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

NIST 800-53 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 @ 15:39:09.000

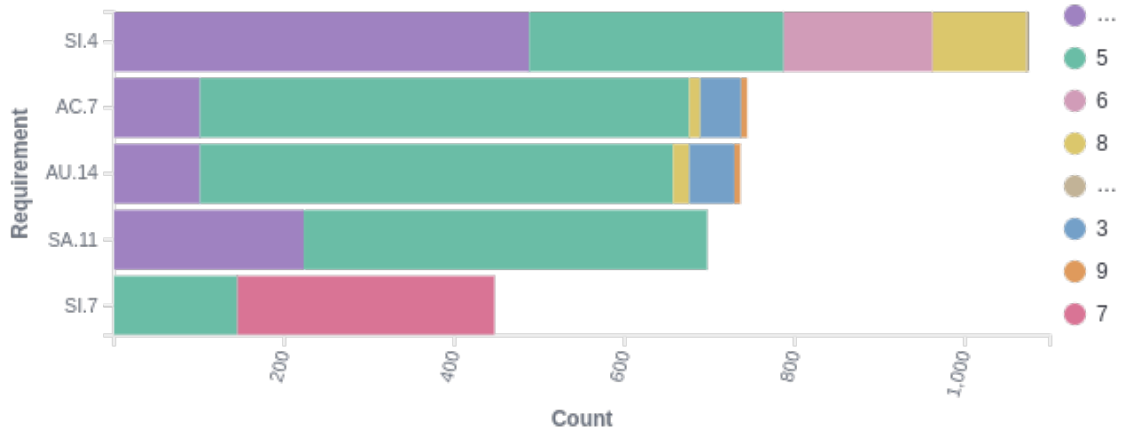
Group: default

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

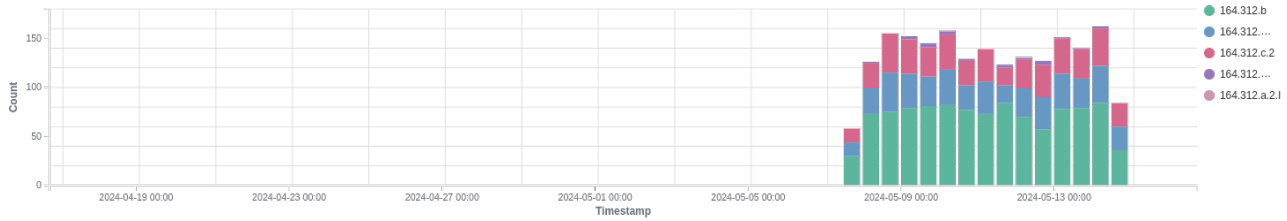
2024-04-16T17:39:15 to 2024-05-16T17:39:15

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

Requirements distributed by level



Requirements over time

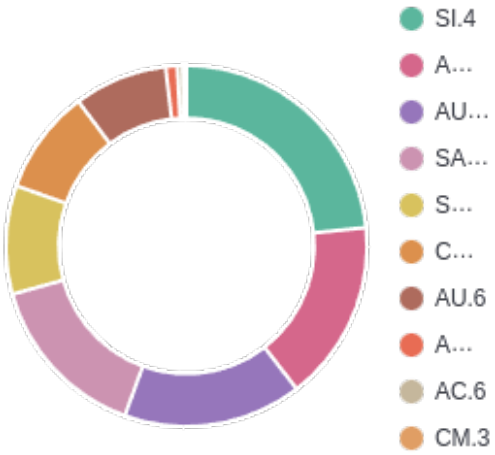


Stats

2,862
Total alerts

12
Max rule level

Top 10 requirements



Alerts summary

Requirement	Level	Description	Count
AC.7	5	Apache: Attempt to access forbidden directory index.	297
AU.14	5	Apache: Attempt to access forbidden directory index.	297
SI.4	10	Multiple web server 400 error codes from same source ip.	223
SI.4	5	Web server 400 error code.	177
SI.4	10	sshd: Possible breakin attempt (high number of reverse lookup errors).	121
SI.4	6	sshd: insecure connection attempt (scan).	108
SI.4	5	sshd: Reverse lookup error (bad ISP or attack).	104
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
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	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	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: 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