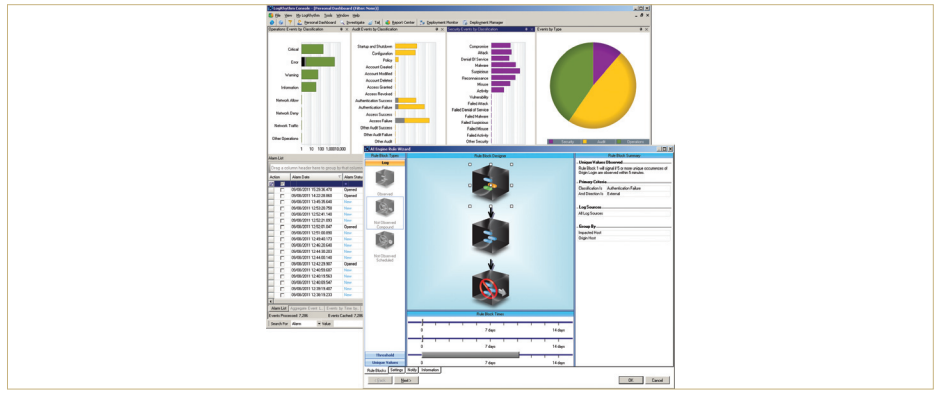
Advanced Intelligence (AI) Engine™ from LogRhythm



PRODUCT REVIEW PRODUCT REVIEW PRODUCT REV

Log management and analysis are essential for achieving regulatory compliance, but successful business intelligence rests on making sense of the huge volumes of raw data that can be gathered from network devices. LogRhythm has always offered an integrated solution for log analysis, file integrity monitoring and SIEM (security information/event management), and its latest addition, Advanced Intelligence (AI) Engine™, takes this to the next level by providing sophisticated correlation and analysis of all log data.

Analysing single events on the network can lead to the often mistaken conclusion that there is no security threat. However, correlation of many seemingly disparate events can show a different picture and reveal threats such as intrusion attempts, the spread of malware, and even fraud.

The core LogRhythm products can monitor for specific events and send out alerts when they are detected. AI Engine takes this process much further as it can link individual and different sets of events together. Its rule sets combine chains of interdependent events so that an alert only occurs if all conditions in the chain are met. AI Engine is an optional component that integrates with any core LogRhythm product, allowing it to have full access to all gathered log data. Its advanced correlation rule sets, looks for patterns such as suspicious or unusual activity and provides alerting facilities, allowing administrators to respond swiftly to potential security threats.

It runs on dedicated hardware and LogRhythm can provide it either as software or preinstalled on a turnkey appliance. For lab testing we were supplied with LogRhythm's mid-range LRX2-XM core appliance and the LR-AIE2 top of the range model, which they claim can process a remarkable one billion logs per day.

Initial installation only takes a few seconds and all ongoing management is from the main LogRhythm console where the Deployment Manager section already has an entry for the AI Engine appliance. Selecting this option brings up the Rule Manager and AI Engine can start processing out of the box, as LogRhythm provides over 100 predefined rule sets.

Rule set creation is wizard driven and you start by selecting what you want to look for, including specific log messages, quantitative thresholds, and unique values. Within each category you can also look for events that have occurred, or those that haven't occurred, but were expected, possibly within a certain timeframe.

These are used to build rule sets containing chains of events, or rule blocks, where each one defines data sources, filter criteria, time frames, and conditions. Each rule block in the chain also has a specific relationship with the one above it.

For example, the first rule block may look for events that occur within a certain time. When satisfied, the next rule block is activated, but the relationship between the two could have a time limit imposed. It sounds complicated, but we found highly complex rule sets could be created easily using multiple rule blocks and relationships. Furthermore, when a rule set is triggered, any of the standard LogRhythm alerting facilities can be used.

Forensics analysis can be carried out swiftly on events by selecting an alarm in the Dashboard and choosing the AI Engine Event Drill Down Manager. This shows all log entries pertaining to that rule set along with event details which could include the log source, the impacted host or application, and the user account login details.

AI Engine provides a real-time visibility of risks and threats in enterprise networks and is capable of detecting many security threats that could easily be missed using traditional methods. It will prove a valuable ally in, for example, achieving regulatory compliance. Its seamless integration makes it the perfect partner for LogRhythm's log data management and analysis systems. NC

Product: Advanced Intelligence (AI) Engine™
Supplier: LogRhythm
Tel: 01628 509070
(303) 413 - 8745
Web site: www.logrhythm.com