PCI DSS report

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

2025-04-06T14:00:05 to 2025-04-11T14:00:05

manager.name: wazuh-server AND rule.pci_dss: *

Most common PCI DSS requirements alerts found

Requirement 6.5

Address common coding vulnerabilities in software development processes as follows:

- Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.
- Develop applications based on secure coding guidelines.

Top rules for 6.5 requirement

Rule ID	Description
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
31509	CMS (WordPress or Joomla) login attempt.

Requirement 10.2.4

Invalid logical access attempts

Top rules for 10.2.4 requirement

Rule ID	Description
12108	Query cache denied (probably config error).
31509	CMS (WordPress or Joomla) login attempt.
3332	Postfix SASL authentication failure.

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
31509	CMS (WordPress or Joomla) login attempt.
3332	Postfix SASL authentication failure.
3904	Courier (imap/pop3) authentication success.

Requirement 10.6.1

Review the following at least daily:

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), authentication servers, ecommerce redirection servers, etc.)

Top rules for 10.6.1 requirement

Rule ID	Description
12108	Query cache denied (probably config error).
3901	New courier (imap/pop3) connection.
3398	Postfix: Illegal address from unknown sender

Requirement 11.4

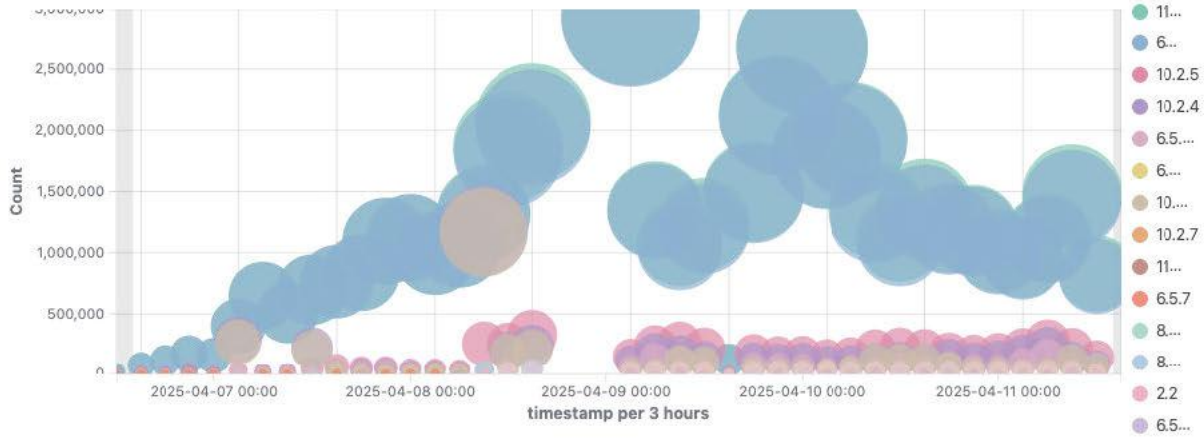
Use intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.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

Top rules for 11.4 requirement

Rule ID	Description

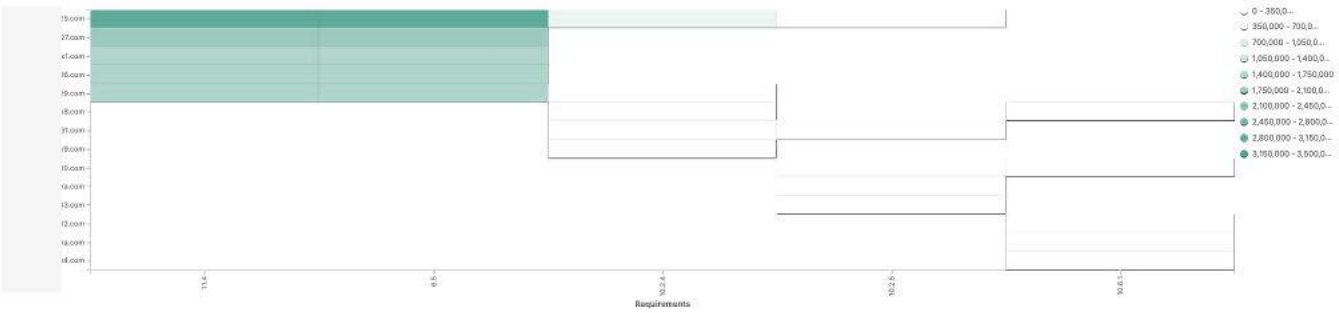
Rule ID	Description
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
31509	CMS (WordPress or Joomla) login attempt.

