DATA SHEET

User and Entity Behaviour Analytics (UEBA)

LogRhythm
The Security Intelligence Company

User accounts are critical attack vectors for hackers intent on stealing valuable data or inflicting crippling damage. Insider threats and compromised credentials introduce significant organisational risk, and you can only shut them down if you can spot them. This challenge is heightened by several factors:

- The intermingling of personal and professional user accounts
- The expansion of the IT landscape to include customers, vendors and technology partners
- The constant pressure to release access to unlock business productivity

LogRhythm User and Entity Behaviour Analytics (UEBA) detects and neutralises both known and unknown user-based threats. It analyses the diverse data ingested by LogRhythm to expose insider threats, compromised accounts, and privilege misuse and abuse – all in real time.

LogRhythm UEBA is built into the LogRhythm platform, saving you from costly data duplication, dual platform administration, and swivel chair analysis. The solution enables end-to-end threat lifecycle management with the following capabilities:

- LogRhythm's patented AI Engine™ detects threats via machine learning, behavioural profiling, peer group analysis and other techniques
- Unstructured and contextual search enable rapid forensic investigations
- Identity Inference uses authentication, access, DHCP, and other data to automatically identify the "who" behind otherwise anonymous data
- Embedded security orchestration and automation standardises and automates a coordinated response
- Smart**Response™** plug-ins automate manual tasks and enable centralised execution of pre-staged countermeasures

UEBA use cases

Insider threat: Users with legitimate access to internal networks often pose the most danger to company security. Insider threats typically begin with a user moving suspiciously and then accessing systems, applications and files in an anomalous fashion. Monitoring for insider threats helps stop data theft, fraud, sabotage, policy violations and other dangerous activity.

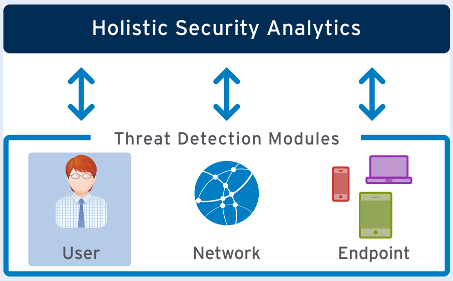
Account takeover: Attackers who have compromised your network will attempt to quickly take control of a user account. They will attempt to expand their footprint until they either accomplish their mission or get caught. LogRhythm UEBA unmasks imposters by baselining and analysing the "normal" behaviour of individual users and associated peer groups. External threats are quickly identified, ensuring that further compromise and damage is avoided.

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

UEBA use cases

- ✓ Insider threats
- ✓ Compromised accounts
- ✓ Privileged account abuse and misuse

> *"We use LogRhythm to detect insider threats and compromised accounts, and to give incident responders deep visibility into our environment."*
>
> – Security Manager,
> Enterprise Computer Hardware Company
>
> TVID: 77A-CD4-677



Holistic Security Analytics

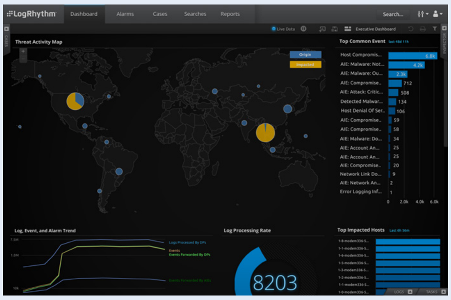
Threat Detection Modules

User

Network

Endpoint

LogRhythm provides threat analytics across the holistic attack surface, including your users and entities, networks, and endpoints.



LogRhythm provides a single pane of glass for threat lifecycle management, including dedicated dashboards for UEBA.

How LogRhythm delivers UEBA

You can enable LogRhythm UEBA through our User Threat Detection Module (UTDM). It surfaces the most concerning activities in your environment with scenario-based algorithms that employ machine learning, behavioural profiling, peer group analytics, statistical analytics, advanced correlation and other analytical techniques. The module utilises primarily user activity, as well as with network and endpoint activity. Applying multiple analytical techniques across a broad dataset enables the UTDM to more accurately prioritise true threats and reduce false positives.

Our security analytics modules are developed and actively maintained by LogRhythm Labs to help ensure you stay ahead of the latest user-based threats. This valuable content is provided at no additional charge, via cloud-based delivery.

The UTDM is provided with a straightforward deployment guide, which is organised by use case and includes detailed implementation instructions and best practices for tuning. Customers often implement the UTDM independently. For expert assistance, you can employ our Co-Pilot Analytics Service, which augments your staff with an assigned LogRhythm resource to guide you through the setup, and ongoing use and optimisation of the UTDM.

LogRhythm UEBA capabilities

Forrester key capabilities*	LogRhythm functionality
1) Collect diverse data–and lots of it.	Collect machine data from across your environment and fill in your forensic gaps with endpoint and network monitoring. Our patented Machine Data Intelligence Fabric ensures that data is optimised for security analytics purposes.
2) Correlate log information to single identities.	Know the actors behind the actions impacting your environment with Identity Inference, which attributes identities to anonymous log messages, streamlining forensic investigations.
3) Create a heuristic baseline of user activity by analysing behaviour..	Perform multidimensional baselining with AI Engine™, enabling the modeling of a broad set of user behaviours. Baselines are used to detect anomalous behaviour via machine learning and other statistical analysis techniques.
4) Use the heuristic baseline to detect unusual behaviours in real time.	Continuously analyse current activity against baselines established for each identity and peer group, with AI Engine™. Detect behavioural deviations from user and peer group baselines.
5) Detect threats of data exfiltration, privileged identity misuse and fraud.	LogRhythm's scenario-based analytics, incorporate behavioural anomalies to detect known suspicious patterns, including data exfiltration, privilege misuse, and fraud.
6) Provide case management, incident investigation, and extensive reporting.	Accelerate investigation and response with embedded security orchestration and automation functionality. Use pre-staged Smart**Response** actions to rapidly collect forensic data and invoke targeted countermeasures. Report on the results of your security program, including detection and response times.

*Forrester, Security User Behaviour Analytics Market Overview, 2016

Benefits of LogRhythm UEBA

- Minimise total cost of ownership with a unified platform built for security intelligence and analytics
- Detect known and unknown threats with multidimensional behavioural analytics
- Corroborate and surface key events that might otherwise go unnoticed
- Deprioritise false positives that aren't corroborated through our risk-based priority algorithm
- Turbocharge analysts with a single pane of glass for holistic detection, response and neutralisation