Peersoc

PCI DSS report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	second_server	167.235.23.58	Wazuh v4.7.5	ubuntu-4gb-nbg1-2	Ubuntu 24.04.1 LTS	Nov 8, 2024 @ 11:02:54.000	Nov 8, 2024 @ 14:34:24.000

Group: default

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

🕘 2024-11-07T17:34:31 to 2024-11-08T17:34:31

🔍 manager.name: ubuntu-4gb-nbg1-2 AND rule.pci_dss: * AND agent.id: 001

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
5710	sshd: Attempt to login using a non-existent user
5503	PAM: User login failed.
5760	sshd: authentication failed.

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
5503	PAM: User login failed.
5760	sshd: authentication failed.

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.

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
5710	sshd: Attempt to login using a non-existent user
510	Host-based anomaly detection event (rootcheck).
5108	System running out of memory. Availability of the system is in risk.

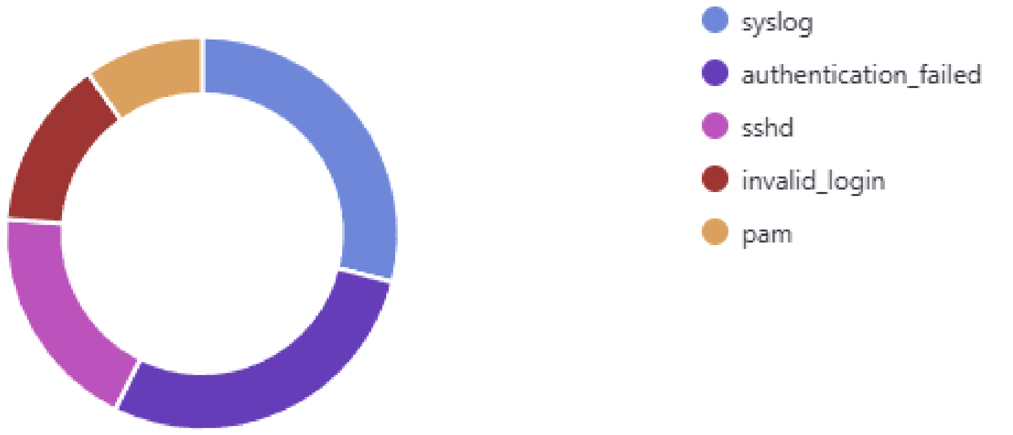
Requirement 11.4

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.

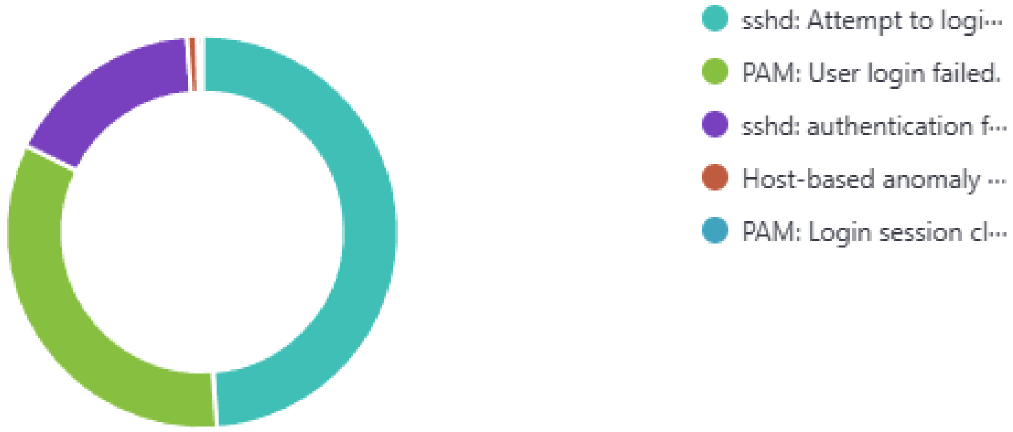
Top rules for 11.4 requirement

Rule ID	Description
5712	sshd: brute force trying to get access to the system. Non existent user.
5551	PAM: Multiple failed logins in a small period of time.
5763	sshd: brute force trying to get access to the system. Authentication failed.

