PRODUCT OVERVIEW

User Threat Analytics Suite

LogRhythm®

User analytics

☑ Privileged user monitoring

☑ Rogue account detection

☑ Compromised account protection

☑ User/group behavioural analytics

Whether they are tied to actual insider threats or the result of external attackers accessing compromised credentials, user accounts have long been one of the most prevalent attack vectors for advanced attacks and data breaches. This threat is increasing in complexity as the definition of insiders or privileged users in a new IT landscape expands to include customers, business and technology partners, service providers, and more. The sheer volume of user activity combined with the fact that malicious activity typically emulates legitimate user behaviour makes detecting real user-based threats nearly impossible without the right tools.

LogRhythm's User Threat Analytics Suite provides organisations with immediate visibility into suspicious or malicious user activity indicative of an attack. The Suite quickly identifies specific threats such as inappropriate insider activity, abuse of privileged accounts, abnormal user behaviour and other indicators of compromised credentials. It acts as an early warning system for security administrators, allowing them to detect and neutralise user-based threats before such behaviour results in a major impact to the business.

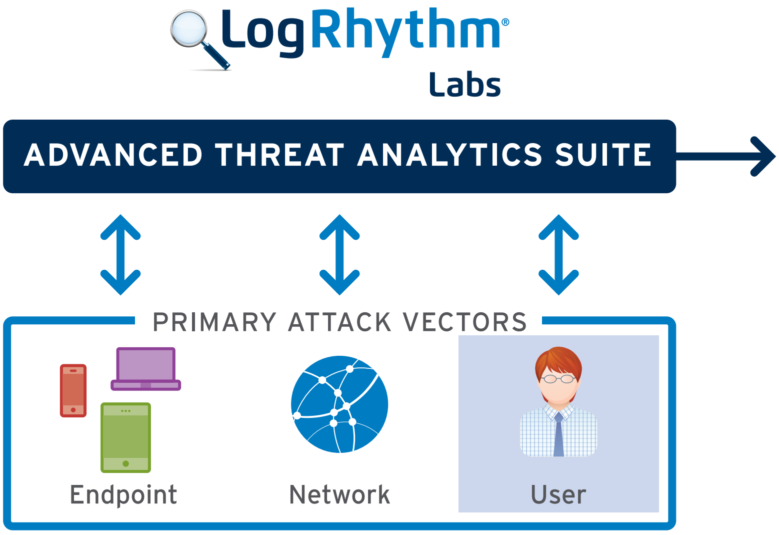
How it works

The User Threat Analytics Suite correlates identity and access management information with other machine data collected in the environment to understand user behaviour and identify unusual user activity. LogRhythm's AI Engine performs real-time advanced behavioural analytics that leverage additional event context to raise these indicators of compromise to the attention of security professionals. The Suite comes with a simplified deployment guide with recommended tuning and setup instructions for adherence to best practices offering a rapid ROI for the enterprise.

Compromised credentials
- Lateral movement following an attack
- Concurrent logins from multiple locations
- Account activity from blacklisted locations
- And more...

Privilege abuse
- Suspicious temporary account activity
- Abnormal account administration
- Unusual account privilege escalation
- And more...

Suspicious user behaviour
- Disabled account logins
- Unusual file modifications
- Abnormal password activity
- Excessive authentication failures
- Multiple account lockouts
- And more...



