1	CVE-2020-1927 affects apache2-bin	12
RHEL7	11.2.3	CVE-2020-1927 affects apache2-bin	12
RHEL7	11.4	Postfix: hostname verification failed	11
RHEL7	11.2.1	CVE-2016-4484 affects cryptsetup	11
RHEL7	11.2.1	CVE-2017-12588 affects rsyslog	11
RHEL7	11.2.1	CVE-2017-15994 affects rsync	11

Agent name	Requirement	Description	Count
RHEL7	11.2.1	CVE-2017-18018 affects coreutils	11
RHEL7	11.2.1	CVE-2020-1752 affects multiarch-support	11
RHEL7	11.2.3	CVE-2016-4484 affects cryptsetup	11
RHEL7	11.2.3	CVE-2017-12588 affects rsyslog	11
RHEL7	11.2.3	CVE-2017-15994 affects rsync	11
RHEL7	11.2.3	CVE-2017-18018 affects coreutils	11
RHEL7	11.2.3	CVE-2020-1752 affects multiarch-support	11
RHEL7	11.4	sendmail: Multiple pre-greetings rejects.	10
RHEL7	11.2.1	CVE-2016-7948 affects libxrandr2	10
RHEL7	11.2.1	CVE-2017-18342 affects python3-yaml	10
RHEL7	11.2.1	CVE-2017-7244 affects libpcre3	10
RHEL7	11.2.1	CVE-2019-18684 affects sudo	10
RHEL7	11.2.3	CVE-2016-7948 affects libxrandr2	10
RHEL7	11.2.3	CVE-2017-18342 affects python3-yaml	10
RHEL7	11.2.3	CVE-2017-7244 affects libpcre3	10
RHEL7	11.2.3	CVE-2019-18684 affects sudo	10
RHEL7	10.2.5	Netscreen firewall: Successfull admin login	10
RHEL7	11.4	Courier brute force (multiple failed logins).	9
RHEL7	11.4	PAM: Multiple failed logins in a small period of time.	9
RHEL7	10.2.4	Courier brute force (multiple failed logins).	9
RHEL7	10.2.4	PAM: Multiple failed logins in a small period of time.	9
RHEL7	11.2.1	CVE-2013-4235 affects passwd	9
RHEL7	11.2.1	CVE-2016-7947 affects libxrandr2	9
RHEL7	11.2.1	CVE-2017-15088 affects krb5-locales	9
RHEL7	11.2.1	CVE-2020-1927 affects apache2	9
RHEL7	11.2.3	CVE-2013-4235 affects passwd	9
RHEL7	11.2.3	CVE-2016-7947 affects libxrandr2	9
RHEL7	11.2.3	CVE-2017-15088 affects krb5-locales	9
RHEL7	11.2.3	CVE-2020-1927 affects apache2	9
RHEL7	10.2.5	Courier brute force (multiple failed logins).	9
RHEL7	10.2.5	PAM: Multiple failed logins in a small period of time.	9
RHEL7	11.4	Postfix: RBL lookup error: Host or domain name not found	8
RHEL7	11.4	sendmail: Multiple relaying attempts of spam.	8
RHEL7	10.2.4	User missed the password to change UID to root.	8
RHEL7	11.2.1	CVE-2019-1003010 affects git	8
RHEL7	11.2.3	CVE-2019-1003010 affects git	8
RHEL7	10.2.5	SonicWall: Firewall administrator login.	8
RHEL7	10.2.5	User missed the password to change UID to root.	8
RHEL7	11.4	sendmail: Multiple attempts to send e-mail from invalid/unknown sender domain.	7
RHEL7	10.2.4	Failed attempt to run sudo.	7
RHEL7	10.2.5	Failed attempt to run sudo.	7

Agent name	Requirement	Description	Count
RHEL7	11.4	Courier: Multiple connection attempts from same source.	6
RHEL7	11.4	Imapd Multiple failed logins from same source ip.	6
RHEL7	11.4	Postfix: IP Address black-listed by anti-spam (blocked).	6
RHEL7	11.4	Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).	6
RHEL7	11.4	sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).	6
RHEL7	10.2.4	Imapd Multiple failed logins from same source ip.	6
RHEL7	10.2.5	Imapd Multiple failed logins from same source ip.	6
RHEL7	10.2.5	Successful sudo to ROOT executed.	6
RHEL7	10.2.4	syslog: Illegal root login.	5
RHEL7	10.2.5	Cisco IOS: Successful login to the router.	5
RHEL7	10.2.5	PIX: AAA (VPN) authentication successful.	5
RHEL7	10.2.5	User successfully changed UID.	5
RHEL7	10.2.5	syslog: Illegal root login.	5
RHEL7	10.2.4	PIX: AAA (VPN) user locked out.	4
RHEL7	10.2.4	PIX: Multiple AAA (VPN) authentication failures.	4
RHEL7	10.2.4	Postfix: Multiple SASL authentication failures.	4
RHEL7	10.2.4	Three failed attempts to run sudo	4
RHEL7	10.2.4	syslog: User missed the password more than one time	3
RHEL7	10.2.4	syslog: Connection blocked by Tcp Wrappers.	2