Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Intelligence in Action: A Review of LogRhythm's SIEM 2.0 Big Data Security Analytics Platform

Copyright SANS Institute
Author Retains Full Rights
Security Intelligence in Action:
A Review of LogRhythm’s SIEM 2.0
Big Data Security Analytics Platform

December 2012
A SANS Whitepaper

Written by: Dave Shackleford

The LogRhythm Interface  PAGE 2
Drill-Down Searching and Analysis  PAGE 4
Advanced Features  PAGE 8
Knowledge Base Modules  PAGE 11
Introduction

Increasingly, organizations are gathering security event data and logs from systems and applications for a broad variety of purposes. According to the SANS 8th Annual Log Management Survey published in 2012, the majority of responding organizations are leveraging security logs and event data for the following reasons:

- Detecting and tracking suspicious behavior
- Supporting forensic analysis and correlation
- Preventing incidents
- Achieving/proving compliance with regulatory requirements

Logs are an excellent starting point for effective security information and event management (SIEM). Respondents to the SANS 8th Annual Log Management Survey, however, are—for the first time in the survey’s eight-year history—regressing in their capability to catch advanced threats. Why? Because they have too much data to analyze and they can’t separate the problems from the noise. The top problem reported by more than 600 responses to the survey was “Identification of key events from normal background activity.” “Lack of correlation” followed as the second most challenging, and “Lack of analytics capabilities” came in third place.

IT and security staff need tools that are just as advanced as the tools threat actors use. In the case of an event, network defenders need to be able to quickly and accurately sort, normalize and analyze large sets of event information from multiple devices. Such capabilities should also be available for alerting and forensics. Analyzing the vast amount of log data is a typical “Big Data” problem, complicated by the need for advanced analysis in real time as well as after the fact.

One such analysis tool is LogRhythm version 6.1, which SANS had the opportunity to review upon the eve of its release. The product can analyze and report on security data in many different ways, and it offers a range of easy-to-use features. New capabilities in this release focused on more complex analytics and analysis, as well as behavioral whitelisting and analysis.

This review looks at the fundamental capabilities of LogRhythm that should be in any logging and event management platform, as well as some of the more innovative new features included in the latest version of the software.

---

1 www.sans.org/reading_room/analysts_program/SortingThruNoise.pdf
2 www.sans.org/reading_room/analysts_program/SortingThruNoise.pdf, page 6
The LogRhythm Interface

Upon logging into the LogRhythm console, the first screen presented is the Personal Dashboard. This screen is a highly customizable interface that enables security analysts to choose from a variety of different views and graphs of security data, as well as specific security events and baselines.

Analytic categories are presented on the left-hand side of the screen for quick display in the dashboard. These categories include the following:

- **General Analysis**: Fundamental operations for a security analyst, including aggregation of logs and events, audit, operations, and security logs and events, are listed by classification categories, logs by type and logs by direction of traffic.

- **Time Analysis**: In this section, analysts can easily view logs and events broken down by time of event occurrence. These items are further broken down by type, direction of traffic and variably granular time options (e.g., weeks versus days).

- **Statistical Analysis**: This category allows security analysts to view granular data and graphs about logs and events from the environment. Analysis categories include log source statistics, origin login and host statistics (i.e., system and user information), impacted hosts and applications, and even vendor message ID values that can be broken down for analysis.

- **TopX Analysis**: The TopX categories are open, flexible containers that analysts can populate with the top events in numerous categories. Examples might include the Top 10 inbound and outbound packet types, the Top 10 user accounts appearing in log events or the Top 20 domain names present in events. These categories can be added to the Personal Dashboard at will, allowing analysts to create elaborate and adaptive monitoring options.

Figure 1 shows an example of a customized Personal Dashboard.
The next function in the interface we analyzed was the ability to use LogRhythm’s Lists feature to build compliance reports, alerts and advanced correlation rule sets. Such a list is a logical grouping of multiple data types or rule aspects within the product, and they can be created by automatic population from APIs or manual import. These lists can greatly simplify rule creation and investigations by grouping common items. For example, Figure 2 shows a simple list of blacklisted hosts.

![Figure 2. A Simple List](image-url)
Drill-Down Searching and Analysis

LogRhythm’s interface offers rich drill-down and analysis capabilities. For this review, we examined these features’ suitability for drilling into events, parsing log entries and events that are monitored, creating various types of targeted investigations, and specifying what data can be delivered in real time.

Event Drill-Down

Although there is no “easy” button in advanced security event analysis and monitoring, the LogRhythm interface was genuinely intuitive, with few frivolous areas of focus. For example, to drill down into events from the Personal Dashboard, one simply has to double-click on any area of a graph or chart, and a more detailed page appears, commencing the investigation. As shown in Figure 3, we drilled into security event logs by Classification, which displayed the last 60 minutes of activity.

