

GDPR report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	wazuh_agent_ub untu_2	172.20.0.7	Wazuh v4.9.0	wazuh- manager-4.9.0-71 02	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

Q 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

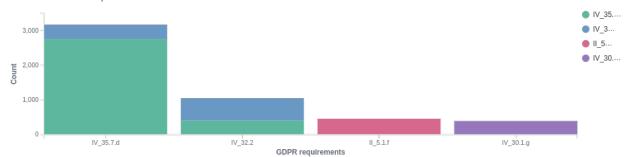
It is necessary to keep all processing activities documented, to carry out an inventory of data from beginning to end and an audit, in order to know all the places where personal and sensitive data are located, processed, stored or transmitted.

Top rules for IV_30.1.g requirement

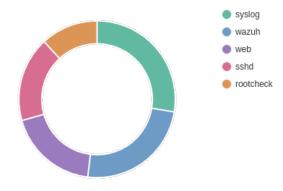
Rule ID	Description
80781	Audit: Command: /usr/sbin/ls
80790	Audit: Command: /usr/sbin/ssh
80784	Audit: Command: /usr/sbin/crond



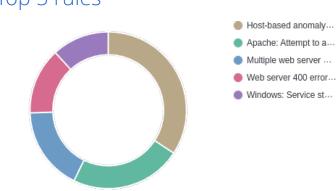
GDPR Requirements



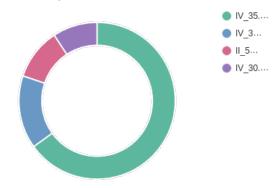




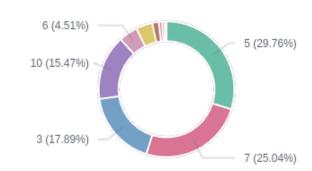
Top 5 rules



Top 5 requirements



Rule level distribution





Last alerts

IV_357.d Host-based anomaly detection event (motcheck). 447 IV_357.d Apache: Attempt to access forbidden directory index. 297 IV_357.d Multiple web server 400 error codes from same source ip. 223 IV_357.d Web server 400 error code. 177 IV_357.d Windows: Service startup type was changed. 153 II.5.1.f Integrity hedekum changed. 153 II.5.1.f File added to the system. 141 IV_357.d shid. Possible breakin attempt (high number of reverse lookup errors). 115 IV_357.d shid. Possible breakin attempt (bod iSP or attack). 104 IV_357.d shid. Possible attack on the sch server (or version gathering). 102 IV_357.d shid. Attempt to login using a non-existent user 93 IV_357.d Shid. Attempt to login using a non-existent user 93 IV_357.d Logon Failure - Unknown user or bad password 48 IV_357.d Shid. Autempt to login using a non-existent user 93 IV_357.d Audit: Command: Assrisbin/sord 46 IV_357.d Shid. Autempt to access to the system. 48	Requirement	Description	Count
N 357.d Multiple web server 400 error codes from same source ip. 223 N 357.d Web server 400 error codes 177 N 357.d Windows: Service startup type was changed. 153 N 357.d Windows: Service startup type was changed. 153 N 357.d Shid: Reverse decided. 149 N 357.d Shid: Reverse lookup error (bad ISP or attack). 141 N 357.d Shid: Reverse lookup error (bad ISP or attack). 104 N 357.d Shid: Reverse lookup error (bad ISP or attack). 107 N 357.d Shid: Reverse lookup error (bad ISP or attack). 107 N 357.d Shid: Reverse lookup error (bad ISP or attack). 107 N 357.d Shid: Reverse lookup error (bad ISP or attack). 107 N 357.d Shid: Reverse lookup aron existent user 93 N 357.d Shid: Attempt to login using a non-existent user 93 N 357.d Logon Failure - Unknown user or bad password 48 N 357.d Logon Failure - Unknown user or bad password 48 N 357.d Logon Failure - Unknown user or bad password 48 N 357.d Shid: Audit: Command: /usr/sbin/issh 48 N 357.d Shid: Authentication failed. 45 N 357.d Shid: Authentication failed. 42 N 357.d Shid: Multiple authentication failed. 42 N 357.d Shid: Multiple authentication failed. 42 N 357.d Shid: Multiple authentication failers. 42 N 357.d Shid: Command: /usr/sbin/sbin/sudo 40 N 357.d Shid: Command: /usr/sbin/sbin/consoletype 36 N 357.d Audit: Command: /usr/sbin/sbin/consoletype 36 N 357.d Shid: Command: /usr/sbin/sbin/consoletype 36 N 357.d Shid: Command: /usr/sbin/sbi	IV_35.7.d	Host-based anomaly detection event (rootcheck).	442
