USE CASE

Visualizing Log & Event Data – Completing the Picture

LogRhythm

A typical IT environment generates far more log and event data than IT administrators can possibly manage. Valuable operations, security and audit information is contained within the logs but the sheer volume can quickly hide relevant information in an avalanche of marginal data. That is one of the reasons enterprises are turning to log management and SIEM solutions to help manage the abundance of data.

Log management and SIEM solutions automate the process of collecting log and event data and making it useful. Even with log aggregation, event filtering, real-time alarms and automated reports, though, some patterns of nefarious behavior can escape detection. Seeing activity trends unfolding over time combined with a map of the relationships between data sources -- inside and outside of the network -- makes threat detection and forensic analysis easier than ever.

LogRhythm's advanced visualization tools help you complete the picture of what is happening when it happens throughout your global IT environment, including where it originated and the scope of impact.

Exposing Significant Patterns

CUSTOMER CHALLENGE

Significant activities related to IT operations or security take place over time and consist of a series of actions that might not individually attract notice. Investigating user behavior may show activities that don't indicate malicious activity when displayed in a typical list view.

LOGRHYTHM SOLUTION

LogRhythm offers trending views within any investigation, providing the means to look at specific user behavior patterns with time-of-day- and day-of-week context. Administrators can easily identify anomalous behavior trends, such as unauthorized users logging in after-hours.

ADDITIONAL BENEFITS

Once a significant pattern is found, simple selection and click-through features allow rapid-zoom views into relevant event data. As search results narrow, users can apply visual analyses to isolate event specifics or use detailed list views that correlate directly to the graphical displays.

Pinpointing the Data

Tracking anomalous behavior for 100s of users and devices is challenging – particularly without a visual point of reference to see behavioral trends. Even with tools to graph network activity, observing network behavior without relevant context allows important events to escape notice.

LogRhythm enables the correlation of flow data with other event data, creating trending views based on logical criteria. It allows for easy focus on details such as activity by specific individuals or user groups, applications and/or devices, from specific network segments, or communication with suspicious locations.

LogRhythm allows mouse-control selection of specific target ranges within a given investigation. Administrators can quickly highlight and zoom in on suspicious activity trends for rapid, click-through forensics.

Global Visibility

Zeroing in on specific event details is critical, but so is understanding its overall impact. Forensic evidence of event propagation may exist in 100s of locations, escaping notice without an additional layer of visual context.

LogRhythm's Network Visualization tool maps communication and relationships between hosts from anywhere in the world – inside or outside the network – with automated geolocation data maximizing relevant context.

When a suspicious source or destination is identified, administrators can right-click to create an automated alarm, allowing real-time reaction as a new host is infected or engages in suspicious behavior with a rogue external destination to quickly minimize additional event propagation.