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

TSC 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 @ 15:46:39.000

Group: default

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

2024-04-16T17:46:43 to 2024-05-16T17:46:43

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

Most common TSC requirements alerts found

Requirement CC7.1

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

- Uses Defined Configuration Standards
- Monitors Infrastructure and Software
- Implements Change-Detection Mechanisms
- Detects Unknown or Unauthorized Components
- Conducts Vulnerability Scans

Top rules for CC7.1 requirement

Rule ID	Description
23503	CVE-2013-4235 affects login
23505	CVE-2020-1747 affects python3-yaml
23504	CVE-2020-1927 affects apache2

Requirement CC6.1

The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's

Copyright © 2023 Wazuh, Inc.

objectives.

- Identifies and Manages the Inventory of Information Assets
- Restricts Logical Access
- Identifies and Authenticates Users
- Considers Network Segmentation
- Manages Points of Access
- Restricts Access to Information Assets
- Manages Identification and Authentication
- Manages Credentials for Infrastructure and Software
- Uses Encryption to Protect Data
- Protects Encryption Keys

Top rules for CC6.1 requirement

Rule ID	Description
3351	Postfix: Multiple relaying attempts of spam.
3335	Postfix: too many errors after RCPT from unknown
3910	Courier brute force (multiple failed logins).

Requirement CC7.2

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

- Implements Detection Policies, Procedures, and Tools
- Designs Detection Measures
- Implements Filters to Analyze Anomalies
- Monitors Detection Tools for Effective Operation

Top rules for CC7.2 requirement

Rule ID	Description
23503	CVE-2013-4235 affects login
23505	CVE-2020-1747 affects python3-yaml
23504	CVE-2020-1927 affects apache2

Requirement CC7.3

Copyright © 2023 Wazuh, Inc.

The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

- Responds to Security Incidents
- Communicates and Reviews Detected Security Events
- Develops and Implements Procedures to Analyze Security Incidents

Top rules for CC7.3 requirement

Rule ID	Description
4507	Netscreen firewall: Successfull admin login
3351	Postfix: Multiple relaying attempts of spam.
3602	Imapd user login.

Requirement CC6.8

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

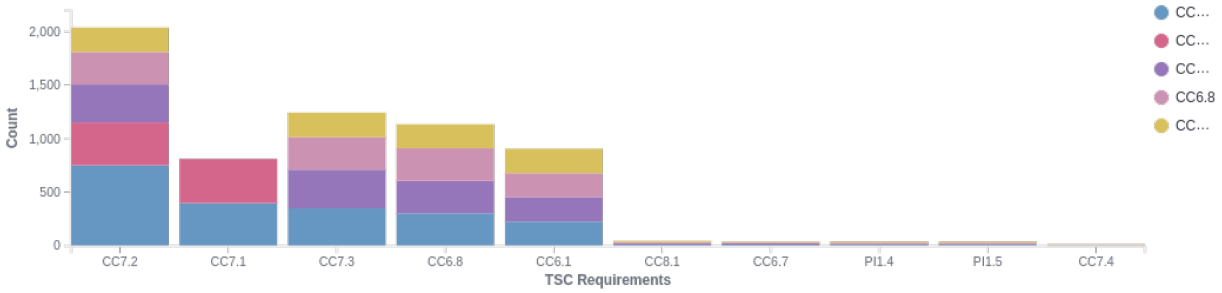
- Restricts Application and Software Installation
- Detects Unauthorized Changes to Software and Configuration Parameters
- Uses a Defined Change Control Process
- Uses Antivirus and Anti-Malware Software
- Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software

Top rules for CC6.8 requirement

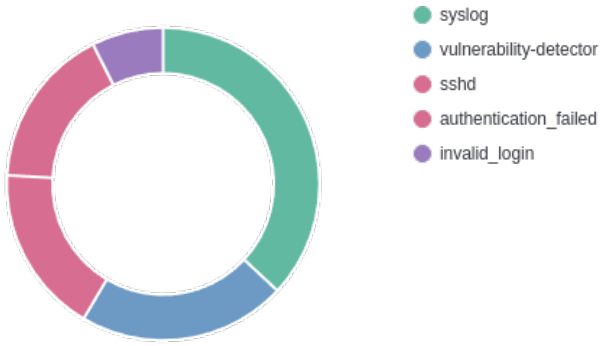
Rule ID	Description
4507	Netscreen firewall: Successfull admin login
3351	Postfix: Multiple relaying attempts of spam.
3602	Imapd user login.

Copyright © 2023 Wazuh, Inc.

