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

GDPR 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 @ 15:37:09.000

Group: default

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

2024-04-16T17:37:15 to 2024-05-16T17:37:15

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

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
510	Host-based anomaly detection event (rootcheck).
30306	Apache: Attempt to access forbidden directory index.
31151	Multiple web server 400 error codes from same source ip.

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

Requirement II_5.1.f

Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, verifying its modifications, accesses, locations and guarantee the safety of them. File sharing protection and file sharing technologies that meet the requirements of data protection.

Top rules for II_5.1.f requirement

Rule ID	Description
550	Integrity checksum changed.
553	File deleted.
554	File added to the system.

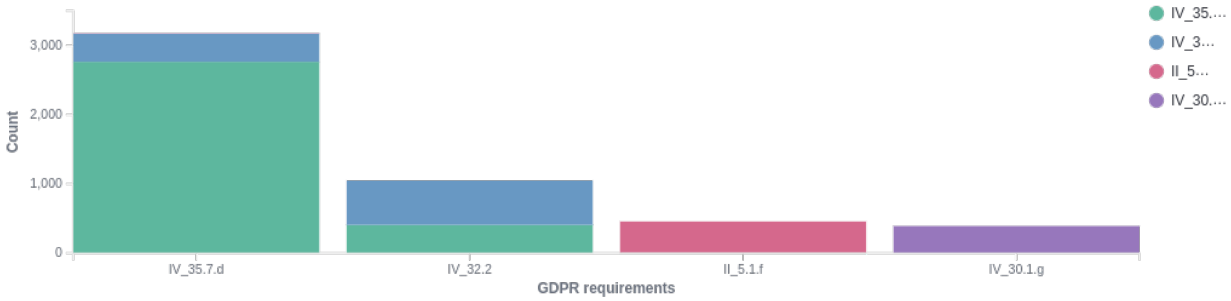
Requirement IV_30.1.g

It is necessary to keep all processing activities documented, to carry out an inventory of data from beginning to end and an audit, in order to know all the places where personal and sensitive data are located, processed, stored or transmitted.

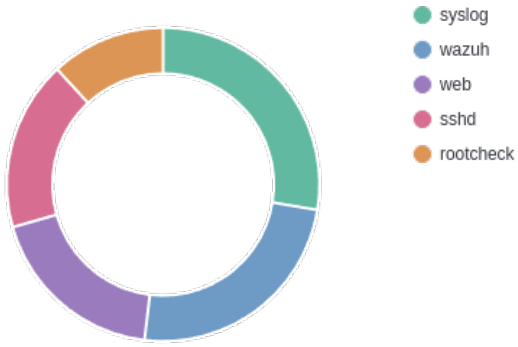
Top rules for IV_30.1.g requirement

Rule ID	Description
80781	Audit: Command: /usr/sbin/ls
80790	Audit: Command: /usr/sbin/ssh
80784	Audit: Command: /usr/sbin/crond

