LogRhythm™

A Guide to User and Entity Behavior Analytics (UEBA)

Contents

01

What is UEBA and Why is it Important?

You are facing a constant barrage of threats — some of which you do not even know exist. The reality is that your users are behind many threats and breaches, whether they are malicious or accidental. As the typical point of entry for an attack, users are a difficult vector to monitor and secure. To confront the tidal wave of attacks, you need to hone your attention on users by harnessing the power of user and entity behavior analytics (UEBA).

UEBA is a cybersecurity solution that applies analytics to track user and entity behavior and detect potential unauthorized activity that may indicate a cyberattack.

In this white paper, discover everything you need to know about UEBA; gain insight into user-based threats, UEBA use cases, how UEBA solutions work, and best practices for analyzing user behavior. Also, learn how LogRhythm UEBA gives you a single view of users and accelerates the qualification and investigation processes of potential threats to minimize your organization's cyber risk.

According to industry research:

52%

of security professionals say reducing negligent insider risk is one of their biggest security challenges.

48%

of respondents suggest reducing malicious insider risk is one of their biggest challenges.

Learn More

02

Focus on User Behavior

When protecting your organization, it is critical to monitor users because they are often the weakest link in your defenses. According to the Verizon 2022 Data Breach Investigations Report, "82% of all security incidents involve a human element."[1] Across all industries, data shows that users are vulnerable to cyberattacks and whether it is the use of stolen credentials, phishing, misuse, or simple error, the people in your organization play a role in incidents or breaches.[2]

Despite educating and training your personnel, implementing measures such as multi-factor authentication (MFA), and enforcing strong password policies, your environment is still at risk. Whether an account has been compromised or the user is behind the attack, a user account that is involved during a cyberattack, leaves a trail of rich forensic evidence.

To improve your security maturity and reduce risk, you need a more proactive approach to defend against user-based threats. Many attacks involve lateral movement and the best way to defend your environment is to continuously analyze all user behavior — regardless of whether threats originate internally or externally. Focusing on your users' activities gives you an important vantage point to identify potential threats before they become damaging breaches.

[1] 2022 Data Breach Investigations Report, Verizon, May 2022

[2] Ibid

03

Use Cases of User-Based Threats

When evaluating UEBA solutions, it is important to keep your top use cases in mind based on your organization's specific needs and requirements. At a high-level, UEBA solutions can help security teams detect and respond to the following attack techniques.

Account compromise

Regardless of the attack vector or malware used in this type of attack, you should monitor if a hacker has acquired and improperly used valid credentials. Advanced persistent threats (APTs) often operate with legitimate user accounts, which can make them difficult to detect with simple analytics, such as pattern matching, thresholds, or correlation rules; however, because a compromised account behaves differently, you can perform behavioral profiling to recognize anomalies related to account logins, data access, and other parameters.

Attack examples

- Intern mistakenly opens a malicious attachment in a phishing email
- Hacker steals a victim's personal Gmail user credentials and uses the same login information to access their company's environment
- Hacker executes a brute force attack due to weak password policies
- Cybercriminal uses a man-in-the-middle attack tactic to intercept competitive intelligence

Potential indicators

1. Unusual authentication patterns (high volume of authentications)
2. Lateral movement following an attack
3. Concurrent logins from multiple locations
4. Account activity from locations never seen before and a password changed shortly after
5. Brief time between authentications indicating an improbable travel

Malicious insider threat

Insider threats are a top concern because it is often difficult to detect when an attack is occurring from within an environment. Insider threats originate from trusted users, such as a current or former employee or a contractor. They are usually motivated by the pursuit of financial gain or the desire to commit sabotage. This means that everyone, including managers and executives, should be inspected. To detect these threats, you should monitor for high-risk deviations from baselined behavior.

