ManageEngine
Log360

THE SOC incident response process

Did you know that according to Ponemon Institute, companies with no formal incident response plan pay **58% more** per breach than those with structured, tested response protocols? Thus, it is important to have an efficient incident response process that enables you to detect, contain, and remediate threats in real time. The following are the seven phases of a SOC's incident response process:

1 Preparation:

This stage makes sure that the SOC team is prepared, well-organized, and able to act swiftly and effectively in the event of an incident.

2 Identification:

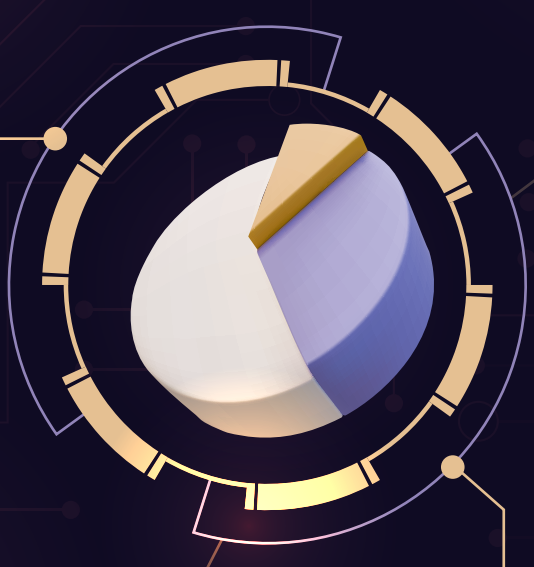
Quick, accurate identification is critical to avoiding false alarms and focusing on real threats.

3 Containment:

This stage makes sure the incident doesn't compromise more assets or escalate further.

4 Eradication:

This stage ensures the environment is clean and safe for recovery.



5 Recovery:

Recovery must be thorough to avoid reintroducing the threat.

6 Lessons learned:

This phase is vital for continuous improvement and better preparedness for future incidents.

7 Documentation and reporting:

Detailed reports should include a timeline, impact analysis, the response actions taken, and recommendations for the future.

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

SIGN UP FOR FREE DEMO