

NIST 800-53 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 @ 15:39:09.000

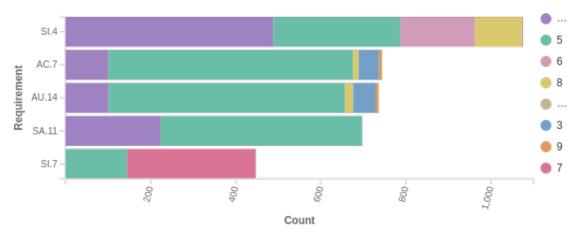
Group: default

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

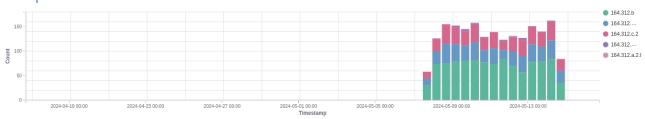
2 2024-04-16T17:39:15 to 2024-05-16T17:39:15

Q rule.nist_800_53: * AND cluster.name: wazuh AND agent.id: 002

Requirements distributed by level



Requirements over time



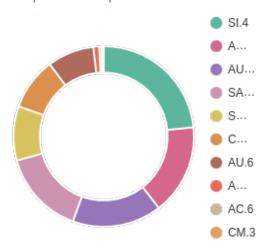


Stats

Top 10 requirements



12 Max rule level





Alerts summary

AC.7 5 Apache: Attempt to access forbidden directory index. 297 AU.14 5 Apache: Attempt to access forbidden directory index. 297 9.4 10 Multiple web server 400 error code. 177 9.4 5 Web server 400 error code. 177 9.4 10 sibht: Possible breakin attempt (high number of reverse lookup errors). 108 9.4 5 sibht: Reverse lookup error (bad 15P or attack). 108 9.4 5 sibht: Reverse lookup error (bad 15P or attack). 104 9.4 5 sibht: Reverse lookup error (bad 15P or attack). 104 9.4 5 sibht: Reverse lookup error (bad 15P or attack). 104 9.4 5 sibht: Reverse lookup error (bad 15P or attack). 104 9.4 5 sibht: Attach or the sibht error (bad 15P or attack). 104 9.4 5 sibht: Attach or the sibht error (bad 15P or attack). 104 4.7 5 sibht: Attach or the sibht error the sibht e	Requirement	Level	Description	Count
SIA 10 Multiplie web server 400 error codes from same source ip. 223 91.4 5 Web server 400 error code. 177 91.4 10 sebbc Possible breakin attempt (pligh number of reverse lookup errors). 121 91.4 6 sebbc Reverse lookup error (bad ISP or attack). 104 91.4 6 sebbc Reverse lookup error (bad ISP or attack). 104 91.4 8 sebbc Possible attack on the sels server (or version gathering). 98 AC.7 5 sebbc Attempt to login using a non-existent user 93 AC.7 5 sebbc Attempt to login using a non-existent user 93 AC.7 5 sebbc Attempt to login using a non-existent user 93 AC.7 5 sebbc authentication failed. 45 AC.7 5 sebbc authentication failed. 45 AC.7 5 sebbc authentication failed. 43 AC.7 5 unix chipwad Password check failed. 43 ALI4 5 unix chipwad Password check failed. 43 ALI4 6				297
SI.4 5 Web server 400 error code. 177 SI.4 10 seshch Possible breakin attempt (high number of reverse lookup errors). 121 SI.4 6 seshch Possible breakin attempt (scan). 108 SI.4 5 seshch Reverse lookup error (bod ISP or attack). 104 SI.4 8 seshch Severse lookup error (bod ISP or attack). 98 AC.7 5 seshch Attempt to login using a non-existent user 93 AU.14 5 seshch Attempt to login using a non-existent user 93 AC.7 5 seshch authentication failed. 45 AC.7 5 unix, chipwoit Peasword check failed. 43 AU.14 5 seshch Multiple authentication failures. 42 AC.7 10 seshch Multiple authentication failures. 42 AU.14 5 PAM: User login failed. <	AU.14	5	Apache: Attempt to access forbidden directory index.	297
Si/L 10 sshick Possible breakin attempt (high number of reverse lookup errors) 121 Si/L 6 sshick insecure connection attempt (scan). 108 Si/L 5 sshick Reverse lookup error (bad ISP or attack). 104 Si/L 8 sshick Possible attack on the sets server (or version gathering). 98 AC.7 5 sshick Attempt to login using a non-existent user 93 AU.14 5 sshick Attempt to login using a non-existent user 93 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 Unknick Chikpwd: Password check failed. 45 AC.7 5 unknick Chikpwd: Password check failed. 43 Si.4 10 unknick Chikpwd: Password check failed. 43 AC.7 5 unknick Chikpwd: Password check failed. 43 AC.7 10 sshid: Williple authentication failures. 42	SI.4	10	Multiple web server 400 error codes from same source ip.	223
SI4 6 sshd: insecure connection attempt (scan). 108 SI4 5 sshd: Reverse lookup error (bad ISP or attack). 104 SI4 8 sshd: Reverse lookup error (bad ISP or attack). 104 AC7 5 sshd: Attempt to login using a non-existent user 93 AC.7 5 sshd: Attempt to login using a non-existent user 93 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 sshd: authentication failed. 45 AC.7 5 sshd: authentication failed. 45 AC.7 5 sshd: authentication failed. 43 AC.7 5 unix chiqwed: Password check failed. 43 AC.7 10 sshd: Multiple authentication failures. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: Multiple proceed priving to get access to the system.	SI.4	5	Web server 400 error code.	177
SIA 5 sshd: Reverse lookup error (bad ISP or attack). 104 SIA 8 sshd: Possible attack on the ssh server (or version gathering). 98 AC.7 5 sshd: Attempt to login using a non-existent user 93 AU.14 5 sshd: Attempt to login using a non-existent user 93 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 sshd: authentication failed. 45 AU.14 5 sshd: authentication failed. 45 AC.7 5 unix chickpoxt: Password check failed. 43 AU.14 5 unix chickpoxt: Password check failed. 43 AU.14 5 unix chickpoxt: Password check failed. 43 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 SIA 10 sshd: brute force trying to get access to the system.	SI.4	10	sshd: Possible breakin attempt (high number of reverse lookup errors).	121
