ManageEngine
Log360

SOLUTION BRIEF

Monitoring privileged user activity using Log360

www.manageengine.com/log-management

Monitoring privileged user activity using Log360

Privileged user accounts have unlimited administrative powers, which is why they're the most crucial and impactful among all user accounts in any organization. These accounts, predominantly belonging to database administrators, system administrators, and other network administrators, are often the primary target for malicious attackers looking to gain complete access to your organization's network resources. On top of this, any mistakes, whether accidental or intentional, by privileged users are dangerous, as they can lead to data exposure or security breaches.

Without continuous monitoring of privileged user accounts, you won't be able to detect anomalies before they cause irreversible damage. On top of this, regulatory compliances including PCI DSS, SOX, and others mandate the continuous monitoring of privileged user activity. This makes privileged user monitoring not a choice, but a top priority.

Monitoring the activities of privileged users in your organization is easy with Log360. Its privileged user activity monitoring provides many capabilities including security analytics to help paint a clear picture of what your privileged users are up to. In this document, we will explore Log360's different capabilities with which you can protect your organization's critical assets, meet compliance requirements, and mitigate both external threats and insider threats.

Log360's machine-learning-based privileged user activity monitoring add-on

When a privileged user logs in at unusual hours, when excessive logon failures occur, or when a file deletion takes place from a host that is not generally used by any of your users, Log360 flags these as anomalies and sends alerts to notify the security team.

Powered by machine learning (ML), the Log360 UEBA add-on helps organizations monitor privileged user activity captured in logs and identifies any behavioral changes. This way, user activities that would otherwise go unnoticed are flagged, reducing the time it takes to detect and respond to threats. With this capability you can:

- Detect anomalies based on time, pattern, and count.
- Identify, qualify, and investigate internal threats.
- Detect unauthorized access to sensitive data and authentication failures.
- Spot configuration changes, registry changes, and other system changes.
- Detect user account compromise and data exfiltration.

Additionally, Log360 couples risk assessment with the behavioral analytics to spot slow attacks and advanced persistent threats. Every anomaly is tied up with a risk score, and user risk scores change based on the activities they perform. You can add a user to the watchlist if you find the activities of that user to be suspicious. Further, the risk level for anomalous events can be dynamically adjusted based on your organization's requirements, so you can easily determine which events are malicious and concentrate on those first.

Predefined audit reports for privileged user monitoring

Log360 simplifies privileged user activity monitoring with predefined reports, which show data in graph form for easy understanding. You can also create custom reports to meet the specific needs of your organization, and export them in different formats such as PDF, XLS, HTML, and CSV. With this capability, you can also:

- Audit administrator activity.
- Track privileged user access to critical data.
- Detect privilege escalation.
- Receive alerts on suspicious activity.

Permission change monitoring using Log360

Log360 offers analytical insights for events such as NTFS permission changes for privileged users and groups. With this capability, you can:

- Automatically lock down privileged accounts that have been inactive for a while.
- Use built-in reports to gain in-depth visibility into the privileged permissions held by users and groups.
- Create privileged roles for task delegation and audit the actions performed by these delegates.

You can also provision user accounts in bulk and assign them the privileges they need using this capability.

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, 2020.

Get the report

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