6 Responding to security incidents

Ensuring incidents are resolved before they result in a breach

Once incidents are flagged by the SIEM solution, they must be investigated and resolved swiftly to avoid breaches. This entails having a team of security administrators available at all times, and implementing technologies such as automation and security orchestration to resolve the incidents. Here are some important requirements from the PCI DSS about incident response:

- **12.5.2** Monitor and analyze security alerts and information, and distribute details to the appropriate personnel.
- **12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach.
- **12.10.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts.
- **12.10.5** Generate alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

Streamlining the process of incident management

The PCI DSS requires personnel to be available on a 24/7 basis to respond to security alerts. Once detected, incidents must be assigned to designated IT technicians to ensure accountability for resolution of the issues. Alerts can be managed from within the console of the SIEM solution, or with the help of a centralized help desk tool to streamline the process of incident management. A process must be defined and implemented to ensure that alerts aren't ignored. The process should:

- Automatically assign alerts to the designated administrator.
- Constantly monitor the performance parameters for incident resolution, such as mean time to respond and the mean time to resolve.

More personnel might need to be added to the incident resolution department for investigation if there are more alerts at any given point of time.

Automated response workflows

Workflows, which are a chain of actions linked by logical operators, can be assigned to alerts so that basic response tasks such as disabling users/computers, ending processes, and shutting down affected systems can be automated as soon as the alert is triggered. This goes a long way towards reducing the time it takes to mitigate a security incident, potentially averting a data breach.

End to end incident management and response with Log360

Log360 helps security teams detect incidents at an early stage, and helps them quickly investigate and respond to the incident. Automatic assignment rules can be configured within the solution to ensure accountable incident resolution. Further, workflows can be defined to ensure response actions are taken automatically when security incidents are detected.