![Figure 3. Basic Event Drill-Down from the Dashboard](image)

We were also able to drill down to events within the timeline graph, and we used a variety of filters to look at the log sources, primary offending hosts, affected systems and applications. Finally, we looked at a network visualization of major event sources, as shown in Figure 4.

![Figure 4. Network Visualization of Event Sources](image)
Analysis

We explored two features in detail: the Tail and Investigations capabilities, which allow real-time event monitoring and more detailed analysis for prioritized events.

The Tail feature simply creates a view of specified logs that updates in real time. One such view appears in Figure 5.

Figure 5. Configuring a Tail
Another example of a Tail in action appears in Figure 6—this one tracking a series of network connectivity events.

![Figure 6. The Tail Feature in Action](image-url)
Analysts can use the Tail tool to quickly get a “big picture” view of all events happening in the environment, at both the log layer and the event layer, across multiple log sources. The live stream of data can also be filtered with Tail to provide focused views. This filtering allows security analysts to see everything happening at once while concentrating on patterns of particular interest, which may lead to more targeted analysis using the Investigations feature.

Investigations was another simple feature to employ, with an intuitive wizard that walks analysts through the process of selecting log and event sources, time and date ranges, specific systems, lists and other rule criteria. We were able to quickly create an Investigation on all events from a defined list of blacklist hosts. Within minutes, we had a wealth of data related to traffic patterns and direction, the hosts involved, affected applications and more. Figure 7 shows a view of this investigation.

With this information, IT groups can target their response and remediation with greater accuracy.

These features demonstrated, in a short time, the powerful analytics capabilities built into LogRhythm for the layperson. The GUI is easy to use and consistent across the various tools and capabilities, and the user can create advanced rule sets quickly using wizards and lists. The tool has the added capability to label all searches and functions as private or public, depending on the sensitivity of the analysis being performed.

Moreover, LogRhythm 6.1 exhibited an exemplary level of ease of use, thereby overcoming a major drawback of traditional SIEM systems that come with a steep learning curve. Tools such as these should also help organizations overcome their problems with security event analysis, which is a clear pain point to the more than 600 respondents taking the SANS log management survey.
Advanced Features

LogRhythm has added a number of advanced analytics features to the product in software version 6.1 that allow analysts to perform in-depth assessments of events within the environment. One of the most intriguing features is that of behavioral whitelisting. Behavioral whitelists help analysts automate the discovery of "what's normal" by allowing searches and baseline definition across users, networks, hosts, applications and both external and internal contexts. Baselining is a critical first step to any security program, but it has traditionally been a challenge for organizations with large, distributed networks. Solid behavioral whitelisting features, combined with advanced intelligence, analysis and reporting, give LogRhythm 6.1 the tools needed to address the “Big Data” problems our Log Management Survey takers face.

Advanced Intelligence Engine

Accessing the whitelisting profiles required getting comfortable with LogRhythm's Advanced Intelligence (AI) Engine. This engine contains many of the more sophisticated analytics capabilities in the product.

The AI Engine concentrates on behavioral profiles and advanced correlation between widely disparate data and event sources. This combination gives analysts the ability to do more Big Data analytics than before.

The AI Engine offers features and capabilities for real-time analysis, detection and response, and support for rapid forensic drill down through the full universe of log, flow and event data recognized by the LogRhythm platform. In short, the AI Engine can detect conditions in the data sets that traditional SIEM rule sets and correlation methods might otherwise overlook.

Rule Management

The AI Engine's front end is the AI Engine Rule Manager, which contains a set of prebuilt rules. The screenshot in Figure 8 lists a variety of rules that fall into the categories of Connections, Behavior, Critical Events and more.

Figure 8. AI Engine Rule Manager
Advanced Features (CONTINUED)

From here, rules can be added or modified with ease, and one can see the parameters for existing rules, as well as how they are configured. A basic behavioral rule set is “Behavior: Baseline Target Hosts,” which allows users to build a network traffic profile of specific systems defined in Lists. Another example, “External: Account Compromise: Account Scan on Multiple Hosts,” specifically alerts on events that include user account guessing attacks across a variety of systems.

Next, we explored the AI Engine Rule Wizard, which is accessed from within the Deployment Manager screen. The layout for this wizard is unique in that one can choose graphical representations of different rule elements, focusing on rule elements that are either present or not present. This facilitates the behavioral baselines and whitelisting capabilities within LogRhythm’s engine.

The AI Engine Rule Wizard screen is shown in Figure 9, with a simple block-based breakdown of a rule focus of Configuration and a filter set to include Target Hosts.

