# LogRhythm erweitert seine Bedrohungserkennung mit innovativen Neuerungen in der Produktsuite

## Neue Versionen der LogRhythm SIEM-Plattform und der NDR- und UEBA-Lösungen steigern die Effizienz und erhöhen die Sicherheit für die Kunden

**Boulder, Colorado — 5. Juli 2022 —** LogRhythm, der Sicherheitsanbieter, der stark geforderten Security-Operations-Teams die Cyberabwehr erleichtert, gab heute den Launch der Version 7.9 der LogRhythm SIEM-Plattform sowie Updates für LogRhythm NDR und LogRhythm UEBA bekannt.

„LogRhythm rüstet die Sicherheitsteams mit intelligenten Analysen und automatisierten Reaktionen aus, um die Cybersecurity-Risiken zu reduzieren, tote Winkel zu beseitigen und Angriffe schnell abzuwehren", so Kish Dill, Chief Product and Customer Officer, LogRhythm. „Zugleich optimieren wir unsere Arbeitsweise, indem wir in sämtlichen Bereichen unseres Unternehmens einen strikt kundenfokussierten Ansatz etablieren. Wir hören unseren Kunden zu und versprechen ihnen, vierteljährlich Innovationen bereitzustellen, die den Herausforderungen gerecht werden, mit denen sie Tag für Tag konfrontiert sind. Wir wissen, dass Sicherheitsteams keine Zeit mit langwierigen Prozessen und ineffizienten Workflows verschwenden können. Mit diesen neuesten Updates erhalten die Sicherheitsteams die Tools, die sie brauchen, um ihre Abläufe effektiver und effizienter zu gestalten und ihr Unternehmen gegen die größten Bedrohungen von heute zu verteidigen."

LogRhythm 7.9, LogRhythm NDR (ehemals Mistnet NDR) und LogRhythm UEBA (ehemals CloudAI) sind darauf ausgelegt, die Hindernisse auszuräumen, denen Sicherheitsteams täglich gegenüberstehen. Mit neuen Funktionen beschleunigen sie die Reaktion auf Bedrohungen, verbessern Arbeitsabläufe und vereinfachen Prozesse:

## Schnellere Wertschöpfung durch verbesserte Arbeitsabläufe für die Sicherheitsteams

- **Erweiterte Automatisierung mit der Admin API**: LogRhythm 7.9 verbessert die Admin API durch die Aufnahme von System Monitoring Management (LogRhythm SysMon)-Endpunkten in die API-Bibliothek. So können sich die SIEM-Administratoren über die Admin-API verbinden und den SysMon-Agenten verwalten, was eine automatisierte Stapelverarbeitung ermöglicht.
- **Integriertes Know-how:** LogRhythm verkürzt die Amortisierungszeit für die Kunden mit seiner „out of the box" verfügbaren LogRhythm SmartResponse™ Library. Die Version 7.9 erweitert die bereits umfangreiche Bibliothek von mehr als 120 Integrationen um zusätzliche und optimierte SmartResponses.
- **Aktivierung der Paketerfassung in der Benutzeroberfläche:** Die Nutzer von LogRhythm NDR können jetzt PCAP-Dateien für spezifische Ereignisse und Fälle herunterladen, um mehr Details zu erhalten, die ihnen bei Untersuchungen helfen und das Threat Hunting verbessern.
- **Einfachere und schnellere Filterung von Ereignisprotokollen**: LogRhythm 7.9 bietet eine neue Möglichkeit, Logs für den Agenten zu filtern. Die Anwender können jetzt auswählen,

welche Arten von Windows-Ereignisprotokollen der Agent abfragen soll. Das beschleunigt die Verarbeitung der Protokolle und entlastet die Pipeline für die Datenerfassung.

## Erweiterte Funktionen zur Erkennung von Bedrohungen

- **Erweiterte Erkennungsmodelle für LogRhythm NDR**: Dank der verbesserten Analysefunktionen von LogRhythm NDR können die Nutzer ein größeres Spektrum von Ransomware-Angriffen erkennen.
- **Fortschrittliche Analysemodelle:** LogRhythm UEBA bietet den Nutzern von LogRhythm 7.9 erweiterte UEBA-Analysen als cloudnatives, einfach zu implementierendes Add-on. Die Modelle wurden optimiert und neue Modelle hinzugefügt, um sicherzustellen, dass auch die heutigen komplexen Angriffe erkannt und Anomalien, die vorrangige Aufmerksamkeit erfordern, ermittelt werden können. Dies trägt zur Verringerung der Alarmmüdigkeit bei und verkürzt die Reaktionszeiten.
- **Warnungen bei Richtlinienverstößen:** LogRhythm NDR bietet Warnungen zu abgelaufenen Zertifikaten, schwacher Verschlüsselung von Verbindungen sowie Authentifizierungsvorgängen, die in Klartext erfolgen, und bietet dadurch zusätzlichen Kontext zu potenziellen Risiken.

## Noch mehr Flexibilität

- **Überwachung auf Lizenzüberschreitungen mit leistungsfähigen Lizenz-Metering-Reports**: LogRhythm hat eine neue Berichtsfunktion hinzugefügt, um Lizenzüberschreitungen besser sichtbar und leichter nachvollziehbar zu machen. Sämtliche Überschreitungen der letzten 30 Tage werden angezeigt. So können die Teams die Lizenznutzung und -kosten besser steuern.
- **Erweiterte Endpunkt-Integrationen:** LogRhythm nimmt jetzt Cisco Secure Endpoint (ehemals AMP for Endpoints) in seine Palette von EDR-Integrationen auf.

Um mehr über die Lösungen von LogRhythm zu erfahren, vereinbaren Sie bitte einen Termin für eine Demo mit einem unserer Experten.

**Über LogRhythm**

LogRhythm hilft stark geforderten Security-Operations-Teams, im täglichen Kampf gegen Cyberangriffe zu bestehen. Auf den Schultern der Sicherheitsexperten lastet eine Menge: der Ruf und Erfolg ihres Unternehmens, der Schutz kritischer Ressourcen und letztlich die Sicherheit von Bürgern und Organisationen auf der ganzen Welt.

LogRhythm erleichtert diese Bürde. Das Unternehmen steht bei der Abwehr gravierender Cyberangriffe an vorderster Front und hilft den Sicherheitsteams, die Herausforderungen einer schnell veränderlichen Bedrohungslandschaft zu meistern. Als Verbündeter im Kampf gegen Cyberangreifer verbindet LogRhythm eine umfassende, flexible Security-Operations-Plattform mit Technologiepartnerschaften und Beratungsleistungen. So können SOC-Teams Personalmangel und Kompetenzlücken überbrücken. Mit LogRhythm bieten Unternehmen Angreifern die Stirn. Erfahren Sie mehr unter logrhythm.com.