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

TSC report

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

2024-04-16T17:40:34 to 2024-05-16T17:40:34

rule.tsc: * AND cluster.name: wazuh

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-2018-1000035 affects unzip
23505	CVE-2020-1747 affects python3-yaml

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 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
593	Microsoft Event log cleared.
3158	sendmail: Multiple pre-greetings rejects.
3104	sendmail: Attempt to use mail server as relay (550: Requested action not taken).

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-2018-1000035 affects unzip
23505	CVE-2020-1747 affects python3-yaml

Requirement CC7.3

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
4506	Netscreen firewall: Successfull admin login
4722	Cisco IOS: Successful login to the router.
4335	PIX: AAA (VPN) authentication successful.

Requirement CC6.8

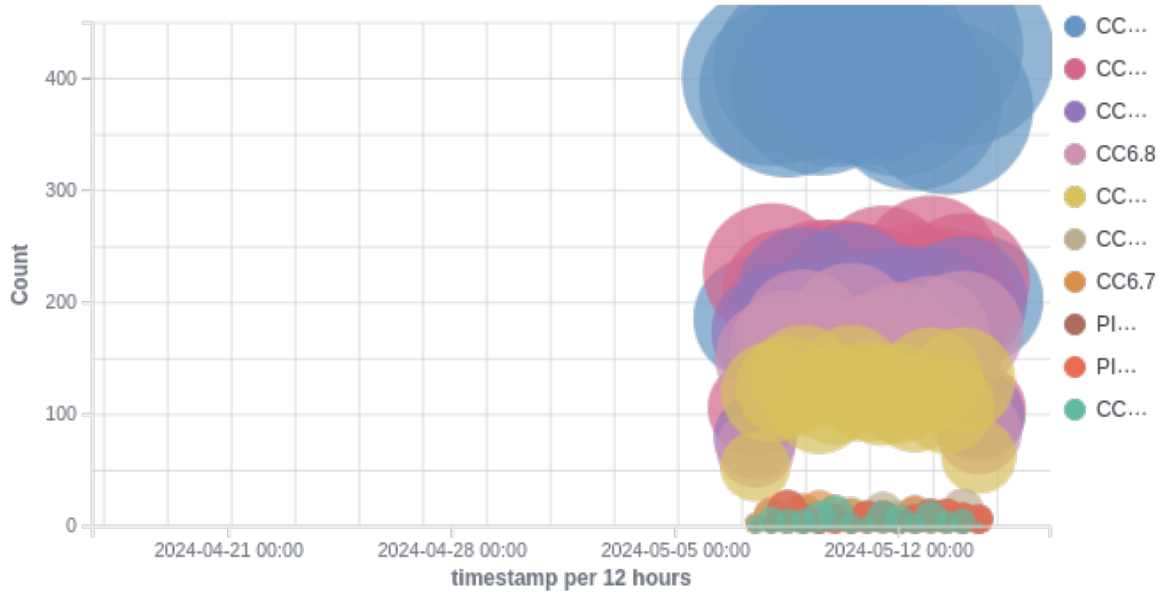
The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

