iletisim@ihsteknoloji.com
www.ihsteknoloji.com

TSC report

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

2025-04-06T16:35:21 to 2025-04-11T16:35:21

manager.name: wazuh-server AND rule.tsc: *

Most common TSC requirements alerts found

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
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
12108	Query cache denied (probably config error).

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
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
31509	CMS (WordPress or Joomla) login attempt.

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
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
12108	Query cache denied (probably config error).

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
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
12108	Query cache denied (probably config error).

Requirement CC6.8

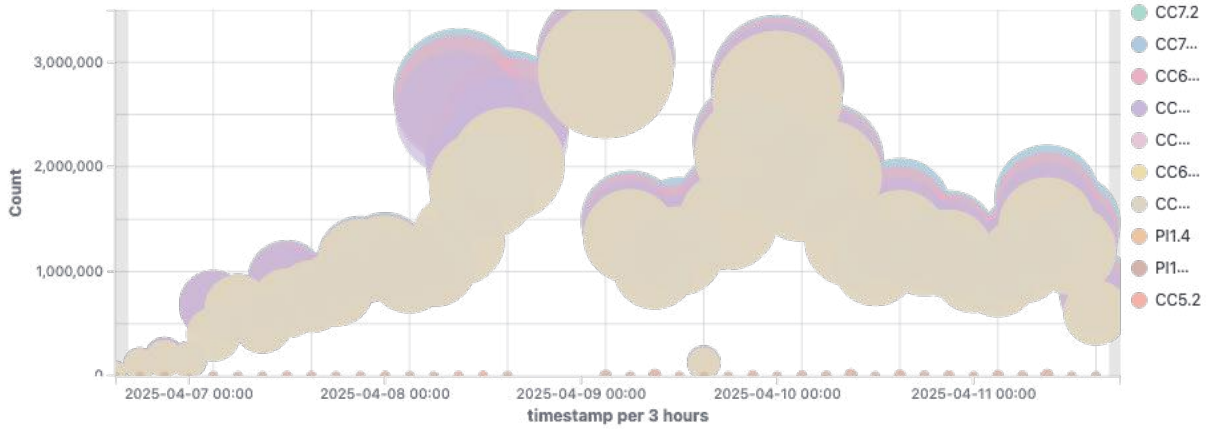
The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

- 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

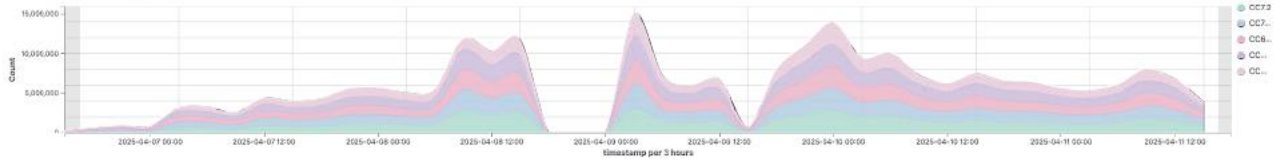
Rule ID	Description
31101	Web server 400 error code.
31151	Multiple web server 400 error codes from same source ip.
12108	Query cache denied (probably config error).

