LogRhythm®
The Security Intelligence Company

User and Entity Behaviour Analytics
Protecting your organisation from within.

Insider threats are inherent to every organisation.

When it comes to detecting and responding to threats, many organisations focus their efforts on potential breaches from external sources. The truth is, an organisation's largest security threat often lies within its own network.

In 63 per cent of cases, current and former employees are the source of security incidents.[1]

Organisations are built around technology, but that technology is still controlled and managed by human hands. For a network to remain secure, both internally and externally, trust is an essential ingredient. Employees need access to critical and sensitive data on a daily basis to carry out their work, and just like security threats themselves, employees aren't static. They come and go, take leaves of absence and retire. While working, they also regularly share information.

For most organisations, the obvious solution to this is to simply control access through the use of passwords or key cards. Monitoring access is essential for gaining internal visibility of staff and understanding their use of sensitive data. This is where many organisations fail.

The risks posed by insider threats

As employee numbers grow, an organisation's vulnerability to insider threats increases dramatically. Sensitive data can be stolen, deleted or exposed by malicious individuals with access to it. However, damage or theft is just as likely to occur as a result of simple carelessness or a successful phishing attack.

On average, 49 per cent of users admit to having shared their network password with at least one other user.[2]

Insider threats can also cause the most long-term damage—with 70 per cent of incidents taking months or even longer to detect.[3] Therefore, having a suitable method for not only controlling access, but also monitoring it, is essential to successful security within an organisation. This can also provide a foundation for securely sharing both information and access levels for an entire organisation, lessening the inherent risk of insider threats.

How can your organisation prevent insider threats?

To prevent and combat the risk of insider threats, organisations first need to gain complete visibility across their networks. Traditionally, this has involved a limited view of only the network perimeter to guard against external threats and security breaches. But by using enhanced internal security controls, an organisation can also defend against insider threats by gaining a more holistic view.

Once those controls are in place, how do you gain organisation-wide visibility?

One such solution is **User and entity behaviour analytics (UEBA).**

[1]The Global State of Information Security Survey 2016, page 24.
[2]From Brutus to Snowden: A Study of Insider Threat Personas, page 3.
[3]Verizon Data Breaches Investigation Report 2016, page 42.

User and Entity Behaviour Analytics
Protecting your organisation from within.

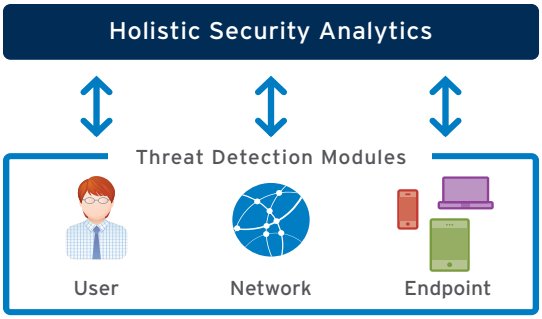
LogRhythm
The Security Intelligence Company

What is UEBA and what role does it play in your security posture?

Gartner defines UEBA as software that "successfully detects malicious and abusive activity that otherwise goes unnoticed, and effectively coordinates and prioritises security alerts sent from other systems".[4]

UEBA is a powerful tool for detecting and responding to threats posed by internal users. Not only does it help businesses uncover threats, it helps prioritise and neutralise them in an effective way by tracking every action each user makes. This goes several steps beyond what most log systems currently track.

With machine learning capabilities and sophisticated analysis, UEBA builds a baseline of what is considered normal user-network interaction so it can flag any anomalies. Red flags could indicate detection of anything from a user login from a new location to exfiltration of data to an external source. For this reason, it's extremely important to have a UEBA solution in place that can assess and prioritise threats.



Reveal blind spots in your organisation with LogRhythm's UEBA solution.

From account takeovers to privileged account abuse, UEBA is the number one solution for detecting, prioritising and responding to insider threats. LogRhythm's UEBA solution takes things one step further, combining user analytics with endpoint and network analytics to offer a single, integrated security intelligence solution. Not only does this give your organisation the visibility it needs to combat both internal and external threats before damage occurs, it accelerates time-to-value and saves resources.

Our aim is to enable organisations to detect, respond to and neutralise threats before any damage is done. To improve your risk posture and increase your security intelligence, contact LogRhythm.

About LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organisations around the globe to rapidly detect, respond to and neutralise 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 behaviour 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 recognised 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.
www.logrhythm.com

[4]Market Guide for User and Entity Behavior Analytics

www.logrhythm.com I +44 (0)1628 918 300