Attack examples

- Disgruntled employee deliberately exfiltrates data before leaving the company
- Employee conducts corporate espionage by selling proprietary product information

Potential indicators

1. New or unusual system access
2. Disabled account logins
3. Unusual file access and modifications
4. Abnormal password activity
5. Excessive authentication failures
6. Multiple account lockouts
7. Authentication into high number of hosts in a short time

Privilege account abuse and misuse

By possessing heightened access to key systems and data, privileged users present a greater risk to your organization. To remain secure, you should closely monitor their behavior and minimize the availability of excessive or improper privileges. This should also help you quickly clean up dormant accounts and user privileges that don't abide by the principle of least privilege (PoLP) per the Zero Trust model.

Attack examples

- Hacker accesses a user account with stolen credentials and executes lateral movement to a privileged account
- An admin clicks on a link that contains malware via a targeted spear-phishing attack

Potential indicators

1. Suspicious temporary account activity
2. Abnormal account administration
3. Unusual privilege escalation
4. Account lockouts
5. New account creation

As you dive deeper to assess and prioritize your specific use cases, you need to create a strategy for robust detection and response. To effectively defend against threats, you can align your use cases to knowledge bases such as MITRE ATT&CK™ and MITRE D3FEND™, which provide a framework of attacker and defender behaviors to help you standardize your process for technical countermeasures.

Let's explore an example of how this works by examining a specific countermeasure technique relating to the MITRE D3FEND category for user behavior analysis (UBA).[3] When assessing the User Geolocation Logon Pattern Analysis (D3-UGLPA[4] technique), MITRE D3FEND mentions that logon activity which deviates from normal patterns can indicate a remote attacker using stolen credentials. Three use cases are listed:

- Logons from locations that are different from where a user usually logs in
- Logons from a location in which an enterprise has no users located
- Logon that is not physically possible given the elapsed time since a logon from another location

By mapping to knowledge bases, you can gain insight into the detections suggested for defending your environment. Now that you know what to look for, your security team needs a solution that can help detect and score abnormal behavior so that you can prioritize your response. For example, all three points mentioned in the use case above require anomaly detection. To offer the best detection coverage, you need domain expertise and machine learning to expand detection and track other behaviors that may not be fully mapped, such as origin host, impacted host, and authentication behavior. Leveraging the power of UEBA solutions can help you get the job done effectively and improve the analyst experience to detect and respond to threats.

[3] User Behavior Analysis, MITRE D3FEND

[4] User Geolocation Logon Pattern Analysis, MITRE D3FEND

04

The Power of UEBA Solutions

UEBA technology provides security operations centers (SOCs) with visibility to uncover user-based threats that might otherwise go undetected, and the capability to defend against a variety of attacks that range in complexity. Effective UEBA solutions can help your team:

- Process machine data into a consistent, security-relevant schema
- Obtain a true view of actual users — not just disparate accounts
- Detect and prioritize complex user-based threats
- Accelerate the qualification and investigation of potential threats
- Streamline response through security operations workflows and automation

An effective UEBA solution requires four elements: correct and consistent data processing (i.e., data normalization), association of data to identities, behavioral anomaly detection, and threat detection.

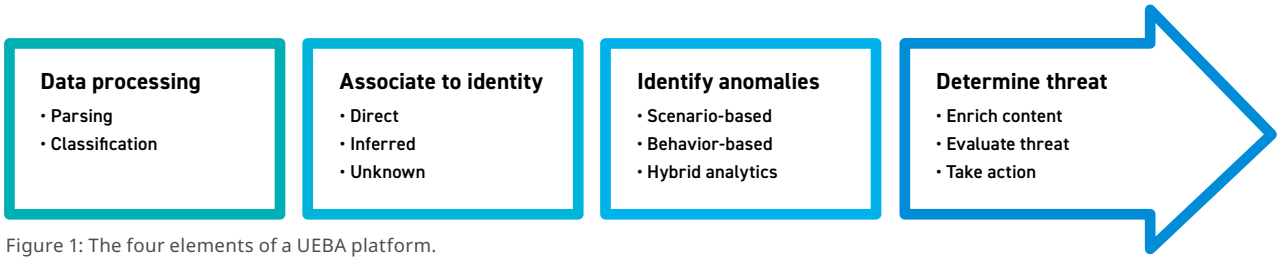

Figure 1: The four elements of a UEBA platform.