LogRhythm® Labs

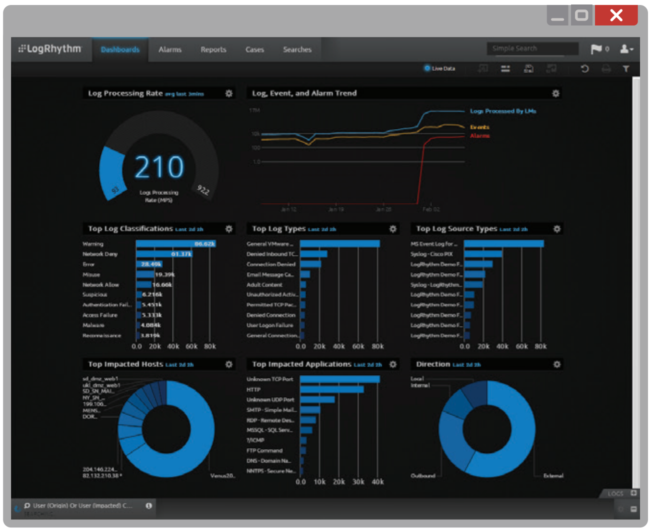
ADVANCED THREAT ANALYTICS SUITE

PRIMARY ATTACK VECTORS

Endpoint

Network

User



Whether they have been compromised or stolen, or belong to a legitimate insider threat, user credentials remain one of the biggest potential security holes in any organisation's network. LogRhythm's User Threat Analytics Suite takes a comprehensive approach to real-time monitoring and analysis of user behaviour using a variety of techniques. It empowers customers by detecting the initial security event, prioritising which activities pose the greatest threat, and initiating automated actions to neutralise attacks before they cause significant damage.

Privilege abuse: Accounts with escalated privileges pose a significant insider threat due to their administrative access and high clearance levels. With their direct access to sensitive data systems, privileged user accounts can be abused to steal sensitive data like intellectual property, Protected Health Information (PHI) and credit card data, making them a key target for attackers. The User Threat Analytics Suite leverages an extensive library of advanced behavioural analytics rules and activity reports that specifically monitor privileged user activity to detect instances of misuse. These tools detect concerning activities such as unusual account administration, suspicious account creation and other forms of privilege abuse. Out-of-the-box Smart**Response**™ plug-ins can automatically neutralise threats by disabling or quarantining privileged user accounts.

Account takeover: Stealing legitimate credentials and taking over user accounts is a common technique employed by hackers trying to infiltrate IT defenses. Abnormal behaviour patterns may be a sign that the user account has been compromised and is being used for malicious activity. The User Threat Analytics Suite uses automated profiling to baseline "normal" user behaviour and can immediately notify the security team of abnormal account activity, such as authentication from a strange location, unusual access of sensitive data, or through the use of unauthorised endpoint devices. Smart**Response**™ can then initiate preventative response actions like disabling the account or quarantining the device from which the actions are being taken.

Account creation/deletion/modification: Attackers who have broken through the IT perimeter may escalate the privileges of compromised accounts or create new accounts on internal systems to move laterally within the network to conduct a broad range of malicious activities. When their objective is accomplished these escalated privileges and new accounts are frequently deleted/reverted to hide the evidence, making both real-time detection and forensic reconstruction difficult. LogRhythm's User Threat Analytics Suite includes out-of-the-box behavioural analytics that will detect the addition of new accounts and changes to existing accounts, as well as associated activity indicative of a potential breach. Administrators are automatically alerted to sophisticated user account manipulations, allowing them to rapidly investigate and take corrective action before significant damage occurs.

Suspicious remote user activity: Unusual remote access activity is also an indicator of account takeover. The proliferation of the mobile workforce has made remote access easier to exploit, while also making it harder to detect. The User Threat Analytics Suite contains multiple rules that detect activity, including multiple VPN logins for the same user, multiple password resets and even multiple login attempts from different locations. Organisations can also quickly modify existing rules to detect other scenarios, such as a user's access badge being used within a short period of time before or after that same user logged in via VPN from a remote location.

Brute force compromises: Despite increased awareness in the importance of security, organisations remain vulnerable to attacks exploiting system and user accounts that are using default or weak passwords. Using simple automation tools, attackers can make a large number of access attempts that target user and/or system accounts that may be using common or overly simple passwords. The User Threat Analytics Suite delivers powerful out-of-the-box behavioural analytics that detect unauthorised access attempts tied to a variety of brute force attacks, including rules that detect malicious activities like distributed brute force attempts, an abnormal number of failed logins on the same host, or an unusual number of failed login attempts using the same account from different machines. Additional rules identify more concerning activity that may be indicative of a successful attack, such as a brute force attack followed by one or more successful logins from the same point of origin. Smart**Response**™ can then take immediate action to neutralise the attack by disabling the compromised accounts or blocking the attack by adding the source IP to a firewall ACL.