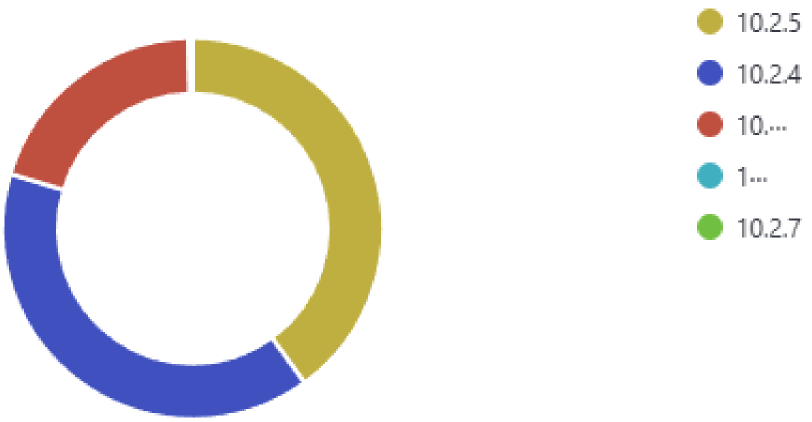
Top 5 rule groups



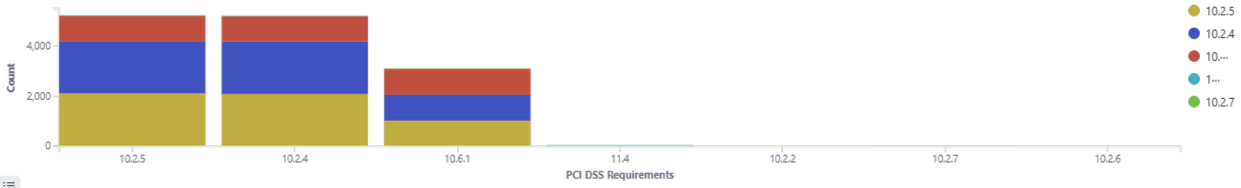
Top 5 rules



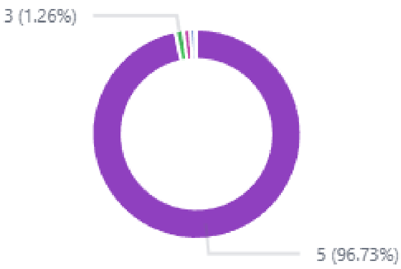
Top 5 requirements



Requirements



Rule level distribution



Last alerts

Requirement	Description	Count
10.2.5	sshd: Attempt to login using a non-existent user	1023
10.2.4	sshd: Attempt to login using a non-existent user	1023
10.6.1	sshd: Attempt to login using a non-existent user	1023
10.2.5	PAM: User login failed.	701
10.2.4	PAM: User login failed.	701
10.2.5	sshd: authentication failed.	346
10.2.4	sshd: authentication failed.	346
10.6.1	Host-based anomaly detection event (rootcheck).	18
10.2.5	PAM: Login session closed.	8
10.2.5	PAM: Login session opened.	8
10.2.5	sshd: brute force trying to get access to the system. Non existent user.	8
10.2.4	sshd: brute force trying to get access to the system. Non existent user.	8
11.4	sshd: brute force trying to get access to the system. Non existent user.	8
10.2.5	PAM: Multiple failed logins in a small period of time.	4
10.2.4	PAM: Multiple failed logins in a small period of time.	4
10.6.1	System running out of memory. Availability of the system is in risk.	4
11.4	PAM: Multiple failed logins in a small period of time.	4
10.2.5	Successful sudo to ROOT executed.	3
10.2.5	syslog: User authentication failure.	3
10.2.5	syslog: User missed the password more than one time	3
10.2.4	syslog: User authentication failure.	3
10.2.4	syslog: User missed the password more than one time	3
10.6.1	Dpkg (Debian Package) half configured.	3
10.2.7	Dpkg (Debian Package) half configured.	3
10.2.2	Successful sudo to ROOT executed.	3
10.2.5	sshd: authentication success.	2
10.6.1	New dpkg (Debian Package) installed.	2
10.6.1	Wazuh agent started.	2
10.6.1	Wazuh agent stopped.	2
10.2.7	New dpkg (Debian Package) installed.	2
10.2.6	Wazuh agent started.	2
10.2.6	Wazuh agent stopped.	2
10.2.5	sshd: brute force trying to get access to the system. Authentication failed.	1
10.2.4	sshd: brute force trying to get access to the system. Authentication failed.	1
10.6.1	New dpkg (Debian Package) requested to install.	1
10.6.1	New wazuh agent connected.	1
11.4	sshd: brute force trying to get access to the system. Authentication failed.	1