Top 10 PCI DSS requirements



Top 10 agents by alerts count

Last alerts



Requirements by agent

Alerts summary

Agent name	Requirement	Description	Count
ns1 .com	6.5	Web server 400 error code.	2574736
ns1 .com	11.4	Web server 400 error code.	2574736
.com	11.4	Web server 400 error code.	1637344
ns1 .com	6.5	CMS (WordPress or Joomla) login attempt.	228852
ns1 .com	11.4	CMS (WordPress or Joomla) login attempt.	228852
ns1 .com	10.2.4	CMS (WordPress or Joomla) login attempt.	228852
ns1 .com	10.2.5	CMS (WordPress or Joomla) login attempt.	228852
ns1 .com	6.5.10	CMS (WordPress or Joomla) login attempt.	228852
ns1 .com	6.5	Multiple web server 400 error codes from same source ip.	148487
ns1 .com	11.4	Multiple web server 400 error codes from same source ip.	148487
ns1 .com	10.2.4	Query cache denied (probably config error).	105470
ns1 .com	10.6.1	Query cache denied (probably config error).	105470
.com	11.4	Multiple web server 400 error codes from same source ip.	84815
ns1 .com	6.5	High amount of POST requests in a small period of time (likely bot).	50164
ns1 .com	11.4	High amount of POST requests in a small period of time (likely bot).	50164
.com	11.4	High amount of POST requests in a small period of time (likely bot).	38408
.com	11.4	CMS (WordPress or Joomla) login attempt.	28518
ns1 .com	6.5	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	11.4	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	10.2.4	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	10.2.5	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	6.5.10	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	6.5	Common web attack.	19171
ns1 .com	11.4	Common web attack.	19171
ns1 .com	6.5.1	Common web attack.	19171
.com	11.4	Common web attack.	17039
ns1 .com	6.5	Suspicious URL access.	5488
ns1 .com	11.4	Suspicious URL access.	5488
.com	11.4	Suspicious URL access.	5164
.com	11.4	Multiple web server 503 error code (Service unavailable).	2763
ns1 .com	6.5	Multiple web server 503 error code (Service unavailable).	2182
ns1 .com	11.4	Multiple web server 503 error code (Service unavailable).	2182
ns1 .com	10.6.1	Multiple web server 503 error code (Service unavailable).	2182
ns1 .com	6.5	Multiple web server 500 error code (Internal Error).	1567
ns1 .com	10.6.1	Multiple web server 500 error code (Internal Error).	1567
ns1 .com	10.2.5	Dovecot Authentication Success.	947
ns1 .com	10.2.4	Postfix SASL authentication failure.	938
ns1 .com	10.2.5	Postfix SASL authentication failure.	938
ns1 .com	10.6.1	Listened ports status (netstat) changed (new port opened or closed).	881