Process data for UEBA

Your organization collects and generates an extraordinary amount of data from diverse sources. Before you analyze that data, you must first normalize and enrich it to enable effective search and machine analytics. Without successfully preparing data for analytics, your UEBA solution will inherently include blind spots, creating false negatives by missing important activities, or worse, creating false positives by mischaracterizing innocuous anomalies as threats.

Data processing begins by parsing machine data into metadata fields specifically structured to enable security analytics. Applying a uniform schema to processed data is table stakes for UEBA. A close examination will reveal wide variance between the power of these capabilities from solution to solution. For example, in a log message that shows an admin changing the permissions of a different user, the schema must be able to distinguish between the admin and the impacted user. Data normalization enhances the accuracy of parsed data by adjusting values based on known variances.

Data enrichment describes the process of adding metadata derived from the log with additional contextual data to enable more effective analysis. Below are a couple examples of data enrichment.

- Using geolocation to convert an IP address into an inferred location
- Decoding esoteric log message codes into a meaningful and vendor-agnostic classification (e.g., Windows Event ID 4624 = successful account logon)

Data classification is particularly valuable to effectively analyze diverse equipment and vendors (e.g., understanding the common meanings behind numerical codes from Check Point, Cisco, and Palo Alto). It is also useful to understand common activities that analytics can leverage, such as all authentications, the authentication type, location, and time used by an account regardless of the underlying infrastructure.

Importance of identities for analytics

For UEBA to function effectively, associating normalized data to an identity is critical. It can be difficult to see the complete picture of a given user's behavior without the use of an associated identity because so many types of identifiers exist, each with potentially different taxonomies, naming conventions, and formats.

Individual actions from different users and hosts are disparate data points that mask security-relevant activities; however, when those actions are associated to a common identity, they tell an important story. UEBA solutions should enable the development of two distinct types of identities.

- **User identity:** Any given user has multiple different accounts, which are represented in data sources with identifiers that vary from account to account. For example, the account identifier for Active Directory (AD) might be "domain name/user," while the account identifier for Office365 might be "user@domain." To achieve accurate analytics, it is vital to associate the activity from each unique account identifier into a single identity or profile.
- **Host identity:** Just like users, a host's activity is represented through multiple different identifiers. For example, a host may be identifiable via a MAC address in one log and a system name in another. By consolidating these data points into a single profile, you can gain a full view into host activity.

05

Defend Against Complex Attacks with Holistic Analytics

The threat landscape is becoming extremely difficult to map as threats grow in complexity and precision in targeted attacks. To properly defend your organization, a holistic analytics approach is required to stay away from silo analysis and it's important to understand that threats are identified through interconnecting factors, variables, and conditions.

Analytics play a key role in detecting user- and entity- based threats. Effective UEBA solutions use multiple and complementary analytic approaches, such as deterministic analytics and anomaly analytics, to help you achieve visibility across the environment and detect complex attacks.

Deterministic analytics

Many attacks follow a predictable sequence or pattern of activity. Deterministic analytics help organizations identify such attacks in real time, which are described by a specific, defined logic rule. UEBA solutions use a series of applied scenario-based analytics against broad sets of environmental data to surface critical threats. Scenario-based analytics recognize established tactics, techniques, and procedures (TTPs) and diverse techniques using statically defined rules.

Anomaly analytics

Anomaly analytics help identify attacks by profiling and detecting unusual activity. In addition to scenario-based analytics, behavior-based analytics strengthen UEBA capabilities through anomaly detection. Behavior-based analytics use machine learning (ML) to surface anomalous behavior. This technique is needed for complex attacks that require more sophisticated detection capabilities.

