Data Sheet

LogRhythm UEBA

LogRhythm
The Security Intelligence Company

As threat actors grow in number and their attacks more sophisticated and frequent, they make the threat landscape increasingly dangerous and unpredictable. From motivated insiders to well-armed nation-states, threats to your organization are myriad in nature and difficult to detect.

Focusing on user-based threats is a key method for combating a growing attack surface. However, many security teams face significant challenges finding sufficient skilled personnel to maintain this focus. Consequently, existing staff are typically charged with doing more with fewer resources leaving them struggling to keep up with an evolving threat landscape.

LogRhythm UEBA enables your security team to quickly and effectively detect, respond to, and neutralize both known and unknown threats. Providing evidence-based starting points for investigation, it employs a combination of scenario analytics techniques (e.g., statistical analysis, rate analysis, trend analysis, advanced correlation), and both supervised and unsupervised machine learning (ML).

Through this variety of analytical techniques, LogRhythm UEBA prepares and analyzes diverse environmental data to uniquely expose user-based threats, such as insider threat, account takeover, and account privilege abuse and misuse. Additionally, it applies risk context to user activities to help you prioritize investigation of potentially malicious behavior. Accounting for the changing threat landscape, LogRhythm UEBA's analytics continue to evolve through additional content from LogRhythm Labs' threat research as well as dynamic global feedback, ensuring emerging threat tactics and techniques are continuously recognized.

Insider Threat by the Numbers

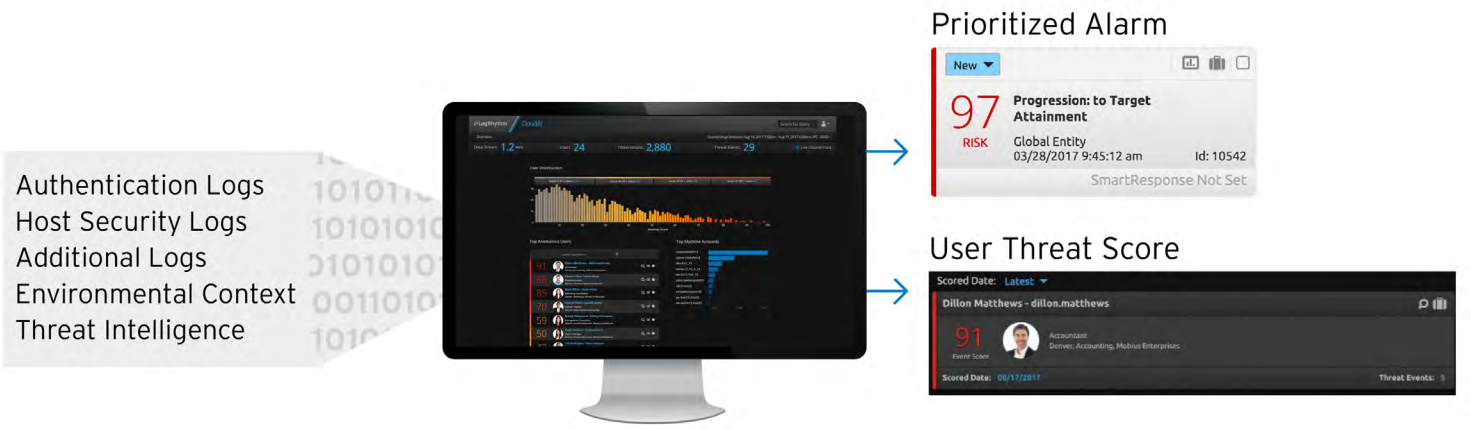
- **91%** of companies report they do not have effective insider threat detection methods[1]
- **25%** of data breaches involve an insider threat[2]
- **69%** of companies surveyed reported incidents of attempted data theft from inside the organization[3]
- **70%** of incidents take months or longer to detect[4]

[1] Verizon Data Breaches Investigation Report 2017, Verizon
[2] Verizon Data Breaches Investigation Report 2017, Verizon
[3] The State of Cybersecurity and Digital Trust 2016, HfS Research
[4] From Brutus to Snowden: A Study of Insider Threat Personas, IS Decisions

Designed for Your Existing Environment

With over a decade of experience developing security solutions focused on recognizing threat activities, LogRhythm understands how to protect your organization from user-based threats. LogRhythm UEBA augments your current security environment, functioning either as a stand-alone UEBA product or as an add-on to existing SIEM or log management solutions. With an Analytics-as-a-Service component, LogRhythm UEBA requires minimal infrastructure. It is licensed annually as a simple subscription based on the number of users you are monitoring. The subscription includes all necessary equipment and maintenance.

How LogRhythm UEBA Works



User-based threats arise in multiple ways and take many forms. To effectively protect your organization, your UEBA solution needs to utilize diverse analytic methodologies to detect, analyze, and prioritize those threats. LogRhythm UEBA provides your organization with intelligent UEBA capabilities to address the entire spectrum of user-based attacks, from known threats using known methods (e.g. brute force attacks) to unknown threats using unknown methods (e.g. insider threats).

LogRhythm UEBA detects advanced threats by applying scenario-based threat models while also identifying significant user behavioral shifts. It learns from your environment, applying ML to recognize changes in user behavior, scoring each observation and generating composite threat scores to indicate high-risk users. Whether recognizing a known scenario or detecting changes to a user's behavior, LogRhythm UEBA provides guided investigation to efficiently understand scope and root cause, leveraging automated workflows and evidence capture.

LogRhythm UEBA leverages our patented Machine Data Intelligence (MDI) Fabric and TrueIdentity to reduce time-to-value and remove taxing data tuning requirements. LogRhythm's MDI Fabric prepares a highly consistent, predictable, and vendor-agnostic data set for accurate analytics. Leveraging classification, contextualization, and time normalization, our MDI Fabric enables your security team to realize use cases quickly and effectively. Search and machine-based analytics utilize LogRhythm TrueIdentity, mapping a user's disparate accounts and related identifiers to build a singular user identity for comprehensive monitoring and more accurate threat detection.

Additionally, LogRhythm's embedded Case Management and SmartReponse™ work in tandem to optimize analyst workflow for faster threat detection and response. Case Management enables rapid case creation to decrease your mean time to detect (MTTD) and facilitates efficient incident investigation. SmartResponse automated playbooks eliminate manual tasks and enable centralized execution of pre-staged countermeasures, allowing rapid response to potentially harmful user activity.

Insider threat: LogRhythm identifies malicious and accidental insiders alike by recognizing established attack scenarios and detecting deviations from normal behavior.

Account takeover: LogRhythm analyzes the behavior of individual users and associated peer groups to unmask attackers who have compromised your network.

Privilege abuse and misuse: LogRhythm reduces organizational risk by monitoring the creation and deletion of privileged accounts, the elevation of permissions, and the suspicious use of privileged accounts.

LogRhythm UEBA enables efficient monitoring of user behavior with the following additional capabilities:

- Direct data collection from third-party SIEMs
- Unstructured and contextual search
- Intuitive visualizations and user-focused dashboards
- Machine-assisted threat hunting

Benefits of LogRhythm UEBA

LogRhythm UEBA improves security coverage across your organization, offering leading analytics accuracy so you can confidently monitor and investigate risky users. Automated data processing, tuneless analytics, and robust visualizations provide pervasive visibility into user behavior, reducing your MTTD. When your security team can deploy rapid threat detection, they can decrease their mean time to respond (MTTR), accelerating qualification and investigation.

Achieve Analytics in Depth

Detect known and unknown threats with self-evolving behavior analytics and real-time scenario analytics for enhanced security.

Leverage UEBA-Oriented Dashboards

Customize analytics with an intuitive graphical user interface leveraging user-focused widgets to easily monitor potentially risky users.

Refine Event Prioritization

Minimize false positives to save time by corroborating events and adjusting for assets-based risk, context, and other factors with Risk-Based Prioritization.

Realize Rapid Time-to-Value

Shorten time-to-value with rapid behavioral learning, out-of-the-box analytics content and Knowledge Base modules developed and maintained by LogRhythm Labs