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

PCI DSS report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	wazuh_agent_ubuntu_2	172.20.0.7	Wazuh v4.9.0	wazuh-manager-4.9.0-7102	Ubuntu 22.04.3 LTS	May 14, 2024 @ 14:50:11.000	May 16, 2024 @ 15:36:49.000

Group: default

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

2024-04-16T17:36:53 to 2024-05-16T17:36:53

rule.pci_dss: * AND cluster.name: wazuh AND agent.id: 002

Most common PCI DSS requirements alerts found

Requirement 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 (CIS, ISO, SANS, NIST).

Top rules for 2.2 requirement

Rule ID	Description
81529	OpenSCAP: Record Events that Modify User/Group Information (not passed)
81530	OpenSCAP: Ensure auditd Collects Information on Kernel Module Loading and Unloading (not passed)
81540	OpenSCAP Report overview.

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
60122	Logon Failure - Unknown user or bad password

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
60122	Logon Failure - Unknown user or bad password
5716	sshd: authentication failed.

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.
5703	sshd: Possible breakin attempt (high number of reverse lookup errors).

Requirement 11.5

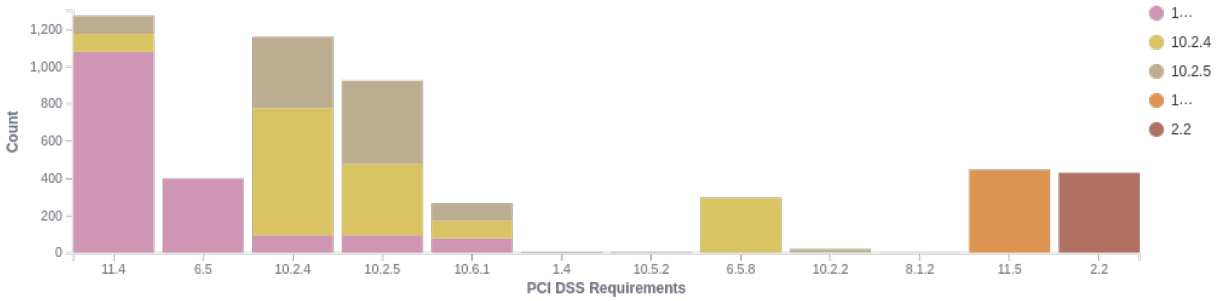
Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Top rules for 11.5 requirement

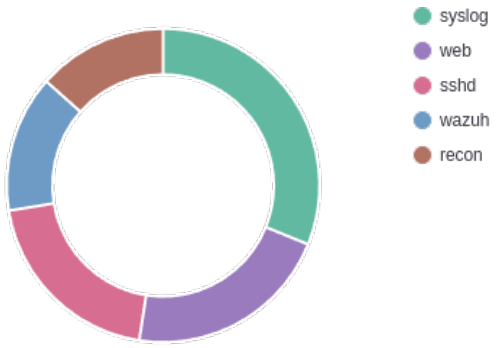
Rule ID	Description
550	Integrity checksum changed.
553	File deleted.

Rule ID	Description
554	File added to the system.

