GDPR report

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

2025-04-09T14:52:46 to 2025-04-10T14:52:46

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

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
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
31509	CMS (WordPress or Joomla) login attempt.

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
31509	CMS (WordPress or Joomla) login attempt.
3332	Postfix SASL authentication failure.
5402	Successful sudo to ROOT executed.

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.
591	Log file rotated.

Requirement IV_30.1.g

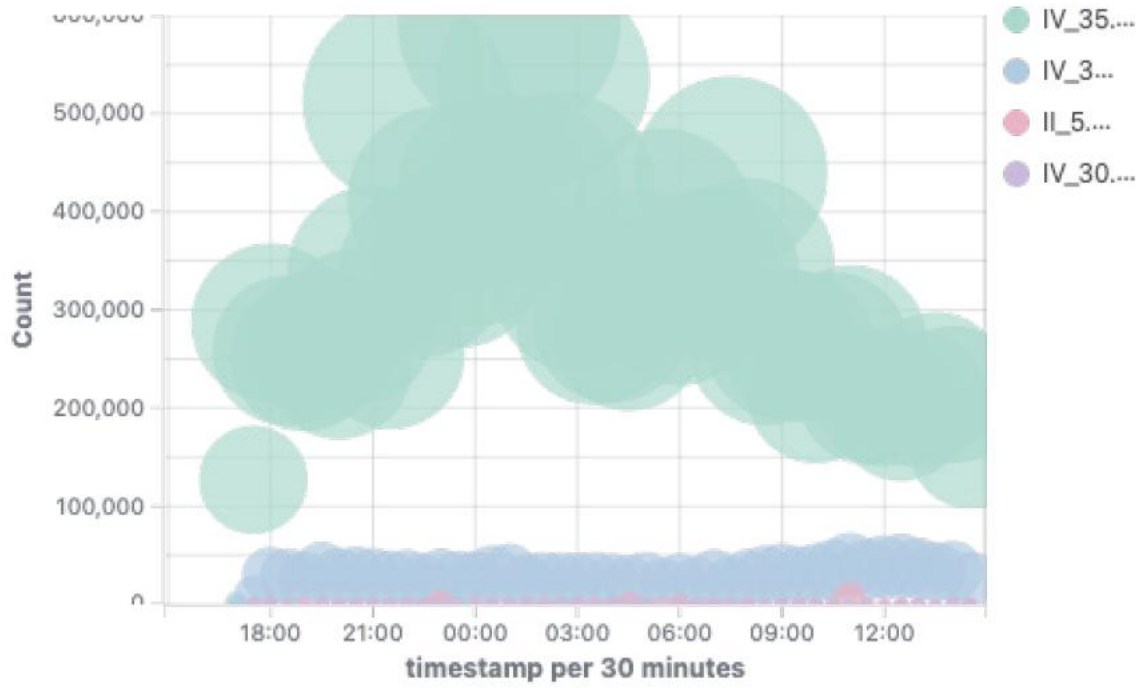
It is necessary to keep all processing activities documented, to carry out an inventory of data from beginning to end and an audit, in order to know all the places where personal and sensitive data are located, processed, stored or transmitted.

Top rules for IV_30.1.g requirement

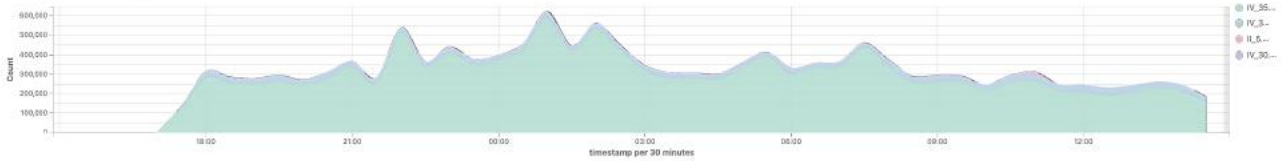
Rule ID	Description
80711	Auditd: Process ended abnormally.