SI.4 8 sshd: Possible attack on the ssh server (or version gathering). 98 AC.7 5 sshd: Attempt to login using a non-existent user 93 AU.14 5 sshd: Attempt to login using a non-existent user 93 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 sshd: authentication failed. 45 AU.14 5 sshd: authentication failed. 45 AC.7 5 unix, chkpwd: Password check failed. 43 AU.14 5 unix, chkpwd: Password check failed. 43 AU.14 5 sshd: Multiple authentication failures. 42 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get acce	SI.4	6	sshd: insecure connection attempt (scan).	108
AC.7 5 sshd: Attempt to login using a non-existent user 93 AU.14 5 sshd: Attempt to login using a non-existent user 93 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 sshd: authentication failed. 45 AC.7 5 sshd: authentication failed. 45 AC.7 5 unix_chkpwd: Password check failed. 45 AC.7 5 unix_chkpwd: Password check failed. 43 AU.14 5 unix_chkpwd: Password check failed. 42 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container nginx_container 29 AU.14 5 Docker: Started shell session in container nginx_container 29 AC.7 8 Netscreen firewall: Successfull admin login 10 AC.7 8 Netscreen firewall: Successfull admin login 10 AC.7 8 Netscreen firewall: Successfull admin login 10 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 User successfull login to the router. 7 AC.7 3 User successfull login to the router. 7 AC.7 3 User successfull login to the router. 7 AC.7 3 User successfull login to the router. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 10 Courier bru	SI.4	5	sshd: Reverse lookup error (bad ISP or attack).	104
AU.14 5 sshd: Attempt to login using a non-existent user 93 AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 sshd: authentication failed. 45 AU.14 5 sshd: authentication failed. 45 AC.7 5 unix_chkpwd: Password check failed. 43 AC.7 5 unix_chkpwd: Password check failed. 43 AU.14 5 unix_chkpwd: Password check failed. 43 SI.4 10 sshd: Multiple authentication failures. 42 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successful admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 AC.7 3 Gisco IOS: Successful login to ror to ror or o	SI.4	8	sshd: Possible attack on the ssh server (or version gathering).	98
AC.7 5 Logon Failure - Unknown user or bad password 48 AC.7 5 sshd: authentication failed. 45 AU.14 5 sshd: authentication failed. 45 AU.14 5 sshd: authentication failed. 45 AC.7 5 unix_chkpwd: Password check failed. 43 AU.14 5 unix_chkpwd: Password check failed. 43 AU.14 5 unix_chkpwd: Password check failed. 43 SI.4 10 sshd: Multiple authentication failures. 42 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container ginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successfull ychanged UID. 7 AC.7 3 User successfully changed UID. 7 AC.7 10 Netscreen firewall: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6	AC.7	5	sshd: Attempt to login using a non-existent user	93
AC.7 5 sshd: authentication failed. 45 AU.14 5 sshd: authentication failed. 45 AU.14 5 sshd: authentication failed. 45 AC.7 5 unix_chkpwd: Password check failed. 43 AU.14 5 unix_chkpwd: Password check failed. 43 SI.4 10 sshd: Multiple authentication failures. 42 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 SI.4 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 3 Cisco IOS: Successfull login to the router. 7 AC.7 3 Cisco IOS: Successfull login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Netscreen firewall: Multiple attempts to send e-mail from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple attempts to send e-mail from black-listed IP address (blocked). 6	AU.14	5	sshd: Attempt to login using a non-existent user	93
AU.145sshd: authentication failed.45AC.75unix_chkpwd: Password check failed.43AU.145unix_chkpwd: Password check failed.43SI.410sshd: Multiple authentication failures.42AC.75PAM: User login failed.42AC.710sshd: Multiple authentication failures.42AU.145PAM: User login failed.42AU.1410sshd: Multiple authentication failures.42AU.1410sshd: brute force trying to get access to the system.38AC.710sshd: brute force trying to get access to the system.38AU.1410sshd: brute force trying to get access to the system.38AU.1410sshd: brute force trying to get access to the system.38AU.145Docker: Started shell session in container nginx_container29SI.46Postfix: Multiple relaying attempts of spam.10AC.78Netscreen firewall: Successfull admin login10SI.46Postfix: too many errors after RCPT from unknown8AC.73Imapel user login.8SI.410Sendmail: Multiple pre-greetings rejects.7SI.410Sendmail: Multiple pre-greetings rejects.7SI.48Interface entered in promiscuous(sniffing) mode.7AC.73Cisco IOS: Successfull login to the router.7AC.73User successfull login to the router.7	AC.7	5	Logon Failure - Unknown user or bad password	48
