CloudAI for UEBA

LogRhythm
The Security Intelligence Company

Detect and Respond to User-Based Threats with Artificial Intelligence

Your organization is facing a growing volume of increasingly complex and ever-changing threats—and the most dangerous threats are those that are most difficult to discover. You may also be dealing with staffing shortages and inefficient, manual workflows. To succeed, your analysts need to offload mundane, time-consuming tasks so they can focus on important problems that require human decision making, and your organization needs improved analytics to surface hidden threats.

LogRhythm CloudAI, an add-on solution for the LogRhythm Threat Lifecycle Management (TLM) Platform, applies artificial intelligence (AI) and machine learning (ML) to help your team detect advanced threats. Architected for the cloud, it uses AI to identify previously hidden threats, enable rapid qualification and investigation, and accelerate time to value.

CloudAI detects insider threats, compromised accounts, administrator abuse and misuse, and other user-based threats. It is particularly suited for machine-assisted monitoring of high-risk users, such as IT, finance, and executive teams. With CloudAI's advanced analytics, your analysts are armed with evidence-based starting points for threat hunting and powerful data visualizations for machine-assisted qualification and investigation.

CloudAI for UEBA at a Glance

- Detect advanced threats with artificial intelligence and machine learning
- Uncover previously unknown attacks and methods
- Detect insider threats, compromised accounts, admin abuse, and other user-based threats
- Qualify and investigate threats with powerful data visualizations
- Empower analysts with efficient workflows and tight integration with the LogRhythm platform
- Achieve rapid time-to-value with cloud delivery, automated data processing, and tuneless analytics

CloudAI's user activity dashboard enables monitoring of potentially risky users and machine accounts and provides immediate drill-down to the anomalous entity.

Address a Spectrum of Attacks with Diverse Analytical Techniques

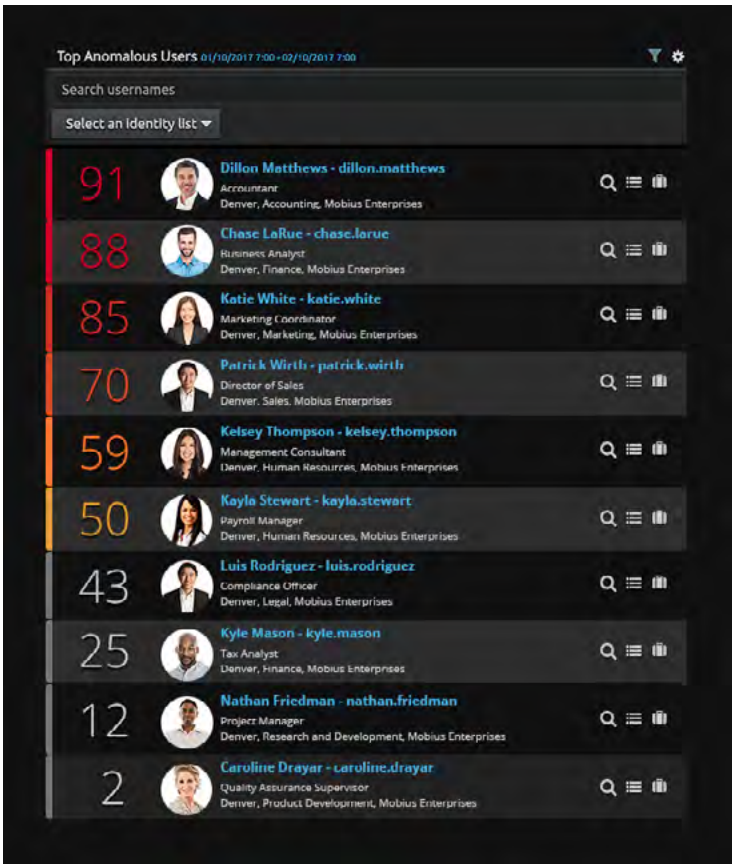
CloudAI identifies hidden threats by recognizing significant changes in user behavior that signal organizational risk, complementing LogRhythm AI Engine's application of field-proven threat models. Employed in tandem, they deliver analytics in depth, applying multiple complementary analytical methods to detect threats along the known/unknown spectrum. These unique methods also enable enhanced corroboration, improving the accuracy of threat prioritization. Together, CloudAI and AI Engine deliver automated real-time analysis of all environmental activity and deep visibility into user-based threats that would otherwise go undetected.

