ManageEngine
Log360

Product Overview

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.

The solution is a tight integration of our following tools:

EventLog Analyzer: For log management and IT compliance reporting. | **ADAudit Plus:** To audit Active Directory changes in real-time.

There are six other modules that can be purchased and integrated separately according to the user's needs. These add-ons further strengthen the security of an organization by monitoring Microsoft Exchange, Microsoft 365, cloud applications and more.

Why organizations need a SIEM solution

As cyber threats have become rampant, businesses need more than just preventive security technology in order to mitigate threats and stay compliant. Today's security teams require a solution that can piece together different capabilities to prevent an attack from disrupting the network. A SIEM tool does that by playing a key role in helping organizations manage security incidents quickly and efficiently.

Ideal target audience for SIEM tools and key pitching points

Compliance managers

- Generate automated compliance reports for regulations such as PCI DSS, SOX, HIPAA, and more.
- 150+ ready-to-use reports to help meet security auditing requirements.
- Get notified whenever there's a compliance requirement violation or suspicious data breach activity.
- Backtrack security incidents using incident timelines when a suspicious activity is recorded.
- Tamper-proof log archive files to ensure the log data is secured for future forensic analysis, compliance and internal audits.

Data Protection officers

- Monitor and manage in Active Directory changes, network perimeter devices, databases and web servers.
- Detect and mitigate both internal and external threats and manage incidents efficiently.
- Keep a tab on privileged user actions and session activity.
- Never miss a single logon activity, access or modification attempt made to files/folders.
- Real-time alerts to stay on top of security incidents.

SOC Professionals

- Block malicious intruders using frequently updated threat feeds.
- Spot security threats using rule-based (correlation), signature-based (MITRE ATT&CK), and ML-based threat detection systems.
- Discover malicious IPs, domains, and URLs through threat intelligence by leveraging STIX/TAXII format threat feeds.
- Find malicious actors and potential hidden attacks by leveraging advanced threat analytics.
- Get alerted about and block malicious traffic to or from blacklisted IP addresses, domains, and URLs in real time, and get recommended options to remediate threats with predefined workflow rules.
- Optimise SOC using incident management dashboard. Get key metrics such as MTTD MTTR. Prioritise and ensure accountability for security incident resolution.

ROI Calculator | Recognized in Gartner MQ for SIEM for the sixth time | 2022 KuppingerCole Leadership Compass for SOAR

www.manageengine.com/log-management