USE CASE

Fraud Detection and Prevention

When it comes to protecting a network from fraud, organizations need to keep a watchful eye on a wide range of activities that are frequently difficult to detect. Acts of fraud frequently involve a series of legitimate activities that individually do not warrant notice. However when they are observed in the right sequence over time, pattern recognition can detect that suspicious activity is taking place.

Compounding the problem is the fact that many organizations fail to maintain a usable digital paper trail or lack the pattern recognition, visualization and anomaly detection capabilities to conduct accurate and quick forensic analysis on user behavior. Performing investigations involves manually looking at audit records and other log data after the fact and real-time detection is frequently nonexistent.

LogRhythm provides organizations with automated log collection and analysis with advanced correlation and pattern recognition to help detect and prevent fraudulent activity.

Exposing External Plots

CUSTOMER CHALLENGE

Many acts of fraud are the work of an internal user, but specific actions can be difficult to pinpoint because they are frequently disguised as legitimate activities. A perpetrator will hide fraudulent activity by creating false or duplicate credentials to perform seemingly legitimate behaviors that might otherwise go undetected.

LOGRHYTHM SOLUTION

LogRhythm's Advanced Intelligence (AI) Engine can immediately recognize and alert on suspicious insider activity, such as unauthorized accounts being granted escalated privileges. Right-click correlation allows instant access to user account details to identify what constitutes appropriate access.

ADDITIONAL FEATURES

Immediate collection by LogRhythm with cryptographic hashing provides a digital chain-of-custody that eliminates the ability for users to tamper with activity records to conceal fraudulent behavior. Administrators can immediately query against any archived data for long term forensic analysis.

Detecting Identity Theft

Enterprise networks are frequently accessed by customers and employees from numerous geographic locations, including users who log in from multiple locations within a short period of time period of time. Identifying improper usage of authorized credentials among thousands of legitimate logins is a difficult task.

LogRhythm's AI Engine automatically detects and alerts on suspicious behavior, such as one user logging in from two different locations at the same time. Visualization tools can be used to see geographic anomalies over any number of activities.

LogRhythm ensures that all events are accurately sequenced and pattern recognition is based on chronological fact. A universal timestamp applied to every log ensures that the actual time of occurrence is recorded accurately – regardless of external factors, such as an out-of-sync server clock, delayed delivery of a log or differences in time zones.

Discovering Acts of Fraud

Suspicious behavior patterns are frequently overlooked because they are designed to look like legitimate transactions using legitimate accounts. Individually unremarkable, ten bank deposits of similar amounts being simultaneously made to one account at ten locations may be related to money laundering or other acts of fraud.

LogRhythm's AI Engine can generate an alarm that detects multiple deposits to the same account from different locations within the same time period. Once the alarm is triggered all activity on that account can be easily accessed from the same window, allowing immediate forensic access to long term behavior trends.

AI Engine's easy-to-use GUI with its drag-and-drop interface allows LogRhythm users to quickly and easily create or modify advanced correlation rules. While common scenarios are provided out-of-the- box, pattern recognition can be quickly tailored to match each organization's unique requirements.