Top 10 agents by alerts number

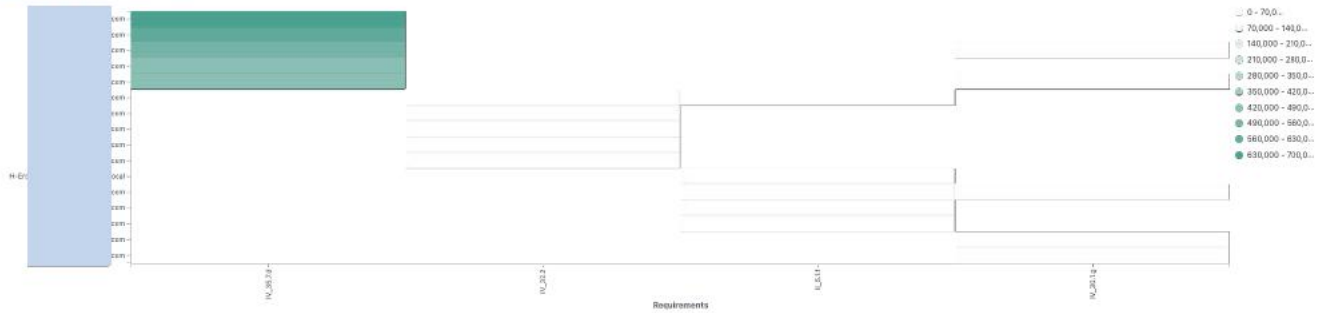
GDPR requirements



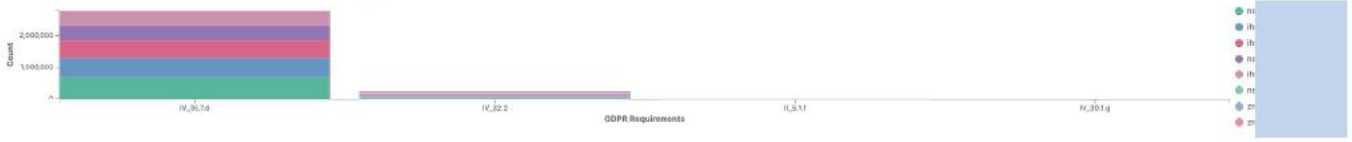
Top requirements over time



Last alerts



Requirements by agent



Alerts summary

Agent name	Requirement	Description	Count
ns1.[redacted]25.com	IV_35.7.d	Web server 400 error code.	588936
[redacted]27.com	IV_35.7.d	Web server 400 error code.	550079
[redacted]32.com	IV_35.7.d	Web server 400 error code.	475219
ns1[redacted].com	IV_35.7.d	Web server 400 error code.	418072
[redacted].com	IV_35.7.d	Web server 400 error code.	405500
ns1[redacted].com	IV_35.7.d	CMS (WordPress or Joomla) login attempt.	41515
ns1[redacted].com	IV_32.2	CMS (WordPress or Joomla) login attempt.	41515
ns1[redacted].com	IV_35.7.d	Multiple web server 400 error codes from same source ip.	35107
[redacted].com	IV_35.7.d	Multiple web server 400 error codes from same source ip.	31692
[redacted].com	IV_35.7.d	Multiple web server 400 error codes from same source ip.	29588
ns1[redacted].com	IV_35.7.d	Multiple web server 400 error codes from same source ip.	24648
[redacted].com	IV_35.7.d	CMS (WordPress or Joomla) login attempt.	13751
[redacted].com	IV_32.2	CMS (WordPress or Joomla) login attempt.	13751
ns1[redacted].com	IV_35.7.d	High amount of POST requests in a small period of time (likely bot).	11194
ns1[redacted].com	IV_35.7.d	High amount of POST requests in a small period of time (likely bot).	10395
[redacted].com	IV_35.7.d	High amount of POST requests in a small period of time (likely bot).	9432
[redacted].com	IV_35.7.d	Host-based anomaly detection event (rootcheck).	9315
[redacted].com	IV_35.7.d	High amount of POST requests in a small period of time (likely bot).	6973
[redacted].com	IV_35.7.d	CMS (WordPress or Joomla) login attempt.	4865
[redacted].com	IV_32.2	CMS (WordPress or Joomla) login attempt.	4865
[redacted].com	IV_35.7.d	Common web attack.	4476
ns1[redacted].com	IV_35.7.d	CMS (WordPress or Joomla) brute force attempt.	4475
ns1[redacted].com	IV_32.2	CMS (WordPress or Joomla) brute force attempt.	4475
ns1[redacted].com	IV_35.7.d	Common web attack.	4438
ns1[redacted].com	IV_35.7.d	CMS (WordPress or Joomla) login attempt.	4291
ns1[redacted].com	IV_32.2	CMS (WordPress or Joomla) login attempt.	4291
ns1[redacted].com	IV_35.7.d	Common web attack.	4265
[redacted].com	IV_35.7.d	Common web attack.	4242
[redacted].com	IV_35.7.d	Multiple web server 503 error code (Service unavailable).	3429
ns1[redacted].com	IV_35.7.d	A web attack returned code 200 (success).	2332
ns1[redacted].com	IV_35.7.d	Suspicious URL access.	1715
[redacted].com	IV_35.7.d	Suspicious URL access.	1498
[redacted].com	IV_35.7.d	Suspicious URL access.	1125
[redacted].com	IV_35.7.d	Host-based anomaly detection event (rootcheck).	1068
[redacted].com	IV_35.7.d	Multiple web server 503 error code (Service unavailable).	1040
[redacted].com	IV_35.7.d	CMS (WordPress or Joomla) brute force attempt.	976
[redacted].com	IV_32.2	CMS (WordPress or Joomla) brute force attempt.	976
ns1[redacted].com	IV_35.7.d	Suspicious URL access.	679
ns1[redacted].com	IV_35.7.d	Multiple web server 503 error code (Service unavailable).	599

