Peersoc

GDPR 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 @ 14:52:24.000

Group: default

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

🕓 2024-11-07T17:52:28 to 2024-11-08T17:52:28

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

Most common GDPR requirements alerts found

Requirement IV_35.7.d

Capabilities for identification, blocking and forensic investigation of data breaches by malicious actors, through compromised credentials, unauthorized network access, persistent threats and verification of the correct operation of all components. Network perimeter and endpoint security tools to prevent unauthorized access to the network, prevent the entry of unwanted data types and malicious threats. Anti-malware and anti-ransomware to prevent malware and ransomware threats from entering your devices. A behavioral analysis that uses machine intelligence to identify people who do anomalous things on the network, in order to give early visibility and alert employees who start to become corrupt.

Top rules for IV_35.7.d requirement

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

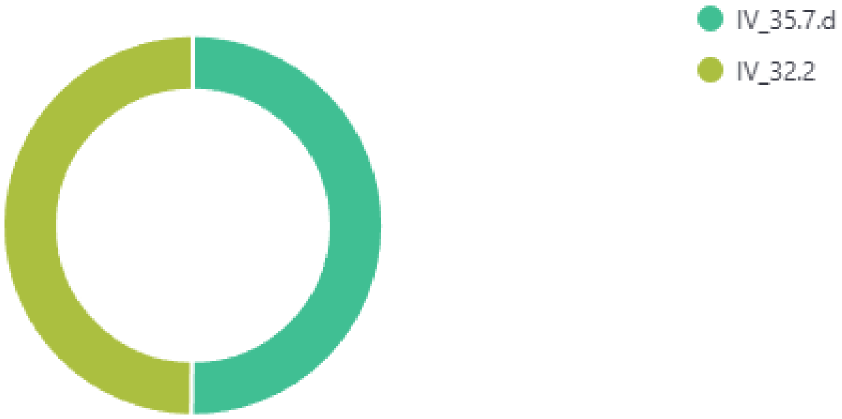
Requirement IV_32.2

Account management tools that closely monitor actions taken by standard administrators and users who use standard or privileged account credentials are required to control access to data.