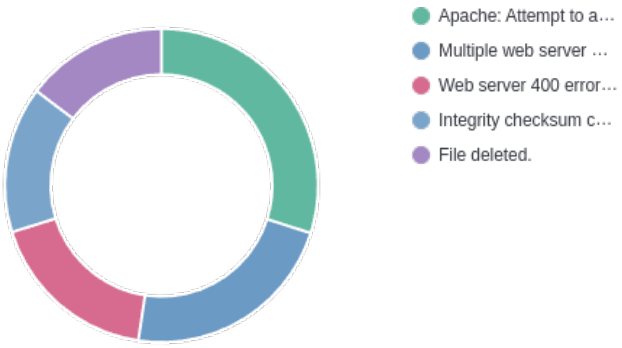
PCI DSS requirements



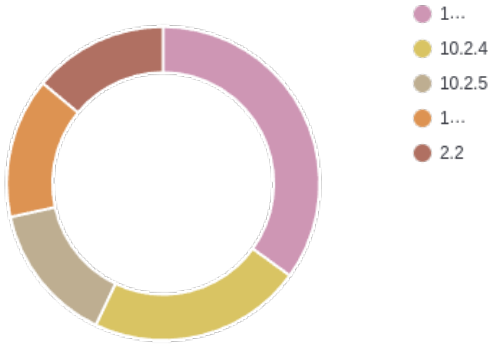
Top 5 rule groups



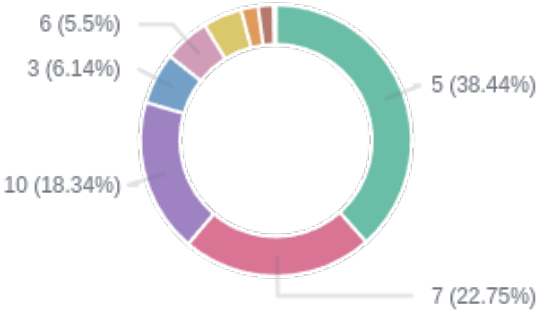
Top 5 rules



Top 5 PCI DSS requirements



Rule level distribution



Last alerts

Requirement	Description	Count
10.2.4	Apache: Attempt to access forbidden directory index.	297
11.4	Multiple web server 400 error codes from same source ip.	223
11.4	Web server 400 error code.	177
11.5	Integrity checksum changed.	153
11.5	File deleted.	149
11.5	File added to the system.	141
11.4	sshd: Possible breakin attempt (high number of reverse lookup errors).	121
11.4	sshd: insecure connection attempt (scan).	108
11.4	sshd: Reverse lookup error (bad ISP or attack).	104
11.4	sshd: Possible attack on the ssh server (or version gathering).	98
10.2.4	sshd: Attempt to login using a non-existent user	93
10.2.5	sshd: Attempt to login using a non-existent user	93
10.2.4	Logon Failure - Unknown user or bad password	48
10.2.5	Logon Failure - Unknown user or bad password	48
10.2.4	sshd: authentication failed.	45
10.2.5	sshd: authentication failed.	45
10.2.4	unix_chkpwd: Password check failed.	43
10.2.5	unix_chkpwd: Password check failed.	43
11.4	sshd: Multiple authentication failures.	42
10.2.4	PAM: User login failed.	42
10.2.4	sshd: Multiple authentication failures.	42
10.2.5	PAM: User login failed.	42
10.2.5	sshd: Multiple authentication failures.	42
11.4	sshd: brute force trying to get access to the system.	38
10.2.4	sshd: brute force trying to get access to the system.	38
10.2.5	sshd: brute force trying to get access to the system.	38
2.2	OpenSCAP: Record Events that Modify User/Group Information (not passed)	27
2.2	OpenSCAP: Ensure auditd Collects Information on Kernel Module Loading and Unloading (not passed)	26
2.2	OpenSCAP Report overview.	22
2.2	OpenSCAP: Ensure auditd Collects File Deletion Events by User (not passed)	22
2.2	OpenSCAP: RHSA-2017:0372: kernel-aarch64 security and bug fix update (Important) (not passed)	20
2.2	OpenSCAP: Set Password Strength Minimum Lowercase Characters (not passed)	18
2.2	OpenSCAP: Ensure auditd Collects Information on the Use of Privileged Commands (not passed)	17
2.2	OpenSCAP: Set Lockout Time For Failed Password Attempts (not passed)	16
2.2	OpenSCAP: Record Attempts to Alter Time Through clock_settime (not passed)	15
2.2	OpenSCAP: Enable Smart Card Login (not passed)	14
2.2	OpenSCAP: Ensure auditd Collects System Administrator Actions (not passed)	14
2.2	OpenSCAP: Verify and Correct File Permissions with RPM (not passed)	14
11.2.1	CVE-2013-4235 affects login	14