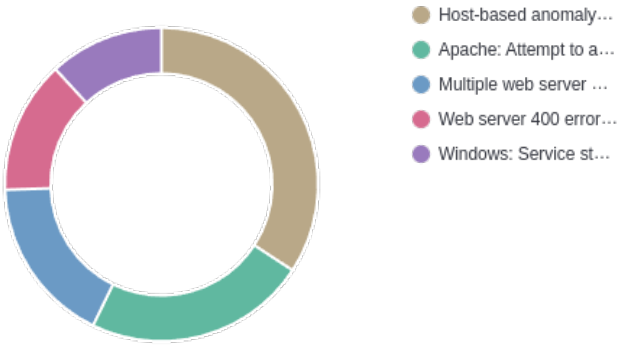
GDPR Requirements



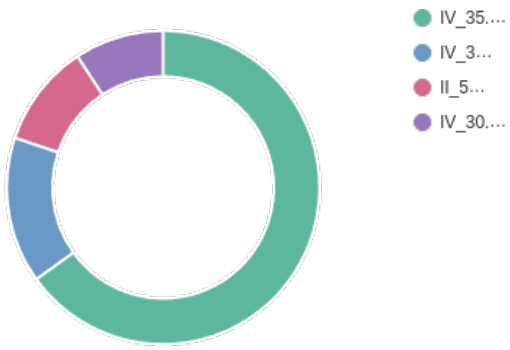
Top 5 rule groups



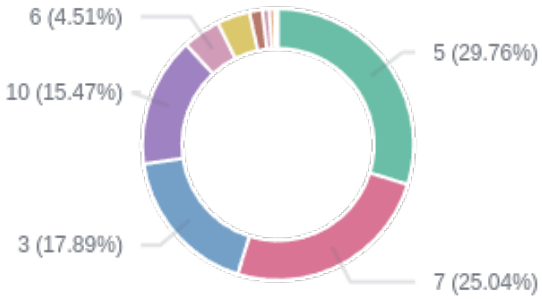
Top 5 rules



Top 5 requirements



Rule level distribution



Last alerts

Requirement	Description	Count
IV_35.7.d	Host-based anomaly detection event (rootcheck).	442
IV_35.7.d	Apache: Attempt to access forbidden directory index.	297
IV_35.7.d	Multiple web server 400 error codes from same source ip.	223
IV_35.7.d	Web server 400 error code.	177
IV_35.7.d	Windows: Service startup type was changed.	153
II_5.1.f	Integrity checksum changed.	153
II_5.1.f	File deleted.	149
II_5.1.f	File added to the system.	141
IV_35.7.d	sshd: Possible breakin attempt (high number of reverse lookup errors).	115
IV_35.7.d	sshd: Reverse lookup error (bad ISP or attack).	104
IV_35.7.d	sshd: insecure connection attempt (scan).	102
IV_35.7.d	sshd: Possible attack on the ssh server (or version gathering).	96
IV_35.7.d	sshd: Attempt to login using a non-existent user	93
IV_32.2	sshd: Attempt to login using a non-existent user	93
IV_30.1.g	Audit: Command: /usr/sbin/ls	50
IV_35.7.d	Logon Failure - Unknown user or bad password	48
IV_32.2	Logon Failure - Unknown user or bad password	48
IV_30.1.g	Audit: Command: /usr/sbin/ssh	48
IV_30.1.g	Audit: Command: /usr/sbin/crond	46
IV_35.7.d	sshd: authentication failed.	45
IV_32.2	sshd: authentication failed.	45
IV_35.7.d	unix_chkpwd: Password check failed.	43
IV_32.2	unix_chkpwd: Password check failed.	43
IV_35.7.d	PAM: User login failed.	42
IV_35.7.d	sshd: Multiple authentication failures.	42
IV_32.2	PAM: User login failed.	42
IV_32.2	sshd: Multiple authentication failures.	42
IV_30.1.g	Audit: Command: /usr/sbin/grep	41
IV_30.1.g	Audit: Command: /usr/sbin/sudo	40
IV_35.7.d	sshd: brute force trying to get access to the system.	38
IV_32.2	sshd: brute force trying to get access to the system.	38
IV_30.1.g	Audit: Command: /usr/sbin/sh	38
IV_30.1.g	Audit: Command: /usr/sbin/consoletype	36
IV_30.1.g	Audit: Command: /usr/sbin/hostname	34
IV_32.2	Docker: Container test_container received the action: die	33
IV_32.2	Docker: Container nginx_container received the action: kill	31
IV_32.2	Docker: Network bridge disconnected	31
IV_30.1.g	Audit: Command: /usr/sbin/id	30
IV_32.2	Docker: Started shell session in container nginx_container	29

Requirement	Description	Count
IV_30.1.g	Audit: Command: /usr/sbin/bash	29
IV_32.2	Docker: Container nginx_container restarted	26
IV_32.2	Docker: Container nginx_container stopped	26
IV_35.7.d	CVE-2013-4235 affects login	14
IV_35.7.d	CVE-2020-1747 affects python3-yaml	14
IV_35.7.d	CVE-2020-1927 affects apache2	14
IV_35.7.d	CVE-2019-1552 affects openssl	13
IV_32.2	Netscreen firewall: Successfull admin login	10
IV_32.2	Imapd user login.	8
IV_32.2	Cisco IOS: Successful login to the router.	7
IV_32.2	Courier brute force (multiple failed logins).	7
IV_32.2	User successfully changed UID.	7
IV_32.2	Root's crontab entry changed.	6
IV_32.2	SonicWall: Firewall administrator login.	6
II_5.1.f	Microsoft Event log cleared.	5
II_5.1.f	Registry Integrity Checksum Changed	4