TSC requirements

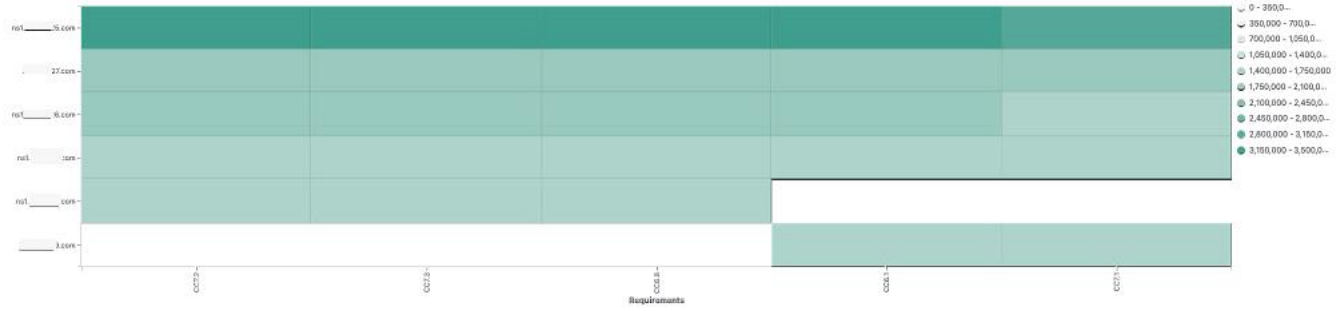


Top 10 agents by alerts number

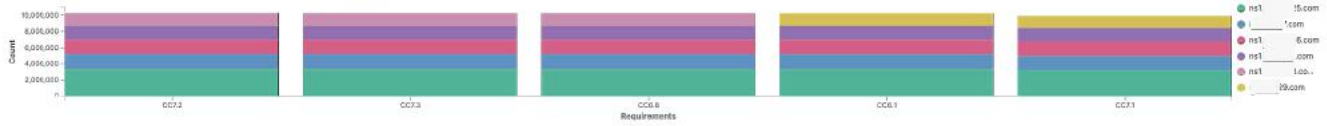
Top requirements over time



Last alerts



Requirements by agent



Alerts summary

Agent name	Requirement	Description	Count
ns1 .com	CC7.2	Web server 400 error code.	2603055
ns1 .com	CC7.3	Web server 400 error code.	2603055
ns1 .com	CC6.8	Web server 400 error code.	2603055
ns1 .com	CC6.1	Web server 400 error code.	2603055
ns1 .com	CC7.1	Web server 400 error code.	2603055
ns1 .com	CC7.2	CMS (WordPress or Joomla) login attempt.	230300
ns1 .com	CC7.3	CMS (WordPress or Joomla) login attempt.	230300
ns1 .com	CC6.8	CMS (WordPress or Joomla) login attempt.	230300
ns1 .com	CC6.1	CMS (WordPress or Joomla) login attempt.	230300
ns1 .com	CC7.1	CMS (WordPress or Joomla) login attempt.	230300
ns1 .com	CC7.2	Multiple web server 400 error codes from same source ip.	149127
ns1 .com	CC7.3	Multiple web server 400 error codes from same source ip.	149127
ns1 .com	CC6.8	Multiple web server 400 error codes from same source ip.	149127
ns1 .com	CC6.1	Multiple web server 400 error codes from same source ip.	149127
ns1 .com	CC7.1	Multiple web server 400 error codes from same source ip.	149127
ns1 .com	CC7.2	Query cache denied (probably config error).	105470
ns1 .com	CC7.3	Query cache denied (probably config error).	105470
ns1 .com	CC6.8	Query cache denied (probably config error).	105470
ns1 .com	CC6.1	Query cache denied (probably config error).	105470
ns1 .com	CC7.2	High amount of POST requests in a small period of time (likely bot).	51597
ns1 .com	CC7.3	High amount of POST requests in a small period of time (likely bot).	51597
ns1 .com	CC6.8	High amount of POST requests in a small period of time (likely bot).	51597
ns1 .com	CC6.1	High amount of POST requests in a small period of time (likely bot).	51597
ns1 .com	CC7.1	High amount of POST requests in a small period of time (likely bot).	51597
ns1 .com	CC7.2	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	CC7.3	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	CC6.8	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	CC6.1	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	CC7.1	CMS (WordPress or Joomla) brute force attempt.	25548
ns1 .com	CC7.2	Common web attack.	19714
ns1 .com	CC7.3	Common web attack.	19714
ns1 .com	CC6.8	Common web attack.	19714
ns1 .com	CC6.1	Common web attack.	19714
ns1 .com	CC7.1	Common web attack.	19714
ns1 .com	CC7.2	Suspicious URL access.	5540
ns1 .com	CC7.3	Suspicious URL access.	5540
ns1 .com	CC6.8	Suspicious URL access.	5540
ns1 .com	CC6.1	Suspicious URL access.	5540
ns1 .com	CC7.1	Suspicious URL access.	5540

