ManageEngine
Log360

Datasheet

Log360's ATTACK DETECT!ON capabilities

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats

Security information and event management like never before

Log360 combines anomaly detection based on machine learning (ML) with rule- and sign-based attack detection techniques to stop attacks in their early stages. Log360's threat intelligence capability coupled with incident response makes it the perfect SIEM solution for all your security needs.

Key product capabilities

ML-powered anomaly detection

- Easily detect insider threats, account compromises, and data exfiltration with ML-powered user and entity behavior analytics (UEBA).
- Baseline user and entity behaviors and detect anomalies based on the count, pattern, and time. Follow anomaly trends with a graphical representation that shows variations in the number of anomalies detected over the selected period.
- Comes with a risk management module that tightly integrates with ML-based UEBA to detect advanced persistent threats and attacks. Maintain a risk score for each and every user and entity profile in your organization.

Rule-based, real-time correlation engine for detecting known attacks

- The real-time correlation engine comes with over 30 predefined rules to capture known attack patterns such as SQL injection attacks, ransomware attacks, etc.
- Intuitive custom correlation rule builders provide the option to create new rules with advanced filters and over 250 network action templates.
- The built-in incident management system tightly integrates with the correlation module to effectively manage incidents.

Signature-based attack detection to formulate a threat-informed defense

- Log360 uses with the MITRE ATT&CK framework to help mitigate advanced cyberthreats and stay ahead of new and sophisticated threats.
- Get detailed insights such as the time the attack occurred, the source, the destination, and the entire attack plot summary through the intuitive graphical MITRE ATT&CK analytics dashboard.
- Conduct extensive incident investigation with visibility into the 12 ATT&CK tactics and expedite effective threat resolution with automated incident workflows and the incident management framework.

Key benefits

- ✓ Cut down malicious communication to command and control servers to ensure data leak prevention.
- ✓ Bolster cloud security and monitor shadow IT with integrated CASB capabilities.
- ✓ Effortlessly comply with regulatory mandates, like the PCI DSS, HIPAA, SOX, the GDPR, and the CCPA.
- ✓ Leverage informative threat feeds to discover malicious IPs, domains, and URLs.
- ✓ Speed up incident mitigation by triaging security threats and automating incident responses with security orchestration, automation, and response.
- ✓ Monitor changes made to your AD environment and tackle privilege escalations.

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