1 Collecting logs

The importance of log management in the PCI DSS

The Payment Card Industry Data Security Standard, more commonly known as the PCI DSS, stresses the importance of maintaining the audit trail of security events as a means to detect and mitigate incidents that may result in the exposure of cardholder data. Requirement 10 of the PCI DSS, and parts of other requirements, elaborate on the implementation of an efficient system and process for monitoring security events. Organizations must identify the systems that must conform to the regulation, enable auditing of relevant security events, and centralize logs from various sources using a security information and event management (SIEM) solution.

Identifying the systems to audit

As a general rule, logs must be collected from all systems, applications, network devices, and security solutions that relate to cardholder data. Some of the most crucial components in the network that need to be audited are:

- Servers
- Files and folders
- Databases
- Business-critical applications
- Network equipment such as firewalls
- Security solutions such as antivirus software

Enabling auditing: What events should we track?

Requirement 10.2 lists the following security events, at a minimum, that must be tracked:

- 10.2.1 All individual user accesses to cardholder data
- 10.2.2 All actions taken by any individual with root or administrative privileges
- 10.2.3 Access to all audit trails
- 10.2.4 Invalid logical access attempts
- 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
- 10.2.6 Initialization, stopping, or pausing of the audit logs
- 10.2.7 Creation and deletion of system-level objects

Logging policies must be enabled on the systems and applications that fall under the scope of the regulations in order to track the security events within Requirement 10.2.

Collecting logs

The logs must be collected in real time, or near real time, from the sources that fall under the scope of the PCI DSS. The mode of log collection can vary based on the log type (Windows security log/syslog/application log) and restrictions in the network, such as the presence of demilitarized zone (DMZs). Logs can be collected using:

- Agents
- Agentless techniques

Security teams must assess their network infrastructure and decide the mode of log collection while listing down the various log sources in their network.

Ease your log management woes with Log360

ManageEngine Log360 can aggregate logs from every critical component in the network, such as servers, network devices, applications, and more. The solution comes with prebuilt auditing capabilities that track the events mandated by the PCI DSS, extracting the required fields with no additional configuration.