AC.7 5 unix_chkpwd: Password check failed. 43 AU.14 5 unix_chkpwd: Password check failed. 43 SI.4 10 sshd: Multiple authentication failures. 42 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 AU.14 10 sshd: Multiple authentication failures. 42 SI.4 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfull plagin to the router. 7 AC.7 3 User successfull plagin to the router. 7 AC.7 3 User successfull ychanged UID. 7 AU.14 10 Netscreen firewall: Multiple rejected e-mails from black-listed IP address (blocked). 6 SI.4 10 Netscreen firewall: Multiple rejected e-mails from black-listed IP address (blocked). 6	AC.7	5	sshd: authentication failed.	45
AU.145unix_chkpwd: Password check failed.435I.410sshd: Multiple authentication failures.42AC.75PAM: User login failed.42AC.710sshd: Multiple authentication failures.42AU.145PAM: User login failed.42AU.1410sshd: Multiple authentication failures.42SI.410sshd: brute force trying to get access to the system.38AC.710sshd: brute force trying to get access to the system.38AU.1410sshd: brute force trying to get access to the system.38AU.1410sshd: brute force trying to get access to the system.38AU.145Docker: Started shell session in container nginx_container29SI.46Postfix: Multiple relaying attempts of spam.10AC.78Netscreen firewall: Successfull admin login10SI.46Postfix: too many errors after RCPT from unknown8AC.73Imapd user login.8SI.410Courier brute force (multiple failed logins).7SI.410Sendmait: Multiple pre-greetings rejects.7SI.48Interface entered in promiscuous(sniffing) mode.7AC.73Cisco IOS: Successful login to the router.7AC.73Cisco IOS: Successful login to the router.7AC.73User successfully changed UID.7AU.1410Courier brute force (multiple failed l	AU.14	5	sshd: authentication failed.	45
SI.4 10 sshd: Multiple authentication failures. 42 AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 SI.4 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container and proper started shell se	AC.7	5	unix_chkpwd: Password check failed.	43
AC.7 5 PAM: User login failed. 42 AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 SI.4 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 postfix: Multiple relaying attempts of span. 10 SI.4 6 Postfix: Multiple failed logins). 7 SI.4 <td>AU.14</td> <td>5</td> <td>unix_chkpwd: Password check failed.</td> <td>43</td>	AU.14	5	unix_chkpwd: Password check failed.	43
AC.7 10 sshd: Multiple authentication failures. 42 AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 SI.4 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 Sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 3 Cisco IOS: Successfull login to the router. 7 AC.7	SI.4	10	sshd: Multiple authentication failures.	42
AU.14 5 PAM: User login failed. 42 AU.14 10 sshd: Multiple authentication failures. 42 SI.4 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imaped user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 Courier brute force (multiple failed logins). 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3	AC.7	5	PAM: User login failed.	42
AU.14 10 sshd: Multiple authentication failures. 42 SI.4 10 sshd: brute force trying to get access to the system. 38 AC.7 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 10 sshd: brute force trying to get access to the system. 38 AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 User successfull login to the router. 7 AC.7 3 User successfull login to the router. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AC.7	10	sshd: Multiple authentication failures.	42
SI.410sshd: brute force trying to get access to the system.38AC.710sshd: brute force trying to get access to the system.38AU.1410sshd: brute force trying to get access to the system.38AU.145Docker: Started shell session in container nginx_container29SI.46Postfix: Multiple relaying attempts of spam.10AC.78Netscreen firewall: Successfull admin login10SI.46Postfix: too many errors after RCPT from unknown8AC.73Imapd user login.8SI.410Courier brute force (multiple failed logins).7SI.410sendmail: Multiple pre-greetings rejects.7SI.48Interface entered in promiscuous(sniffing) mode.7AC.73Cisco IOS: Successful login to the router.7AC.73User successfully changed UID.7AU.1410Courier brute force (multiple failed logins).7SI.410Netscreen firewall: Multiple aritempts to send e-mail from black-listed IP address (blocked).6SI.410sendmail: Multiple attempts to send e-mail from black-listed IP address (blocked).6SI.410sendmail: Multiple rejected e-mails from same source ip.6	AU.14	5	PAM: User login failed.	42