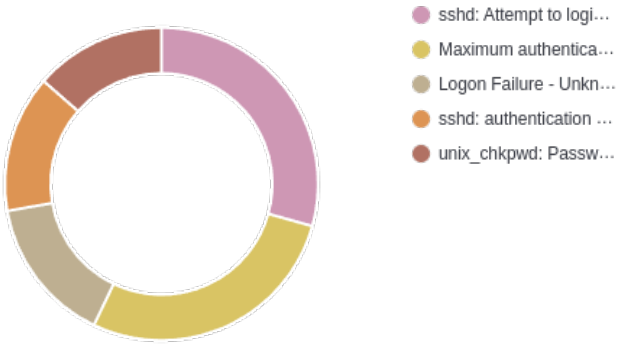
TSC Requirements



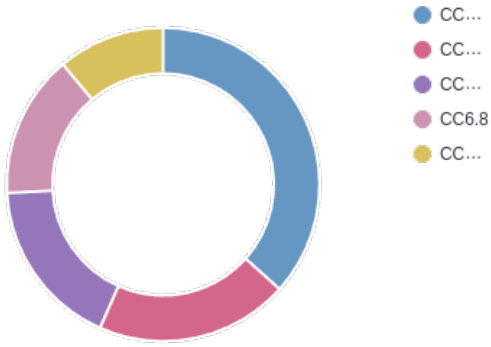
Top 5 rule groups



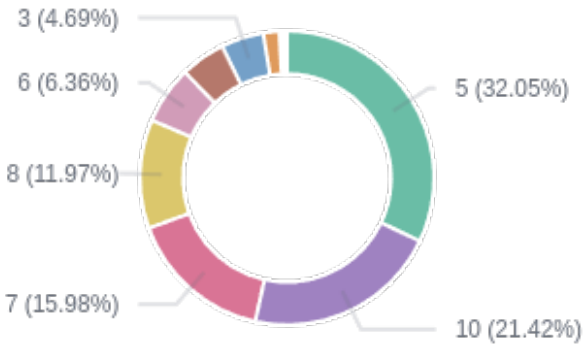
Top 5 rules



Top 5 TSC requirements



Rule level distribution



Copyright © 2023 Wazuh, Inc.

Alerts summary

Agent name	Requirement	Description	Count
Amazon	CC7.2	CVE-2013-4235 affects login	14
Amazon	CC7.2	CVE-2020-1747 affects python3-yaml	14
Amazon	CC7.2	CVE-2020-1927 affects apache2	14
Amazon	CC7.1	CVE-2013-4235 affects login	14
Amazon	CC7.1	CVE-2020-1747 affects python3-yaml	14
Amazon	CC7.1	CVE-2020-1927 affects apache2	14
Amazon	CC7.2	CVE-2019-1552 affects openssl	13
Amazon	CC7.1	CVE-2019-1552 affects openssl	13
Amazon	CC7.2	CVE-2015-2987 affects ed	12
Amazon	CC7.1	CVE-2015-2987 affects ed	12
Amazon	CC7.2	CVE-2018-1000035 affects unzip	11
Amazon	CC7.2	CVE-2018-15919 affects openssh-client	11
Amazon	CC7.2	CVE-2019-1003010 affects git	11
Amazon	CC7.1	CVE-2018-1000035 affects unzip	11
Amazon	CC7.1	CVE-2018-15919 affects openssh-client	11
Amazon	CC7.1	CVE-2019-1003010 affects git	11
Amazon	CC7.2	CVE-2013-4235 affects passwd	10
Amazon	CC7.2	CVE-2016-4484 affects cryptsetup	10
Amazon	CC7.2	CVE-2017-18018 affects coreutils	10
Amazon	CC7.2	CVE-2018-20217 affects libkrb5-3	10
Amazon	CC7.2	CVE-2019-19645 affects sqlite3	10
Amazon	CC7.2	CVE-2020-1927 affects apache2-data	10
Amazon	CC7.2	Netscreen firewall: Successfull admin login	10
Amazon	CC7.2	Postfix: Multiple relaying attempts of spam.	10
Amazon	CC7.1	CVE-2013-4235 affects passwd	10
Amazon	CC7.1	CVE-2016-4484 affects cryptsetup	10
Amazon	CC7.1	CVE-2017-18018 affects coreutils	10
Amazon	CC7.1	CVE-2018-20217 affects libkrb5-3	10
Amazon	CC7.1	CVE-2019-19645 affects sqlite3	10
Amazon	CC7.1	CVE-2020-1927 affects apache2-data	10
Amazon	CC7.3	Netscreen firewall: Successfull admin login	10
Amazon	CC7.3	Postfix: Multiple relaying attempts of spam.	10
Amazon	CC6.8	Netscreen firewall: Successfull admin login	10
Amazon	CC6.8	Postfix: Multiple relaying attempts of spam.	10
Amazon	CC6.1	Postfix: Multiple relaying attempts of spam.	10
Amazon	CC7.2	CVE-2019-18684 affects sudo	9
Amazon	CC7.2	CVE-2019-9169 affects libc6	9
Amazon	CC7.1	CVE-2019-18684 affects sudo	9
Amazon	CC7.1	CVE-2019-9169 affects libc6	9

Copyright © 2023 Wazuh, Inc.

