ManageEngine
Log360

USE CASE

Discovering and securing credit card information using Log360

Discovering and securing credit card information using Log360

In today's digitized world, paying bills and shopping online has become increasingly popular. However, we hear stories of hackers stealing credit card information that is stored in our systems almost daily. The compromise of such sensitive information damages both our security and privacy.

Recognizing these threats, the Payment Card Industry Data Security Standard (PCI DSS) has made it mandatory to protect card holder data and increase control over it to reduce credit card fraud. Therefore, having a strong solution that can detect and secure such sensitive data is the need of the hour.

Log360 addresses all these issues with its various capabilities. This document helps you understand how you can discover and secure credit card information using Log360.

Discover credit card data using Log360

Log360 gives you visibility into stored cardholder data, including details on file type, size, owner, and more.

Log360 provides multiple preconfigured rules and policies to find the data of different types of credit cards. This includes Visa, MasterCard, Discover, American Express, InstaPay, and more. Log360 checks for patterns of data that correlate with known credit card formats in different locations including file servers, so you can locate credit card information stored in systems within the network and secure it. Log360 also allows you to categorize and catalogue personal data across Windows file servers.

Securing credit card data using Log360

After discovering sensitive data like card holder data, you should secure it from being exposed or stolen. This way, all your data and sensitive information is in safe hands. To ensure credit card data security, Log360 provides various options outlined below.

Detect data thefts by correlating log data in real-time

Log360's correlation engine helps you promptly detect potential attacks and threats by correlating log data using predefined threat detection rules. These rules help correlate data in real-time to detect data theft, brute-force attacks, account lockouts and more.

Log360's real-time correlation engine allows you to create custom correlation rules to detect data misuse and exfiltration. You can select individual actions that make up the rule, search for actions using the search bar, drag and drop the actions to rearrange their order, and detect repeated actions within a particular time interval.

Log360 also provides you with incident timeline reports that help you effectively investigate a security incident. From network intrusion to lateral movement and data exfiltration, attack patterns can be visualized better using this report.

Identify data exfiltration with behavioral analytics

Data exfiltration can be quite a pesky issue, especially when it is done by malicious insiders. With Log360's user entity and behavioral analytics (UEBA) capability, you can effortlessly monitor the activities of your employees and detect any anomalies in their behavior. Using the Log360's UEBA add-on, you can detect unusual data transfers, first time access of critical data, permission changes to sensitive data files, and more.

Ensure integrity of card holder data with file integrity monitoring

made to files and folders and ensures the accuracy of data by preempting unauthorized changes such as the creation, deletion, access, and modification along with any failed attempts at trying to make these changes. Log360 capabilities also extend to detecting unauthorized permission modification made to files and folders before they manifest into data theft or manipulation.

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.

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