Key techniques include:

- **Individual behavioral profiling:** Recognizes changes in user behavior by detecting and characterizing deviations of the user compared to the user's own baseline activity
- **Group behavioral profiling:** Recognizes changes in user behavior by detecting and characterizing deviations of the user compared to all monitored users' baseline activity
- **Peer group analysis:** Recognizes outliers in the behavior of a group of users by comparing users to their peers

As part of identifying anomalies, UEBA solutions must quantify or score abnormal behavior automatically, and output as much contextualization as possible about the findings. To set the score correctly, it is especially important to appropriately apply data science and machine learning to your security strategy.

Cybersecurity is a unique field and machine learning models that are successful in other domains may not perform well in this industry. Some of the challenges involved with model development for cybersecurity are:

- Building domain expertise in the field takes time
- Collecting more logs for the models is not always the solution in cybersecurity because of the complexity of the metadata involved
- Tactics and techniques of attacks are constantly evolving
- Remote work creates challenges with predicting user behavior
- Lack of focus on enhancing the data treatment and feature extraction

To get the most value out of your security solution, it is important to keep ML models as simple as possible and focus on the detection capabilities rather than on the model complexity. Security teams must have a deep understanding of attack techniques and the logs and metadata involved in the attack. For example, applying only computer science or math and statistics knowledge to machine-learning models in cybersecurity may lead to low-added value and outcomes. Domain expertise is necessary because of the complex nature of data used for ML models in the security industry. It is important to know that not all logs contain the same metadata fields, not all vendors define the log fields in the same manner, different activities produce a different number and type of log, and log distribution may not be as repeatable as expected.

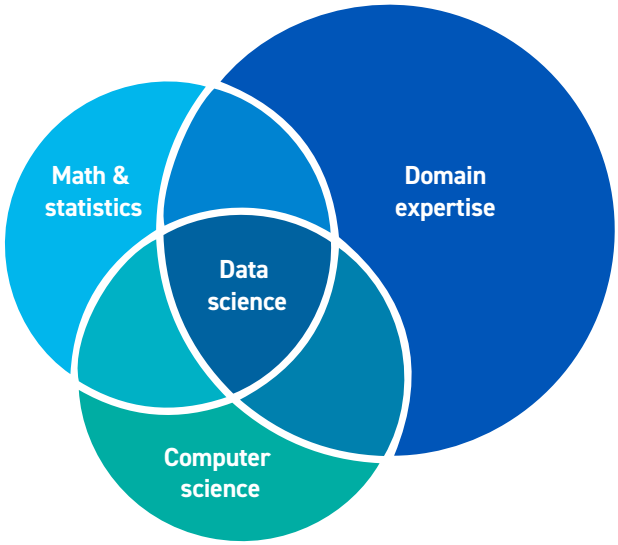

Figure 2: Key elements in data science.

Linking deterministic and anomaly analytics to detect user-based threats

Using a combination of deterministic analytics and anomaly analytics can help you detect suspicious activity across the entire spectrum of complex threats. Explore an example of how this works with the MITRE ATT&CK technique below.

MITRE ID: T1558.003—Steal or Forge Kerberos Tickets[5]

According to MITRE ATT&CK, "adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force." This will expose your environment to an attack.

Detecting this technique can be split into two parts. Each part is best achieved using a different detection type, as shown in the table below.

Detection	Analytics Detection Type
Investigate irregular patterns of Kerberos activity (e.g., accounts making numerous requests, Event ID 4769, within a small timeframe)	Anomaly
Monitor for service ticket requests with RC4 encryption [Type 0x17]	Deterministic

Table 1: Detecting MITRE ID: T1558.003 with anomaly and deterministic analytics.

This example, and many other MITRE ATT&CK techniques, reinforce how holistic analytics is the best approach because a comprehensive variety of models and algorithms are used to detect threats accurately. While deterministic and anomaly analytics each provide independent value, there is greater advantage with using them as complementary approaches. By implementing both methods, you can achieve complete coverage across the environment, allowing you to monitor and minimize the risk associated with all types of users.

If each activity is isolated, analysts may lack insight into which threats to prioritize, allowing attacks to go unnoticed for longer periods of time. The combination of these analytic techniques helps with risk-based prioritization, expedites investigation, and enables task automation. This enhanced workflow improves your likelihood of detecting true threats and reduces the generation of false positives.

[5] Steal or Forge Kerberos Tickets: Kerberoasting, MITRE ATT&CK, last modified March 8, 2022

06

UEBA and SIEM Integration

Once you discover suspicious activity indicative of a true threat, there is more work to do. An effective UEBA solution can fully integrate with a security information and event management (SIEM) to help you further qualify, investigate, neutralize, and respond to a threat.

After flagging a potential threat, leveraging UEBA and SIEM capabilities together can help you qualify and investigate the activity through search analytics. Purpose-built dashboards and data visualizations enable you to explore and assess data associated with a specific identity or event. These visualization tools should be highly configurable to offer custom views of your datasets. Forensic search capabilities should allow you to conduct unstructured and structured queries during your response.

UEBA and SIEM solutions that provide embedded security orchestration, automation, and response (SOAR) accelerate threat qualification and investigation to expedite mitigation. Case management and incident management workflows support the standardization of key processes and let multi-tier SOC teams work seamlessly together. Automated actions accelerate response with triggered investigatory steps and countermeasures, while playbooks make the most of security resources using collaboration, guided workflows, and best practices.

07

Reduce Risk with LogRhythm UEBA

It is important to implement a comprehensive UEBA solution that helps you quickly detect, respond, and remediate user-based threats across the environment. LogRhythm UEBA is LogRhythm's advanced user and entity behavior analytics solution that helps you identify, qualify, investigate, and remediate threats that might otherwise go unnoticed. It empowers analysts to monitor user behavior, applying both deterministic and anomaly analytics to achieve visibility across a variety of complex threats.

Leverage LogRhythm's Machine Data Intelligence Fabric

A clean, consistent, and predictable dataset is critical to perform accurate analytics. LogRhythm's Machine Data Intelligence (MDI) Fabric enables you to accurately identify and prioritize true threats and anomalies by helping you make sense of your organization's log and machine data.

LogRhythm's MDI Fabric processes your logs into over 100 searchable fields. With out-of-the-box support for twice as many data sources as competing solutions, it accelerates time-to-value and decreases the burden on your analysts. To glean more information from your logs and to provide additional context, MDI Fabric also enriches your data. Specifically, TrueGeo™ uses IP geolocation to determine the origin and destination of activity and TrueTime™ normalizes timestamps across time zones. Additionally, a three-tier classification taxonomy automatically deciphers your data into actionable and vendor-agnostic information that enables rapid use case implementation.

LogRhythm also enables secure investigation with embedded incident response capabilities, case management, and collaborative workflows to ensure qualified threats are vetted. LogRhythm uses case dashboards and a secure evidence locker to centralize forensic data to give you greater visibility into active investigations and threats. Finally, risk-based event determination assigns a risk score to each log message based on reconfigurable parameters to help you determine which threats merit investigation.

Download the Data Sheet

To learn more about LogRhythm UEBA and how it works, read the product data sheet.

Download

Consolidate and establish identities to improve your analysis

LogRhythm understands identity. LogRhythm TrueIdentity™ consolidates a user's disparate account types and identifiers (e.g., Active Directory work email, personal email, and badge PIN) into a single identity. LogRhythm's TrueHost™ feature combines multiple host identifiers into a single profile. By achieving comprehensive visibility into the activity of specific users and hosts, you benefit from greater security and operational context to power effective analysis.

