

LogRhythm Unveils Major Advancements to Cloud-Native SIEM Platform, LogRhythm Axon

New platform automations and optimizations empower SOC team to more efficiently mitigate threats and reduce the skills gap

BROOMFIELD, Colo., October 2, 2023--(BUSINESS WIRE)-- [LogRhythm](#), the company helping security teams stop breaches by turning disconnected data and signals into trustworthy insights, today announced its 6th consecutive quarterly release and the one-year anniversary of its groundbreaking cloud-native SaaS SIEM platform, LogRhythm Axon. This quarterly release introduces significant enhancements and expansion to Axon and the full suite of LogRhythm solutions, underscoring the company's commitment to continuous innovation in the global cybersecurity landscape.

"In a dynamic and ever-evolving cybersecurity landscape, LogRhythm is obsessed with delivering value our customers care about," said Chris O'Malley, CEO of LogRhythm. "As we celebrate the one-year anniversary of Axon's launch, customer satisfaction is our first priority, guiding every decision we make. We believe that by driving continuous improvements in innovation delivery rooted in well understood customer needs, we can empower our product users to navigate the complex world of cybersecurity with confidence and efficiency."

SOC Efficiency and Streamlined Analyst Workflows

LogRhythm's latest Axon release rounds out the ability to seamlessly detect, investigate, and respond to potential threats within a security operations center. With the foundation of incident response, security teams can now leverage Axon to automate team workflows through case management. Case management enables analysts to automatically create cases that enable investigative workflows to track responses to threats, thus mitigating duplication of efforts and optimizing threat mitigation strategies. In addition, Axon's new Signal Replay feature enables SOC teams to test analytics rules to ensure detections are optimized for their environment.

Continuing the effort to advance SOC efficiency, LogRhythm SIEM now provides seamless integration of log source onboarding through centralized management. This enhanced SIEM capability eliminates the need for administrators to navigate several servers and UIs to complete onboarding, thereby streamlining workflows through a single interface, increasing productivity, and reducing the administrative process in half.

Bridging the Skills Gap

LogRhythm continues to address the industry-wide skills gap by providing features that enhance the productivity and onboarding processes for security analysts. The new in-product resource centers for both LogRhythm SIEM and LogRhythm Axon equip security teams with tools they need to quickly understand how to best utilize the platforms and realize a faster time to value. This comprehensive resource hub provides quick access to tutorials, documentation, release information, and the LogRhythm Community for support from the security community.

LogRhythm Expands Cloud-native SIEM Platform to APAC

LogRhythm is also pleased to announce the successful expansion of their LogRhythm Axon SIEM platform to the APAC region. With a new instance in Australia, LogRhythm Axon's cloud-native SIEM will

be available to provide customers with a flexible solution to strengthen security operations and ensure comprehensive protection.

In partnership with Seamless Intelligence, LogRhythm's partner of the year in Australia, a managed services layer will also be available for LogRhythm Axon customers. "LogRhythm Axon significantly advances what customers can and should expect from a cloud-native SaaS SIEM platform. We've been impressed with its platform design and architecture, as well as the continuous pace of innovation," said Chris Bolan, Managing Director of Seamless Intelligence. "Our Axon managed services are being developed to take advantage of the platform's capabilities and to provide our clients with the world-class cybersecurity solution and services needed to keep their organisations safe."

Additional enhancements with LogRhythm SIEM, LogRhythm NDR and LogRhythm Axon solutions released in this quarterly rollout include:

LogRhythm Axon:

- User anomaly detection for improbable travel allows protection against abnormal access attempts into an organization's environment
- New case management feature automates incident response and investigative workflows, helping SOC teams delegate resources, prioritize their work and improve efficiency. Cases and email notifications can be automatically created or sent when an analytic rule is triggered, indicating an event requires immediate attention
- Ability to search common events allows analysts to find relevant security events across different vendors' log sources without having prior knowledge of the underlying log structure
- New signal replay enhances threat detection development process by allowing testing for analytics rules to ensure they are fine-tuned and optimized for their environment

LogRhythm SIEM:

- Streamlined onboarding of Beats and Open Collectors, a collection of LogRhythm services that gather and normalize data from various cloud providers, in a single location to cut the workflow in half
- Enhanced API log source onboarding for easier management of Open Collectors and Beats
- Expanded library of supported log sources and parsing for improved correlation and analysis
- In-product Resource Center for access to tutorials, announcements, docs, and support

LogRhythm NDR:

- IP Behind Load Balancer Tracking for faster triage capabilities when responding to incidents
- Enhanced model output contextualization to empower quicker action to threats as relevant information is readily available

In addition to LogRhythm's commitment to innovation and seamless cybersecurity solutions, Novacoast has also emerged as the first Axon services provider for LogRhythm's customer base. Novacoast's expertise in delivering innovative cybersecurity services adds a new layer of value to the already impressive suite of LogRhythm Axon capabilities.

“This strategic partnership reflects the platform's efficacy and flexibility in enhancing security programs across diverse environments,” said Jonathan Poon, CISO at Novacoast. “As LogRhythm continues to adapt its Axon offerings to address customer requirements, we are proud to be part of this evolution, propelling the cybersecurity landscape forward. Together, we are addressing industry needs and setting the standard for security services.”

To learn more about LogRhythm's offerings, please visit: <https://logrhythm.com/>.

About LogRhythm

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights. From connecting the dots across diverse log and threat intelligence sources to using sophisticated machine learning that spots suspicious anomalies in network traffic and user behavior, LogRhythm accurately pinpoints cyberthreats and empowers professionals to respond with speed and efficiency.

With cloud-native and self-hosted deployment flexibility, out-of-the-box integrations, and advisory services, LogRhythm makes it easy to realize value quickly and adapt to an ever-evolving threat landscape. Together, LogRhythm and our customers confidently monitor, detect, investigate, and respond to cyberattacks. Learn more at logrhythm.com.

Media Contact

Olivia Farber

logrhythm@10fold.com

949-542-9232