Service
Analytic Co-Pilot

Detect Threats with Greater Precision

The Analytic Co-Pilot Service helps you accelerate threat detection and response—and maximize the effectiveness of scarce security personnel—using LogRhythm security analytics. The service provides you an assigned LogRhythm resource, known as an Analytic Co-Pilot, who guides you through the implementation, use, and optimization of security analytics content and even custom use cases that are most important for your company.

Your Analytic Co-Pilot helps you more precisely and efficiently detect threats by aligning security analytics content to your LogRhythm deployment. Your deployment will be enriched giving you targeted analytics, dashboards, searches, and reports, helping you detect and respond to the threats targeting your enterprise. Working with a Co-Pilot helps you grow into a power user of LogRhythm security analytics through a better understanding of AI Engine rules and how to create custom content for your deployment.

Analytic Co-Pilot Service Options

▶ Analytic Co-Pilot

LogRhythm content to choose from:

- User-Borne Threats
- Network-Borne Threats
- Endpoint-Borne Threats
- Financial Fraud
- Retail Cyber Crime
- Honeypot

+ Analytic Co-Pilot Custom

Examples of customer-driven content with service:

- Phishing
- Malware
- Healthcare
- Retail
- Financial fraud

+ Analytic Co-Pilot Accelerator

Additional time with Co-Pilot weekly to get more accomplished

+ Analytic Co-Pilot Accelerator

Additional time with Co-Pilot weekly to get more accomplished

Benefits

- **Expand your platform's threat detection** capabilities with your most pressing use cases
- **Grow into a LogRhythm power user** with help from an expert
- **Minimize false positives** by corroborating events across multiple dimensions
- **Achieve rapid ROI** by implementing the valuable threat detection content

Features

- **Implement specific security analytics content** to detect advanced cyberthreats
- **Tune and optimize security analytics content** for your environment, guided by a LogRhythm expert
- **Meet regularly with your Analytic Co-Pilot** to answer questions and ensure optimal content use

How Analytic Co-Pilot Service Works

The Analytic Co-Pilot Service includes the initial implementation of threat detection content, behavioral and statistical baselining, and ongoing alarm tuning. Your service will begin with a kick off call and the creation of your content roadmap plan. Your Analytic Co-Pilot will update your content roadmap with you monthly and create a report at the end of the service to show you everything that was accomplished.

Your Analytic Co-Pilot maps out all the content that your organization needs and whether any custom work is required.

Onboarding the content chosen is performed during scheduled weekly meetings.

The Analytic Co-Pilot Service is sold as an annual subscription, with pricing based on the type of content delivered. With this service, you can select modules in the LogRhythm library or if you need specialized content, your Analytic Co-Pilot can create the custom content you suggest. If you have critical use cases that you need immediately, then add an Accelerator to deliver content rapidly for faster time-to-value.

Threat Content Implementation:
Work with your Analytic Co-Pilot to configure your LogRhythm platform and deployment:

- Validate configuration of the entity structure and lists relevant to each module
- Configure AI Engine rules, advanced behavior analytics, and SmartResponse™
- Implement module-specific dashboards and reports to provide rapid access to the most important information

Analytics Tuning:
When security analytics content is set up, your Co-Pilot ensures the content is optimized for your unique IT environment. To do so, they update environmental factors leveraged by risk prioritization scores, and adjust statistical trending and behavioral whitelisting rules based on initial learning metrics, in order to:

- Expose previously unseen threats
- Prioritize threats in a precise way
- Drive down false positives through greater corroboration

Weekly Meetings:
During weekly meetings, your Analytic Co-Pilot will align your LogRhythm platform with best practices, review and tune content further, implement new content, and measure performance over time.

> "Analytic Co-Pilot Service has rapidly enhanced our monitoring capabilities. We've already thwarted multiple attacks thanks to the security analytics content LogRhythm is showing us how to deploy and optimize."
>
> **– Security Officer, Large US Retailer**

Want to learn more? Contact your Customer Success Manager today.
CSM@logrhythm.com

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301

www.logrhythm.com