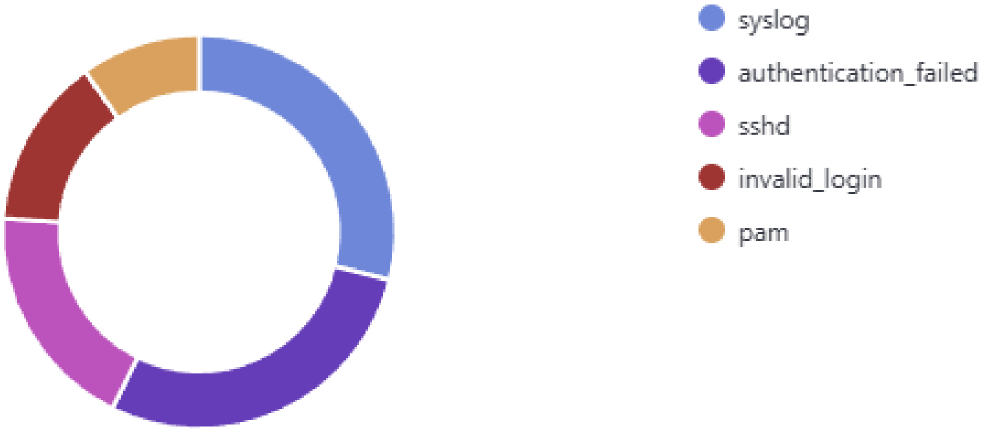
Top rules for IV_32.2 requirement

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

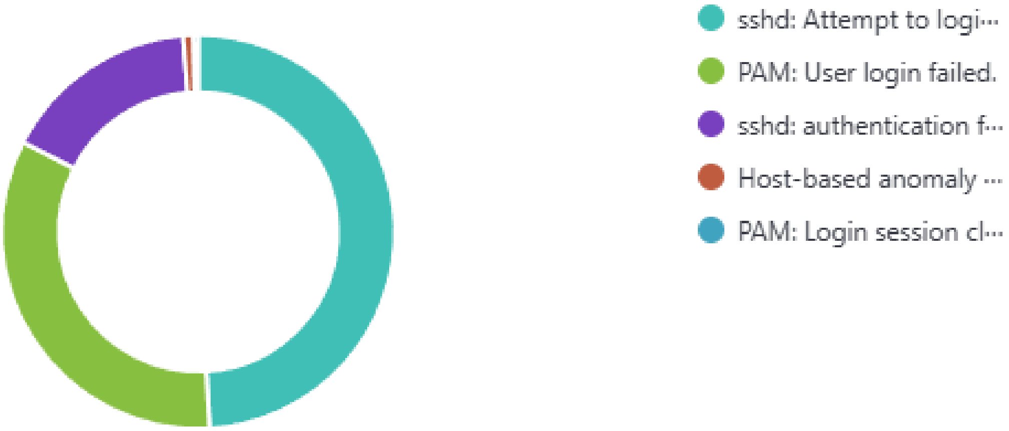
Top 5 requirements



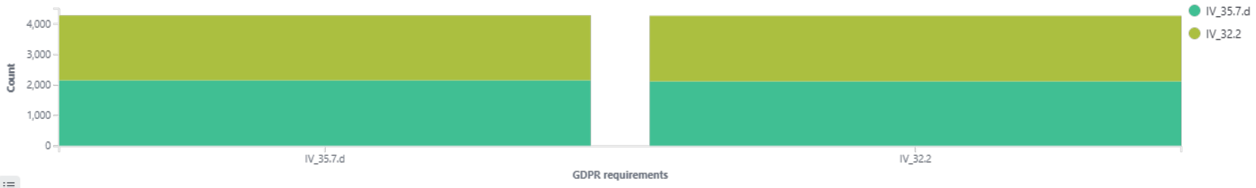
Top 5 rule groups



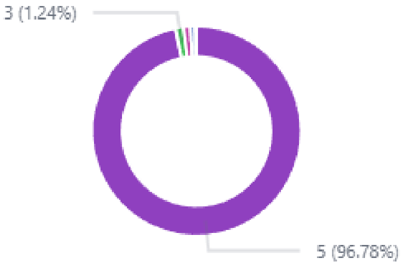
Top 5 rules



Requirements



Rule level distribution



Last alerts

Requirement	Description	Count
IV_35.7.d	sshd: Attempt to login using a non-existent user	1045
IV_32.2	sshd: Attempt to login using a non-existent user	1045
IV_35.7.d	PAM: User login failed.	712
IV_32.2	PAM: User login failed.	712
IV_35.7.d	sshd: authentication failed.	346
IV_32.2	sshd: authentication failed.	346
IV_35.7.d	Host-based anomaly detection event (rootcheck).	18
IV_35.7.d	sshd: brute force trying to get access to the system. Non existent user.	8
IV_32.2	PAM: Login session closed.	8
IV_32.2	PAM: Login session opened.	8
IV_32.2	sshd: brute force trying to get access to the system. Non existent user.	8
IV_35.7.d	PAM: Multiple failed logins in a small period of time.	4
IV_35.7.d	System running out of memory. Availability of the system is in risk.	4
IV_32.2	PAM: Multiple failed logins in a small period of time.	4
IV_35.7.d	Dpkg (Debian Package) half configured.	3
IV_35.7.d	syslog: User authentication failure.	3
IV_35.7.d	syslog: User missed the password more than one time	3
IV_32.2	Successful sudo to ROOT executed.	3
IV_32.2	syslog: User authentication failure.	3
IV_32.2	syslog: User missed the password more than one time	3
IV_35.7.d	New dpkg (Debian Package) installed.	2
IV_35.7.d	Wazuh agent started.	2
IV_35.7.d	Wazuh agent stopped.	2
IV_32.2	sshd: authentication success.	2
IV_35.7.d	New dpkg (Debian Package) requested to install.	1
IV_35.7.d	New wazuh agent connected.	1
IV_35.7.d	sshd: brute force trying to get access to the system. Authentication failed.	1
IV_32.2	sshd: brute force trying to get access to the system. Authentication failed.	1