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

GDPR report

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

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

rule.gdpr: * AND cluster.name: wazuh

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
5712	sshd: brute force trying to get access to the system.
5557	unix_chkpwd: Password check 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.
554	File added to the system.
553	File deleted.

Requirement IV_30.1.g

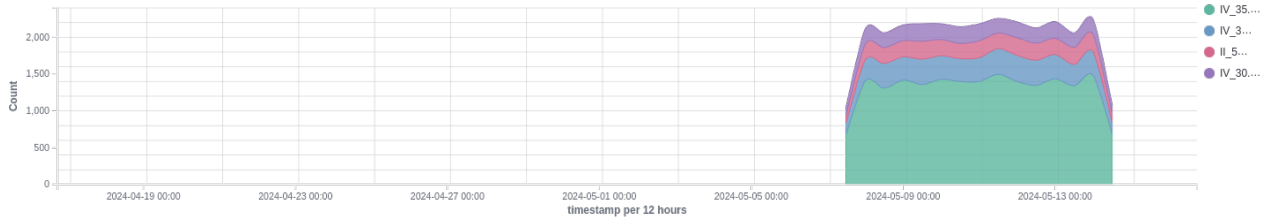
It is necessary to keep all processing activities documented, to carry out an inventory of data from beginning to end and an audit, in order to know all the places where personal and sensitive data are located, processed, stored or transmitted.

Top rules for IV_30.1.g requirement

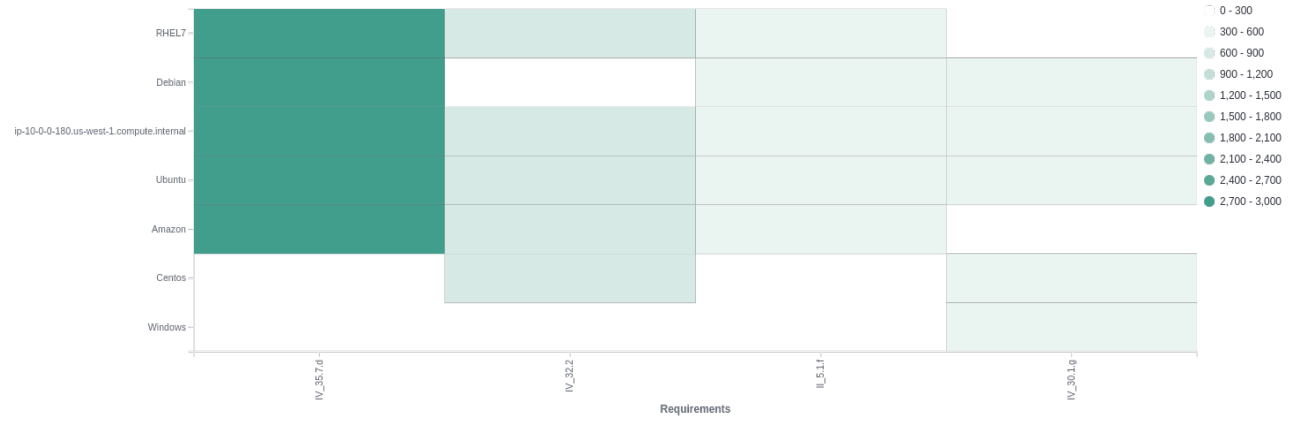
Rule ID	Description
80784	Audit: Command: /usr/sbin/hostname
80790	Audit: Command: /usr/sbin/ssh
80781	Audit: Command: /usr/sbin/sudo

