ManageEngine
Log360

How SIEM helps businesses comply with PCI DSS

www.manageengine.com/log-management

Introduction

The Payment Card Industry (PCI) Security Standards Council was founded by five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard, and Visa. These five payment brands had a common vision of strengthening security policies across the industry to prevent data breaches for businesses that accept and process payment cards. Together they drafted and released the first version of PCI Data Security Standard (PCI DSS 1.0) on December 15, 2004. PCI DSS 3.0 was released in November 2013 and the current version (PCI DSS 3.2.1) was released in May 2018.

PCI DSS is a regulation with twelve requirements that serve as a security baseline to secure payment card data. This regulation stresses that compliance is a continuous process involving assessments, repairs, and reporting, and that compliance needs to be maintained between PCI DSS assessments as well. Achieving PCI DSS compliance involves implementing several security controls, including deploying various security solutions. This guide elaborates on requirements 10 and 11.5 and how ManageEngine's SIEM solution, Log360, can satisfy these requirements.

Requirements 10 and 11.5

PCI DSS states that the goal of requirements 10 and 11.5 is to regularly monitor and test networks. The following descriptions are taken directly from PCI DSS:

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Requirement 11.5

Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files. Configure the software to perform critical file comparisons at least weekly. Implement a process to respond to any alerts generated by the change-detection solution.

The role of SIEM in PCI DSS compliance

Requirements 10 and 11.5 deal with implementing regular monitoring of networks and change detection mechanisms respectively. The reason PCI DSS lays a lot of emphasis on these two aspects is because system logs are the only way to investigate and respond to security incidents such as data breaches.

Once security auditing is enabled on the required systems, a security information and event management (SIEM) solution can continuously monitor networks, which is a must for meeting PCI DSS requirements. A SIEM solution can generate reports needed to periodically review audit information and also trigger alerts for suspicious activities that pose a threat to data security.

Features of Log360 that help with PCI DSS compliance

Log360 is a comprehensive SIEM solution that can monitor security events occurring in a network in real time. Log360 provides security monitoring capabilities including built-in reports and alert profiles needed for PCI DSS requirements 10 and 11.5. Here are the product's features that help with PCI DSS compliance:

Centralized log collection

Security teams must first identify the different systems in their environment that store or process cardholder data, and then configure logging on them. Logging should be enabled for all network systems and devices that fall in the scope of PCI DSS. This allows IT security professionals to track accesses and other activity on network resources that deal with cardholder data. For example, to track file accesses, object access auditing should be enabled on the concerned servers. Log360 can then collect logs from all the different systems that store or process cardholder data. The solution aggregates log data from servers, databases, network devices, and other systems for effective analysis of audit information.

Continuous log reviewing and reporting

Log360 transforms the collected raw log data into actionable information. The audit information is presented as intuitive graphs and dashboards. Security teams can also schedule reports to review security events on a daily basis. The reports for requirements 10 and 11.5 are available out-of-the-box, meaning they're generated automatically once log sources are added for monitoring. The reports list the PCI DSS sections in a systematic manner and are mapped to their relevant sub-sections.

The solution's sophisticated log search engine allows security personnel to pick out and analyze events of interest while investigating a security incident. Log360's search feature includes basic functionalities such as the use of phrases and boolean operators as well as advanced capabilities like correlating multiple events and attributes.

Log retention

PCI DSS requires collected log data to be stored for at least one year. The stored log data should be easily accessible if needed for forensic investigation. Log360 can be configured to retain collected log data for any desired retention period. If a forensic investigation needs to be carried out, the archived log data can easily be reloaded into the database and search operations can be performed on it.

Log protection

Malicious actors often try to modify audit logs so that their activity goes unnoticed. This is why PCI DSS expects log data to be protected and tamper-proof. Log360 encrypts the archived log files to ensure security. Further, Log360 employs techniques such as hashing and time stamping to ensure that the archived logs aren't tampered with.