Agent name	Requirement	Description	Count
ns1 .com	CC7.2	Multiple web server 503 error code (Service unavailable).	2205
ns1 .com	CC7.3	Multiple web server 503 error code (Service unavailable).	2205
ns1 .com	CC6.8	Multiple web server 503 error code (Service unavailable).	2205
ns1 .com	CC6.1	Multiple web server 503 error code (Service unavailable).	2205
ns1 .com	CC7.1	Multiple web server 503 error code (Service unavailable).	2205
ns1 .com	CC7.2	Multiple web server 500 error code (Internal Error).	1593
ns1 .com	CC7.3	Multiple web server 500 error code (Internal Error).	1593
ns1 .com	CC7.1	Multiple web server 500 error code (Internal Error).	1593
ns1 .com	CC7.2	Dovecot Authentication Success.	947
ns1 .com	CC7.3	Dovecot Authentication Success.	947
ns1 .com	CC6.8	Dovecot Authentication Success.	947
ns1 .com	CC7.2	Postfix SASL authentication failure.	938
ns1 .com	CC7.3	Postfix SASL authentication failure.	938
ns1 .com	CC6.8	Postfix SASL authentication failure.	938
ns1 .com	CC6.1	Postfix SASL authentication failure.	938
ns1 .com	CC7.2	Listened ports status (netstat) changed (new port opened or closed).	906
ns1 .com	CC7.3	Listened ports status (netstat) changed (new port opened or closed).	906
ns1 .com	CC6.8	Listened ports status (netstat) changed (new port opened or closed).	906
ns1 .com	CC7.2	Integrity checksum changed.	677
ns1 .com	CC7.3	Integrity checksum changed.	677
ns1 .com	CC6.8	Integrity checksum changed.	677
ns1 .com	CC6.1	Integrity checksum changed.	677
ns1 .com	CC7.2	A web attack returned code 200 (success).	385
ns1 .com	CC7.3	A web attack returned code 200 (success).	385
ns1 .com	CC6.8	A web attack returned code 200 (success).	385
ns1 .com	CC6.1	A web attack returned code 200 (success).	385
ns1 .com	CC7.1	A web attack returned code 200 (success).	385
ns1 .com	CC7.2	SQL injection attempt.	294
ns1 .com	CC7.3	SQL injection attempt.	294
ns1 .com	CC6.8	SQL injection attempt.	294
ns1 .com	CC6.1	SQL injection attempt.	294
ns1 .com	CC7.1	SQL injection attempt.	294
ns1 .com	CC7.2	Dovecot Session Disconnected.	292
ns1 .com	CC7.3	Dovecot Session Disconnected.	292
ns1 .com	CC6.8	Dovecot Session Disconnected.	292
ns1 .com	CC6.1	Dovecot Session Disconnected.	292
ns1 .com	CC7.2	Postfix: Illegal address from unknown sender	267
ns1 .com	CC7.3	Postfix: Illegal address from unknown sender	267
ns1 .com	CC6.8	Postfix: Illegal address from unknown sender	267
ns1 .com	CC6.1	Postfix: Illegal address from unknown sender	267
ns1 .com	CC7.2	Postfix: hostname verification failed	151

Agent name	Requirement	Description	Count
ns1 .com	CC7.3	Postfix: hostname verification failed	151
ns1 .com	CC6.8	Postfix: hostname verification failed	151
ns1 .com	CC6.1	Postfix: hostname verification failed	151
ns1 .com	CC7.2	Dovecot Invalid User Login Attempt.	101
ns1 .com	CC7.3	Dovecot Invalid User Login Attempt.	101
ns1 .com	CC6.8	Dovecot Invalid User Login Attempt.	101
ns1 .com	CC6.1	Dovecot Invalid User Login Attempt.	101
ns1 .com	CC6.8	PAM: Login session opened.	34
ns1 .com	CC6.1	Multiple common web attacks from same source ip.	19
ns1 .com	CC7.1	Multiple common web attacks from same source ip.	19
ns1 .com	CC6.1	Postfix: Attempt to use mail server as relay (client host rejected).	16
ns1 .com	CC6.1	XSS (Cross Site Scripting) attempt.	12
ns1 .com	CC7.1	PHPMyAdmin scans (looking for setup.php).	10
ns1 .com	CC7.1	XSS (Cross Site Scripting) attempt.	10
ns1 .com	CC7.1	Multiple SQL injection attempts from same source ip.	7
ns1 .com	CC7.1	Blacklisted user agent (known malicious user agent).	6
ns1 .com	CC7.1	URL too long. Higher than allowed on most browsers. Possible attack.	6
ns1 .com	CC7.1	Log file rotated.	2
ns1 .com	CC7.1	PHP CGI-bin vulnerability attempt.	2