# 3 Reviewing logs

## Extracting insights from logs

Log messages contain valuable security information in their fields that must be extracted for analysis. According to **requirement 10.3,** a minimum of the following entries must be recorded:

- ✓ 10.3.1 User identification
- ✓ 10.3.2 Type of event
- ✓ 10.3.3 Date and time
- ✓ 10.3.4 Success or failure indication
- ✓ 10.3.5 Origination of event
- ✓ 10.3.6 Identity or name of affected data, system component, or resource

## Visualizing log data

According to **requirement 10.6,** logs must be reviewed daily to identify anomalies and suspicious activity. Viewing reports and dashboards is the most convenient way of monitoring important security events occurring in the network. The details cited above must appear in the reports to comply with the PCI DSS.

## Dashboard requirements

**Events overview:** The total number of events collected, log trends, alerts triggered, categorizing events based on severity, and other important details.

**Network overview:** The allowed and denied connections by firewalls, analysis of the traffic trends, VPN logons, and more.

**Security overview:** The threats that have been flagged from threat sources, IDS/IPS, vulnerabilities, and alerts triggered.

## Scheduling audit reports

Audit reports must be scheduled and generated daily for swift detection of suspicious actions. These actions include logons, configuration changes, system events, and IDS/IPS threats. The PCI DSS' effective log monitoring guide recommends developing metrics such as "top 10 users affected", "average number of alerts per system, per day", "number of baseline violations per week", and others that help analyze the efficiency of the log management process.

## Out-of-the-box reporting for PCI DSS with Log360

Log360 comes with audit-ready PCI DSS report and alert profiles.The reports have been mapped to the requirements, and track the required events of interest, capturing the details mentioned above from log entries. The reports can be scheduled to review the logs on a daily basis.

**Note:** It is crucial to have a process in place for following up on the security events that have been flagged during the review of security events. Refer to "Responding to security incidents" found on the Resource page for additional information.