Top 10 agents by alerts number

Top requirements over time

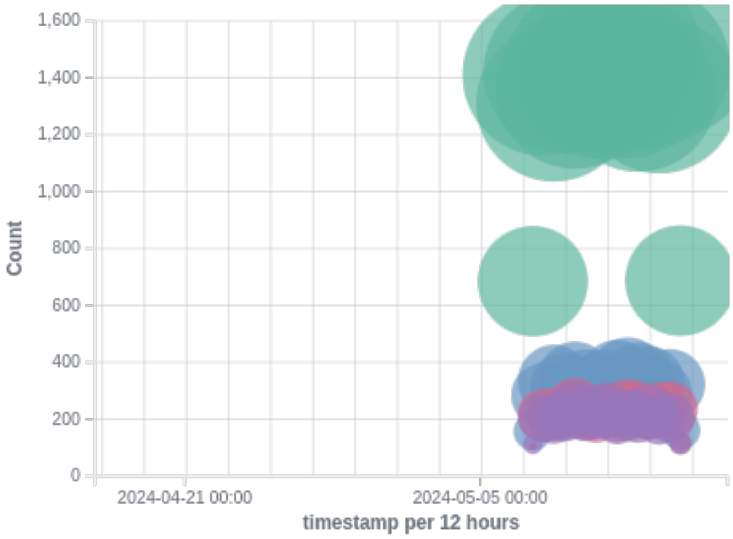


Last alerts



Requirements by agent

GDPR requirements



Alerts summary

Agent name	Requirement	Description	Count
RHEL7	IV_35.7.d	Host-based anomaly detection event (rootcheck).	451
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	Host-based anomaly detection event (rootcheck).	428
RHEL7	IV_35.7.d	Apache: Attempt to access forbidden directory index.	311
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	Apache: Attempt to access forbidden directory index.	257
RHEL7	IV_35.7.d	Web server 400 error code.	230
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	Multiple web server 400 error codes from same source ip.	229
RHEL7	IV_35.7.d	Multiple web server 400 error codes from same source ip.	222
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	Web server 400 error code.	216
ip-10-0-0-180.us-west-1.compute.internal	II_5.1.f	Integrity checksum changed.	165
RHEL7	II_5.1.f	File deleted.	156
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	Windows: Service startup type was changed.	153
RHEL7	IV_35.7.d	Windows: Service startup type was changed.	143
ip-10-0-0-180.us-west-1.compute.internal	II_5.1.f	File deleted.	141
RHEL7	II_5.1.f	Integrity checksum changed.	139
ip-10-0-0-180.us-west-1.compute.internal	II_5.1.f	File added to the system.	135
RHEL7	II_5.1.f	File added to the system.	134
RHEL7	IV_35.7.d	sshd: Reverse lookup error (bad ISP or attack).	125
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: Possible attack on the ssh server (or version gathering).	114
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: Possible breakin attempt (high number of reverse lookup errors).	114
RHEL7	IV_35.7.d	sshd: insecure connection attempt (scan).	108
RHEL7	IV_35.7.d	sshd: Possible breakin attempt (high number of reverse lookup errors).	106
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: Reverse lookup error (bad ISP or attack).	97
RHEL7	IV_35.7.d	sshd: Possible attack on the ssh server (or version gathering).	96
RHEL7	IV_35.7.d	sshd: Attempt to login using a non-existent user	86
RHEL7	IV_32.2	sshd: Attempt to login using a non-existent user	86
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: insecure connection attempt (scan).	85
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: Attempt to login using a non-existent user	72
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	sshd: Attempt to login using a non-existent user	72
RHEL7	IV_35.7.d	Logon Failure - Unknown user or bad password	54
RHEL7	IV_32.2	Logon Failure - Unknown user or bad password	54
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: brute force trying to get access to the system.	52
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	sshd: brute force trying to get access to the system.	52
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/bash	51
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/grep	50
RHEL7	IV_35.7.d	unix_chkpwd: Password check failed.	49
RHEL7	IV_32.2	unix_chkpwd: Password check failed.	49
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/ssh	48
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: Multiple authentication failures.	46
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	sshd: Multiple authentication failures.	46

Agent name	Requirement	Description	Count
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/crond	45
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/ls	45
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	unix_chkpwd: Password check failed.	45
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	unix_chkpwd: Password check failed.	45
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/sh	43
RHEL7	IV_35.7.d	sshd: Multiple authentication failures.	42
RHEL7	IV_32.2	sshd: Multiple authentication failures.	42
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/sudo	41
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Docker: Container nginx_container received the action: kill	41
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/hostname	40
RHEL7	IV_35.7.d	sshd: brute force trying to get access to the system.	39
RHEL7	IV_32.2	sshd: brute force trying to get access to the system.	39
RHEL7	IV_35.7.d	sshd: authentication failed.	37
RHEL7	IV_32.2	Docker: Container nginx_container received the action: kill	37
RHEL7	IV_32.2	sshd: authentication failed.	37
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	Logon Failure - Unknown user or bad password	37
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	PAM: User login failed.	37
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Logon Failure - Unknown user or bad password	37
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	PAM: User login failed.	37
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/id	36
RHEL7	IV_32.2	Docker: Container test_container received the action: die	35
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	sshd: authentication failed.	35
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	sshd: authentication failed.	35
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Docker: Network bridge disconnected	34
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Docker: Started shell session in container nginx_container	34
RHEL7	IV_35.7.d	PAM: User login failed.	33
RHEL7	IV_32.2	PAM: User login failed.	33
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Docker: Container test_container received the action: die	33
RHEL7	IV_32.2	Docker: Started shell session in container nginx_container	32
RHEL7	IV_32.2	Docker: Network bridge disconnected	31
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Docker: Container nginx_container restarted	31
RHEL7	IV_32.2	Docker: Container nginx_container stopped	28
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	CVE-2013-4235 affects login	27
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Docker: Container nginx_container stopped	26
RHEL7	IV_32.2	Docker: Container nginx_container restarted	25
RHEL7	IV_30.1.g	Audit: Command: /usr/sbin/consoletype	23
RHEL7	IV_35.7.d	CVE-2018-1000035 affects unzip	21
RHEL7	IV_35.7.d	CVE-2013-4235 affects login	19
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	CVE-2019-15847 affects gcc	17
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	CVE-2019-17543 affects liblz4-1	15
RHEL7	IV_35.7.d	CVE-2018-6485 affects libc-bin	14

Agent name	Requirement	Description	Count
RHEL7	IV_35.7.d	CVE-2020-1747 affects python3-yaml	14
ip-10-0-0-180.us-west-1.compute.internal	IV_35.7.d	CVE-2020-1752 affects multiarch-support	14
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Netscreen firewall: Successfull admin login	11
RHEL7	IV_32.2	Netscreen firewall: Successfull admin login	10
RHEL7	IV_32.2	Courier brute force (multiple failed logins).	9
RHEL7	IV_32.2	PAM: Multiple failed logins in a small period of time.	9
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Courier brute force (multiple failed logins).	9
RHEL7	IV_32.2	SonicWall: Firewall administrator login.	8
RHEL7	IV_32.2	User missed the password to change UID to root.	8
RHEL7	IV_32.2	Failed attempt to run sudo.	7
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Postfix: Multiple SASL authentication failures.	7
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	Three failed attempts to run sudo	7
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	User added to group.	7
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	telnetd: Multiple connection attempts from same source (possible scan).	7
RHEL7	IV_32.2	Imapd Multiple failed logins from same source ip.	6
RHEL7	II_5.1.f	Registry Entry Deleted.	6
ip-10-0-0-180.us-west-1.compute.internal	IV_32.2	PIX: Multiple AAA (VPN) authentication failures.	6
RHEL7	II_5.1.f	Microsoft Event log cleared.	5
RHEL7	II_5.1.f	Registry Integrity Checksum Changed	2