Logsign®

Logsign Next-Gen SIEM for PCI DSS Compliance

How to Stay Compliant With PCI DSS

Datasheet

Logsign Next-Gen SIEM for PCI DSS Compliance

Logsign SIEM provides a single platform to automate PCI DSS compliance needs. Customers benefit from all the advantages of easy compliance reporting with high level reports while updated versions meet all requirements. For PCI audit requirements, Logsign SIEM allows continuous logging, monitoring, backing up and reporting for all network connections and changes made to firewall and router configurations. Logsign SIEM has the ability to track user activities which is critical in preventing, detecting or minimizing the impact of compromised data. As mandated by PCI, Logsign SIEM collects logs in a secure way to manage, analyze and store log data to meet PCI audit requirements.

Logsign SIEM identifies, categorizes and normalizes log data to enable easy analysis and reporting. Log and machine data collection, archiving and recovery are fully automated across the entire IT infrastructure. In Logsign SIEM platform, log review is automated by creating correlation content. Matching related events trigger notifications automatically. Moreover, creating rules for real time detected threats can trigger notifications in sms or e-mail formats.

Highlights

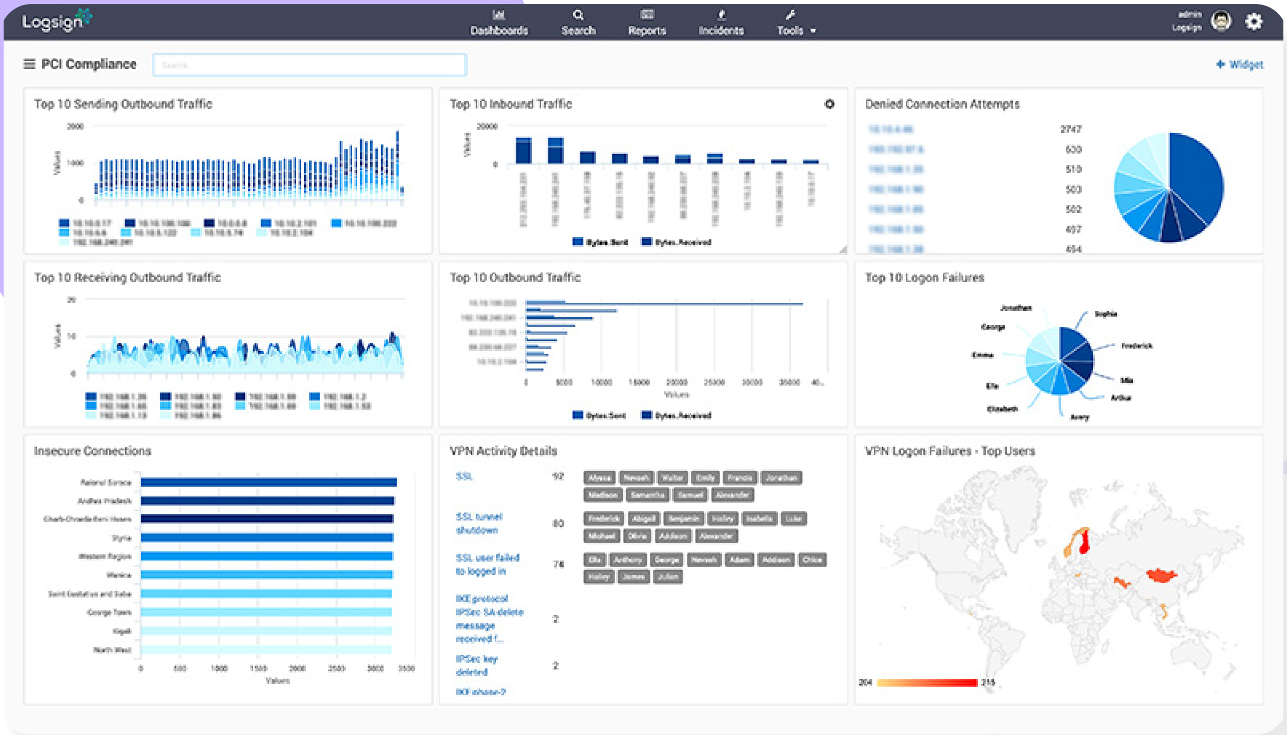
Real-Time monitoring and reporting capabilities for PCI DSS Compliance.

Flexible and simple search and reporting capabilities to quickly answer any data request.

Predefined dashboards and reports.

Abnormal traffic or suspicious activity detection.

Detection of transmission of the cardholder data in public or open networks.



SSL	92	Alyssa Nevaeh Walter Emily Francis Jonathan Madison Samantha Samuel Alexander
SSL tunnel shutdown	80	Frederick Abigail Benjamin Hailey Isabella Luke Michael Olivia Addison Alexander
SSL user failed to logged in	74	Ella Anthony George Nevaeh Adam Addison Chloe Hailey James Julian
IKE protocol IPSec SA delete message received f...	2	
IPSec key deleted	2	
IKE phase-2		

PCI Data Security Standard Overview

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI Data Security Standard Requirements and Security Assessment Procedures, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process. PCI DSS comprises a minimum set of requirements for protecting account data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations.

