5 File integrity monitoring

Ensuring the integrity of cardholder data

Preventing unauthorized accesses and tampering of cardholder data is one of the main objectives of the PCI DSS. A crucial measure in ensuring the security of cardholder data is implementing file integrity monitoring (FIM). Put simply: FIM is used to keep track of and validate changes made to files and folders.

Requirement 11.5 of the PCI DSS requires a file integrity monitoring (FIM) solution to be deployed to track changes made to files, and provide alerts about unauthorized actions. Most SIEM solutions come with a built-in FIM component to make compliance easier.

Note: The files of concern include system files and log files in addition to files that store sensitive data.

Implementing FIM

The entire set of changes performed on files such as creations, deletions, accesses, modifications, and copies must be tracked. Actions that indicate failed attempts must also be recorded. The following details must be analyzed and documented:

- **Who** made the change
- **Which** file was changed
- **When** the change was made
- **What** the change is

FIM use cases

FIM adds to the security measures of files and folders by:

- Generating granular reports to validate changes made to files and folders.
- Alerting about repeated failed attempts to access/modify files and folders.
- Identifying changes made to permissions that may unwittingly expose sensitive data.
- Detecting anomalous file actions that might indicate an ongoing attack.

Log360's file integrity monitoring capabilities

Log360 comes with built-in FIM for Windows file servers, failover clusters, Linux file servers, EMC servers and NetApp filers. Log360 audits changes made to files and folders, and issues alerts for unauthorized accesses and modifications made to files.