LogRhythm
The Security Intelligence Company

LogRhythm Co-Pilot Services are ideal for organizations that may be short-staffed, not yet platform experts, or expect rapid ROI from their security investment.

These services are designed to help you get the maximum value out of your LogRhythm platform.

### LogRhythm Co-Pilot Services:

- Admin Co-Pilot for platform health
- Analytics Co-Pilot for threat detection
- Content Co-Pilot for content customization

# Analytics Co-Pilot Service

Analytics 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 Analytics Co-Pilot, who guides you through the implementation, use, and optimization 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 grow into a power user of LogRhythm security analytics through a better understanding of AI Engine rules.

## Security Analytics for Your Organization

Each security analytics module distills decades of security expertise into specialized content. LogRhythm Labs develops the modules to detect threats in your environment before a damaging 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 for threat detection (e.g., User, Network, Endpoint, Holistic, Core, and Retail Cyber Crime)
- ✓ Tune and optimize analytics for your environment, guided by a LogRhythm expert
- ✓ Check in regularly to ensure optimal use of module content with your Analytics Co-Pilot and experts from LogRhythm Labs

## Benefits of Analytics Co-Pilot Service

- Expand your platform's threat detection capabilities
- Minimize false positives by corroborating events across multiple dimensions
- Grow into a LogRhythm security analytics power user
- Achieve rapid ROI by implementing the valuable content provided to all LogRhythm customers

> **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 optimize.**
>
> — Security Officer, Large US Retailer

## How Analytics Co-Pilot Service Works

Analytics Co-Pilot Service includes initial implementation of a selected module, behavioral and statistical baselining, and ongoing alarm tuning. These tasks are performed during scheduled and ad hoc check-ins. 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 behavior analytics, and SmartResponse™ plug-ins
- Implement module-specific dashboards and reports to provide rapid access to the most important information


**Analytics Tuning:**
When the security analytics module is set up, your Co-Pilot ensures the module 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

**Regular Check-ins:**
Upon operationalization 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.

## Security Analytics Modules Eligible for Analytics Co-Pilot Service

| HOLISTIC THREAT DETECTION |
|---|
| 3 Modules in 1 Analytics Co-Pilot Service: |
| • User Threat Detection Module<br>• Network Threat Detection Module<br>• Endpoint Threat Detection Module |

| USER THREAT DETECTION MODULE | NETWORK THREAT DETECTION MODULE | ENDPOINT THREAT DETECTION MODULE |
|---|---|---|
| Harness User & Entity Behavior Analytics (UEBA) | Harness Network Behavior Analytics (NBA) | Harness Endpoint Behavior Analytics (EBA) |
| • Insider threats<br>• Account takeover<br>• Privilege abuse and misuse<br>• And many more use cases… | • Malware command and control communication<br>• Remote zero-day attacks<br>• Network data exfiltration<br>• And many more use cases… | • Advanced local malware detection<br>• Suspicious processes<br>• Local data exfiltration<br>• And many more use cases… |

| Core Threat Detection Module | Retail Cyber Crime Detection Module |
|---|---|
| Foundational use cases from the User, Network and Endpoint Threat Detection Modules, including: | Designed for retail customers with point of sale (POS) systems to: |
| • Account probe, account compromise, VPN takeover, privilege escalation after an attack, user created and added to admin group<br>• Endpoint compromise, suspicious connections, malware outbreak | • Identify high-value data files that may be targeted by criminals<br>• Baseline processes and user activities on POS systems<br>• Build behavioral system and network profiles in POS networks to identify malicious activity |