

For immediate release...for immediate release...for immediate release...for immediate release...

# LogRhythm Introduces Standalone User and Entity Behavior Analytics Offering

*LogRhythm UEBA provides increased security coverage, faster threat detection with minimal investment*

**Dubai - Dec 21, 2017:**

[LogRhythm](http://www.tcfnewswire.net/en/company/logrhythm), The Security Intelligence Company, today announced it has entered the User and Entity Behavior Analytics (UEBA) market with the introduction of LogRhythm UEBA, an independent analytics product that enhances the security of environments for customers that wish to augment a non-LogRhythm SIEM or introduce a standalone UEBA product if there is no formal SIEM in place. LogRhythm's UEBA offering applies both machine learning-based behavioral analytics and real-time scenario-based threat detection to provide complete coverage in detecting user-based threats. These capabilities are combined within LogRhythm's integrated workflow for detection and response, providing a highly efficient solution in recognizing and mitigating user-based threats.

Based on advanced analytics of user behavior, LogRhythm UEBA provides increased security coverage with minimal investment for security professionals in enterprise and SME organizations who need protection from insider threats, compromised accounts, admin abuse and other user-based threats.

“Organizations are under siege by an ecosystem of threat actors, from motivated insiders to well-armed nation-states,” said Chris Brazdziunas, VP of products at LogRhythm. “Meanwhile, many security teams face significant obstacles securing qualified personnel to combat these threats. These challenges are sometimes heightened by organizational pressure to relax controls to unlock business productivity. UEBA arms organizations to detect and respond to user-based threats. Analysts are provided evidence-based starting points for investigation, rich visualizations for effective analysis, and direct access to data for rapid response.”

LogRhythm UEBA is distinct in the marketplace because, unlike other UEBA point solutions that use limited analytical methods, LogRhythm UEBA detects known and unknown threats via in-depth analytics, applying machine learning and scenario analytics to quickly surface and prioritize critical events. Further, LogRhythm UEBA employs cloud-based analytics that can evolve over time, taking into account feedback from customers to hone accuracy. LogRhythm UEBA collects threat training data from the whole of an organization's activity and across its extended customer footprint. Collecting feedback from a global set of SOC analysts and incident responders makes the product smarter and faster. Additionally, LogRhythm provides customers with a library of field-proven user-based threat scenarios that operate in coordination with ML-observed activities to corroborate security relevancy for greater precision in identifying threats.

LogRhythm UEBA breathes life into existing and legacy SIEM deployments with an easy to deploy, highly effective UEBA solution that delivers fast ROI. Specific use cases for LogRhythm UEBA include:

<ul>

<li><strong>Insider threat</strong>: A new study finds that most security professionals (88 percent) view insider threats as a dangerous and growing concern for their organization. LogRhythm UEBA provides machine-assisted monitoring of contractors and high-impact teams such as IT, finance and sales to prevent data theft, fraud, sabotage, policy violations and other dangerous activity. It uses behavioral profiling to spot deviations from normal behavior and scenario analytics to recognize established patterns.</li>

<li><strong>Account takeover</strong>: Attackers who have compromised a network will attempt to take control of an account and move laterally until they attain their target. LogRhythm UEBA unmaskes these imposters by examining the behavior of individual users and associated peer groups. External threats are quickly identified, preventing further compromise and damage.</li>

<li><strong>Privilege abuse and misuse</strong>: With extensive access to systems and data, privileged users present heightened risk to the organization. LogRhythm UEBA helps ensure access rights are used appropriately. Its algorithms automatically monitor the creation and deletion of privileged accounts, the elevation of permissions, and the suspicious use of privileged accounts.</li>

</ul>

<p>“A significant number of large enterprises are replacing their legacy SIEMs with <a href="http://www.tcfnewswire.net/en/company/logrhythm/news-stories/logrhythm-unveils-self-evolving-cloud-based-analytics">LogRhythm’s next-gen platform</a>, but not every organization is able to do that today,” said Matt Winter, vice president of marketing and business development at LogRhythm. “With LogRhythm UEBA, customers that aren’t yet ready for full replacement no longer have to settle for an unproven and functionally limited ‘SIEM helper’ or similar point product to get more value out of their existing SIEMs. Instead, LogRhythm now offers them a full-featured solution that’s architected to scale, can seamlessly grow with them as their needs evolve and has been repeatedly proven in large global deployments.”</p>

<p><br />

LogRhythm UEBA is a standalone version of the LogRhythm product set for non-LogRhythm Enterprise or XM customer environments. The product is commercially available, and pricing is based on a per-user model, with hardware included through a subscription.</p>

### ENDS ###

#### **About LogRhythm:**

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company’s patented award-winning threat lifecycle management platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner’s SIEM Magic Quadrant report for five consecutive years, named a ‘Champion’ in Info-Tech Research Group’s 2014-15 SIEM Vendor Landscape report, received SC Labs ‘Recommended’ 5-Star rating for SIEM and UTM for 2016 and earned Frost & Sullivan’s 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award.

LogRhythm is headquartered in Boulder, Colorado, with operations throughout North and South America, Europe and

the Asia Pacific region.

**For media enquiries, please contact:**

Grace Sescon

Office: +971 (4) 447 2501

E-mail: [grace@tcf-me.com](mailto:grace@tcf-me.com)

THECONTENT|FACTORY

<http://www.tcf-me.com/>