- 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

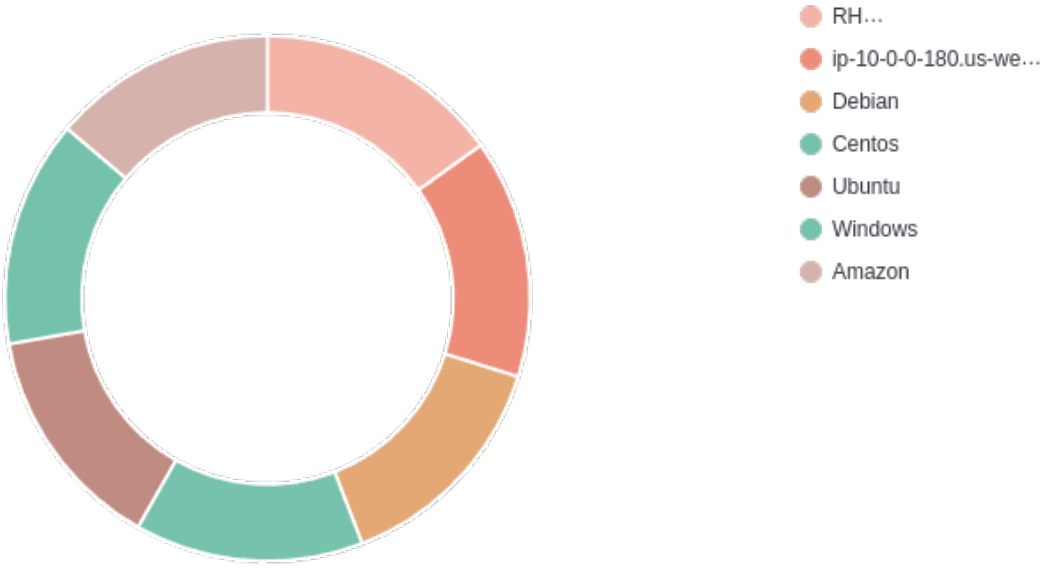
Top rules for CC6.8 requirement

Rule ID	Description
4506	Netscreen firewall: Successfull admin login
4722	Cisco IOS: Successful login to the router.
4335	PIX: AAA (VPN) authentication successful.