File integrity monitoring

PCI DSS explicitly states that a change tracking tool like a file integrity monitoring (FIM) tool must be deployed to alert security teams about unauthorized modifications of critical system files. With Log360's FIM capabilities, security professionals can centrally track changes being made to sensitive files and folders, such as files and folders being created, accessed, viewed, deleted, modified, and renamed.

Log360 provides answers to the four vital Ws; security teams will know who accessed an object, which object was accessed, when the operation was done, and what the new value of an object is. This ensures that the accesses and modifications made to data are authorized, and that the integrity of cardholder data is maintained.

Real-time alerting

Log360 can generate alerts for the occurrence of critical events that may jeopardize the security of the systems that store or process payment card data. The solution's prepackaged PCI DSS alerts can be enabled and the alert profiles can be customized based on thresholds and other conditions. Security teams can receive these alerts either through email or SMS. Additionally, the solution allows them to execute a custom script when an alert is triggered in order to automate their threat response.

User activity monitoring

User activity monitoring is a must for keeping internal threats under check. Log360 monitors users in real time and provides a complete audit trail of all user activities with its reports. It also focuses on tracking privileged users' actions, including the critical changes they make to systems. The solution also goes one step further with its user behavior analytics (UBA) module, which can profile user behavior and identify anomalies using unsupervised machine learning and statistical analysis. This allows security teams to instantly detect suspicious login and file access activities.

PCI DSS requirements fulfilled by Log360

The table below gives details about the PCI DSS requirements that Log360 can fulfill.

Requirement	Requirement description	How Log360 helps
10.2	Implement automated audit trails for all system components to reconstruct the following events: (From 10.2.1 to 10.2.7)	Log360's integrated components automate the log management process and provide security teams with the complete audit trail needed to gain full network visibility into both on-premises and cloud platforms.
10.2.1	All individual user accesses to cardholder data.	Log360 continuously audits accesses and modifications made to files and databases that store cardholder data as well as log files. The solution tracks every individual user access to cardholder data. The following report provides the required details: • Individual user action
10.2.2	All actions taken by any individual with root or administrative privileges.	Log360 monitors privileged user activity and tracks the various actions performed by them in real time. In-depth audit reports give a complete picture of administrator activity, and alerts are triggered for suspicious login activity and other security threats. The following report provides the required details: • Administrative user actions

10.2.3	Access to all audit trails.	File integrity monitoring can be enabled for the files that store log data to track accesses to audit trails. The following reports help with tracking policy changes: • User policy changes • Domain policy changes • User session tracking • Audit policy changes
10.2.4	Invalid logical access attempts.	Log360 comprehensively tracks login activity on systems, including both successful logins and failed attempts. The event correlation engine can detect suspicious login activity, including brute force attacks. The following reports provide the required logon details: • Logon failures • Logon failures based on user • Logon failures based on DC
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.	Log360 can track critical changes such as the elevation of privileges. Reports can be generated for user account creations, deletions, and changes. Log360 monitors security group membership changes in Active Directory in real time and triggers alerts when users are added to high privilege groups such as the Domain Admins group. Individual server reports for other servers are also available out-of-the-box. The following reports provide the required change details: • Recently created users • Recently deleted users • Recently modified users • Recently created groups • Recently deleted groups • Modified admin groups

10.2.6	Initialization, stopping, or pausing of the audit logs.	Log360 generates alerts if someone disables logging or clears the audit logs. The following reports provide the required log information: • System logs • Audit logs cleared
10.2.7	Creation and deletion of system-level objects.	Log360 monitors system-level objects such as application executables, configuration files, system configuration files, and system executables with the following out-of-the-box reports: • Object accessed • Object created • Object deleted • Object deleted • Object handled
10.3	Record at least the following audit trail entries for all system components for each event: (From 10.3.1 to 10.3.6).	Log360 records all critical audit trail entries from servers, databases, file/folders, network devices, and more.
10.3.1	User identification.	Log360 helps verify user identification included in log entries with its in-depth logon/logoff reports. The following report categories provide the required user identification details: • User logon • Local logon-logoff • ADFS auditing
10.3.2	Type of event.	Log360 categorizes the type of event in the log entry based on its severity, such as error, warning, information, and more. The following reports provide the required event details: • Failure events • Success events • Warning events • Information events • Error events • Critical events overview