Agent name	Requirement	Description	Count
ns1 .com	10.2.7	Listened ports status (netstat) changed (new port opened or closed).	881
ns1 .com	11.5	Integrity checksum changed.	677
ns1 .com	6.5	A web attack returned code 200 (success).	382
ns1 .com	11.4	A web attack returned code 200 (success).	382
ns1 .com	6.5	SQL injection attempt.	369
ns1 .com	11.4	SQL injection attempt.	369
ns1 .com	6.5.1	SQL injection attempt.	369
ns1 .com	10.2.5	Dovecot Session Disconnected.	292
ns1 .com	8.1.5	Dovecot Session Disconnected.	292
ns1 .com	11.4	Postfix: Illegal address from unknown sender	267
ns1 .com	10.6.1	Postfix: Illegal address from unknown sender	267
.com	11.4	SQL injection attempt.	239
.com	11.4	A web attack returned code 200 (success).	197
.com	11.4	Simple shell.php command execution.	196
.com	11.4	Postfix: Illegal address from unknown sender	190
ns1 .com	11.4	Postfix: hostname verification failed	151
ns1 .com	10.6.1	Postfix: hostname verification failed	151
.com	11.4	CMS (WordPress or Joomla) brute force attempt.	130
ns1 .com	10.2.4	Dovecot Invalid User Login Attempt.	101
ns1 .com	10.2.5	Dovecot Invalid User Login Attempt.	101
ns1 .com	10.6.1	Agent event queue is full. Events may be lost.	93
.com	11.4	Postfix: Attempt to use mail server as relay (client host rejected).	72
.com	11.4	Multiple common web attacks from same source ip.	35
ns1 .com	10.2.5	PAM: Login session opened.	34
ns1 .com	10.6.1	Host-based anomaly detection event (rootcheck).	30
.com	11.4	Postfix: hostname verification failed	29
ns1 .com	6.5	Multiple common web attacks from same source ip.	19
ns1 .com	11.4	Multiple common web attacks from same source ip.	19
ns1 .com	11.4	Postfix: Attempt to use mail server as relay (client host rejected).	16
ns1 .com	10.6.1	Postfix: Attempt to use mail server as relay (client host rejected).	16
ns1 .com	10.2.5	PAM: Login session closed.	14
ns1 .com	10.6.1	Agent event queue is flooded. Check the agent configuration.	14
ns1 .com	6.5	XSS (Cross Site Scripting) attempt.	12
ns1 .com	11.4	XSS (Cross Site Scripting) attempt.	12
.com	11.4	PHP CGI-bin vulnerability attempt.	11
.com	11.4	XSS (Cross Site Scripting) attempt.	11
ns1 .com	6.5	PHPMyAdmin scans (looking for setup.php).	10
ns1 .com	11.4	PHPMyAdmin scans (looking for setup.php).	10
ns1 .com	11.5	File added to the system.	10
ns1 .com	11.5	File deleted.	10
ns1 com	6.5	Multiple SQL injection attempts from same source ip.	9

Agent name	Requirement	Description	Count
ns1 .com	11.4	Multiple SQL injection attempts from same source ip.	9
ns1 .com	6.5.1	Multiple SQL injection attempts from same source ip.	9
ns1 .com	11.4	Postfix: Rejected by access list (Requested action not taken).	7
ns1 .com	10.6.1	Postfix: Rejected by access list (Requested action not taken).	7
.com	11.4	Postfix: Rejected by access list (Requested action not taken).	7
ns1 .com	6.5	Blacklisted user agent (known malicious user agent).	6
ns1 .com	6.5	URL too long. Higher than allowed on most browsers. Possible attack.	6
ns1 .com	11.4	Blacklisted user agent (known malicious user agent).	6
ns1 .com	11.4	URL too long. Higher than allowed on most browsers. Possible attack.	6
ns1 .com	10.2.4	URL too long. Higher than allowed on most browsers. Possible attack.	6
ns1 .com	10.2.4	Postfix: Multiple SASL authentication failures.	3
ns1 .com	10.2.5	Postfix: Multiple SASL authentication failures.	3
ns1 .com	10.6.1	Agent event queue is 90% full.	3
ns1 .com	10.6.1	Wazuh agent started.	3
ns1 .com	10.6.1	Wazuh agent stopped.	3
ns1 .com	6.5	PHP CGI-bin vulnerability attempt.	2
ns1 .com	10.2.5	sshd: authentication success.	1
ns1 .com	10.6.1	New wazuh agent connected.	1
ns1 .com	10.6.1	Postfix: too many errors after RCPT from unknown	1