4 Identifying suspicious activities & anomalies

Detecting security threats

The objective of implementing a log management process is to detect and mitigate security threats at an early stage. Security teams must be instantly notified about potential security threats in order to investigate and mitigate breaches. Identifying security threats is like looking for a needle in a haystack. A combination of log analytics using traditional SIEM techniques, and new-age techniques based on machine learning must be leveraged by security teams to achieve this objective.

Three key mechanisms to identify incidents

- **Alerting rules:** Rules must be configured for detecting a wide range of indicators of compromise (IoCs). Alerting rules are effective in detecting individual events, such as a member being added to a privileged security group, that can jeopardize the security of an organization.

- **Correlation algorithms:** Oftentimes, attacks consist of a chain of security alarms triggered on multiple sources, such as VPNs, servers, and applications. Correlation algorithms watch out for suspicious patterns of events across the entire network, and help identify complex attack patterns before it's too late.

- **User and entity behavior analytics (UEBA):** Machine learning-based analytics can profile the behaviors of users and systems in a network to identify anomalous actions that deviate from the baseline. For example, if a user who normally works from 9am to 5pm tries to access a sensitive file at 2am, a UEBA tool can flag this anomaly and raise the risk score of the user.

Security teams must employ all the techniques above to view security threats holistically and maximize their chances of detecting a threat at an early stage.

Log360's robust analytical capabilities

Log360, along with its UEBA add-on, provide cutting-edge analytical capabilities that bring together the power of rule-based incident detection and machine learning-based anomaly detection. With both of these capabilities, Log360 monitors suspicious events pertaining to user access to cardholder data, and helps mitigate such incidents before they result in a data breach.

Note: It is crucial to have a process in place to follow up on security incidents. Refer to the resource on "Responding to security incidents" on the Resource page to learn more.