Detect Threats Faster

CloudAI combines a wide array of behavioral models with artificial intelligence and machine learning to detect and characterize shifts in how users interact with the IT environment. This prepares your analysts to pursue user-based threats, including signatureless and hidden threats.

With LogRhythm TrueIdentity, CloudAI maps disparate user accounts (e.g., VPN, work email, personal cloud storage) and related identifiers (e.g., username, email address) to the actual user's identity to build comprehensive behavioral baselines. By associating user activity to an identity, regardless of how their accounts are represented, you can be sure that all of their relevant behavior is represented during analysis.

CloudAI builds user profiles with numerous relevant data features that reflect the user's activity in high detail. CloudAI tests these models with profile baselining, comparing a user's activity to a historical baseline of the same user's activity.



CloudAI's lists of top anomalous users and top anomalous machine accounts provide a natural starting point for threat hunting.

Leave Data Preparation to LogRhythm

LogRhythm's significant experience in security analytics provides vital expertise in the preparation and analysis of machine data for security use cases. With CloudAI, you have access to the industry's cleanest and most security-relevant data, prepared by the LogRhythm Machine Data Intelligence (MDI) Fabric. This built-in support allows your organization to forgo the professional services engagements required by other UEBA vendors. The application of advanced AI and machine learning against high-fidelity data enables CloudAI to more effectively surface potential threats.

LogRhythm MDI Fabric Data Enrichment

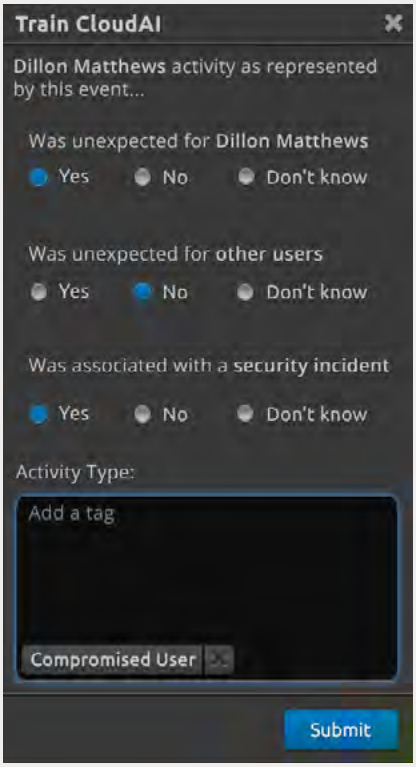
- Data parsing
- Event classification
- Geolocation
- Risk-based prioritization
- TrueTime normalization
- And more...

Get Smarter, Faster

CloudAI is architected to learn from your environment so that it can protect your organization from both current and future threats. The solution self-evolves, providing value in just days and enabling continuous tuning without manual intervention. Additionally, CloudAI is trained by analysts during the normal course of an investigation. This hybrid approach delivers the full benefits of both unsupervised learning (streamlined adoption and use) and supervised learning (more accurate threat detection) so the solution can grow smarter even more quickly.

The CloudAI user interface encourages analyst feedback by collecting relevant information in the natural workflow of the security operation. When viewing an event on the user timeline, your analyst is prompted to indicate whether it constitutes a potential threat. This feedback allows CloudAI to determine whether observed anomalies constitute true threats with increasingly high confidence.

In addition to learning from the whole of your organization's activity, the solution is architected to collect threat training data from across CloudAI's extended customer footprint. Collecting feedback from a global set of SOC analysts and incident responders accelerates the development of CloudAI's behavioral models, benefiting each customer.



CloudAI collects analyst feedback to grow smarter over time.

Maximize Analyst Efficiency

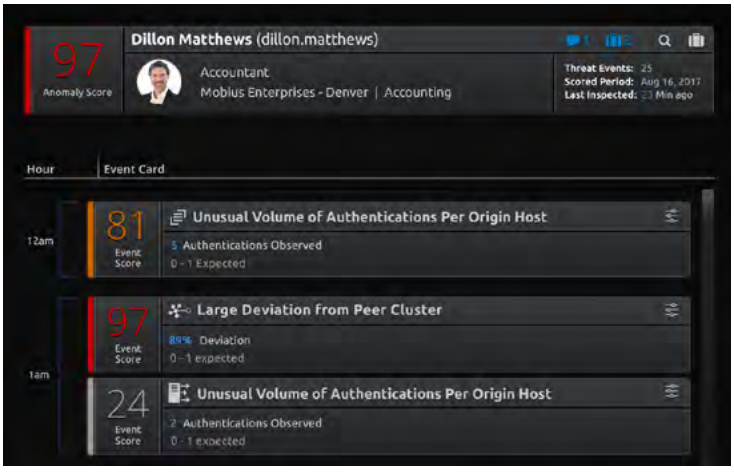
CloudAI vastly improves the efficacy and efficiency of your security team. Its continuous, automated analytics eliminate the need for manual threat monitoring, allowing your analysts to focus on the highest-priority threats. With further development, CloudAI will ultimately enable autonomous automation of a wide range of SOC tasks.

Machine-assisted threat hunting and investigation is enabled via CloudAI's powerful visualizations. Its tight integration with the full LogRhythm TLM Platform eliminates the inefficiencies and gaps caused by fragmented processes. The solution natively supports LogRhythm's embedded security automation and orchestration function, including its case and incident management workflows and SmartResponse™ automated response actions.

CloudAI's user activity dashboard provides broad visibility and supports the monitoring of high-risk users (e.g., executives, IT staff, and departing personnel). These groups can be customized to meet your organizational needs. Related visualizations allow the monitoring of services accounts.

With CloudAI, your team can analyze a user's behavior from multiple dimensions. A timeline of user behavior reveals the threat events contributing to their threat score so your analysts can determine whether the user's behavior is malicious. In addition, peer group comparisons illustrate a user's behavior relative to dynamic lists of true peers, as revealed by similarities in their actual behavior.

Throughout the investigative workflow, CloudAI automatically presents identity information from Windows Active Directory. It allows immediate access to underlying log and event data, which can be saved to an associated case with a single click. These integrated capabilities support the TLM workflow, improving analyst productivity and accelerating incident response.



CloudAI's user timeline enables rapid investigation of user behavior and provides efficient workflows for further action.

Achieve Rapid Time to Value

CloudAI is a cloud-delivered, subscription-based add-on solution for the LogRhythm platform. Without on-premises hardware or rules to implement and optimize, you'll realize a low cost of adoption. With flexible licensing options, you can start by monitoring key insiders and scale up when resources allow. Further, turnkey delivery streamlines administration and maintenance, so your security team can focus on its core mission.

CloudAI's architecture minimizes operational impact for your organization and prioritizes data security. Implementation entails configuring your LogRhythm platform to transmit metadata from high-value data sources (e.g., authentication activity, application and host access, and location) to CloudAI's SOC 2-compliant PaaS infrastructure. Since CloudAI uses metadata rather than logs, bandwidth requirements are minimal. Data transits over TLS 1.2 and is protected with symmetric two-way certification. CloudAI uses secure storage and data is programmatically destroyed as it becomes obsolete.

Power Your SOC with CloudAI

Your security team is charged with keeping your organization safe, overcoming an ever-expanding attack surface and limited resources. CloudAI extends the LogRhythm platform to detect user-based threats with AI, spotting hidden threats and empowering your analysts. The solution is delivered as a service, making its advanced analytics highly accessible. Built with a cloud architecture, it gets smarter over time through machine learning. These capabilities improve the productivity of your analysts and accelerate detection and response.

Detect hidden threats

Maximize analyst efficiency

Achieve rapid return on investment

Learn more. Contact our sales team today.
sales@logrhythm.com