Requirement	Description	Count
11.2.1	CVE-2020-1747 affects python3-yaml	14
11.2.1	CVE-2020-1927 affects apache2	14
2.2	OpenSCAP: Install AIDE (not passed)	13
2.2	OpenSCAP: Record Attempts to Alter the localtime File (not passed)	13
2.2	OpenSCAP: Record attempts to alter time through settimeofday (not passed)	13
2.2	OpenSCAP: Set Password Minimum Length (not passed)	13
11.2.1	CVE-2019-1552 affects openssl	13
2.2	OpenSCAP Report overview: Score less than 80	12
2.2	OpenSCAP: Ensure auditd Collects Information on Exporting to Media (successful) (not passed)	12
2.2	OpenSCAP: Record Attempts to Alter Logon and Logout Events (not passed)	12
2.2	OpenSCAP: Record Events that Modify the System's Discretionary Access Controls - removexattr (not passed)	12
11.2.1	CVE-2015-2987 affects ed	12
11.2.1	CVE-2018-1000035 affects unzip	11
11.2.1	CVE-2018-15919 affects openssh-client	11
11.2.1	CVE-2019-1003010 affects git	11
11.4	Postfix: Multiple relaying attempts of spam.	10
10.2.5	Netscreen firewall: Successfull admin login	10
11.2.1	CVE-2013-4235 affects passwd	10
11.2.1	CVE-2016-4484 affects cryptsetup	10
11.2.1	CVE-2017-18018 affects coreutils	10
11.2.1	CVE-2018-20217 affects libkrb5-3	10
11.2.1	CVE-2019-19645 affects sqlite3	10
11.2.1	CVE-2020-1927 affects apache2-data	10
11.2.1	CVE-2019-18684 affects sudo	9
11.4	Postfix: too many errors after RCPT from unknown	8
10.2.5	Imapd user login.	8
11.4	Courier brute force (multiple failed logins).	7
11.4	Interface entered in promiscuous(sniffing) mode.	7
11.4	sendmail: Multiple pre-greetings rejects.	7
10.2.4	Courier brute force (multiple failed logins).	7
10.2.5	Cisco IOS: Successful login to the router.	7
10.2.5	Courier brute force (multiple failed logins).	7
10.2.5	User successfully changed UID.	7
11.4	Netscreen firewall: Multiple critical messages from same source IP.	6
11.4	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	6
11.4	Postfix: Rejected by access list (Requested action not taken).	6
11.4	sendmail: Multiple attempts to send e-mail from a previously rejected sender (access).	6
11.4	sendmail: Multiple rejected e-mails from same source ip.	6
10.2.5	SonicWall: Firewall administrator login.	6
10.2.5	User successfully changed UID to root.	6
11.4	Courier: Multiple connection attempts from same source.	5

Requirement	Description	Count
11.4	Log file size reduced.	5
10.2.5	PIX: AAA (VPN) authentication successful.	5
10.2.4	User missed the password to change UID to root.	4
10.2.4	syslog: User missed the password more than one time	4
10.2.5	User missed the password to change UID to root.	4
10.2.5	syslog: User missed the password more than one time	4
11.5	Registry Integrity Checksum Changed	4
10.2.4	PAM: Multiple failed logins in a small period of time.	3
10.2.4	PIX: Multiple AAA (VPN) authentication failures.	3
10.2.4	syslog: Connection blocked by Tcp Wrappers.	3
10.2.4	syslog: Illegal root login.	3
10.2.5	Courier (imap/pop3) authentication success.	3
10.2.5	PAM: Login session opened.	3
10.2.5	PAM: Multiple failed logins in a small period of time.	3
10.2.4	Failed attempt to run sudo.	2
10.2.4	Imapd Multiple failed logins from same source ip.	2
10.2.4	PIX: AAA (VPN) user locked out.	1
10.2.4	Postfix: Multiple SASL authentication failures.	1
10.2.4	Three failed attempts to run sudo	1