ManageEngine
Log360

DATASHEET

Detection engineering of Log360

Overview

Threat detection isn't just about more alerts—it's about smarter ones. When every alert counts, Log360's re-engineered detection mechanism helps cut through the noise. With centralized visibility, precision rule controls, and behavior-aware logic, security teams can spot real threats faster and ignore what's safe.

Key capabilities

Centralized detection console

Access and manage detections from a unified console that spans MITRE ATT&CK®-based rules, user behavior anomalies, correlation-driven detections, and threat intelligence hits.

Object-level filtering

Reduce false positives by applying filters across users, groups, and OUs. Fine-tune prebuilt rules to monitor only high-risk or sensitive AD objects, improving the signal-to-noise ratio.

Advanced rule creation framework

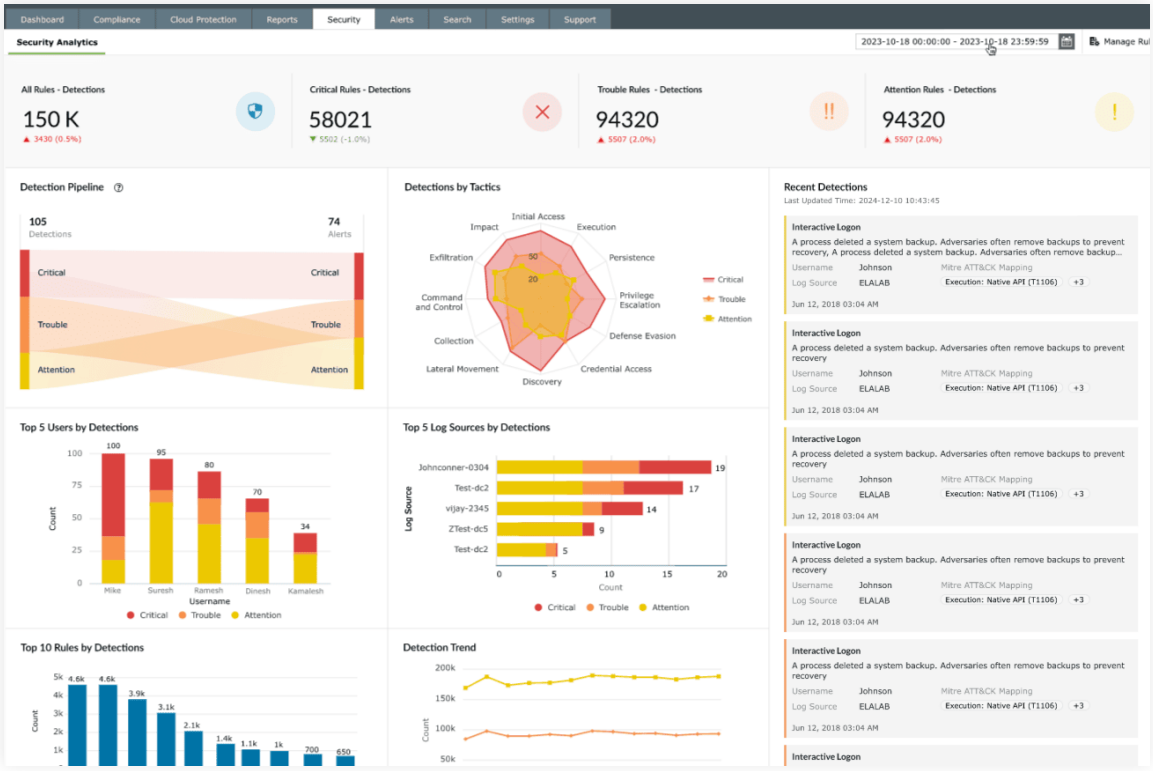
Support for standard, anomaly-based, and advanced detection logic empowers security teams to scale detection maturity at their own pace.

Built-in rule optimization insights

Get visibility into noisy rules and receive tuning recommendations based on alert volume, false positive trends, and asset criticality.

Cloud-delivered security content

Stay current with 2,000+ rules spanning MITRE techniques, threat intelligence, anomalies, and correlation automatically updated via cloud.



Highlights of Log360's detection engineering

- **No-code filtering interface:**
  Streamlines rule tuning across skill levels: No KQL, SPL, or AQL needed.

- **Cross-module context:**
  Get behavioral, threat, correlation, and asset intelligence in one rule.

- **Tuned for efficiency:**
  Optimized for reducing both mean time to detect and mean time to respond.

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, an analytical Incident Workbench, ML-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effective remediation. With reengineered detection—including a centralized detection console, multi-mode rule creation, tuning insights, and object-level filters—Log360 elevates signal quality and reduces false positives. The solution provides holistic visibility across on-premises, cloud, and hybrid environments with intuitive security analytics and monitoring.

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

$ Get Quote Download