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

PCI DSS report

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

2024-10-17T03:38:07 to 2024-10-18T03:38:07

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

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
19009	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure updates, patches, and additional security software are installed.
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.

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
60106	Windows Logon Success
5501	PAM: Login session opened.
5502	PAM: Login session closed.

Requirement 10.2.7

Creation and deletion of system level objects

Top rules for 10.2.7 requirement

Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
533	Listened ports status (netstat) changed (new port opened or closed).

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

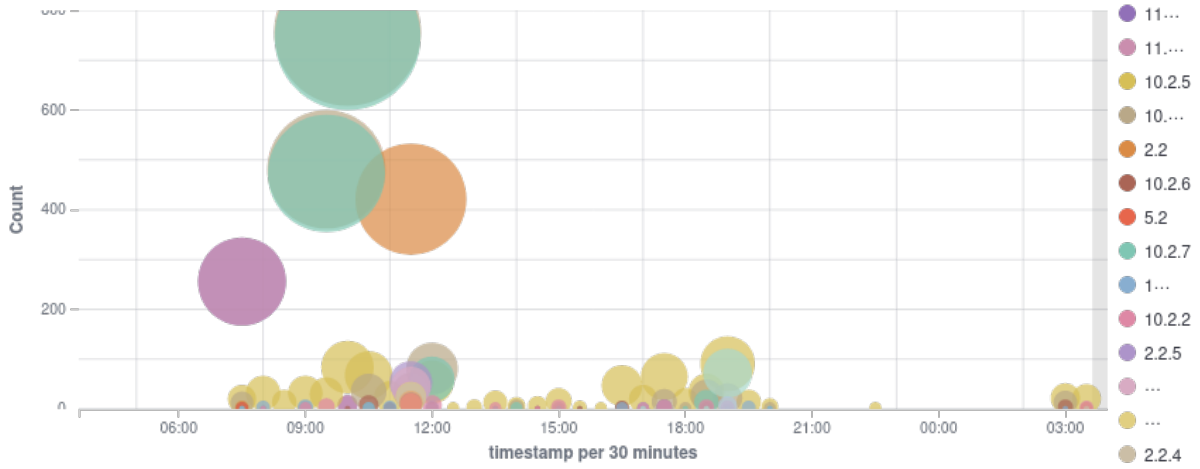
Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
510	Host-based anomaly detection event (rootcheck).

Requirement 11.2.1

Top rules for 11.2.1 requirement

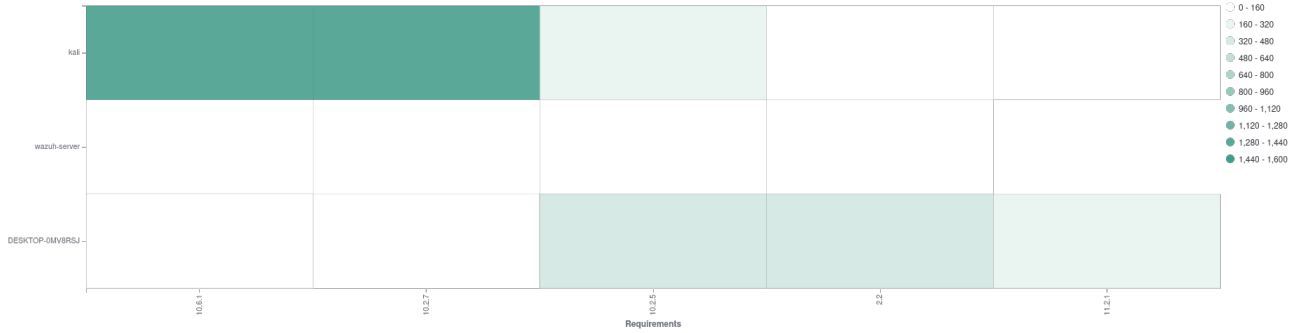
Rule ID	Description
23505	CVE-2024-20652 affects Microsoft Windows 10 Home
23505	CVE-2024-20653 affects Microsoft Windows 10 Home
23505	CVE-2024-20654 affects Microsoft Windows 10 Home