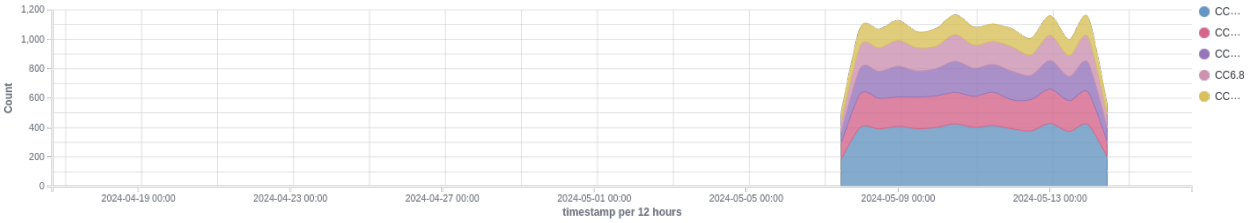
TSC requirements



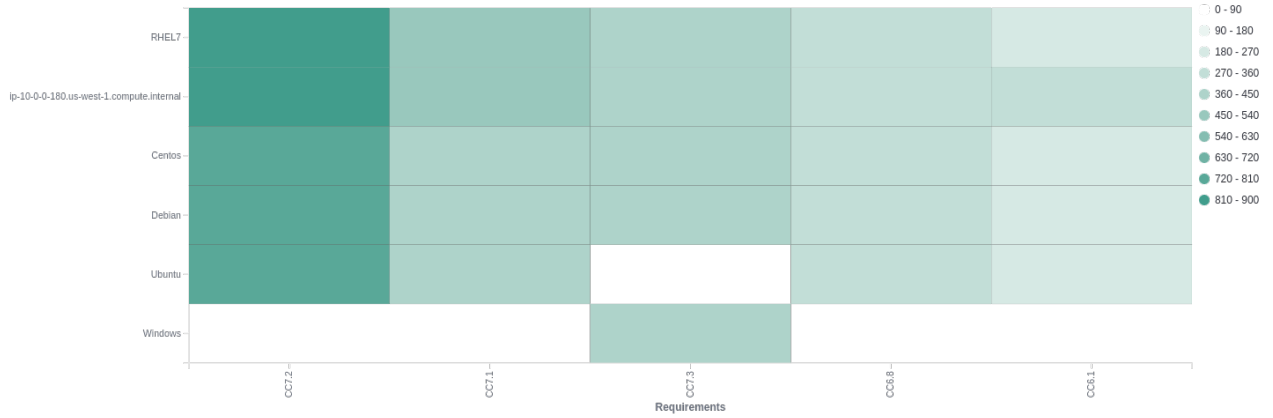
Top 10 agents by alerts number



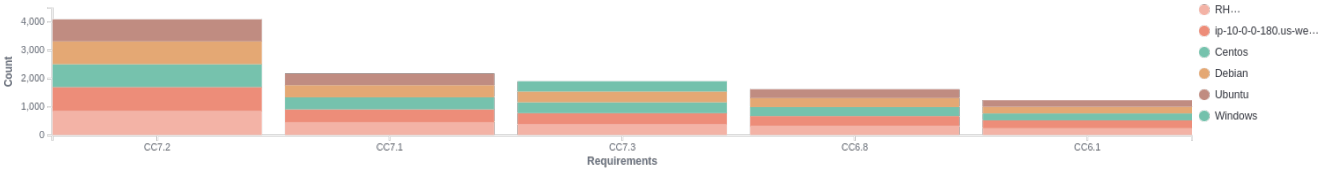
Top requirements over time



Last alerts



Requirements by agent



Alerts summary

Agent name	Requirement	Description	Count
RHEL7	CC7.2	CVE-2018-1000035 affects unzip	21
RHEL7	CC7.1	CVE-2018-1000035 affects unzip	21
RHEL7	CC7.2	CVE-2013-4235 affects login	19
RHEL7	CC7.1	CVE-2013-4235 affects login	19
RHEL7	CC7.2	CVE-2018-6485 affects libc-bin	14
RHEL7	CC7.2	CVE-2020-1747 affects python3-yaml	14
RHEL7	CC7.1	CVE-2018-6485 affects libc-bin	14
RHEL7	CC7.1	CVE-2020-1747 affects python3-yaml	14
RHEL7	CC7.2	CVE-2018-20482 affects tar	13
RHEL7	CC7.1	CVE-2018-20482 affects tar	13
RHEL7	CC7.2	CVE-2020-1927 affects apache2-bin	12
RHEL7	CC7.1	CVE-2020-1927 affects apache2-bin	12
RHEL7	CC7.2	CVE-2016-4484 affects cryptsetup	11
RHEL7	CC7.2	CVE-2017-12588 affects rsyslog	11
RHEL7	CC7.2	CVE-2017-15994 affects rsync	11
RHEL7	CC7.2	CVE-2017-18018 affects coreutils	11
RHEL7	CC7.2	CVE-2020-1752 affects multiarch-support	11
RHEL7	CC7.2	Postfix: hostname verification failed	11
RHEL7	CC7.1	CVE-2016-4484 affects cryptsetup	11
RHEL7	CC7.1	CVE-2017-12588 affects rsyslog	11
RHEL7	CC7.1	CVE-2017-15994 affects rsync	11
RHEL7	CC7.1	CVE-2017-18018 affects coreutils	11
RHEL7	CC7.1	CVE-2020-1752 affects multiarch-support	11
RHEL7	CC7.3	Postfix: hostname verification failed	11
RHEL7	CC6.8	Postfix: hostname verification failed	11
RHEL7	CC6.1	Postfix: hostname verification failed	11
RHEL7	CC7.2	CVE-2016-7948 affects libxrandr2	10
RHEL7	CC7.2	CVE-2017-18342 affects python3-yaml	10
RHEL7	CC7.2	CVE-2017-7244 affects libpcre3	10
RHEL7	CC7.2	CVE-2019-18684 affects sudo	10
RHEL7	CC7.2	Netscreen firewall: Successfull admin login	10
RHEL7	CC7.2	sendmail: Multiple pre-greetings rejects.	10
RHEL7	CC7.2	sshd: insecure connection attempt (scan).	10
RHEL7	CC7.1	CVE-2016-7948 affects libxrandr2	10
RHEL7	CC7.1	CVE-2017-18342 affects python3-yaml	10
RHEL7	CC7.1	CVE-2017-7244 affects libpcre3	10
RHEL7	CC7.1	CVE-2019-18684 affects sudo	10
RHEL7	CC7.3	Netscreen firewall: Successfull admin login	10
RHEL7	CC7.3	sendmail: Multiple pre-greetings rejects.	10

