ManageEngine
Log360

DATASHEET

INCIDENT WORKBENCH

Revolutionize the way you investigate threats

Log360's Incident Workbench is a cutting-edge solution for simplifying and accelerating cybersecurity threat analysis and resolution. With its unified platform and advanced analytics, it enables effective identification, in-depth analysis, and efficient neutralization of threats.

Challenges in current threat investigation processes

- Lack of context: Security analysts may struggle to gather sufficient context about potential threats, which can lead to overlooking genuine threats.
- False positives: The lack of advanced analytics, ML, enhanced data correlation, and alert thresholds leads to an increased number of false positives, wasting valuable time and resources on non-critical issues.
- Complex process relationships: Tracking malicious processes is difficult due to intricate parent-child connections, hindering understanding of activity flow.
- Need for efficient investigation: Evolving threats require rapid and effective investigation to stay ahead of attackers.

Log360's Incident Workbench: How it helps

Log360's Threat investigation workbench enhances cybersecurity analysis through key features:

- Unified analytics: Integrates and analyzes key digital artifacts like users, devices, and processes for a comprehensive security view.
- ML-based user analytics and advanced integrations: Combines unified and entity behavior analysis (UEBA) with external tools like VirusTotal for layered threat analysis.
- Process hunting with visualizations: Utilizes visual tools like parent-child trees and Sankey charts for clear identification of suspicious activities.
- Enriched incident building: Compiles diverse analytical data into a singular incident report, streamlining the response process.

These features allow you to have a nuanced, efficient, and user-friendly platform for threat investigation, catering to the diverse cybersecurity needs of organizations.

Key benefits

- Significantly reduce investigation time with streamlined data integration and analysis.
- Simplify complex analytical processes with an intuitive and user-friendly interface.
- Enable deeper insights and accurate threat assessment through a data-centric, analytical console.
- Reduce false positives with advanced analytics and ML integration.
- Analyze security comprehensively with a full spectrum of threat investigation tools, from initial detection to in-depth analysis.

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected 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.

$ Get Quote Download