Top 10 PCI DSS requirements

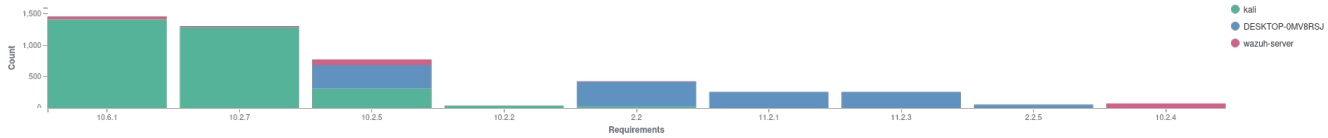


Top 10 agents by alerts count

Last alerts



Requirements by agent



Alerts summary

Agent name	Requirement	Description	Count
kali	10.6.1	Dpkg (Debian Package) half configured.	1014
kali	10.2.7	Dpkg (Debian Package) half configured.	1014
DESKTOP-0MV8RSJ	10.2.5	Windows Logon Success	359
kali	10.6.1	New dpkg (Debian Package) installed.	278
kali	10.2.7	New dpkg (Debian Package) installed.	278
kali	10.2.5	PAM: Login session opened.	141
kali	10.2.5	PAM: Login session closed.	128
kali	10.6.1	Host-based anomaly detection event (rootcheck).	80
kali	10.2.5	Successful sudo to ROOT executed.	38
kali	10.2.2	Successful sudo to ROOT executed.	38
kali	10.6.1	New dpkg (Debian Package) requested to install.	21
DESKTOP-0MV8RSJ	10.2.5	Windows Workstation Logon Success	18
kali	10.6.1	Wazuh agent started.	11
kali	10.2.6	Wazuh agent started.	11
kali	10.6.1	Wazuh agent stopped.	5
kali	10.2.6	Wazuh agent stopped.	5
kali	10.6.1	sshd: cannot bind to configured address.	3
kali	10.2.5	PAM: User login failed.	2
kali	2.2	SCA summary: System audit for Unix based systems: Score less than 30% (18)	2
kali	10.2.4	PAM: User login failed.	2
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	2
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	2
kali	10.6.1	Listened ports status (netstat) changed (new port opened or closed).	1
kali	10.6.1	Syslogd exiting (logging stopped).	1
kali	10.6.1	Wazuh agent disconnected.	1
kali	10.2.7	Listened ports status (netstat) changed (new port opened or closed).	1
kali	2.2	System audit for Unix based systems: Ensure CUPS is not enabled	1
kali	2.2	System audit for Unix based systems: Ensure SELinux or AppArmor are installed	1
kali	2.2	System audit for Unix based systems: Ensure auditd service is enabled	1
kali	2.2	System audit for Unix based systems: Ensure lockout for failed password attempts is configured	1
kali	2.2	System audit for Unix based systems: Ensure password expiration is 365 days or less	1
kali	2.2	System audit for Unix based systems: Ensure password hashing algorithm is SHA-512	1
kali	2.2	System audit for Unix based systems: Ensure passwords are longer than 14 characters	1
kali	2.2	System audit for Unix based systems: Ensure passwords contain at least one digit	1
kali	2.2	System audit for Unix based systems: Ensure passwords contain at least one lowercase character	1
kali	2.2	System audit for Unix based systems: Ensure passwords contain at least one special character	1
kali	2.2	System audit for Unix based systems: Ensure passwords contain at least one uppercase	1

Agent name	Requirement	Description	Count
		character	
kali	2.2	System audit for Unix based systems: Ensure passwords in /etc/shadow are hashed with SHA-512 or SHA-256	1
kali	2.2	System audit for Unix based systems: Ensure retry option for passwords is less than 3	1
kali	2.2	System audit for Unix based systems: SSH Hardening: Empty passwords should not be allowed	1
kali	2.2	System audit for Unix based systems: SSH Hardening: Ensure SSH HostbasedAuthentication is disabled	1
kali	2.2	System audit for Unix based systems: SSH Hardening: Grace Time should be one minute or less.	1
kali	2.2	System audit for Unix based systems: SSH Hardening: No Public Key authentication	1
kali	2.2	System audit for Unix based systems: SSH Hardening: Password Authentication should be disabled	1
kali	2.2	System audit for Unix based systems: SSH Hardening: Port should not be 22	1
kali	10.2.6	Wazuh agent disconnected.	1
kali	11.2.1	The CVE-2023-26112 that affected configobj was solved due to an update in the agent or feed.	1
kali	11.2.1	The CVE-2024-35195 that affected requests was solved due to an update in the agent or feed.	1
kali	11.2.1	The CVE-2024-3651 that affected idna was solved due to an update in the agent or feed.	1
kali	11.2.1	The CVE-2024-39689 that affected certifi was solved due to an update in the agent or feed.	1
kali	11.2.1	The CVE-2024-41671 that affected Twisted was solved due to an update in the agent or feed.	1
kali	11.2.1	The CVE-2024-41810 that affected Twisted was solved due to an update in the agent or feed.	1
kali	11.2.1	The CVE-2024-45230 that affected Django was solved due to an update in the agent or feed.	1
kali	11.2.1	The CVE-2024-45231 that affected Django was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2023-26112 that affected configobj was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2024-35195 that affected requests was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2024-3651 that affected idna was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2024-39689 that affected certifi was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2024-41671 that affected Twisted was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2024-41810 that affected Twisted was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2024-45230 that affected Django was solved due to an update in the agent or feed.	1
kali	11.2.3	The CVE-2024-45231 that affected Django was solved due to an update in the agent or feed.	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: Empty passwords should not be allowed	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: Grace Time should be one minute or less.	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: No Public Key authentication	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: Password Authentication should be disabled	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: Port should not be 22	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: Protocol should be set to 2	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: Rhost or shost should not be used for authentication	1
kali	2.2.4	System audit for Unix based systems: SSH Hardening: Wrong Maximum number of authentication attempts	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename administrator account'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename guest account'.	1

Agent name	Requirement	Description	Count
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message text for users attempting to log on'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message title for users attempting to log on'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)').	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Administrator account status' is set to 'Disabled'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Guest account status' is set to 'Disabled'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana above lock screen' is set to 'Disabled'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana' is set to 'Disabled'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'.	1
DESKTOP-0MV8RSJ	2.2	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'.	1
DESKTOP-0MV8RSJ	10.2.5	Windows User Logoff	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20652 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20653 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20654 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20657 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20658 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20660 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20661 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20663 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20664 affects Microsoft Windows 10 Home	1
DESKTOP-0MV8RSJ	11.2.1	CVE-2024-20666 affects Microsoft Windows 10 Home	1