PCI DSS Compliance Standard Checklist

http://www.correlog.com/support.html

The PCI DSS Standard (Payment Card Industry Data Security Standard) is worldwide enforceable set of guidelines created by the Payment Card Industry Security Standards Council (PCI SSC). The standard is required by all organizations and businesses that process, or otherwise interact, with credit cards and cardholders.

The current version of the PCI DSS standard consists of twelve different sections, dealing with securing a network against unauthorized access. This includes physical security, information security, and security policies. CorreLog Server furnishes ready-to-run components that directly support sections 10 and 11 of the PCI DSS Compliance standard, as detailed below.

10.5 Secure audit trails so they cannot be altered.

CorreLog receives information from managed devices in real-time, securing this information at a remote location as it is generated, preventing alteration or loss of this data by any action that can occur at the managed node. Additionally, this log information is compressed, moved to a new location (i.e. a secure archive), and an MD5 checksum is created. The MD5 checksum is encrypted, preventing any tampering with the file or checksum. This secures audit trails so they cannot be altered.

10.5.1 Limit viewing of audit trails to those with a job-related need.

CorreLog provides a verifiably secure way of limiting access to log data and audit trails. A secure login is needed to view data within CorreLog Server, employing public key encryption, and optional AES-256 encryption. Data cannot be accessed remotely except via a web browser (or some other secure external mechanism, such as a remote terminal.) Within CorreLog, users are granted a permission level that can limit the view of data and operations performed on the data. CorreLog supports "admin", "user", "guest", "dashboard", "ticket", and "report" type logins, which grant specific capabilities to users based upon their job-related needs.

10.5.2 Protect audit trail files from unauthorized modifications via access control mechanisms, physical segregation and/or network segregation.

Correlog uses various techniques to protect audit trails: the data is physically segregated from the system that generates it, immediately forwarding (in real time) audit messages from managed devices to the secure CorreLog Server. Additionally, access controls are applied (in the form of secure encrypted logins to the system) to ensure that unauthorized access to the files does not occur. CorreLog logs all to access controls so that the audit trail incorporates system configuration changes that affect internal security.

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

CorreLog automatically backs up log file data nightly, including any filtered data. This data can be stored on a separate disk, possibly a network drive or SANS storage. The data cannot be altered because an encrypted checksum is made of the data using a private key, making it impossible to alter the data without detection. Additionally, because the data has been forwarded to CorreLog at real time, and the CorreLog server itself is protected from unauthorized access, it is not possible for users to modify an audit trail on the managed platform (such as clearing log files) because that data has already been backed up to the centralized CorreLog Server.

10.5.4 Write log files for external facing technologies onto a server on an internal LAN. Verify that logs are offloaded or copied onto a secure centralized internal log server or media.

The location where log data and archive data is stored is configurable within the CorreLog server, so that log files can be protected via network routing, firewalls, and gateways. CorreLog automatically creates secure archives on the local disk drive, but these archives can also be stored on remote disks that are deeply internal to the enterprise, accessible only by the CorreLog Server.

10.5.5 Use file integrity monitoring or change detection software to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert.)

CorreLog provides an audit trail of all modifications to internal configuration data, including the CorreLog data store. An indication is sent each day that the data is correctly backed up. Any changes to the archive at any other time will generate an alert, and optionally open a ticket.

10.6. Review logs for all systems at least daily. Log reviews must include those servers that perform security functions.

CorreLog excels at this particular requirement. The program includes a simple workflow, where tickets are generated on certain key items. The closure of tickets is automatically noted in the archived data, making it easy to demonstrate that the data is being periodically reviewed, or not. Ticket assignees close their tickets individually, or all of their tickets, via a few simple clicks, writing optional ticket resolutions.

10.7 Retain audit trail history for at least one year, with minimum of three months immediately available for analysis.

CorreLog retains online data for up to 500 days, and archived data to a maximum of 5000 days (12 years.) Archived data can be re-imported into CorreLog for analysis using an "Import" utility.

11. Regularly Monitor and Test Security.

CorreLog provides built-in test and monitor software, including the following: CorreLog includes a File Integrity Monitor (FIM) that periodically scans files on the system and checks for additions, deletions, and changes to directories of files; CorreLog incorporates SNMP and Ping scanners that continuously test for device availability and performance changes; CorreLog interfaces to a variety of intrusion detection systems to aggregate test results with other data on the system.

Additional Notes

Further information on PCI DSS and CorreLog support for this standard, as well as other compliance standards and their support, is available from CorreLog at our website below. Find information on how CorreLog helps address your log management and correlation needs. We provide papers on PCI/DSS, HIPAA, and FISMA specifications, as well as other technical application notes to assist you in achieving regulatory compliance, and a more secure enterprise.

CorreLog, Inc.
http://www.correlog.com
mailto:info@correlog.com