ManageEngine
Log360

Advanced threat detection for Australian financial institutions

www.manageengine.com/log-management/

Introduction

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.

Addressing high-impact threat use cases in BFSI

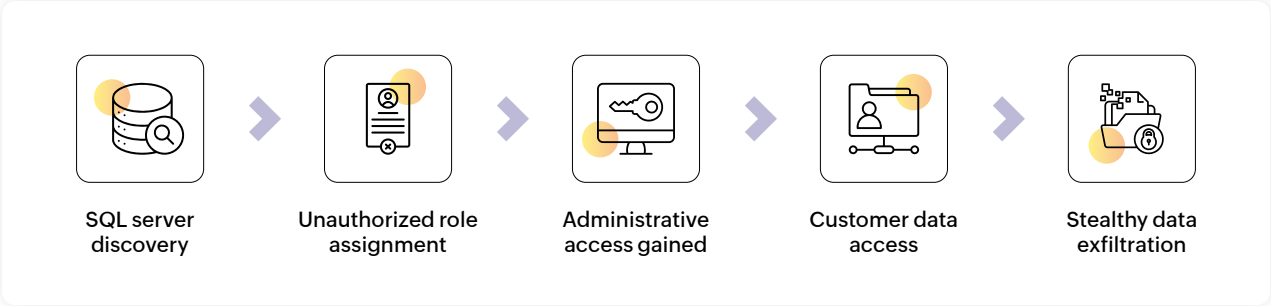
Modern cyberattacks targeting financial institutions are multi-layered and capable of bypassing conventional defenses. Log360 provides the sophisticated monitoring necessary to intercept advanced attack vectors before they compromise sensitive financial data or disrupt critical services.

1. Database and SQL server attacks

Database instances are prime targets for privilege escalation and persistence. Log360 monitors SQL environments for high-risk administrative changes that bypass standard change management workflows.

A) Unauthorized privilege escalation

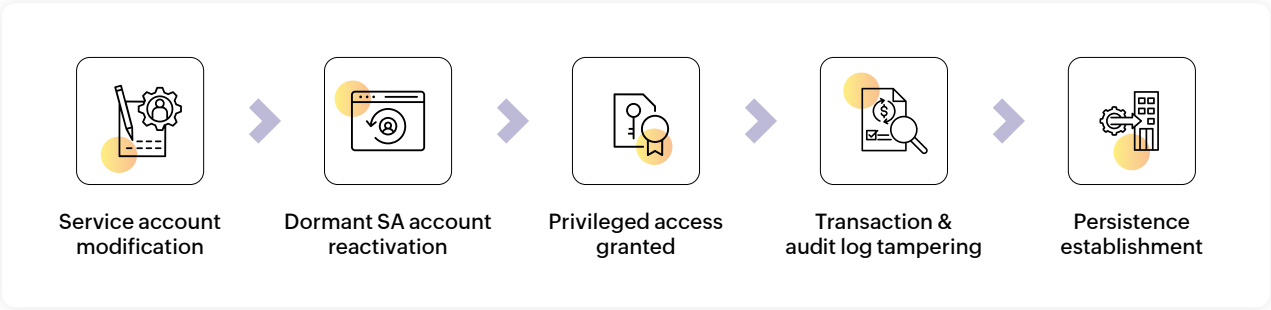
Detect unauthorized privilege changes on critical SQL servers that enable persistent access to sensitive customer and transaction data.



How Log360 helps: Log360 provides real-time, comprehensive monitoring of audit logs across critical SQL databases. It looks beyond simple errors, focusing on suspicious changes in security configuration. 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.

B) System administrator account exploitation

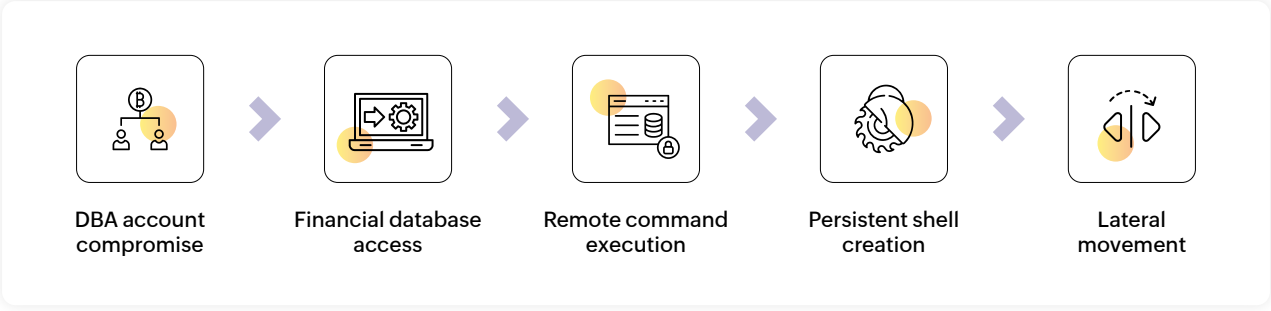
Detect unauthorized activation of system administrator (SA) account and suspicious changes that could compromise data integrity.



How Log360 helps: Log360 detects when the built-in SQL server 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.

C) Remote shell injection

Identify command execution attempts that establish unauthorized remote access to critical databases.



