

Der Dienst Analytics Co-Pilot hilft Ihnen, mit den Sicherheitsanalysen von LogRhythm die Erkennung und Bewältigung von Bedrohungen zu beschleunigen – und die Effizienz von knappem Sicherheitspersonal zu steigern. Der Dienst bietet Ihnen eine zugewiesene LogRhythm-Ressource – den Analytics Co-Pilot –, der Ihnen bei der Implementierung, Nutzung und Optimierung eines spezifischen LogRhythm Analyse-Moduls assistiert. Ihr Analytics Co-Pilot unterstützt Sie dabei, Bedrohungen präziser und effizienter zu erkennen, indem er die Inhalte der Sicherheitsanalysen auf Ihre LogRhythm-Implementierung abstimmt. Wenn Sie mit einem Co-Pilot arbeiten, können Sie Bedrohungen noch präziser erkennen und dabei zum LogRhythm Power-User werden.

## Sicherheitsanalysen für Ihr Unternehmen

Jedes einzelne Sicherheitsanalyse-Modul destilliert das Sicherheitswissen aus Jahrzehnten und bündelt es in spezifischen Inhalten. Die Sicherheitsexperten bei LogRhythm Labs entwickeln die erforderlichen Module, um Bedrohungen in Ihrer Umgebung zu erkennen, bevor Cyber-Angriffe Schaden anrichten, und aktualisieren die Inhalte laufend um die neuesten Forschungsergebnisse. Die Module werden über das cloudbasierte Bereitstellungssystem von LogRhythm automatisch zur Verfügung gestellt und aktualisiert. Mit der Implementierung eines Moduls erhalten Sie zielgerichtete Analysen, Dashboards, Suchmöglichkeiten und Berichte, die Ihnen helfen, Bedrohungen für Ihr Unternehmen zu erkennen und entsprechend zu reagieren.

### Analytics Co-Pilot im Überblick

- ✓ Implementierung eines spezifischen Moduls für Sicherheitsanalysen
- ✓ Optimierung der Analysen und genaue Abstimmung auf Ihre Umgebung unter Anleitung eines LogRhythm-Experten
- ✓ Regelmäßiger Check-in, um sicherzustellen, dass Sie die Modul-Inhalte optimal nutzen
- ✓ Bei Bedarf stehen Ihnen die Experten für Störungsbehebung von LogRhythm zur Verfügung

## Sicherheitsanalyse-Module, die mit Analytics Co-Pilot kompatibel sind



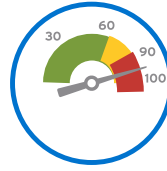
### So funktioniert der Dienst Analytics Co-Pilot

Der Dienst Analytics Co-Pilot umfasst die erste Implementierung eines ausgewählten Moduls, Verhaltens- und Statistik-Baselining sowie die laufende Abstimmung der Alarme. Diese Aufgaben werden während planmäßiger oder Ad-hoc-Check-ins durchgeführt. Zudem umfasst der Dienst einen Block von Service-Stunden zur Untersuchung und Bewältigung von Ereignissen, sodass Sie sich bei Bedarf an einen Experten für Störungsbehebung bei LogRhythm wenden können. Der Dienst Analytics Co-Pilot wird als Jahresabonnement angeboten; der Preis richtet sich nach der Größe der Implementierung.



**Implementierung der Module:** Konfigurieren Sie mit Ihrem Analytics Co-Pilot Ihre LogRhythm-Plattform und deren Bereitstellung:

- Überprüfen Sie die Konfiguration der Entitätsstruktur und der Listen für jedes Modul
- Konfigurieren Sie die AI Engine-Regeln, erweiterten Verhaltensanalysen und SmartResponse™-Plug-ins
- Implementieren Sie modulspezifische Dashboards und Berichte, damit Sie schnell Zugriff auf die wichtigsten Informationen erhalten



**Abstimmung der Analysen:** Nachdem das Sicherheitsanalyse-Modul eingerichtet ist, sorgt Ihr Analytics Co-Pilot dafür, dass es für Ihre spezifische IT-Umgebung optimiert wird. Dazu aktualisiert er die Umgebungsfaktoren, die von der Risikobewertung genutzt werden, und passt statistische Trends und verhaltensbezogene Whitelisting-Regeln auf Grundlage einer Lernmetrik an. Dies ermöglicht es:

- zuvor unerkannte Bedrohungen aufzudecken
- Bedrohungen präzise zu priorisieren
- falsch-positive Ergebnisse durch zusätzliche Bestätigungen zu verringern



**Regelmäßiger Check-in:** Nach der Operationalisierung des Sicherheitsanalyse-Moduls hilft Ihnen Ihr Analytics Co-Pilot, sich kontinuierlich auf Veränderungen der internen Risiko- und externen Bedrohungsfaktoren einzustellen. Bei den Check-ins können Sie Ihre Plattform an Best Practices anpassen, Inhalte prüfen und noch feiner abstimmen, neue Inhalte implementieren und die Leistungsentwicklung messen.



**Dienste zur Untersuchung und Bewältigung von Ereignissen:**

Der Dienst Analytics Co-Pilot umfasst einen Block von Servicestunden zur Untersuchung und Bewältigung von Ereignissen. Wenn Ihre Plattform einen Angriff erkennt und Sie Unterstützung benötigen, können Sie sich an die Experten für forensische Untersuchungen und Malware-Analysen bei LogRhythm Labs wenden.

“ Der Service Analytics Co-Pilot hat unsere Überwachungsfunktionen umgehend verbessert. Dank der Sicherheitsanalysen haben wir bereits mehrere Angriffe vereitelt, und LogRhythm zeigt uns, wie wir sie bereitstellen und optimieren können. ”

- Sicherheitsverantwortlicher einer großen US-Einzelhandelskette

### Vorteile des Dienstes Analytics Co-Pilot



Erweiterung der Bedrohungserkennungsfunktionen Ihrer Plattform



Minimierung falsch-positiver Ergebnisse, indem Ereignisse über verschiedene Dimensionen hinweg bestätigt werden



Fortlaufende Optimierung und Abstimmung der Analysen im Einklang mit den Entwicklungen Ihrer Umgebung



Schneller ROI durch Implementierung der wertvollen Inhalte, die LogRhythm allen Kunden zur Verfügung stellt



LogRhythm Power-User werden



Zugang zu Diensten für die Untersuchung und Bewältigung von Ereignissen