USE CASE

Privileged User Monitoring

When it comes to protecting a network from insider threats, organizations need the ability to keep a watchful eye on its privileged users. This includes business users with direct access to confidential data systems, as well as administrators with the ability to create and modify permissions, privileges and access to any device.

The challenge is finding a way to keep an eye on all systems within a large, heterogeneous environment and quickly identify improper or malicious behavior when, in most cases, the people responsible for the behavior in question are the ones with access to the log files that record all user activity.

LogRhythm provides unprecedented auditing and insight into privileged user activity, across the enterprise.

Watching Privileged Users

CUSTOMER CHALLENGE

"Administrator" privileges usually include the ability to modify or even remove activity log data. While most administrators use their access privileges responsibly, it is imperative to establish an independent and automated means of capturing and storing log data associated with administrator activity and alerting on concerning behavior.

LOGRHYTHM SOLUTION

LogRhythm's real-time, automated, centralized and secure collection of log data provides independent access to privileged user activity logs without relying on the privileged user for collection.

ADDITIONAL BENEFITS

Using the alarming tool, LogRhythm users can set up alerts to send out notifications any time a privileged user account is added or modified, including information about who created the account.

Maintaining Log Integrity

Most privileged users behave in a responsible and ethical manner. But, the high-level access tied to their user permissions means that a single privileged user with malicious intent can cause enormous damage to an organization. Because they have the means to modify data of recorded activity, tracking the culprit can be difficult.

LogRhythm provides independent access to privileged user activity logs without relying on the privileged user for collection.

Immediate collection by LogRhythm with cryptographic hashing provides a digital chain-of-custody that eliminates the ability for privileged users to tamper with activity records and conceal nefarious activity.

LogRhythm's SecondLook™ archive restoration wizard allows administrators to immediately query against any archived data, which is automatically validated to maintain the digital chain-of-custody.

Powerful, Rapid Forensics

Recording log data related to privileged user activity is a start. However, gaining meaningful and timely insight into inappropriate and/or concerning behavior with intelligent and automated correlation, alerting and reporting is like trying to find a needle in a haystack.

LogRhythm provides Intelligent IT Search™ capabilities for rapid user-level investigations, displays aggregate and trending visualization to identify behavior based patterns, and delivers automated alerting on specific privileged user activity.

LogRhythm users can quickly use the investigate tool on all activity performed by a newly created user, using a combination of detailed forensic views and interactive graphical analyses. A simple, wizard-based GUI makes investigations quick-to-run and easy to save for future use.