SERVICE OVERVIEW

Analytics Co-Pilot Service

LogRhythm
The Security Intelligence Company

Analytics Co-Pilot Service helps you accelerate threat detection and response—and maximise the effectiveness of scarce security personnel—using LogRhythm security analytics. The service provides you an assigned LogRhythm resource, known as an Analytics Co-Pilot, who guides you through the implementation, use, and optimisation of a specific LogRhythm security analytics module. Your Analytics Co-Pilot helps you more precisely and efficiently detect threats by aligning security analytics content to your LogRhythm deployment. Working with a Co-Pilot helps you detect threats with greater precision, and in the process, helps you grow into a power user of LogRhythm security analytics.

Security analytics for your organisation

Each security analytics module distils decades of security expertise into specialised content. LogRhythm Labs develops the modules to detect threats in your environment before a damaging cyber incident occurs. They continually update the content to reflect their latest research. The modules are automatically delivered and updated via LogRhythm's cloud-based intelligence delivery system. Implementing a module gives you targeted analytics, dashboards, searches, and reports, helping you detect and respond to the threats targeting your enterprise.

Analytics Co-Pilot at a glance

- Implement a specific security analytics module
- Tune and optimise analytics for your environment, guided by a LogRhythm expert
- Check in regularly to ensure optimal use of module content
- Escalate to LogRhythm incident response experts, when necessary

Security analytics modules eligible for Analytics Co-Pilot Service

Holistic threat detection

3 Modules in 1 Analytics Co-Pilot Service:

- User Threat Detection Module
- Network Threat Detection Module
- Endpoint Threat Detection Module

User Threat Detection Module

Harness User Behaviour Analytics (UBA):

- Insider threats
- Account takeover
- Privilege abuse and misuse
- And many more use cases...

Network Threat Detection Module

Harness Network Behaviour Analytics (NBA):

- Malware command and control communication
- Remote zero-day attacks
- Network data exfiltration
- And many more use cases...

Endpoint Threat Detection Module

Harness Endpoint Behaviour Analytics (EBA):

- Advanced local malware detection
- Suspicious processes
- Local data exfiltration
- And many more use cases...

Core Threat Detection Module

Foundational use cases from the User, Network and Endpoint Threat Detection Modules, including:

- Account probe, account compromise, VPN takeover, privilege escalation after an attack, user created and added to admin group
- Endpoint compromise, suspicious connections, malware outbreak

Retail Cyber Crime Detection Module

- Identify high-value data files that may be targeted by criminals
- Baseline processes and user activities on POS systems
- Build behavioural system and network profiles in POS networks identifying malicious activity

How Analytics Co-Pilot Service works

Analytics Co-Pilot Service includes initial implementation of a selected module, behavioural and statistical baselining, and ongoing alarm tuning. These tasks are performed during scheduled and ad hoc check-ins. The service also includes a block of Incident Investigation and Response Services hours, enabling you to escalate to a LogRhythm incident response expert when needed. Analytics Co-Pilot Service is sold as an annual subscription, with pricing based on deployment size.

Module Implementation: Work with your Analytics 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 behaviour analytics, and SmartResponse™ plug-ins
- Implement module-specific dashboards and reports to provide rapid access to the most important information

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

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

Regular Check-ins: Upon operationalisation of the security analytics module, work with your Analytics Co-Pilot to continually adapt to evolving internal risk and external threat factors. During check-in meetings, align your platform with best practices, review and tune content further, implement new content, and measure performance over time.

Incident Investigation & Response Services: Analytics Co-Pilot Service includes a block of Incident Investigation & Response Services hours. When your platform detects an attack and you need assistance, escalate to the experts in LogRhythm Labs for support with forensic investigation and malware analysis.

> **Analytics 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 optimise.**
>
> –Security Officer, Large US Retailer

Benefits of Analytics Co-Pilot Service

Expand your platform's threat detection capabilities

Minimise false-positives by corroborating events across multiple dimensions

Optimise and tune analytics over time, as your environment evolves

Achieve rapid ROI by implementing the valuable content provided to all LogRhythm customers

Grow into a LogRhythm security analytics power user

Gain access to Incident Investigation and Response Services