ManageEngine
Log360

DATASHEET

Behavior analytics in Log360

Traditional security systems follow rule-based threat detection mechanisms, like correlation, to analyze log data and detect malicious activities. Unlike traditional security solutions, user and entity behavior analytics (UEBA) focuses on user activities and behavioral patterns. This technology takes into account these patterns of usage to detect anomalous behavior, helping you spot them quickly and minimize damage.

Log360, a simple-to-use but powerful security information and event management (SIEM) solution, combines the power of both rule-based and behavioral analytics-based threat detection. The solution's UEBA component helps detect cybersecurity threats in your work environment through behavior analytics.

Product features

Log360's UEBA add-on focuses on monitoring actions across the network. Using analytics based on the actions of users and entities, it can detect count, time, and pattern anomalies, and solve real-world challenges like insider threats, data exfiltration, account compromise, malware, and logon anomalies.

The add-on's training period is one week, in which it creates a standard baseline for each user and entity after observing their behavior. Any deviation from the normal behavior is then marked as anomalous activity, and security analysts are alerted over email and SMS. The UEBA add-on also comes with a built-in risk management system that assigns risk scores for every anomaly based on its severity. Security professionals can then investigate the suspicious event and respond immediately, preempting attacks.

Below are some security threats that Log360's behavior analytics help detect.

• Insider threat detection

An insider threat is a malicious security threat to the organization's data posed by an individual operating inside the organization. Here's an example of how Log360 can help organizations detect insider threats by monitoring user behavior.

Imagine a malicious insider trying to sabotage their organization by gaining access to sensitive files unrelated to their job function at an unusual hour. The solution marks this event as suspicious behavior, and triggers a pattern anomaly and a time anomaly. This is followed by a sudden increase in the malicious insider's risk score based on their unusual behavior, notifying the security admin instantly so they can investigate the insider's activities and take appropriate action.

Log360 UEBA can detect suspicious activities that might indicate insider threats, such as irregular online behavior, unusual access activities, credential abuse, and abnormally large uploads or downloads of data. As part of your organization's insider threat management program, you can also put users with high risk scores on a watch list and monitor them closely.

• Account compromise

A compromised account is a user account accessed by someone unauthorized to access that account. Cyberattackers use a number of methods, like password spray attacks, brute-force attacks, pass-the-hash attacks, and more to gain unauthorized access to accounts. Here's an example of how Log360 can help organizations detect account compromise by monitoring user behavior.

Imagine a hacker trying to gain access to an employee's user account by sending a phishing email with downloadable malware in it. The malware causes suspicious services to be installed on the host machine. This event of suspicious software installation triggers a pattern anomaly, instantly resulting in an increase in the user's risk score.

The hacker then proceeds to access the account from a remote location, moving laterally across the network to obtain further access to other accounts. Once again, the risk score is increased, and as the incident continues to become a critical security threat, it can attract the attention of the security admin immediately, and enable them to respond to the issue.

Log360 constantly monitors log data to find indicators of account compromise like Windows Registry anomalies, event logs being cleared, multiple file modifications, and much more.

- **Data exfiltration**

Data exfiltration is the act of unauthorized transfer of data from an organization to somewhere outside. It can either be carried out manually with the use of an external storage device like a flash drive, or automatically through a malware script. Here's an example of how Log360 can help organizations detect data exfiltration attempts by monitoring user behavior.

Imagine a malicious insider attempting to exfiltrate the organization's customer database. First, they log in to an SQL server and perform multiple data manipulation language (DML) queries, and eventually create numerous files with the customer information. The events immediately trigger back-to-back count anomalies.

Then, the insider plugs in a USB drive to download the files, which in turn triggers a pattern anomaly. The suspicious activities of the user increases their risk score, alerting the security admin, who can then respond to the incident quickly.

Log360 monitors changes like abnormal file reads, abnormal file downloads, unusual removable disk operations, and much more, which can mitigate a potential data exfiltration attempt, saving the organization time, effort, and money.

- **Advanced persistent threat detection**

During an advanced persistent threat, attackers use continuous hacking techniques to gain access to a system and remain in the network for a prolonged period of time, which can cause immense damage. While the end goal may differ, advanced persistent threats usually follow a pattern that involves gaining access, establishing a foothold in the network, obtaining privileges, moving laterally to access other systems or servers, and creating a backdoor to access the system again in the future.

Log360 UEBA is able to detect these changes, and mark them as suspicious activities after triggering pattern anomalies for the compromised user or account. The risk management component assigns risk scores for every anomaly based on its severity, enabling the security admin to quickly investigate the threat.

With the risk management component, security admins can prioritize the highest risks, perform proactive risk assessments at regular intervals, increase productivity by saving time and effort, and detect and respond to persistent threats.

Log360 UEBA benefits

- Analyzes anomalies across your environment's users, servers, datastores, cloud infrastructures, workstations, firewalls, Active Directory, and network devices in real time.
- Provides risk scores for each anomaly; this feature can be customized to your needs. This risk-based assessment helps prioritize threats based on severity.
- The dashboard and reports provide actionable insights into each event based on their source and timestamp, helping you investigate threats quickly and thoroughly.

Supported sources:

Log360 UEBA analyzes log data from different sources in your environment, including:

- Windows devices
- Firewalls
- Routers
- Workstations
- Databases
- Microsoft SQL servers
- File servers

About 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, 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.

ManageEngine
Log360

$ Get Quote

Download