Agent name	Requirement	Description	Count
Amazon	CC7.2	CVE-2017-12588 affects rsyslog	8
Amazon	CC7.2	CVE-2017-15088 affects krb5-locales	8
Amazon	CC7.1	CVE-2017-12588 affects rsyslog	8
Amazon	CC7.1	CVE-2017-15088 affects krb5-locales	8
Amazon	CC7.1	CVE-2017-15994 affects rsync	8
Amazon	CC7.1	CVE-2018-14036 affects accountsservice	8
Amazon	CC7.3	Imapd user login.	8
Amazon	CC7.3	Postfix: too many errors after RCPT from unknown	8
Amazon	CC6.8	Imapd user login.	8
Amazon	CC6.8	Postfix: too many errors after RCPT from unknown	8
Amazon	CC6.1	Postfix: too many errors after RCPT from unknown	8
Amazon	CC7.3	Cisco IOS: Successful login to the router.	7
Amazon	CC7.3	Courier brute force (multiple failed logins).	7
Amazon	CC7.3	Interface entered in promiscuous(sniffing) mode.	7
Amazon	CC7.3	PIX: Firewall configuration changed.	7
Amazon	CC7.3	User successfully changed UID.	7
Amazon	CC7.3	sendmail: Multiple pre-greetings rejects.	7
Amazon	CC6.8	Cisco IOS: Successful login to the router.	7
Amazon	CC6.8	Courier brute force (multiple failed logins).	7
Amazon	CC6.8	Interface entered in promiscuous(sniffing) mode.	7
Amazon	CC6.8	PIX: Firewall configuration changed.	7
Amazon	CC6.8	User successfully changed UID.	7
Amazon	CC6.8	sendmail: Multiple pre-greetings rejects.	7
Amazon	CC6.1	Courier brute force (multiple failed logins).	7
Amazon	CC6.1	Interface entered in promiscuous(sniffing) mode.	7
Amazon	CC6.1	PIX: Firewall configuration changed.	7
Amazon	CC6.1	sendmail: Multiple pre-greetings rejects.	7
Amazon	CC7.3	Netscreen firewall: Multiple critical messages from same source IP.	6
Amazon	CC7.3	Postfix process error.	6
Amazon	CC7.3	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	6
Amazon	CC7.3	Postfix: Rejected by access list (Requested action not taken).	6
Amazon	CC7.3	Root's crontab entry changed.	6
Amazon	CC7.3	SonicWall: Firewall administrator login.	6
Amazon	CC7.3	SonicWall: Multiple firewall error messages.	6
Amazon	CC7.3	User successfully changed UID to root.	6
Amazon	CC7.3	sendmail: Multiple attempts to send e-mail from a previously rejected sender (access).	6
Amazon	CC7.3	sendmail: Multiple rejected e-mails from same source ip.	6
Amazon	CC6.8	Netscreen firewall: Multiple critical messages from same source IP.	6
Amazon	CC6.8	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	6
Amazon	CC6.8	Postfix: Rejected by access list (Requested action not taken).	6
Amazon	CC6.8	Root's crontab entry changed.	6

Copyright © 2023 Wazuh, Inc.

Agent name	Requirement	Description	Count
Amazon	CC6.8	SonicWall: Firewall administrator login.	6
Amazon	CC6.8	User successfully changed UID to root.	6
Amazon	CC6.8	sendmail: Multiple attempts to send e-mail from a previously rejected sender (access).	6
Amazon	CC6.8	sendmail: Multiple rejected e-mails from same source ip.	6
Amazon	CC6.8	sshd: Possible breakin attempt (high number of reverse lookup errors).	6
Amazon	CC6.8	sshd: insecure connection attempt (scan).	6
Amazon	CC6.1	Netscreen firewall: Multiple critical messages from same source IP.	6
Amazon	CC6.1	Postfix: Multiple attempts to send e-mail from black-listed IP address (blocked).	6
Amazon	CC6.1	Postfix: Rejected by access list (Requested action not taken).	6
Amazon	CC6.1	sendmail: Multiple attempts to send e-mail from a previously rejected sender (access).	6
Amazon	CC6.1	sendmail: Multiple rejected e-mails from same source ip.	6
Amazon	CC6.1	sshd: Possible breakin attempt (high number of reverse lookup errors).	6
Amazon	CC6.1	sshd: insecure connection attempt (scan).	6
Amazon	CC6.1	Courier: Multiple connection attempts from same source.	5
Amazon	CC6.1	Log file size reduced.	5
Amazon	CC6.1	Microsoft Event log cleared.	5
Amazon	CC6.1	PIX: Firewall configuration deleted.	5
Amazon	CC6.1	Postfix: IP Address black-listed by anti-spam (blocked).	5
Amazon	CC6.1	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	5

Copyright © 2023 Wazuh, Inc.