AC.7 10 sshd: brute force trying to get access to the system. AU.14 10 sshd: brute force trying to get access to the system. AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relegying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 User successfull ogin to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip.	AU.14	10	sshd: Multiple authentication failures.	42
AU.14 10 sshd: brute force trying to get access to the system. AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 User successfull ogin to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip.	SI.4	10	sshd: brute force trying to get access to the system.	38
AU.14 5 Docker: Started shell session in container nginx_container 29 SI.4 6 Postfix: Multiple relaying attempts of spam. 10 AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 User successfull login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple rejiected logins). 7 SI.4 10 Netscreen firewall: Multiple rotical messages from same source IP. 6 SI.4 10 Sendmail: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AC.7	10	sshd: brute force trying to get access to the system.	38
SI.46Postfix: Multiple relaying attempts of spam.10AC.78Netscreen firewall: Successfull admin login10SI.46Postfix: too many errors after RCPT from unknown8AC.73Imapd user login.8SI.410Courier brute force (multiple failed logins).7SI.410sendmail: Multiple pre-greetings rejects.7SI.48Interface entered in promiscuous(sniffing) mode.7AC.710Courier brute force (multiple failed logins).7AC.73Cisco IOS: Successful login to the router.7AC.73User successfully changed UID.7AU.1410Courier brute force (multiple failed logins).7SI.410Netscreen firewall: Multiple afiled messages from same source IP.6SI.410Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).6SI.410sendmail: Multiple rejected e-mails from same source ip.6	AU.14	10	sshd: brute force trying to get access to the system.	38
AC.7 8 Netscreen firewall: Successfull admin login 10 SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AU.14	5	Docker: Started shell session in container nginx_container	29
SI.4 6 Postfix: too many errors after RCPT from unknown 8 AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	SI.4	6	Postfix: Multiple relaying attempts of spam.	10
AC.7 3 Imapd user login. 8 SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AC.7	8	Netscreen firewall: Successfull admin login	10
SI.4 10 Courier brute force (multiple failed logins). 7 SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	SI.4	6	Postfix: too many errors after RCPT from unknown	8
SI.4 10 sendmail: Multiple pre-greetings rejects. 7 SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AC.7	3	Imapd user login.	8
SI.4 8 Interface entered in promiscuous(sniffing) mode. 7 AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	SI.4	10	Courier brute force (multiple failed logins).	7
AC.7 10 Courier brute force (multiple failed logins). 7 AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	SI.4	10	sendmail: Multiple pre-greetings rejects.	7
AC.7 3 Cisco IOS: Successful login to the router. 7 AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	SI.4	8	Interface entered in promiscuous(sniffing) mode.	7
AC.7 3 User successfully changed UID. 7 AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AC.7	10	Courier brute force (multiple failed logins).	7
AU.14 10 Courier brute force (multiple failed logins). 7 SI.4 10 Netscreen firewall: Multiple critical messages from same source IP. 6 SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AC.7	3	Cisco IOS: Successful login to the router.	7
SI.410Netscreen firewall: Multiple critical messages from same source IP.6SI.410Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).6SI.410sendmail: Multiple rejected e-mails from same source ip.6	AC.7	3	User successfully changed UID.	7
SI.4 10 Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked). 6 SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	AU.14	10	Courier brute force (multiple failed logins).	7
SI.4 10 sendmail: Multiple rejected e-mails from same source ip. 6	SI.4	10	Netscreen firewall: Multiple critical messages from same source IP.	6
	SI.4	10	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	6
SI.4 6 Postfix: Rejected by access list (Requested action not taken). 6	SI.4	10	sendmail: Multiple rejected e-mails from same source ip.	6
	SI.4	6	Postfix: Rejected by access list (Requested action not taken).	6