Agent name	Requirement	Description	Count
RHEL7	CC7.3	sshd: insecure connection attempt (scan).	10
RHEL7	CC6.8	Netscreen firewall: Successfull admin login	10
RHEL7	CC6.8	sendmail: Multiple pre-greetings rejects.	10
RHEL7	CC6.8	sshd: insecure connection attempt (scan).	10
RHEL7	CC6.1	sendmail: Multiple pre-greetings rejects.	10
RHEL7	CC6.1	sshd: insecure connection attempt (scan).	10
RHEL7	CC7.2	CVE-2013-4235 affects passwd	9
RHEL7	CC7.1	CVE-2013-4235 affects passwd	9
RHEL7	CC7.1	CVE-2016-7947 affects libxrandr2	9
RHEL7	CC7.1	CVE-2017-15088 affects krb5-locales	9
RHEL7	CC7.1	CVE-2020-1927 affects apache2	9
RHEL7	CC7.3	Courier brute force (multiple failed logins).	9
RHEL7	CC7.3	PAM: Multiple failed logins in a small period of time.	9
RHEL7	CC6.8	Courier brute force (multiple failed logins).	9
RHEL7	CC6.8	PAM: Multiple failed logins in a small period of time.	9
RHEL7	CC6.1	Courier brute force (multiple failed logins).	9
RHEL7	CC6.1	PAM: Multiple failed logins in a small period of time.	9
RHEL7	CC7.1	CVE-2019-1003010 affects git	8
RHEL7	CC7.3	Ossec agent disconnected.	8
RHEL7	CC7.3	Postfix: RBL lookup error: Host or domain name not found	8
RHEL7	CC7.3	SonicWall: Firewall administrator login.	8
RHEL7	CC7.3	User missed the password to change UID to root.	8
RHEL7	CC7.3	sendmail: Multiple relaying attempts of spam.	8
RHEL7	CC6.8	Ossec agent disconnected.	8
RHEL7	CC6.8	Postfix: RBL lookup error: Host or domain name not found	8
RHEL7	CC6.8	SonicWall: Firewall administrator login.	8
RHEL7	CC6.8	User missed the password to change UID to root.	8
RHEL7	CC6.8	sendmail: Multiple relaying attempts of spam.	8
RHEL7	CC6.1	Postfix: RBL lookup error: Host or domain name not found	8
RHEL7	CC6.1	User missed the password to change UID to root.	8
RHEL7	CC6.1	sendmail: Multiple relaying attempts of spam.	8
RHEL7	CC7.3	Connection to rshd from unprivileged port. Possible network scan.	7
RHEL7	CC7.3	Failed attempt to run sudo.	7
RHEL7	CC7.3	sendmail: Multiple attempts to send e-mail from invalid/unknown sender domain.	7
RHEL7	CC7.3	xinetd: Excessive number connections to a service.	7
RHEL7	CC6.8	Failed attempt to run sudo.	7
RHEL7	CC6.8	sendmail: Multiple attempts to send e-mail from invalid/unknown sender domain.	7
RHEL7	CC6.1	Failed attempt to run sudo.	7
RHEL7	CC6.1	sendmail: Multiple attempts to send e-mail from invalid/unknown sender domain.	7
RHEL7	CC7.3	Courier: Multiple connection attempts from same source.	6
RHEL7	CC7.3	Imapd Multiple failed logins from same source ip.	6

Agent name	Requirement	Description	Count
RHEL7	CC7.3	PIX: ARP collision detected.	6
RHEL7	CC7.3	PIX: The PIX is disallowing new connections.	6
RHEL7	CC7.3	Postfix: IP Address black-listed by anti-spam (blocked).	6
RHEL7	CC6.8	Courier: Multiple connection attempts from same source.	6
RHEL7	CC6.8	Imapd Multiple failed logins from same source ip.	6
RHEL7	CC6.8	Postfix: IP Address black-listed by anti-spam (blocked).	6
RHEL7	CC6.8	Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).	6
RHEL7	CC6.8	Registry Entry Deleted.	6
RHEL7	CC6.8	Successful sudo to ROOT executed.	6
RHEL7	CC6.8	sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).	6
RHEL7	CC6.1	Courier: Multiple connection attempts from same source.	6
RHEL7	CC6.1	Imapd Multiple failed logins from same source ip.	6
RHEL7	CC6.1	Postfix: IP Address black-listed by anti-spam (blocked).	6
RHEL7	CC6.1	Postfix: Recipient address must contain FQDN (504: Command parameter not implemented).	6
RHEL7	CC6.1	Registry Entry Deleted.	6
RHEL7	CC6.1	sendmail: SMF-SAV sendmail milter unable to verify address (REJECTED).	6
RHEL7	CC6.1	Microsoft Event log cleared.	5
RHEL7	CC6.1	Postfix: Multiple attempts to send e-mail from a rejected sender IP (access).	5
RHEL7	CC6.1	Postfix: Multiple relaying attempts of spam.	5