Figure 9. AI Engine Rule Wizard

All log sources are included, and the rule block was set to trigger an event when any configuration change is detected on specified hosts previously included in a LogRhythm List.

Overall, the rule engine provided sophisticated correlation capabilities in an interface that was simple to use. The graphical engine for adding Observed and Not Observed events and event types was easy to work with, and it allowed us to create very complex correlation rules within a matter of minutes.
Behavioral Analysis

From there, we were able to access the behavioral whitelisting capabilities by selecting the Behavioral tab and creating whitelist profiles that are based on certain traffic types, network flow data or particular lists or events. Behavioral whitelisting allows the analyst to take sophisticated AI Engine correlation rules and build on them with whitelisting profiles. This ties back to a problem for many security analysts: defining a “normal” baseline of traffic and behavior.

The behavioral analysis features in LogRhythm help automate the process of evaluating user, system and application behaviors over time, building baselines and then looking for events or behaviors that deviate from that baseline.

As event collection time periods are defined, they can be stamped as “normal” or “not normal” after the data is collected. This determination is based on inclusion and exclusion filters, time and date stamps, log source information, and more, as shown in Figure 10.

Figure 10. Whitelist Profile Configuration
Another new feature evaluated was the Knowledge Base Modules. These modules offer analysts an expert system for security and compliance assessment. These features include:

- Auditor-approved frameworks that map all in-scope devices and applications
- Out-of-the-box alerts, investigations and reports
- A combination of exception-based alerting with compliance assurance reporting

**Classifying Events and Alerting**

One of the most impressive features in this category was the Common Event Manager, which allows analysts to define specific custom events and event categories that meet alerting criteria within their organizations. An example of a simple test event is shown in Figure 11, which includes account modification events, with a BugTraq ID thrown in for good measure. (The BugTraq ID appears in the Associated Knowledge Base Artifacts tab.)

![Figure 11. A Sample Common Event Manager Entry](image-url)
Reporting

LogRhythm 6.1 includes a wealth of general purpose and compliance-specific reports, as well. The most useful aspect of this feature is the Knowledge Base Modules element. This knowledge base includes the experience of LogRhythm's team, and even other companies using the product, to define reports and event criteria that meet specific compliance mandates. These Knowledge Base Modules are shown in Figure 12.

Sharing the Knowledge

Another beneficial feature is LogRhythm’s Universal Descriptor Language (UDL). The UDL is a simple rule and module definition format that allows the software to create new reports, rule modules and correlation routines, much like the standard definition language used by the open source IDS/IPS Snort tool. Thanks to UDL, all LogRhythm customers become part of a larger community that can share with each other and receive intelligence from the LogRhythm team—and in a shorter time frame than most SIEM platform users normally could.

This method of returning to the community doesn’t require sharing proprietary data or compromising trade secrets; in effect, it turns the entire LogRhythm customer base into an early warning system. Probing attacks that might otherwise have been ignored or dismissed can be correlated against the larger user population, allowing all participants to be better prepared.
Conclusion

This review scratches only the surface of LogRhythm’s advanced analytics capabilities. The product is remarkably easy to use—analysts can get started very quickly, data can quickly be gathered and correlated, and rule sets can be combined with robust reporting in a relatively short period. Extensive rule sets can be created, both signature-driven and behaviorally driven, for correlation and reporting.

After exploring the new 6.1 version of LogRhythm for several weeks, its wide range of features continued to impress. The usefulness of these features will become apparent to organizations as they use them to detect and react to more automated, advanced threats their standalone monitoring systems aren’t catching.

The new features in version 6.1 that deserve particular attention include:

- User, system and application behavioral event analysis
- Out-of-the-box reporting and expert reporting modules
- Capability to set standardized and custom alerts
- Expert-driven knowledge modules to aid in analysis

Although these are certainly not the only new and useful features in this product, these are the most critical, given the issues with which SANS survey respondents are grappling. This new release provides a much more advanced engine for event correlation, analysis and data mining than many comparable tools on the market.

With the addition of the Knowledge Base reporting modules, analysts can create a vast number of reports and dashboard elements for analysis. LogRhythm’s 6.1 SIEM platform doesn’t skimp on features.

These new features should help IT teams to monitor more effectively and respond more quickly to advanced threats.
Dave Shackleford, founder and principal consultant with Voodoo Security, is a SANS analyst, instructor and course author, as well as a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert, and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft and CTO for the Center for Internet Security. Dave is the author of *Virtualization Security: Protecting Virtual Environments* from Sybex. Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently leads the Atlanta chapter of the Cloud Security Alliance and sits on the board of the SANS Technology Institute.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Date Range</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>