A. Build and Maintain a Secure Network and Systems
1- Install and maintain a firewall configuration to protect cardholder data
2- Do not use vendor-supplied defaults for system passwords and other security parameters
B. Protect Cardholder Data
3- Protect stored cardholder data
4- Encrypt transmission of cardholder data across open, public networks
C. Maintain a Vulnerability Management Program
5- Protect all systems against malware and regularly update anti-virus software or programs
6- Develop and maintain secure systems and applications
D. Implement Strong Access Control Measures
7- Restrict access to cardholder data by business need to know
8- Identify and authenticate access to system components
9- Restrict physical access to cardholder data
E. Regularly Monitor and Test Networks
10- Track and monitor all access to network resources and cardholder data
11- Regularly test security systems and processes
F. Maintain an Information Security Policy
12- Maintain a policy that addresses information security for all personnel

PCI V 3.2 Requirement	Description	Logsign SIEM Solution
1.1.1, 1.1.5, 1.1.6, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.5, 1.4.a	1- Install and maintain a firewall configuration to protect data	Logsign SIEM provides detailed monitoring for permitted or denied network protocols and ports within the organizer on network infrastructure. Track and report on firewall changes and rule usage to ensure that the firewalls are protecting the cardholder environment as expected. Logsign SIEM provides the details of firewall and router configuration or policy changes via investigations and reports.
2.1, 2.2.2.a, 2.2.2.b, 2.3.b	2- Do not use vendor-supplied defaults for system passwords and other security parameters	Logsign SIEM detects well-known vendor default account failures or successes, authentication in secure process or non-encrypted protocols. Logsign SIEM supports this by providing alarms and reports.
3.6.7	3- Protect stored cardholder data. PCI requires that you protect the data at rest on the cardholder systems	Logsign SIEM provides alarms or reports on actions that affect specific files or objects, for example, if a cryptographic key is altered, deleted or modified, the details of "who, when and where" are listed.
4.1	4- Encrypt transmission of cardholder data across open, public networks.	Logsign SIEM provides monitoring, alerts and reports on unauthorized or unencrypted services when encrypted or authorized traffic is expected.
5.1, 5.2.b, 5.2.c, 5.2.d	5- Protect all systems against malware and regularly update anti-virus software or programs	Logsign SIEM identifies operational errors from endpoint threat detection and response software, anti-malware applications, IPS rules, firewall vulnerability detections and new zero day attacks, detects and incorporates new signatures and alerts on malware detected within the cardholder data environment.
6.1.a, 6.1.b, 6.2.a, 6.2.b, 6.3.a, 6.4.1, 6.4.2, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.7, 6.5.8, 6.5.9, 6.6	6- Develop and maintain secure systems and applications	Logsign SIEM monitors patch management systems logs and reports and alerts if critical patches are not installed.

7.1.2, 7.1.3	7- Restrict access to cardholder data by business need to know	All access attempts to applications and hosts in scope of PCI can be collected, monitored and reported by Logsign SIEM. Logsign SIEM can also automatically take action and trigger an alarm on indexed data in real-time against employee directories when someone is trying to log into the PCI environment and should not be doing this based on their role or department.
8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5.a, 8.1.5.b, 8.1.6.a, 8.1.7.a, 8.2.4.a, 8.5.a, 8.7.a	8- . Identify and authenticate access to system components	Logsign SIEM reports and creates alarms on all account activity from account creation, removal, privilege escalation.
10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.a, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5, 10.6.a, 10.7.a	10- Track and monitor all access to network resources and cardholder data	Logsign SIEM provides details of privileged account management such as creation, deletion, modification, authentication failures and successes, granting or revoking of access, privilege escalation and failures or successes to access files, objects, and applications via alerts and reports. Logsign SIEM can also retain this access data for three months or more to meet PCI requirements, and its search interface and visualizations make it simple to perform critical log reviews daily.
11.1.d, 11.4.b, 11.5.a, 11.5.b	11- Regularly test security systems and processes	Logsign SIEM provides real-time monitoring and alerts on IPS/IDS events and indexing penetration of test results in XML file format. Dashboards can easily be created to trend the number of vulnerabilities by CVSS number.
12.3.8, 12.3.9	12- Maintain a Policy that Addresses Information Security for All Personnel	Logsign SIEM supports details report and alert on vendor account management activity, VPN activity access to cardholder data and system components and vendor authentication successes or failures.

About Us

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com

support.logsign.net

0 850 660 0 850

Info Security Products Guide 2020 GLOBAL EXCELLENCE BRONZE ★★★★★

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE SILVER ★★★★★

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD ★★★★★

CYBER DEFENSE GLOBAL AWARDS CYBER DEFENSE MAGAZINE 2018 WINNER