USE CASE

Advanced Correlation for Operations

LogRhythm

Advanced correlation and pattern recognition in log management and SIEM solutions has traditionally been limited to identifying and alerting on security specific events. However, the same type of logic that can detect a security incident can apply to operational issues as well. The problem with most SIEM solutions is that they tend to filter out the bulk of log data before it is ever processed by the correlation engine.

LogRhythm's Advanced Intelligence (AI) Engine™ changes all of that by allowing companies to identify and respond to complex and oftentimes undetectable operations events in real-time. By collecting and analyzing *all log data* without worrying about performance-related filtering requirements, LogRhythm provides valuable insight into operational issues that can impact system-wide IT performance, company productivity and even revenue.

LogRhythm collects and processes all log data, performing advanced correlation on over 50 different fields, including data related to operations as well as security.

Detecting Application Failures

CUSTOMER CHALLENGE

IT systems have a constant flow of processes and services stopping and starting, but keeping track of them in an enterprise environment is difficult due to the sheer volume. Without a way to automatically detect that a critical process or service has failed to restart, an organization may not know that mission critical applications and devices are not operating correctly.

LOGRHYTHM SOLUTION

AI Engine™ provides preconfigured advanced correlation rules to identify in real time when a critical process or service does not restart within an expected period of time. The wizard-based, drag-and-drop GUI provides an easy interface for modifying and creating additional rules specific to each environment or potential scenario.

ADDITIONAL BENEFITS

LogRhythm can create an independent log of all processes with valuable context, including process name, user or account that owns the process, and process start time and duration. This helps close the information gap created by the fact that many systems do not consistently log processes on their own.

Enforcing Operational Control

CUSTOMER CHALLENGE

Many operational issues are the result of human error – such as a mistake made during a routine task or a failure to follow proper change management procedures. Many times a change will be made without detecting a resulting error.

LOGRHYTHM SOLUTION

LogRhythm can automatically alert whenever a configuration change is followed by any sort of error condition, such as a server entering into a loop of shutting down and restarting, indicating a misconfigured device. Alarms can be configured to be as general or specific as is appropriate to a given situation.

ADDITIONAL BENEFITS

LogRhythm helps administrators enforce policy and make sure that unauthorized changes do not impact production operations or critical updates through rapid root cause analysis and response. Identifying additional systems that may be impacted during change control provides administrators better information for improving on the change management process in the future.

Reducing Downtime

CUSTOMER CHALLENGE

Physical issues, such as a failing hard drive or fan failure causing a server to overheat, can disrupt operations but aren't always detected automatically or are difficult to associate to a specific issue. Determining the origin and scope of a failure is difficult when a server or device is offline, slowing the time it takes to troubleshoot and resolve the issue.

LOGRHYTHM SOLUTION

AI Engine™ can automatically generate an alert when a hardware-related warning condition, such as a high temperature warning or fan failure, is immediately followed by a system shutdown. This ties the shutdown to the cause of the system failure, allowing quick resolution and preventing repeat incidents.

ADDITIONAL BENEFITS

LogRhythm can identify performance issues tied to user behavior, such as excessive browsing or streaming large amounts of data and other activity that may impact WAN performance. Logical entity grouping can organize log and event data by department and executive level and detailed reports can correlate all activity by business unit, providing easy access to relevant usage details for shared resources.