Requirement	Level	Description	Count
SI.4	6	sendmail: Multiple attempts to send e-mail from a previously rejected sender (access).	6
AC.7	3	SonicWall: Firewall administrator login.	6
AC.7	3	User successfully changed UID to root.	6
SI.4	10	Courier: Multiple connection attempts from same source.	5
SI.4	10	sendmail: Sender domain has bogus MX record. It should not be sending e-mail.	5
SI.4	5	sendmail: Sender domain does not have any valid MX record (Requested action aborted).	5
SI.4	6	Postfix: IP Address black-listed by anti-spam (blocked).	5
SI.4	6	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	5
SI.4	6	sendmail: Attempt to use mail server as relay (550: Requested action not taken).	5
SI.4	6	sendmail: Sendmail rejected due to pre-greeting.	5
SI.4	8	Log file size reduced.	5
AC.7	3	PIX: AAA (VPN) authentication successful.	5
SI.4	10	sshd: Possible scan or breakin attempt (high number of login timeouts).	4
SI.4	5	Postfix: Sender domain is not found (450: Requested mail action not taken).	4
SI.4	5	sendmail: Sender domain is not found (553: Requested action not taken).	4
SI.4	6	sendmail: Multiple relaying attempts of spam.	4
SI.4	6	sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).	4
AC.7	10	syslog: User missed the password more than one time	4
AC.7	9	User missed the password to change UID to root.	4
AU.14	10	syslog: User missed the password more than one time	4
SI.4	10	PAM: Multiple failed logins in a small period of time.	3
SI.4	10	PIX: Multiple AAA (VPN) authentication failures.	3
SI.4	10	Postfix: Multiple attempts to send e-mail from invalid/unknown sender domain.	3
SI.4	10	sendmail: Multiple attempts to send e-mail from invalid/unknown sender.	3
SI.4	12	Postfix: Multiple misuse of SMTP service (bad sequence of commands).	3
AC.7	5	syslog: Connection blocked by Tcp Wrappers.	3
AC.7	10	PAM: Multiple failed logins in a small period of time.	3
AC.7	10	PIX: Multiple AAA (VPN) authentication failures.	3
AC.7	3	Courier (imap/pop3) authentication success.	3
AC.7	3	PAM: Login session opened.	3
AC.7	9	syslog: Illegal root login.	3
AU.14	5	syslog: Connection blocked by Tcp Wrappers.	3
AU.14	10	PAM: Multiple failed logins in a small period of time.	3
AU.14	10	PIX: Multiple AAA (VPN) authentication failures.	3
SI.4	10	Imapd Multiple failed logins from same source ip.	2
SI.4	10	sendmail: Multiple attempts to send e-mail from invalid/unknown sender domain.	2
SI.4	5	Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).	2
SI.4	5	sendmail: Sender address does not have domain (553: Requested action not taken).	2
SI.4	6	Postfix: Attempt to use mail server as relay (client host rejected).	2
SI.4	6	Postfix: Illegal address from unknown sender	2
SI.4	6	Postfix: RBL lookup error: Host or domain name not found	2



