PCI DSS report

Global security standard for entities that process, store or transmit payment cardholder data.

2019-09-11T16:18:37 to 2019-09-11T18:18:37

manager.name: S-DEMO-SEC01.example.com AND rule.pci_dss: exists

Most common PCI DSS requirements alerts found

Requirement 2.2

Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry accepted system hardening standards (CIS, ISO, SANS, NIST).

Top rules for 2.2 requirement

Rule ID	Description
81542	OpenSCAP Report overview: Score less than 80
81530	OpenSCAP: Ensure auditd Collects File Deletion Events by User (not passed)
81530	OpenSCAP: Ensure auditd Collects Information on Exporting to Media (successful) (not passed)

Requirement 10.2.2

All actions taken by any individual with root or administrative privileges.

Top rules for 10.2.2 requirement

Rule ID	Description
5402	Successful sudo to ROOT executed

Requirement 10.2.5

Use of and changes to identification and authentication mechanisms including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges.

Top rules for 10.2.5 requirement

Rule ID	Description
5502	PAM: Login session closed.
5501	PAM: Login session opened.
5715	sshd: authentication success.

Requirement 10.6.1

Review the following at least daily:

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), authentication servers, ecommerce redirection servers, etc.)

Top rules for 10.6.1 requirement

Rule ID	Description
60104	Windows audit failure event
503	Ossec agent started.
502	Ossec server started.

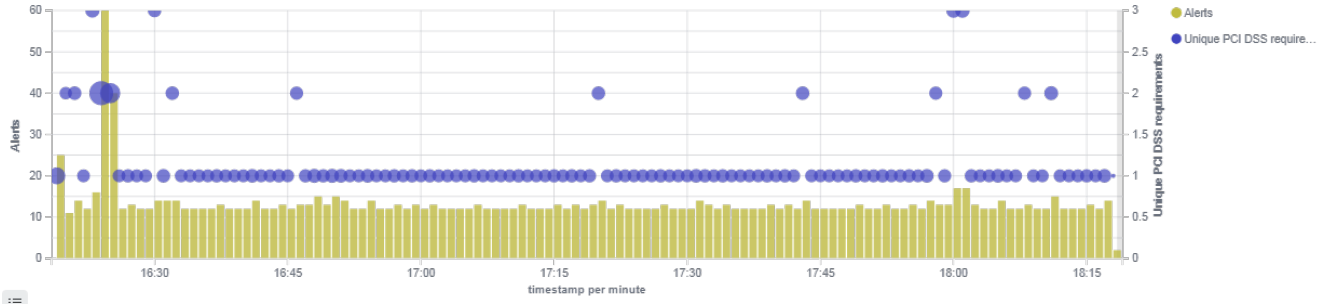
Requirement 11.5

Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Top rules for 11.5 requirement

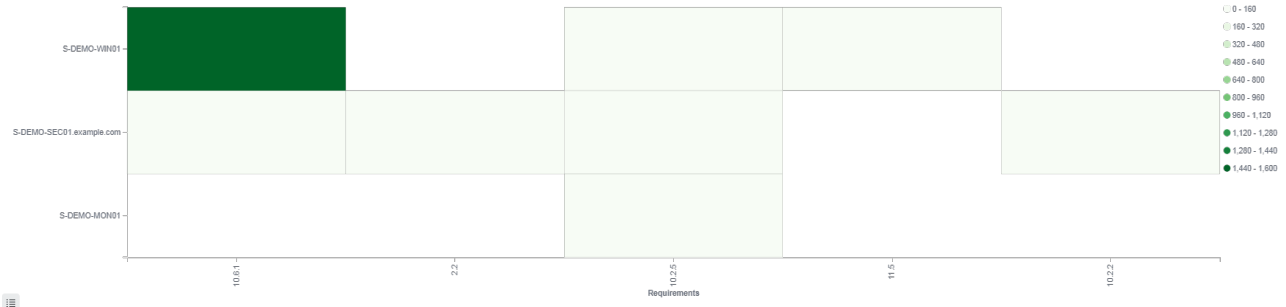
Rule ID	Description
550	Integrity checksum changed.

PCI requirements

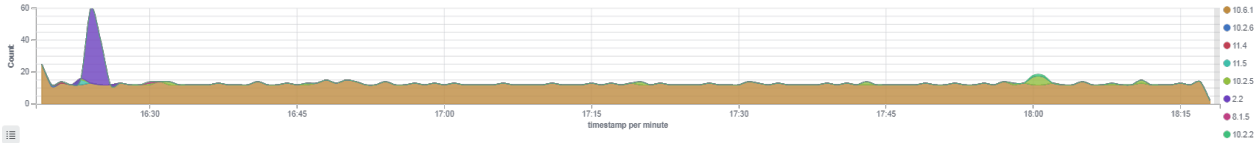


Requirements by agent

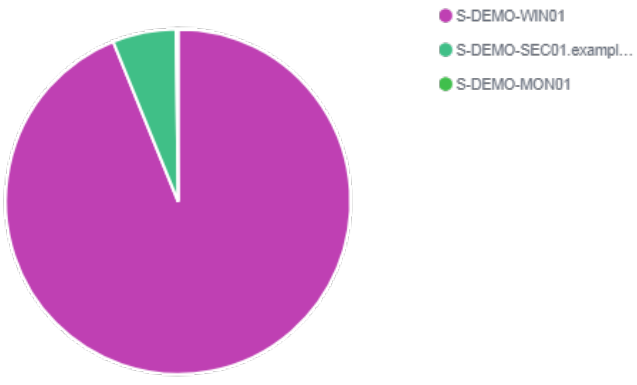
PCI requirements heatmap



Requirements over time



Agents



info@example.com
https://example.com

Alerts summary

Agent name	Requirement	Rule description	Count
S-DEMO-WIN01	10.6.1	Windows audit failure event	1490
S-DEMO-SEC01.example.com	10.2.5	PAM: Login session closed.	7
S-DEMO-SEC01.example.com	10.2.5	PAM: Login session opened.	7
S-DEMO-WIN01	11.5	Integrity checksum changed.	3
S-DEMO-SEC01.example.com	10.2.5	sshd: authentication success.	3
S-DEMO-MON01	10.2.5	PAM: Login session closed.	3
S-DEMO-SEC01.example.com	2.2	OpenSCAP Report overview: Score less than 80	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Ensure auditd Collects File Deletion Events by User (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Ensure auditd Collects Information on Exporting to Media (successful) (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Ensure auditd Collects Information on Kernel Module Loading and Unloading (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Ensure auditd Collects Information on the Use of Privileged Commands (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Ensure auditd Collects System Administrator Actions (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful) (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Record Attempts to Alter Time Through clock_settime (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Record Attempts to Alter the localtime File (not passed)	2
S-DEMO-SEC01.example.com	2.2	OpenSCAP: Record Events that Modify User/Group Information (not passed)	2
S-DEMO-SEC01.example.com	10.2.5	Successful sudo to ROOT executed	2
S-DEMO-SEC01.example.com	10.2.2	Successful sudo to ROOT executed	2
S-DEMO-WIN01	10.6.1	Ossec agent started.	1
S-DEMO-WIN01	10.2.5	Windows User Logoff	1
S-DEMO-WIN01	10.2.6	Ossec agent started.	1
S-DEMO-WIN01	11.4	Windows Audit event.	1
S-DEMO-WIN01	8.1.5	Session reconnected/disconnected to winstation	1
S-DEMO-SEC01.example.com	10.6.1	Ossec server started.	1