ManageEngine
Log360

DATASHEET

Incident detection and investigation in Log360

A security incident is an indication that systems and data in your network may have been compromised. At first glance, a single security incident may not seem like a huge threat to your organization; however, it can very well be part of a bigger cyberattack such as a distributed denial-of-service attack, ransomware campaign, or advanced persistent attack. This is where the importance of detecting a security incident as soon as it occurs lies. A recent industry report states that it takes 170 days to detect an incident, 39 days to contain it, and 43 days to remediate it on average.

Log360 is a security information and event management solution that is simple yet effective in its approach to reducing the mean time to detect security incidents, enabling you to investigate and respond to threats as quickly as possible.

Incident detection

• File integrity monitoring

Files that contain sensitive information are critical to any type of business. Any unauthorized changes to these files can threaten an organization's cybersecurity. These changes may include creation, deletion, access, modification, or renaming of files and folders, including failed attempts at performing any of these actions.

Log360's file integrity monitoring feature ensures the accuracy of data by detecting any unauthorized changes made to your organization's files and folders. The module continuously monitors files and the changes made to them. The details include what file was changed, who made the change, when it was altered, and what was modified. The solution then triggers alerts for every unauthorized action, enabling you to quickly investigate the event and respond to it. This keeps the integrity of your organization's information intact.

• Event log correlation engine

When an organization deals with millions of logs a day on average, it may be overwhelming to detect suspicious activities accurately without falling victim to false positives. The basic course of every cyberattack is to gain entry to the network by exploiting vulnerabilities, explore the network to gain further access and establish a foothold, and finally breach critical data or resources.

Log360's correlation engine takes these stages into account and helps detect activity patterns that signal an upcoming breach. The different security events occurring throughout your network are analyzed together to identify indicators of an attack. Log360 uses over 30 predefined correlation rules to detect several common attacks. For example, the following events can indicate a cryptojacking attack: a suspicious software installation on a machine, followed by continuous alerts for high machine temperature and then alerts for prolonged high CPU usage by the same software on the same machine.

Log360 analyzes log data in real time from multiple sources in your environment and delivers a detailed event timeline for each detected incident, enabling you to get in-depth information on compromised accounts, infected devices, and more. The information includes details like the changes that were made, who made them, when they were made, how often, and how they were made. This in-depth information enables you to investigate security incidents thoroughly to find each one’s origin and cause.

• Behavior analytics

Unlike log correlation, which functions on a rule-based detection system, user and entity behavior analytics (UEBA) focuses on analyzing user behavior to detect anomalous activities in your network. Log360's UEBA module observes each user and entity for a period of time before creating a standard baseline of their behavior. Any deviation from their usual behavior is recorded as an anomalous activity and further assigned a risk score based on the event's severity.

For example, if a user logs in at an unusual hour from a remote location and gains access to sensitive files in your network, the transpired events will trigger a time anomaly and a pattern anomaly, respectively. This will result in an immediate increase in the user's risk score. With alerts on users and entities with high risk scores, you can immediately attend to the related security events. By further investigating the detected incident, the security admin can determine the cause and respond to it, minimizing the damage.

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.