Detect complex threats with deterministic and anomaly detection analytics

LogRhythm enables the detection and prioritization of threats across the environment through an array of analytics techniques. LogRhythm AI Engine applies deterministic analytics in real time, leveraging diverse techniques (e.g., correlation, pattern matching, and statistical analysis) to detect threats. AI Engine automatically corroborates and links related alarms, identifies threat progression along the stages of the cyberattack lifecycle, and elevates risk scoring as appropriate.

LogRhythm UEBA anomaly detection identifies potential threats with machine learning, complementing AI Engine's application of field-proven threat models. It detects and characterizes shifts in how users interact with the IT environment and identifies behavior that deviates significantly from dynamically established peer groups. LogRhythm UEBA forwards anomaly-based observations to LogRhythm SIEM, enabling enhanced correlation with AI Engine, improving the workflow with SIEM capabilities such as dashboards, searches, cases, automated response, and more.

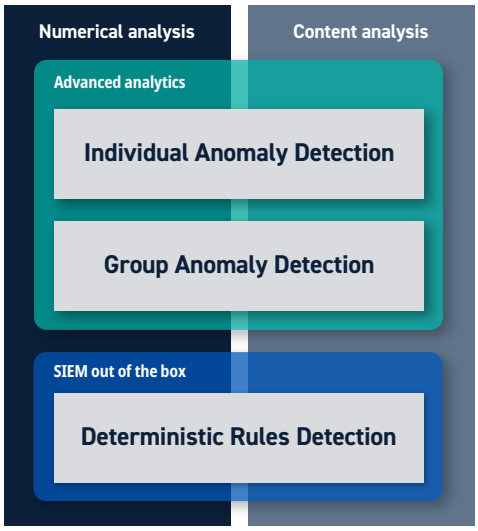

Figure 3: LogRhythm's holistic UEBA analytics approach.

To further protect your organization, LogRhythm Labs, our dedicated team of threat researchers, develops security research, threat intelligence, and threat scenarios using our Current Active Threats (CAT) module, LogRhythm's IOC-based detection content.

Streamline your security operations team

LogRhythm accelerates your response to user-based threats with embedded SOAR capabilities, providing automation-enabled workflows that speed threat qualification, investigation, and remediation. Integrated playbooks streamline and standardize the work of multi-tier security operations teams, improving their effectiveness and efficiency. For less experienced analysts, playbooks provide repeatable procedures to expedite onboarding and rapidly develop necessary skill sets. LogRhythm SmartResponse™ further accelerates response through automated, approval-driven, or manually triggered investigatory steps and countermeasures.

08 ___

Get Started with UEBA

It is more important than ever to protect your organization from increasingly sophisticated and numerous threats that can lead to a damaging breach. To win this battle, you need to focus on your users and the degrees of risk that they introduce to your organization. The most effective way to accomplish this is by analyzing rich user data through the power of UEBA.

LogRhythm can help you understand what your top use cases are based on the latest trends in your region and industry and align to knowledge bases such as MITRE ATT&CK and MITRE D3FEND. LogRhythm UEBA maps the authentications and tracks anomalies grouped by the following behavior types:

- Origin hosts
- Impacted hosts
- Authentication classification
- Origin location
- Peer group

To uncover threats to which you were previously blind, LogRhythm's deterministic and anomaly detection analytics provide essential visibility into your users and their activity, giving you the tools to protect your organization and reduce risk.

Speak with one of our security experts to get a first-hand look at LogRhythm UEBA and learn how we can address your specific use cases.

Schedule Custom Demo

About LogRhythm

LogRhythm helps busy and lean security operations teams save the day—day after day. There's a lot riding on the shoulders of security professionals—the reputation and success of their company, the safety of citizens and organizations across the globe, the security of critical resources—the weight of protecting the world.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an ever-changing threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Together, we are ready to defend.
Learn more at logrhythm.com.

www.logrhythm.com // info@logrhythm.com

United States: 1.866.384.0713 // United Kingdom: +44 (0)1628 918 330
Singapore: +65 6222 8110 // Australia: +61 2 8019 7185