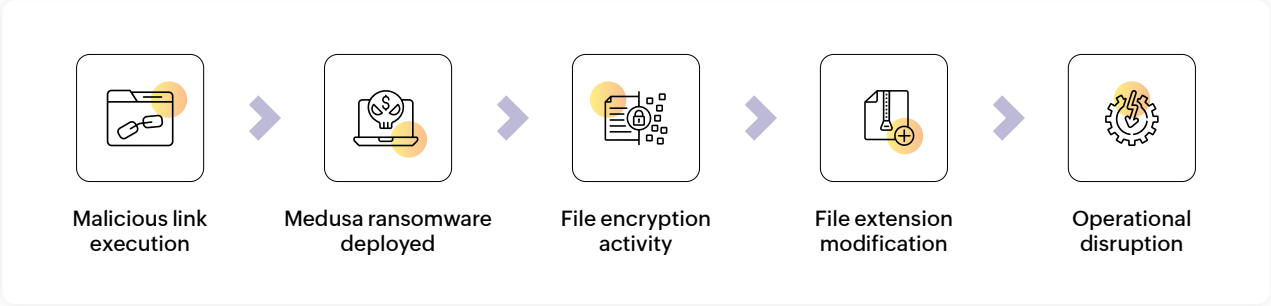
How Log360 helps: Log360 correlates SQL audit events with OS process creation telemetry. When any command shell or scripting engine is spawned with a database service account as its parent, and instantly triggers a critical alert. Log360 also surfaces the full attack chain, from database query to shell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

2. Ransomware mitigation: Medusa and BlackSuit

Ransomware remains a top-tier risk for Australian enterprises. Log360 utilizes its detection engine, behavioral analytics, and file integrity monitoring capabilities to stop encryption events in their tracks.

A) Medusa ransomware file encryption activity

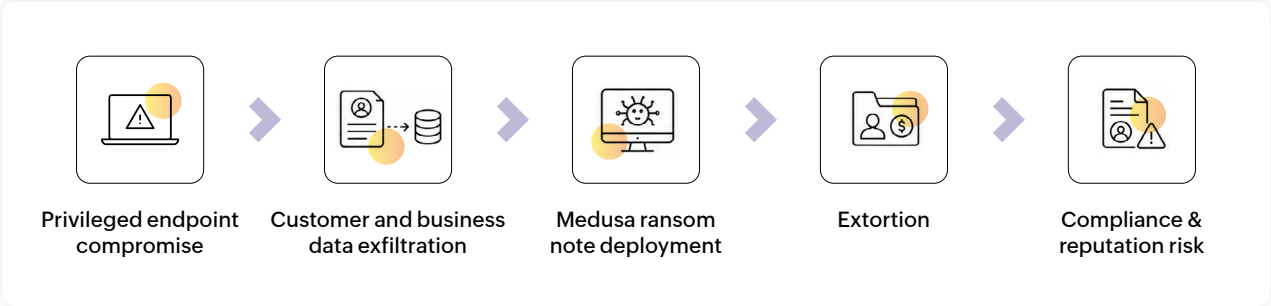
Detect Medusa ransomware encryption activity targeting sensitive financial records and business-critical data.



How Log360 helps: 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.

B) Medusa ransom note deployment

Identify Medusa ransomware extortion activity involving data theft and ransom demand.



How Log360 helps: 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.

C) BlackSuit ransomware: Post-compromise encryption activity

Detect ransomware operators preparing and executing large-scale encryption attacks.

How Log360 helps: 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.

3. Defense evasion and weaponized system utilities

Attackers frequently use legitimate system tools to evade traditional detection. Log360's correlation engine identifies the misuse of these utilities by analyzing their execution context.

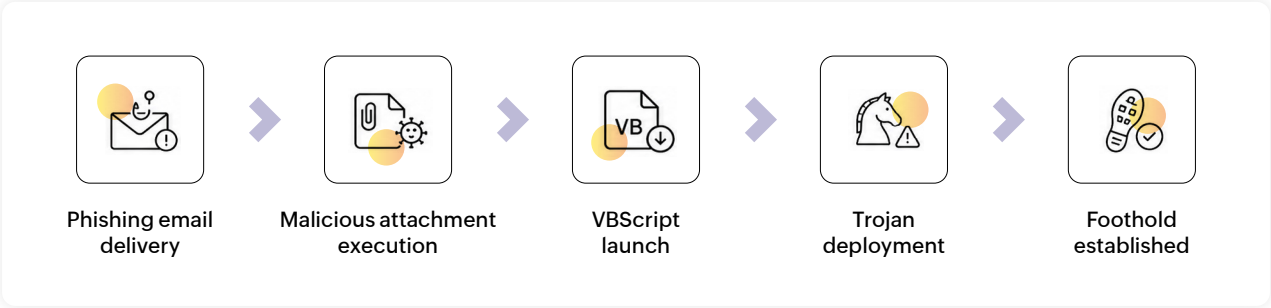
A) Binary masquerading

Detect attempts to evade security controls by disguising malicious executables as legitimate processes.

How Log360 helps: 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.

B) VBScript Dropper prevention

Detect script-based malware delivery used to establish initial access and deploy banking Trojans.



How Log360 helps: 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.

C) Supply chain security

Detect malicious activity introduced through compromised software dependencies and build pipelines.

How Log360 helps: 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.

Detection inventory

DETECTION RULE	MITRE ATT&CK® TECHNIQUE	CATEGORY
MSSQL Server - Instance level privilege grant detected	T1098.007	Database
SQL SA Admin user enabled	T1136.001	Database
Metasploit reverse shell injection in SQL Server	T1059.003	Database
Medusa File Encryption Extension	T1486	Ransomware
Medusa Ransom Note File Creation	T1486	Ransomware
BlackSuit Extension File Rename	T1486	Ransomware
PowerShell Executable Running Under Non-Standard Name	T1059 T1202	Defense evasion
VBScript Dropper Execution via cscript from temp directory	T1059.005 T1059.007	Defense evasion
Suspicious NPM Post-Install Script Execution	T1059.001 T1059.003 T1059.006 T1071.001	Supply chain

Data sources

Windows Sysmon MSSQL

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

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus