Data Sheet

# Unified UEBA and Threat Lifecycle Management

LogRhythm
The Security Intelligence Company

Organisations are under siege by an ecosystem of threat actors, from motivated insiders to well-armed nation-states. Meanwhile, many security teams face significant obstacles securing qualified personnel to combat this threat. These challenges are sometimes heightened by organisational pressure to relax controls to unlock business productivity.

User and Entity Behaviour Analytics (UEBA) arms your organisation to detect and respond to user-based threats. It operates without the use of agents, automatically analysing the diverse data generated by your IT environment to expose insider threats, compromised accounts, and privilege misuse and abuse. Analysts are provided evidence-based starting points for investigation, rich visualisations for effective analysis, and direct access to data for rapid response.

UEBA is built into the LogRhythm Threat Lifecycle Management (TLM) Platform, eliminating the inefficiencies caused by costly data duplication, dual platform administration, and swivel-chair analysis. The solution provides rapid time to value through out-of-the-box data processing, automated identity contextualisation, powerful search analytics tools, and embedded security orchestration and automation (SAO).

## Diverse threats demand diverse detection methods

The threats facing your organisation vary in method, exploited vulnerability, and velocity. To stay safe, your team needs to detect both familiar attacks (e.g., session hijacking) and signatureless attacks (e.g., zero-day malware). Addressing this broad set of threats requires the application of analytical techniques suited to specific types of attacks.

LogRhythm employs the industry's broadest set of threat detection methods, allowing you to implement analytics techniques well-suited to the detection and prioritisation of a wide range of suspicious behaviour. LogRhythm's patented AI Engine detects threats in real time with scenario analytics, identifying threatening events and spotting advancement along the Cyber Attack Lifecycle. LogRhythm CloudAI applies artificial intelligence (AI) and machine learning (ML) to detect advanced user-based attacks and provide anomaly-based event data for AI Engine. Employed in tandem, the platforms provide the breadth of analytics necessary to detect threats across the known/unknown spectrum.

### LogRhythm Platform for UEBA benefits at a glance

- ✓ Detect known and unknown threats with scenario analytics and AI/ML
- ✓ Dismiss false positives through corroboration and prioritisation
- ✓ Accelerate hunting and investigation with user contextualisation, data visualisations, and direct access to underlying data
- ✓ Streamline your security operations with security automation and orchestration
- ✓ Minimise total cost of ownership with a unified and field-proven platform

## UEBA use cases

**Insider threat:** Users with legitimate access to internal networks pose a material risk to company security. Machine-assisted monitoring of contractors and high-impact teams (e.g., IT, Finance, Sales) can prevent data theft, fraud, sabotage, policy violations, and other dangerous activity. LogRhythm uses behavioural profiling to spot deviations from normal behaviour (e.g., abnormal authentication activity, abnormal host access) and scenario analytics to recognise established patterns (e.g., accessing a new server and then logging into a personal cloud storage website).

**Account takeover:** Attackers who have compromised your network will attempt to take control of an account and move laterally until they attain their target. LogRhythm unmasks these imposters by examining the behaviour of individual users and associated peer groups. External threats are quickly identified, preventing further compromise and damage.

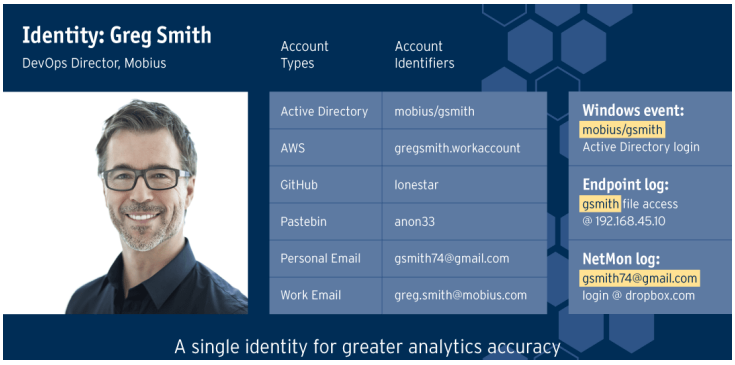
**Privilege abuse and misuse:** With extensive access to systems and data, privileged users present heightened risk to the organisation. LogRhythm's UEBA capabilities help ensure that access rights are used appropriately. Its algorithms automatically monitor the creation and deletion of privileged accounts, the elevation of permissions, and the suspicious use of privileged accounts.

> "We use LogRhythm to detect insider threats and compromised accounts and to give our incident responders deep environmental visibility."
> —Security Manager, Enterprise Technology Firm

## Prepare data for accurate analysis

Analytics are only as effective as their underlying data. LogRhythm's patented Machine Data Intelligence (MDI) Fabric provides security-relevant processing support for a leading number of data sources. By extracting metadata, normalising time of occurrence, classifying security events, and more, LogRhythm optimally prepares your data for accurate analysis.

## Build and analyse full behaviour profiles



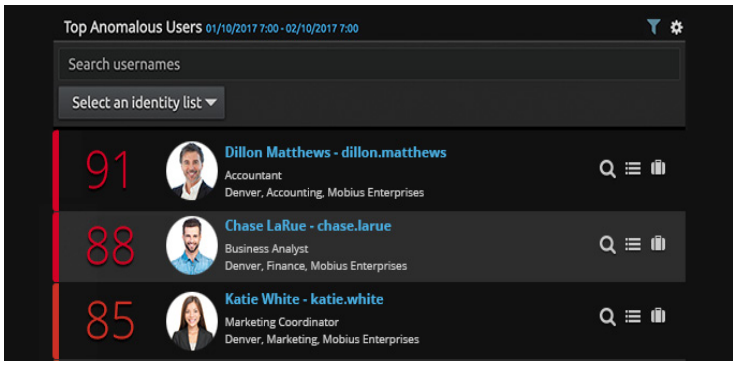

How many different sets of login credentials do your employees use in a typical workweek? LogRhythm TrueIdentity builds comprehensive behaviour profiles by associating your logs to your real users, not just disparate account identifiers, powering machine analytics and analyst-driven investigations.

## Spot dangerous user activity in real time

LogRhythm performs real-time scenario analytics with AI Engine, uncovering user-based threats, such as data exfiltration, privilege abuse, and fraud. It applies diverse analytical techniques (e.g., statistical analytics, rate analysis, trend analysis, advanced correlation) suited to recognising different types of scenarios. These algorithms expose advancement along the Cyber Attack Lifecycle, enabling rapid detection of emerging threats. AI Engine prioritises true threats and minimises false positives by adjusting risk scores based on multiple factors, including event corroboration.

The LogRhythm Labs team helps you stay ahead of the latest user-based threats by developing and maintaining out-of-the-box scenario analytics content for UEBA. This valuable content, delivered from the cloud, is provided at no additional charge. It is organised by use case and includes a deployment guide with detailed implementation instructions and tuning best practices.

## Detect hidden threats with AI and ML




LogRhythm CloudAI detects behavioural anomalies by applying multiple AI and ML models across long periods of user data. Observations are generated and scored, with the most notable marked as events. Composite threat scores for risky users are generated from observations, giving hunters evidence-based leads for investigation. CloudAI incorporates real-world feedback on specific judgements from across its many customers, improving its accuracy over time.

## Streamline your security operations

LogRhythm accelerates your response to user-based threats with embedded security orchestration and automation (SAO). Case management helps coordinate your team, while SmartResponse™ automates the gathering of forensic data and the invocation of targeted countermeasures. Dashboard widgets showing mean time to detect (MTTD) and mean time to respond (MTTR) help you monitor the effectiveness of your security program.

### A unified UEBA and TLM solution

The LogRhythm TLM Platform delivers UEBA through AI Engine and CloudAI, detecting known and unknown threats alike through scenario analytics and AI/ML. The solution provides prioritised threat scores for risky users and events and gives analysts direct access to underlying data. It uses the industry's most security-relevant data, the clarity offered by TrueIdentity user contextualisation, and LogRhythm's embedded security automation and orchestration function. Together, the capabilities of the LogRhythm TLM Platform give your organisation a powerful and efficient solution to address user-based threats.

### Further reading

- LogRhythm UEBA webpage
- LogRhythm CloudAI webpage
- LogRhythm TLM Platform webpage