ManageEngine
Log360

for Australian financial institutions

www.manageengine.com/log-management/

Overview

In the high-stakes environment of the Australian banking, financial services, and insurance (BFSI) sector, regulatory compliance and operational resilience are critical. From state-sponsored attacks targeting payment infrastructure to ransomware groups that selectively strike high-value financial data, the threats the sector faces are escalating. With increasing reliance on digital banking, APIs, and data-driven operations, early threat detection has become a business-critical priority. To combat these challenges, enterprise security teams require granular visibility and automated detection.

ManageEngine Log360 is a unified security platform that delivers enterprise-grade SIEM capabilities tailored to the regulatory and threat challenges of Australia's BFSI sector. ManageEngine Log360 is a scalable and resilient SIEM solution that consolidates distributed telemetry into a unified console for centralized visibility, real-time threat detection, and automated response.

BFSI use cases

Log360 equips BFSI institutions to detect and contain risky cyberthreats across their networks, databases, and user accounts in real time.

- **SQL privilege change monitoring:** Log360 provides real-time, comprehensive monitoring of audit logs across critical SQL databases. For example, when a new, high-level permission is granted to a user account that shouldn't require it, or when permissions are granted outside of pre-approved change windows, Log360 correlates the event with the user's prior behavior baseline and change management records and flags it as a high-priority risk. Security teams receive full context—who, what host, and what preceded it—in a single alert and can intervene before any data is compromised.
- **Protecting dormant administrator accounts:** Log360 detects when the built-in SQL server system administrator (SA) account is re-enabled. Every SA re-enablement on a monitored instance triggers an immediate high-fidelity alert, enriched with session details and correlated authentication events to support rapid forensic triage and regulatory disclosure.

- **Blocking unauthorized remote shells:** Log360 correlates SQL audit events with OS process creation telemetry. When any command shell or scripting engine is spawned with a database service account as its parent, it instantly triggers a critical alert. Log360 also surfaces the full attack chain, from database query to shell command, and provides a clear timeline of the event, including details such as the parent and child processes involved.

- **Detecting ransomware file renames:** Log360's file integrity monitoring continuously scans for mass file manipulation. It can immediately identify a sudden, localized burst of file rename activity consistent with known ransomware extensions, including the .medusa extension. Log360 then triggers an automated response to alert the SOC team and initiate containment playbooks, shrinking the blast radius and preventing the encryption from spreading to shared network drives and critical financial servers.

- **Identifying ransom note creation:** Log360 monitors file system activity across endpoints for the creation of *!!!READ_ME_MEDUSA!!!.txt,* the signature ransom note of the Medusa ransomware group. Detection is triggered at file creation, enabling response before lateral movement.

- **Mitigating post-compromise encryption:** Log360 leverages detection rules and behavioral baselining to identify the file renaming and extension change patterns consistent with BlackSuit's post-compromise encryption activity, even before ransom notes appear. It also correlates these file activity patterns with preceding attacker behaviors (privilege escalation, defense evasion, and lateral movement) to reveal the broader attack chain rather than isolated symptoms.

- **Preventing binary masquerading:** Log360 identifies the execution of PowerShell regardless of its running filename by checking embedded PE metadata against known PowerShell binary names. When the binary's actual identity mismatches its claimed name, Log360 flags the execution as binary masquerading, catching the evasion technique before credential theft or data staging can succeed.

- **Stopping malicious script execution:** Log360 detects instances where cscript.exe (the Windows Script Host command-line engine) is invoked to execute a VBScript file located in a temp directory. Alerts are triggered before secondary malware components can download and establish persistence, giving the SOC team an early intervention opportunity at the very start of the kill chain.

- **Securing software supply chains:** Log360 detects the anomalous execution of system-level scripting tools or command-line utilities, such as cmd.exe or powershell.exe, when the parent process is an npm or Node.js runtime. By correlating the process ancestry chain, Log360 identifies malicious post-install hooks at the moment they execute, giving security teams visibility into supply chain attacks before the malicious payload can establish persistence or reach production systems.

Log360 highlights

Log collection

Support for diverse log sources and integration

Custom parsing

Ability to parse and analyze logs in various formats

Scalable processing

Reliable and efficient log processing for large volumes

Unified visibility

Centralized view of security events across systems

Threat detection

Advanced analytics to identify and respond to threats

Incident response

Streamlined processes for rapid and effective incident handling

Reporting

Flexible reporting for compliance and insights

Archival

Secure and tamper-proof storage of log data

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.

Request a demo **Download**

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus