2 Securing log data

The need for log archives

Security teams often discover breaches weeks or months after the attack. In such scenarios, log archives play a crucial role in helping security teams conduct a forensic investigation and analyze the attack to assess the impact and determine the root cause. Secure log collection and storage is a fundamental requirement of the PCI DSS. Measures must be implemented to ensure that the logs are protected from collection to processing to storage.

PCI DSS requirements for log archival

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:

- ✓ **Requirement 10.5** requires the audit trails to be secured to prevent alteration.
- ✓ **Requirement 10.7** requires logs to be stored for at least a year, with the data being immediately available if required for investigations.

Secure log management

First, the log processing must use secure communication protocols to prevent unauthorized exposure of data. Second, the log archives must be secured to ensure no one is trying to tamper the records. Third, proper access controls must be implemented in the log management solution so that only authorized personnel have access to the collected logs. These three measures ensure that log data is reliable for forensic analysis in the worst-case scenario of a data breach.

Keeping log archives secure

Below are three crucial techniques for ensuring the security of log archives:

- ✓ **Encryption:** Log archives must be encrypted using strong encryption algorithms.
- ✓ **Time-stamping:** The archives must be time-stamped as a measure to ensure the reliability of the log data for a forensic investigation.
- ✓ **Integrity check:** Measures to check for tampering and ensure the integrity of the log data must be implemented.

Secure log management with Log360

Log360 ensures secure and reliable log collection so that no log data is lost. The solution employs protocols including WMI/DCOM, TLS and HTTPS to securely collect and transmit the log data. Further, the collected logs can be archived for the required time period. The archives are secured using the techniques mentioned above. The data can be reloaded into Log360's search engine swiftly for conducting a forensic investigation.