10.3.3	Date and time.	Log360 parses time stamp data in the log entries to ensure accurate reporting and alerting.
10.3.4	Success or failure indication.	Log360 parses the success or failure information of an event and reports the details of each event in the following reports: • Success events • Failure events
10.3.5	Origination of event.	Log360 helps verify an event's origin by parsing relevant information—such as host, IP, or application—from log entries.
10.3.6	Identity or name of affected data, system component, or resource.	Log360's advanced correlation, user behavior analytics, and alerting engine help security teams instantly identify affected data and systems.
10.5	Secure audit trails so they cannot be altered.	Log360 protects audit trails from unauthorized modifications by immediately archiving, encrypting, and time-stamping the collected logs.
10.5.1	Limit viewing of audit trails to those with a job-related need.	Log360's role-based access settings can restrict the viewing of audit trails to those who are authorized. Admin, guest, or operator roles can be assigned to technicians.
10.5.2	Protect audit trail files from unauthorized modifications.	File integrity monitoring can be set up for Log360's audit trail files, which will send alerts when someone tries to make unauthorized modifications to files.
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Log360 securely archives collected log data to a specified location. The archived log data is further secured by hashing and time-stamping mechanisms.

10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	Log360 stores log data generated by external-facing technologies such as firewalls, DNS, and mail servers in a secure internal server.
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Log360 can implement file integrity monitoring on the files that store log data and generate alerts when log data is accessed, deleted, or modified.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	Log360 can help security teams conduct daily log reviews to identify suspicious activity and mitigate breaches at an early stage.
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. • 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, e-commerce redirection servers, etc.).	Log360's out-of-the-box and custom reports, correlation rules, alert profiles, and log search engine allow security teams to efficiently review the required security events on a daily basis. Furthermore, the trend reports provide deep insights into historical event trends and flag anomalous behavior.
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	In addition to the wide range of devices that Log360 supports out-of-the-box, Log360's custom log parser and universal log parsing and indexing feature extends its auditing capabilities to any system component that generates logs in a human-readable format.

10.6.3	Follow up exceptions and anomalies identified during the review process.	Log360's built-in incident management console creates an accountable process for the resolution of the triggered alerts. Alerts can be automatically raised as tickets to the designated administrator either in-product or by integrating with a ticketing tool.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Log360 can retain logs for any custom period. Archived log data can be swiftly reloaded into the search engine for analysis at any point in time.
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Log360's file integrity monitoring feature audits accesses and modifications made to critical files in a network. Weekly file integrity monitoring reports can be scheduled and alerts can be configured to notify security personnel about unauthorized modifications. The following reports provide information on file and folder events: • All file or folder changes • File/folder deleted • File/folder renamed • File/folder moved • File/folder modified • File/folder created • File read access

Conclusion

The increasing sophistication of cyberattacks and the rising number of credit card breaches have made PCI DSS compliance more important than ever before. The importance of being PCI DSS compliant was highlighted in Verizon's 2015 PCI compliance report, which said that among the breached companies that their forensics team investigated over the preceeding ten years, none of them were compliant at the time of the breach.

PCI DSS compliance must not be seen as a separate information security exercise. Rather, it should be intertwined with an organization's overall IT security strategy. It is important for organizations to evaluate their current security posture and take steps to fill any security gaps, which typically involves implementing security policies and deploying various solutions.

A SIEM solution such as Log360 can play a pivotal role in your journey toward continuous PCI DSS compliance. Download a free, fully functional 30-day trial of Log360 and start maintaining compliance today.

About the author

Siddharth Sharath Kumar is an IT security and compliance specialist on ManageEngine's product marketing team. He writes articles and e-books, regularly hosts webinars on key IT security topics, and presents at ManageEngine's conferences and other industry events across the globe.