Requirement	Level	Description	Count
SI.4	6	Postfix: hostname verification failed	2
AC.7	5	Failed attempt to run sudo.	2
AC.7	5	Unauthorized user attempted to use sudo.	2
AC.7	10	Imapd Multiple failed logins from same source ip.	2
AC.7	3	PIX: Successful login.	2
AC.7	8	PIX: User created or modified on the Firewall.	2
AU.14	5	Failed attempt to run sudo.	2
AU.14	5	Unauthorized user attempted to use sudo.	2
AU.14	10	Imapd Multiple failed logins from same source ip.	2
SI.4	10	Postfix: Multiple SASL authentication failures.	1
SI.4	10	Postfix: Multiple attempts to send e-mail to invalid recipient or from unknown sender domain.	1
SI.4	5	Postfix: Improper use of SMTP command pipelining (503: Bad sequence of commands).	1
SI.4	6	sendmail: Rejected by access list (55x: Requested action not taken).	1
AC.7	10	Postfix: Multiple SASL authentication failures.	1
AC.7	10	Three failed attempts to run sudo	1
AC.7	3	Successful sudo to ROOT executed.	1
AC.7	8	PIX: AAA (VPN) user locked out.	1
AU.14	10	Postfix: Multiple SASL authentication failures.	1
AU.14	10	Three failed attempts to run sudo	1