

USE CASE

Using Log360 to detect changes to sensitive data stored in databases



Using Log360 to detect changes to sensitive data stored in databases

Protecting the confidentiality of data collected from your employees and clients is an integral part of ensuring an organization's security posture. In addition to protecting your databases by restricting access and utilizing encryption, it is imperative that you ensure the quality of the stored data by auditing your databases. Unauthorized modifications to sensitive data can lead to operational disruptions, inadvertent data exposure, and security breaches. However, analyzing database audit trails is a cumbersome task because of the sheer volume of logs that are generated. How do you ensure data integrity and compliance with data privacy regulations?

How Log360 can help

ManageEngine Log360, an easy-to-use SIEM solution, supports comprehensive database activity monitoring for Microsoft SQL and Oracle servers. It provides multiple security dashboards that offer in-depth information to enable administrators to monitor and detect unauthorized changes to sensitive data in real time.

User access auditing:

To protect your data from illicit access, it is imperative to track who's accessing what, from where, and when. Log360 provides dashboards to monitor all user accesses in real time.

DDL and DML activity auditing:

Log360 tracks changes made to your databases and tables by auditing data definition language (DDL) and data machine language (DML) activity. You can also set up alerts to notify you of critical events in real time. For example, if an attacker has gained access to your databases and is enacting mass deletion of tables, Log360 can alert you immediately, enabling you to act quickly to safeguard the sensitive information.

Column integrity monitoring:

For institutions, such as banks and other financial service organizations, unauthorized modifications to customer data can result in disastrous consequences. It is essential to protect databases from tampering. Log360 helps you monitor changes to columns of data, and provides you with security analytics reports showing how and who made changes, and to what sensitive data. This helps you ensure the integrity of specific data stored in the database.

User permission change monitoring:

Malicious actors might try to access sensitive data legitimately by modifying the file permissions of a compromised account. Log360 provides in-depth information on who changes what permissions and when.

The role of correlation in detecting illicit database activity

Attackers do their best to remain inconspicuous while operating in your network. To differentiate between everyday database operation logs and malicious activity logs, sysadmins need more context. While they can gain context by looking through various logs, it is highly time-consuming and a tedious process. Log360 comes with a powerful correlation engine that provides prebuilt rules to detect suspicious patterns in generated logs in real time.

For example, the predefined Suspicious SQL Server Backup rule identifies situations where a brute-force attack against Windows machines is followed by a SQL backup event. By providing context, this rule helps the sysadmin identify and act against a seemingly harmless event that indicates a possible data breach. You can also build your own correlation rules to suit the security needs of your network.

Armed with these Log360 capabilities, you can ensure the confidentiality and integrity of your databases.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a
Customers' Choice for SIEM

[Check out why](#)

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in
Gartner's Magic Quadrant for
Security Information and Event
Management, 2024.

[Get the report](#)

Log360, a comprehensive SIEM solution, helps you to detect, investigate, and mitigate security threats and cyberattacks. With its intuitive security analytics, log correlation, threat intelligence, advanced threat analytics, machine-learning based user and entity behavior analytics, and end-to-end incident management capabilities, the solution helps you enhance and maintain the cybersecurity posture of your company, detect intruders and often pre-empt their attack attempts. Automate incident resolution with Log360's workflow and incident management console. Secure data residing in your physical and cloud platforms with advanced security monitoring. Further, the solution also helps you comply with the regulatory mandates with its audit-ready report templates..

For more information about Log360, visit our website.