N 35.7 d Web server 400 error code. 177 N 35.7 d Windows Service startup type was changed. 153 II.5.1.f Integrity chedeum changed. 153 II.5.1.f File deleted. 149 II.5.1.f File deleted. 149 II.5.1.f File added to the system. 141 N.35.7 d Shdr Possible breakin attempt (high number of reverse lookup errors). 115 N.35.7 d Shdr Possible attack on the sh server (or version gathering). 102 N.35.7 d Shdr Possible attack on the sh server (or version gathering). 96 N.35.7 d Shdr Attempt to login using a non-existent user 93 N.35.7 d Shdr Attempt to login using a non-existent user 93 N.30.1 g Audic Command: Justrishin/is 50 N.35.7 d Logon Failure - Unknown user or bad password 48 N.30.1 g Audic Command: Justrishin/isch 48 N.30.1 g Audic Command: Justrishin/sch 48 N.30.1 g Audic Command: Justrishin/sch 48 N.35.7 d Shd Justrintitation failed. 45	IV_35.7.d	Apache: Attempt to access forbidden directory index.	297
N_35.7.d Windows: Service startup type was changed. 153 L_5.1.f Integrity checksum changed. 153 L_5.1.f File deleted. 149 L_5.1.f File deleted. 149 L_5.1.f File deleted to the system. 141 W 35.7.d sshd: Possible breakin attempt (high number of reverse lookup errors). 115 N_35.7.d sshd: Reverse lookup error (bad ISP or attack). 104 W 35.7.d sshd: Reverse lookup error (bad ISP or attack). 102 W 35.7.d sshd: Possible attack on the ssh server (or version gathering). 96 W_35.7.d sshd: Attempt to login using a non-existent user 93 W_35.7.d sshd: Attempt to login using a non-existent user 93 W_30.1.g Audit: Command: /usr/sbin/ls 50 W_35.7.d Logon Failure - Unknown user or bad password 48 W_30.1.g Audit: Command: /usr/sbin/crond 46 W_35.7.d sshd: authentication failed. 45 W_35.7.d sshd: authentication failed. 45 W_35.7.d unix_chlpwd: Password check failed. 45 W_35.7.d unix_chlpwd: Password check failed. 43 W 35.7.d pAM: User login failed. 42 W 35.7.d pAM: User login failed. 42 W 35.7.d pAM: User login failed. 42 W 35.7.d authentication failed. 42 W 35.7.d pAM: User login failed. 43 W 35.7.d pAM: User login failed. 44 W 35.7.d pAM: User login failed. 45 W 30.1.g Audit: Command: /usr/sbin/sudo 40 W 35.7.d pAM: User login failed. 42 W 30.1.g Audit: Command: /usr/sbin/sudo 40 W 30.1.g Audit: Command: /usr/sbin/sudo 40 W 30.1.g Audit: Command: /usr/sbin/sudo 40 W 30.1.g Audit: Command: /usr/sbin/sushone 34 W 30.1.g Audit: Command: /usr/sbin/hostname 34 W 30.1.g Audit: Command: /usr/sbin/hostname 34 W 30.1.g Audit: Command: /usr/sbin/hostname 34 W 30.1.g Audit: Command: /usr/sbin/h	IV_35.7.d	Multiple web server 400 error codes from same source ip.	223
15.1.f Integrity checksum changed. 153 15.1.f File deleted. 149 15.1.f File deleted. 141 17.35.7.d sshd: Possible breakin attempt (high number of reverse lookup error). 115 17.35.7.d sshd: Reverse lookup error (bad ISP or attack). 104 17.35.7.d sshd: Insecure connection attempt (scan). 102 17.35.7.d sshd: Possible attack on the ssh server (or version gathering). 96 18.35.7.d sshd: Attempt to login using a non-existent user 93 18.35.7.d sshd: Attempt to login using a non-existent user 93 18.30.1.g Audit: Command: /usr/sbin/ISP 50 18.35.7.d Logon Failure - Unknown user or bad password 48 18.35.7.d Logon Failure - Unknown user or bad password 48 18.35.7.d Sudit: Command: /usr/sbin/rssh 45 18.35.7.d Unix_chipwd: Password check failed. 45 18.35.7.d Unix_chipwd: Password check failed. 43 18.35.7.d Unix_chipwd: Password check failed. 43 18.35.7.d Sudit: Multiple authentication failures. 42 18.35.7.d Sudit: Command: /usr/sbin/sude 40 18.35.7.d Sudit: Command: /usr/sbin/sudin 38 18.35.1.g Audit: Command: /usr/sbin/shin/sudama 34 18.35.1.g Audit: Command: /usr/sbin/shin/sudama 34 18.35.1.g Docker: Container reserved the action: kill 31 18.35.1.g Docker: Container reserved the action: kill 31 18.35.1.g Docker: Container reserved the action: kill 3	IV_35.7.d	Web server 400 error code.	177
1.5.1.f File deleted.	IV_35.7.d	Windows: Service startup type was changed.	153
IL.5.1.f File added to the system.	II_5.1.f	Integrity checksum changed.	153
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: 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_35.7.d sshd: Attempt to login using a non-existent user 93 IV_30.1.g Audit: Command: /usr/sbin/Is 50 IV_35.7.d Logon Falure - Unknown user or bad password 48 IV_30.1.g Audit: Command: /usr/sbin/rsh 48 IV_30.7.d sshd: authentication failed. 45 IV_35.7.d unix. chkpwd: Password check failed. 43 IV_35.7.d PAM: User login failed. 42 IV_35.7.d PAM: User login failed. 4	II_5.1.f	File deleted.	149
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/Is 50 IV_35.7.d Logon Failure - Unknown user or bad password 48 IV_30.1 g Audit: Command: /usr/sbin/rssh 48 IV_30.1 g Audit: Command: /usr/sbin/rssh 48 IV_30.1 g Audit: Command: /usr/sbin/rsnd 46 IV_35.7.d sshd: authentication failed. 45 IV_35.7.d unix_chkpwd: Password check failed. 43 IV_35.7.d unix_chkpwd: Password check failed. 43 IV_35.7.d sshd: Multiple authentication failures. 42 IV_32.2 pAM: User login failed. 42 IV_30.1 g Audit: Command: /usr/sbin/grep 41 IV_30.1 g Audit: Command: /usr/sbin/sud 40	II_5.1.f	File added to the system.	141
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.30.1.g Audit: Command: /usr/sbin/ls 50 IV.35.7.d 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/ssh 48 IV.30.1.g Audit: Command: /usr/sbin/crond 46 IV.35.7.d sshd: authentication failed. 45 IV.35.7.d sshd: authentication failed. 45 IV.35.7.d unix_chkpwd: Password check failed. 43 IV.35.7.d pAM: User login failed. 42 IV.35.7.d pAM: User login failed. 42 IV.35.7.d pAM: User login failed. 42 IV.30.1.g Audit: Command: /usr/sbin/grep 41 IV.30.1.g Audit: Command: /usr/sbin/grep 41 IV.30.1.g Audit: Command: /usr/sbin/sbin/sbin/sbin/sbin/sbin/sbin/sbin	IV_35.7.d	sshd: Possible breakin attempt (high number of reverse lookup errors).	115
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_30.1.g Audit: Command: /usr/sbin/ssh 48 IV_30.1.g Audit: Command: /usr/sbin/ssh 48 IV_30.1.g Audit: Command: /usr/sbin/ssh 48 IV_30.1.g Audit: Command: /usr/sbin/rond 46 IV_35.7.d sshd: authentication failed. 45 IV_32.2 sshd: authentication failed. 45 IV_32.2.d sshd: Multiple authentication failed. 43 IV_35.7.d sshd: Multiple authentication failures. 42 IV_32.2 pAM: User login failed. 42 IV_30.1.g Audit: Command: /usr/sbin/sprep 41 IV_30.1.g Audit: Command: /usr/sbin/sbin/sbin/sbin/sbin/sbin/sbin/sbin	IV_35.7.d	sshd: Reverse lookup error (bad ISP or attack).	104
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_30.1.g Audit: Command: /usr/sbin/ssh 48 IV_30.1.g Audit: Command: /usr/sbin/rond 46 IV_35.7.d Ashd: authentication failed. 45 IV_35.7.d sshd: authentication failed. 45 IV_35.7.d unix_chkpwd: Password check failed. 43 IV_35.7.d unix_chkpwd: Password check failed. 43 IV_35.7.d sshd: Multiple authentication failures. 42 IV_35.7.d 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_30.1.g Audit: Command: /usr/sbin/sudo 40 IV_30.1.g Audit: Command: /usr/sbin/sbin/sh 38 IV_30.1.g Audit: Command: /usr/sbin/sbin/sh 38 IV_30.1.g<	IV_35.7.d	sshd: insecure connection attempt (scan).	102
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_30.1.g Audit: Command: /usr/sbin/ssh 48 IV_30.1.g Audit: Command: /usr/sbin/crond 46 IV_30.7.d sshd: authentication failed. 45 IV_32.2 sshd: authentication failed. 45 IV_35.7.d 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 pAM: User login failed. 42 IV_32.2 pAM: User login failed. 42 IV_30.1.g Audit: Command: /usr/sbin/sudo 40 IV_30.1.g Audit: Command: /usr/sbin/sudo 40 IV_30.1.g Sshd: brute force trying to get access to the system. 38 IV_30.1.g Audit: Command: /usr/sbin/consoletype 36 IV_30.1.g Audit: Command: /usr/sbin	IV_35.7.d	sshd: Possible attack on the ssh server (or version gathering).	96
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/ssh 48 IV_30.1.g Audit: Command: /usr/sbin/ssh 48 IV_35.7.d sshd: authentication failed. 45 IV_35.7.d sshd: authentication failed. 45 IV_35.7.d unix_chkpwd: Password check failed. 43 IV_32.2 unix_chkpwd: Password check failed. 42 IV_35.7.d sshd: Multiple authentication failures. 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_32.2 sshd: Multiple authentication failures. 42 IV_30.1.g Audit: Command: /usr/sbin/sbin/sep 41 IV_30.1.g Audit: Command: /usr/sbin/sbin/sep 38 IV_30.1.g Au	IV_35.7.d	sshd: Attempt to login using a non-existent user	93
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_35.7.d sshd: authentication failed. 45 IV_35.7.d 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_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_33.7.d 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/shostname 34 IV_30.2.g <t< td=""><td>IV_32.2</td><td>sshd: Attempt to login using a non-existent user</td><td>93</td></t<>	IV_32.2	sshd: Attempt to login using a non-existent user	93
IV_32.2 Logon Failure - Unknown user or bad password 48 IV_30.1g Audit: Command: /usr/sbin/ssh 48 IV_30.1g 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_32.2 sshd: Multiple authentication failures. 42 IV_32.1.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_30.1.g Audit: Command: /usr/sbin/sh 38 IV_30.1.g Audit: Command: /usr/sbin/consoletype 36 IV_30.1.g Audit: Comm	IV_30.1.g	Audit: Command: /usr/sbin/ls	50
IV_30.1g Audit: Command: /usr/sbin/ssh 48 IV_30.1g Audit: Command: /usr/sbin/crond 46 IV_35.7.d sshd: authentication failed. 45 IV_35.7.d 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_32.2 sshd: Multiple authentication failures. 42 IV_32.1.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_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_30.2.g Docker: Container	IV_35.7.d	Logon Failure - Unknown user or bad password	48
N_30.1g Audit: Command: /usr/sbin/crond 46 N_35.7.d sshd: authentication failed. 45 N_32.2 sshd: authentication failed. 45 N_35.7.d unix_chkpwd: Password check failed. 43 N_32.2 unix_chkpwd: Password check failed. 43 N_35.7.d PAM: User login failed. 42 N_35.7.d sshd: Multiple authentication failures. 42 N_32.2 PAM: User login failed. 42 N_32.2 sshd: Multiple authentication failures. 42 N_30.1g Audit: Command: /usr/sbin/grep 41 N_30.1g Audit: Command: /usr/sbin/sudo 40 N_35.7.d sshd: brute force trying to get access to the system. 38 N_32.2 sshd: brute force trying to get access to the system. 38 N_30.1g Audit: Command: /usr/sbin/sbh 38 N_30.1g Audit: Command: /usr/sbin/consoletype 36 N_30.1g Audit: Command: /usr/sbin/hostname 34 N_32.2 Docker: Container test_container received the action: die 33 N_32.2 Docker: Container nginx_container received the action: kill 31 <	IV_32.2	Logon Failure - Unknown user or bad password	48
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_35.7.d 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/sbin/sh 38 IV_30.1.g Audit: Command: /usr/sbin/hostname 34 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_30.1.g Audit: Command: /usr/sbin/id 30	IV_30.1.g	Audit: Command: /usr/sbin/ssh	48
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_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_30.2. Docker: Container test_container received the action: die 33 IV_32.2 Docker: Container nginx_container received the action: kill 31 IV_30.1.g Audit: Command: /usr/sbin/id 30	IV_30.1.g	Audit: Command: /usr/sbin/crond	46
V_35.7.dunix_chkpwd: Password check failed.43IV_32.2unix_chkpwd: Password check failed.43IV_35.7.dPAM: User login failed.42IV_35.7.dsshd: Multiple authentication failures.42IV_32.2PAM: User login failed.42IV_32.2sshd: Multiple authentication failures.42IV_30.1.gAudit: Command: /usr/sbin/grep41IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_35.7.d	sshd: authentication failed.	45
W_32.2unix_chkpwd: Password check failed.43IV_35.7.dPAM: User login failed.42IV_35.7.dsshd: Multiple authentication failures.42IV_32.2PAM: User login failed.42IV_32.2sshd: Multiple authentication failures.42IV_30.1.gAudit: Command: /usr/sbin/grep41IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_32.2	sshd: authentication failed.	45
V_35.7.dPAM: User login failed.42IV_35.7.dsshd: Multiple authentication failures.42IV_32.2PAM: User login failed.42IV_30.1.gAudit: Command: /usr/sbin/grep41IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_30.2.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_35.7.d	unix_chkpwd: Password check failed.	43
IV_35.7.dsshd: Multiple authentication failures.42IV_32.2PAM: User login failed.42IV_32.2sshd: Multiple authentication failures.42IV_30.1.gAudit: Command: /usr/sbin/grep41IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_32.2	unix_chkpwd: Password check failed.	43
IV_32.2PAM: User login failed.42IV_32.2sshd: Multiple authentication failures.42IV_30.1.gAudit: Command: /usr/sbin/grep41IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_35.7.d	PAM: User login failed.	42
IV_32.2sshd: Multiple authentication failures.42IV_30.1.gAudit: Command: /usr/sbin/grep41IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_35.7.d	sshd: Multiple authentication failures.	42
IV_30.1.gAudit: Command: /usr/sbin/grep41IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_32.2	PAM: User login failed.	42
IV_30.1.gAudit: Command: /usr/sbin/sudo40IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_32.2	sshd: Multiple authentication failures.	42
IV_35.7.dsshd: brute force trying to get access to the system.38IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_30.1.g	Audit: Command: /usr/sbin/grep	41
IV_32.2sshd: brute force trying to get access to the system.38IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_30.1.g	Audit: Command: /usr/sbin/sudo	40
IV_30.1.gAudit: Command: /usr/sbin/sh38IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_35.7.d	sshd: brute force trying to get access to the system.	38
IV_30.1.gAudit: Command: /usr/sbin/consoletype36IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_32.2	sshd: brute force trying to get access to the system.	38
IV_30.1.gAudit: Command: /usr/sbin/hostname34IV_32.2Docker: Container test_container received the action: die33IV_32.2Docker: Container nginx_container received the action: kill31IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_30.1.g	Audit: Command: /usr/sbin/sh	38
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_30.1.g	Audit: Command: /usr/sbin/consoletype	36
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_30.1.g	Audit: Command: /usr/sbin/hostname	34
IV_32.2Docker: Network bridge disconnected31IV_30.1.gAudit: Command: /usr/sbin/id30	IV_32.2	Docker: Container test_container received the action: die	33
IV_30.1.g Audit: Command: /usr/sbin/id 30	IV_32.2	Docker: Container nginx_container received the action: kill	31
	IV_32.2	Docker: Network bridge disconnected	31
IV_32.2 Docker: Started shell session in container nginx_container 29	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