

Advanced Intelligence (AI) Engine™

LogRhythm's Advanced Intelligence (AI) Engine is an optional module for any LogRhythm deployment, offering sophisticated correlation and analysis of all enterprise log data in a uniquely intuitive fashion. With a practical combination of flexibility, usability and comprehensive data analysis, AI Engine delivers real-time visibility to risks, threats and critical operations issues that are otherwise undetectable in any practical way. AI Engine is Correlation That Works!

With over 100 preconfigured, out-of-the-box correlation rule sets and a wizard-based drag-and-drop GUI for creating and customizing even complex rules, AI Engine enables organizations to predict, detect and swiftly respond to:

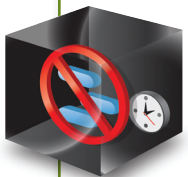
- Sophisticated intrusions
- Insider threats
- Fraud
- Compliance violations
- Disruptions to IT Services
- And many other critical actionable events...

Comprehensive Advanced Correlation

Unlike legacy SIEM solutions, AI Engine leverages its integration with the log and event management functions within the LogRhythm platform to correlate against all log data – not just a pre-filtered subset of security events. Seamless integration also enables immediate access to all forensic data directly related to an event.

AI Engine rules draw from over 50 different metadata fields that provide highly relevant data for analysis and correlation. Whether detected by out-of-the-box rules or user-created/modified rules, AI Engine identifies and alerts on actionable events with tremendous precision, for operations, security and compliance assurance. AI Engine can also be used to cast a wide net through generalized correlation rules for broader visibility that accommodate changes in event behavior.

TrueTime™



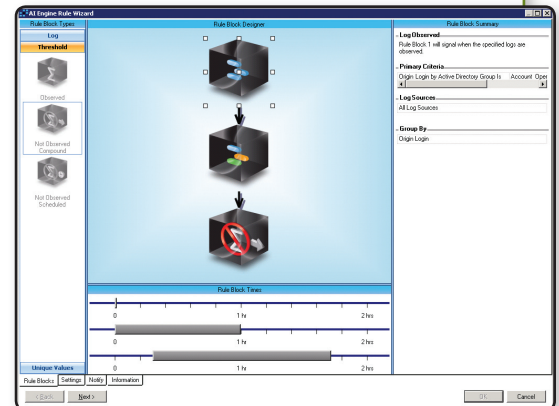
LogRhythm applies a universal timestamp to every log as it is processed. This ensures that the actual time of occurrence of an activity is recorded accurately – regardless of external factors, such as an out-of-sync server clock, delayed delivery of a log or differences in time zones. TrueTime™ guarantees that advanced correlation within AI Engine is based on chronological fact – recognizing the true sequence of events – minimizing false positives and avoiding false negatives.

AI Engine Delivers

- Advanced Correlation Against All Log Data
- TrueTime™ Event Sequencing
- Immediate Access to Underlying Forensic Data
- Generalized and Targeted Rules
- Extensive Out-of-the-Box Advanced Correlation Rules
- Unparalleled Ease of Use

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 unique requirements of any organization.



Secure

A single event is not always enough to indicate a breach or show the true reach of a security incident. AI Engine recognizes common security incidents and automatically correlates them against suspicious behavior patterns to automatically identify and alert on aberrant activity. For example, malware can invade and spread through an organization quickly, exposing data and weakening security faster than administrators can react. In many cases, the extent of damage is unknown.

Examples:

- Malware is detected on one host followed by attacks from that affected host.
- Suspicious communication from an external IP Address is followed by data being transferred to the same IP Address.
- A user logs in from one location, does not log out, but logs in from another city or country in a short timeframe.

Comply

AI Engine can assist in automating compliance controls, generating events when specific policy violations occur. These include protecting cardholder data or Protected Health Information (PHI) from unauthorized access and actively monitoring privileged user behavior.

Examples:

- Five failed authentication attempts followed by a successful login to a database containing ePHI followed by a large data transfer to the user’s machine all within 30 minutes.
- A file containing credit card data is accessed, followed by an attempt to transfer information from the same host to a USB thumb drive within 10 minutes.
- Creating one or multiple accounts and escalating their privileges in a short period of time.

Optimize

Advanced correlation offers substantial value for operational insight and IT services assurance. Slight variations in specific activities or a particular sequence of more common operations events may indicate critical operations issues.



Examples:

- A backup process is started, but no log for backup completed is generated.
- A critical process stops and doesn’t start back up within a specific timeframe.
- A large group of servers shuts down followed by a smaller group of servers starting back up.
- High I/O rates on a critical server usually only observed during backup procedures are observed during normal business hours.

AI Engine Deployment Options

Designed to integrate with any core LogRhythm deployment AI Engine can be purchased as a turnkey appliance, installed as software on dedicated customer equipment or deployed on multiple virtualization platforms, including 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 follows LogRhythm’s building-block architecture – expansion is as simple as plugging in an additional appliance. All appliances are centrally configured, monitored, and managed through LogRhythm’s universal console.



APPLIANCE LINE	LPS/LPD*	CPU	Memory	RAID	Storage	Chassis	Power	Ethernet	Dimensions	Weight
 LR-AIE1	1,150 / 100 Million	1 Quad Core	32GB	PERC H200, RAID 1 (Data, OS)	272GB	1U	100-240V	Broadcom 5809C (2 cards / 4 ports)	H4.26cm x W48.24cm x D77.2cm	17.69kg
 LR-AIE2	11,150 / 1 Billion	2 Quad Core	96GB	PERC H700, RAID 1 (OS), RAID 10 (DATA)	540GB	1U	100-240V	Broadcom 5809C (2 cards / 4 ports)	H4.26cm x W48.24cm x D77.2cm	17.69kg

*Logs Per Second/Logs Per Day

LogRhythm Headquarters

3195 Sterling Circle
Boulder, CO 80301
303-413-8745

LogRhythm EMEA

Siena Court, The Broadway
Maidenhead Berkshire SL6 1NJ
United Kingdom
+44 (0) 1628 509 070

LogRhythm Asia Pacific Ltd.

8/F Exchange Square II
8 Connaught Place, Central
Hong Kong
+852 2297 2812