USE CASE

Actionable Intelligence Through Interactive Displays

LogRhythm™

With the steady flow of information flooding any monitoring tool, consolidating meaningful data points and allowing the user to focus on relevant information in a single, dynamic view is critical for usability. In order to accomplish this it is imperative to be able to quickly organize and filter information in real time, without having to jump through multiple screens and views to tie event data together.

With most solutions, sifting through large amounts of heterogeneous data requires paging through or loading different preconfigured screens – easy access to associated context remains limited. An initial search or preconfigured view rarely yields the refined results needed to provide actionable intelligence. The ability to work directly with data in an efficient and intuitive manner is a critical component of usability.

LogRhythm's fully interactive interface provides true access to all event data directly on-screen, maximizing its effectiveness.

Easy Access to Relevant Data

CUSTOMER CHALLENGE

Many consoles limit the ability for users to interact directly with forensic data as it appears on the screen. Accessing additional event detail or correlating multiple data points on the fly for root cause analysis is difficult, requiring the user to page through multiple screens or views.

LOGRHYTHM SOLUTION

LogRhythm allows administrators to sort and filter data directly on-screen, providing instant access to the right data directly in a single view. Administrators can filter and sort on any combination of over 100 data enrichment fields for unprecedented and immediate forensic insight.

ADDITIONAL BENEFITS

LogRhythm users can easily select what information is displayed and how it is presented, tailoring each view to fit any situation. A consistent look and feel allows users to easily duplicate this process within any of LogRhythm's tools.

Rapid Drill-Down

CUSTOMER CHALLENGE

Macro-level visualization is critical for understanding enterprise-wide asset relationships, behavioral trends, and event patterns. But many tools don't allow users to quickly and easily access the underlying event data for rapid forensics and incident response.

LOGRHYTHM SOLUTION

LogRhythm administrators can click through any visualization tool for immediate drill-down access to relevant log and event detail. Users can also mouse-select specific time frames on trending graphs to zoom in on interesting trends without having to modify query parameters.

ADDITIONAL BENEFITS

Once any investigation is complete the data can be run as a report through a simple right-click process. Information can be sent directly to the people who need it in the appropriate, usable format (.pdf, .xls, etc.).

Delivering Actionable Information

CUSTOMER CHALLENGE

With most tools, adding context to event data involves running several queries and jumping from one screen to the next. Identifying a significant event in one view and having to page through information or use a different tool to investigate the details is inefficient and time-consuming.

LOGRHYTHM SOLUTION

With any event LogRhythm provides instant access to multiple avenues for further forensic analysis without leaving the initial screen. Administrators can right-click to extract host, network or user-related context, perform extended event correlation, or create detailed and/or summary reports.

ADDITIONAL BENEFITS

Once an investigation is complete, administrators can use the same right-click process to create an alarm that is preconfigured to alert on any event(s) identified as significant. Alarm parameters can be easily tuned for additional accuracy in an intuitive wizard-based interface.