Feature Brief

AI Engine for Advanced Security Correlation

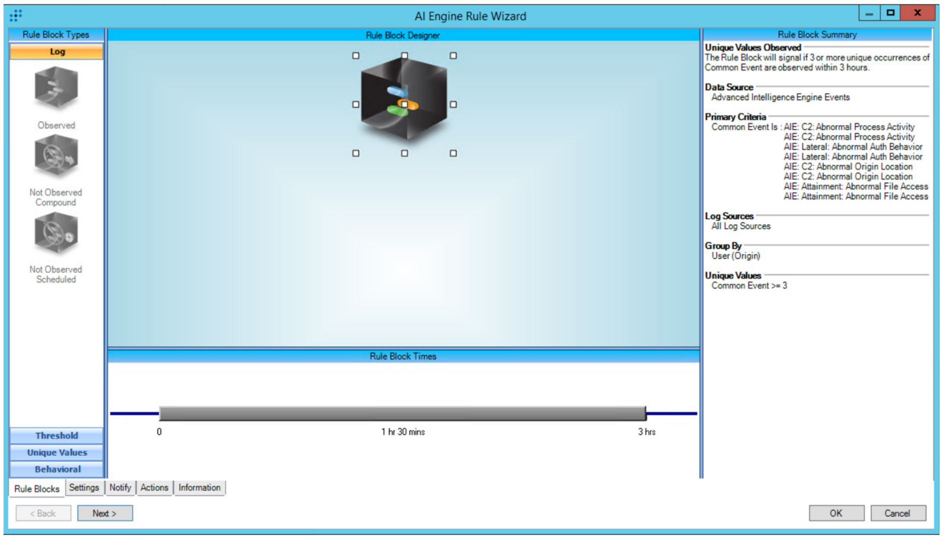
Discover Operations and Security Risks in Real Time

Understanding what's happening within your organization's log data is key to uncovering abnormalities or threats in your environment. LogRhythm's AI Engine, an integrated component of the LogRhythm NextGen SIEM Platform, evaluates log data and performs advanced analysis on all log messages in real time. AI Engine detects conditions over multiple data sources and time spans, giving your security team greater visibility into potential anomalies or issues. What's more, AI Engine employs scenario-based analytics, which is often the best way to incorporate detection of indicators.

Real-Time Visibility to Threats

AI Engine identifies statistical deviations and behavioral abnormalities that occur in real time using advanced pattern recognition. Our patented technology uncovers sophisticated threats and critical operations issues that otherwise might go undetected. With over 900 preconfigured, out-of-the-box correlation rule sets and a wizard-based drag-and-drop graphical user interfaces, AI Engine make it easy to create and customize rules that predict, detect, and respond to critical events in your environment, including:

- Sophisticated intrusions
- Insider threats
- Fraud
- Compliance violations
- Disruptions to IT services
- Behavioral anomalies



Unique Values Observed
The Rule Block will signal if 3 or more unique occurrences of Common Event are observed within 3 hours.

Data Source
Advanced Intelligence Engine Events

Primary Criteria
Common Event Is : AIE: C2: Abnormal Process Activity
AIE: C2: Abnormal Process Activity
AIE: Lateral: Abnormal Auth Behavior
AIE: Lateral: Abnormal Auth Behavior
AIE: C2: Abnormal Origin Location
AIE: C2: Abnormal Origin Location
AIE: Attainment: Abnormal File Access
AIE: Attainment: Abnormal File Access

Log Sources
All Log Sources

Group By
User (Origin)

Unique Values
Common Event >= 3

Figure 1: AI Engine Feedback Rule references AI Engine Events

Benefits

- **Simplified threat detection** with an extensive set of out-of-the-box correlation rules
- **Real-time identification** of statistical deviations and suspect behavior
- **Focused security responses** guided by Risk-Based Prioritization

AI Engine in Action

AI Engine's numerous predefined advanced correlation rule sets are configured to run out-of-the-box and act as templates for easy customization. All rules within AI Engine can be quickly modified through a highly intuitive GUI to address the unique requirements of any organization. AI Engine can uniquely collect a variety of events, such as the absence of events in real time. In this case, the service restart event can be seen, but not the service startup on the same host for the same process name.

AI Engine can also maintain context within the rule for things like temporary account usage (i.e., account created). The account that was created was then used to authenticate or do some kind of activity, so the target of the first event is the actor of the second event. Then the account was deleted by the original actor.

Comprehensive Advanced Correlation

Unlike legacy SIEM solutions, AI Engine correlates against all data — not just a pre-filtered subset of security events. Its seamless integration also enables immediate access to all forensic data directly related to an event. AI Engine rules can be defined using all of the LogRhythm schema, and includes context about directionality. These rules can also correlate across different data sources. Our patented Risk Based Prioritization (RBP) value set is assigned to on log data as it's processed. AI Engine also calculates RBP when a rule fires. This enables AI Engine to build trends and expose statistical anomalies based on the risk level associated with specific activity on the network. This ensures analysts address the highest risk alarms first, enabling an automated and effective risk-based monitoring strategy.

Feedback Rules

LogRhythm offers feedback rules in which the output of AI Engine is fed back through AI Engine to allow for higher order correlation and complex event processing. This helps eliminate false positives by automating the process of learning what constitutes "normal" behavior for users, hosts, applications, and devices.

Flexible Deployment Options

AI Engine can be deployed as a dedicated, high-performance appliance, installed as software on dedicated customer equipment, or deployed on multiple virtualization platforms (VMware ESX, Microsoft Hyper-V, and Citrix XenServer). High-performance appliances can process tens of thousands of logs per second and billions of logs per day.

AI Engine possesses a horizontally scalable architecture, allowing for simplified, incremental expansion of the deployment to meet any processing volume requirements. In conjunction with LogRhythm's AI Engine, CloudAI uses behavioral and scenario-based analytics to broaden user and entity behavioral analytics (UEBA) capabilities. All instances of AI Engine are centrally managed through the LogRhythm client console.

Appliance Specifications

Model Series:	AIE7500
Max Processing Rate:	75,000 MPS
Chassis Rack Units:	1U
CPU Cores:	24
Memory (Expendable):	128 (768) GB
Internal Storage:	2.1 TB / 4.48 TB
Max Storage:	N/A
Ethernet:	Intel x550 DP (2 x 10Gb) 10GBASE-T Intel I350 DP (2 x 1Gb)
Power:	100-240 VAC
Height:	1.68 in / 4.28 cm
Width:	18.98 in / 48.2 cm
Length:	29.29 in / 74.4 cm
Weight:	42.99 lb / 19.5 kb

Learn more about our available AI Engine rules on the LogRhythm Community.