Agent name	Requirement	Description	Count
ns1 .com	IV_35.7.d	Multiple web server 500 error code (Internal Error).	431
ns1 .com	IV_35.7.d	Multiple web server 500 error code (Internal Error).	346
.com	IV_35.7.d	Multiple web server 500 error code (Internal Error).	318
ns1 .com	IV_35.7.d	Multiple web server 503 error code (Service unavailable).	312
.com	II_5.1.f	Integrity checksum changed.	238
ns1 .com	IV_35.7.d	SQL injection attempt.	231
.com	IV_35.7.d	Agent event queue is full. Events may be lost.	220
ns1 .com	II_5.1.f	Integrity checksum changed.	216
.com	II_5.1.f	Integrity checksum changed.	201
ns1 .com	IV_35.7.d	Listened ports status (netstat) changed (new port opened or closed).	199
.com	IV_35.7.d	SQL injection attempt.	185
ns1 .com	IV_35.7.d	Listened ports status (netstat) changed (new port opened or closed).	179
.com	IV_35.7.d	Multiple web server 500 error code (Internal Error).	149
ns1 .com	IV_35.7.d	Agent event queue is full. Events may be lost.	97
.com	IV_35.7.d	Listened ports status (netstat) changed (new port opened or closed).	93
.com	IV_35.7.d	Simple shell.php command execution.	92
ns1 .com	IV_35.7.d	SQL injection attempt.	77
ns1 .com	IV_35.7.d	A web attack returned code 200 (success).	76
ns1 .com	IV_35.7.d	Agent event queue is full. Events may be lost.	67
.com	IV_35.7.d	A web attack returned code 200 (success).	45
.com	IV_35.7.d	Agent event queue is full. Events may be lost.	44
.com	IV_35.7.d	SQL injection attempt.	40
ns1 .com	II_5.1.f	Integrity checksum changed.	40
ns1 .com	IV_35.7.d	CMS (WordPress or Joomla) brute force attempt.	34
ns1 .com	IV_32.2	CMS (WordPress or Joomla) brute force attempt.	34
.com	IV_35.7.d	A web attack returned code 200 (success).	32
.com	IV_35.7.d	Listened ports status (netstat) changed (new port opened or closed).	32
.com	IV_35.7.d	Auditd: Process ended abnormally.	18
.com	IV_30.1.g	Auditd: Process ended abnormally.	18
.com	II_5.1.f	File added to the system.	16
.com	IV_35.7.d	Agent event queue is flooded. Check the agent configuration.	13
.com	IV_35.7.d	Multiple SQL injection attempts from same source ip.	12
.com	II_5.1.f	File added to the system.	11
ns1 .com	IV_35.7.d	PHP CGI-bin vulnerability attempt.	11
ns1 .com	IV_35.7.d	PHPMyAdmin scans (looking for setup.php).	10
.com	IV_35.7.d	Multiple common web attacks from same source ip.	10
.com	IV_35.7.d	Log file rotated.	9
.com	II_5.1.f	Log file rotated.	9
.com	II_5.1.f	File deleted.	8
.com	IV_35.7.d	XSS (Cross Site Scripting) attempt.	8
ns1 .com	IV_35.7.d	Host-based anomaly detection event (rootcheck).	6

Agent name	Requirement	Description	Count
ns1 .com	IV_35.7.d	Multiple SQL injection attempts from same source ip.	5
.com	IV_35.7.d	Agent event queue is flooded. Check the agent configuration.	5
.com	IV_35.7.d	PHP CGI-bin vulnerability attempt.	5
ns1 .com	IV_35.7.d	Host-based anomaly detection event (rootcheck).	4
ns1 .com	II_5.1.f	File deleted.	4
ns1 .com	IV_35.7.d	Agent event queue is flooded. Check the agent configuration.	3
.com	IV_35.7.d	Auditd: Process ended abnormally.	3
.com	IV_30.1.g	Auditd: Process ended abnormally.	3
ns1 .com	IV_35.7.d	Agent event queue is 90% full.	2
ns1 .com	IV_35.7.d	URL too long. Higher than allowed on most browsers. Possible attack.	2
.com	IV_35.7.d	Agent event queue is 90% full.	2
.com	IV_35.7.d	Agent event queue is 90% full.	2
ns1 .com	IV_35.7.d	Agent event queue is 90% full.	2
ns1 .com	IV_35.7.d	XSS (Cross Site Scripting) attempt.	2
ns1 .com	IV_35.7.d	Log file rotated.	1
ns1 .com	II_5.1.f	Log file rotated.	1
.com	IV_35.7.d	Blacklisted user agent (known malicious user agent).	1
.com	II_5.1.f	File deleted.	1
ns1 .com	IV_35.7.d	Multiple SQL injection attempts from same source ip.	1