

Top 13 Use Cases for User and Entity Behavior Analytics (UEBA)

With an overwhelming number of security tools, along with staffing shortages and skills gaps, security teams struggle to solve threat detection, investigation, and response (TDIR) challenges. The problem? Many tools rely on predefined correlation rules and attack patterns spanning multiple organizational systems and data sources. That's where UEBA solutions come in. Unlike traditional tools, UEBA solutions build profiles that model standard behavior for users and entities — such as servers, routers, and data repositories — in an IT environment. Using the power of machine learning and analytics, UEBA technology can establish a baseline of users' and devices' normal behavior patterns and identify any anomalous activity. This translates to improved capability to detect, investigate, and respond to even the most elusive threats.

Organizations evaluate UEBA across four primary categories:

Prioritization: Security analysts face a constant stream of daily alerts, leading to a need for efficient prioritization. UEBA helps overwhelmed, resource-strapped security operations center (SOC) teams by identifying and prioritizing alerts, ensuring focus on the ones that matter most.

Threat Detection: A security solution's value lies in its ability to detect attacks. UEBA excels in detecting challenging threats, including compromised credentials, insider threats, and external attacks.

Investigation: Security teams often struggle with compiling incident details and conducting timely, holistic investigations. UEBA streamlines this process by combining event data with contextual information about users, assets, threats, and vulnerabilities, enabling risk scoring and alert prioritization, and expediting investigations.

Response: After identifying an attack, incident response teams need to swiftly and decisively assess and remediate to ensure the attacker isn't still lurking in the network. UEBA guides efficient and effective response by detailing affected areas, actions taken, and accounts used during the incident.

Top 13 UEBA Use Cases

In evaluating UEBA solutions, it's important to understand the capabilities of AI-driven analytics. Organizations should ensure vendors support the following use cases and, most importantly, that this support is demonstrated within the POC or pilot.

Detection Use Cases

The earlier an organization can detect a cyberattack, the less impact it has. The following UEBA use cases enable better detection, and an effective solution will handle all of these:

1. Compromised User Credentials:

Detecting compromised credentials of any employee or contractor within the organization is foundational for UEBA. The solution should easily detect unauthorized control of network user credentials, irrespective of attack vectors. This includes detection of malware and attacks like pass-the-hash, and should work across credentials, devices, and IP addresses.

2. Privileged User Compromise:

Identifying attacks on privileged users, such as database administrators (DBAs) or system administrators with special access to sensitive systems, is paramount. It is essential for UEBA to immediately detect any compromise of their credentials, even in instances where attackers gain direct entry to critical systems. Detecting attacks targeting these users presents a unique challenge due to potential deviations from established behavior patterns, due to the nature of their roles. Nevertheless, UEBA solutions should have the capability to effectively identify such deviations.

3. Executive Assets Accessed:

Executive assets, like the CEO's laptop, are prime targets for attacks because they contain sensitive financial and competitive data. For instance, cybercriminals steal millions yearly using webmail schemes tricking executives into approving fraudulent wire transfers. An effective UEBA solution should automatically build an asset model, identifying executive systems and monitoring them for any unusual access.

4. Insider Threats:

Although many major breaches result from compromised credentials, the rogue insider remains a significant data loss threat. A UEBA solution must promptly detect any user, privileged or not, engaging in activities outside their typical behavior.

Each of these use cases is connected to the detection of cyberthreats. It's important to note that they are not mutually exclusive; an effective UEBA solution should be able to handle all of the abovementioned use cases.

Prioritization, Investigation, and Response Use Cases

Although many UEBA vendors talk about threat detection, only a few can actually support the use cases that improve the productivity of SOC and IT staff. The following UEBA use cases focus on improving incident prioritization, streamlining investigations, and increasing overall incident response efficiency. A good UEBA solution should be able to support all of these simultaneously:

5. Account Lockouts:

Account lockouts are a significant drain on administrative resources, especially in larger organizations. It's common for them to allocate a full-time position annually solely for analyzing user account lockouts. Admins spend four to five hours per lockout investigating whether it's a simple mistake or a potential account takeover. An effective UEBA solution should automate this process and render a swift verdict on account risk. This automation has the potential to save the equivalent of a full-time position annually in larger organizations.

6. Account Creation:

Attackers may infiltrate a network using malware on one system, leveraging this entry point to create unrelated new accounts. Even if IT re-images the compromised machine, attackers persist in the system with a new credential. The UEBA solution must monitor account creation, quickly identifying anomalies like unauthorized credential creation or procedural violations.

7. Account Sharing:

Organizations face challenges when users share credentials — a policy violation and security risk. For instance, DBAs might share a customer database account for tasks like issue resolution and performance tuning. The UEBA solution should detect such cases, specifying users involved and facilitating efficient remediation.

8. Service Account Classification:

IT security often lacks visibility into high-privilege service accounts, making them prime targets for attackers. Take the SAP “Firefighter” account, for example, with significant privileges in a critical application. A UEBA solution should automatically identify and flag any abnormal behavior in service accounts.

9. Dormant User Accounts:

Organizations often have policies for dormant accounts. If users don’t log in for 30 days, they may have left the company, and regular processes may not deactivate their accounts. The UEBA solution should continuously track employees and contractors with inactive credentials.

10. Security Alert Investigation:

Various security products like anti-malware, DLP, and network access control coexist with UEBA organizations, generating alerts requiring investigation. However, these alerts often lack essential information (for example, owner name and department), posing challenges for SOC first responders. The UEBA solution must offer detailed context for third-party security alerts, allowing SOC teams to input an alert ID and instantly access all context information for that alert.

11. Account Investigations:

Legal and HR departments often request a month’s user activity history, a task traditionally involving manual and time-consuming extraction across various systems. A UEBA solution simplifies this by offering an automated timeline view of network activity, including VPN logins and credential switches. This efficient approach not only highlights access patterns and anomalies, but also assigns a risk score to activities, potentially saving days of investigative effort.

12. Breach Forensics Review:

After a data breach, teams typically spend weeks manually assembling the incident sequence to identify the responsible parties, the sequence of events, and the impacted systems. A UEBA solution should automate this process, streamlining the effort and presenting a comprehensive explanation of the individuals and systems involved.

Testing and Training

13. Red Team Timelines:

SOCs often employ Red Team testing to expose vulnerabilities and train analysts for future attacks. A UEBA solution should seamlessly assist Red Team testing by illustrating the complete attack chain during and after security event simulations. This aids in improving internal understanding of weaknesses and vulnerabilities.

Conclusion

UEBA provides tangible benefits in detecting, investigating, and responding to modern threats effectively. When selecting a solution, prioritize architecture supporting basic and advanced cases, including unidentified scenarios. Consider whether you prefer a standalone UEBA solution or integrated SIEM with UEBA functionality.

Some systems combine SIEM's data breadth with UEBA's analytics. Standalone UEBA solutions offer flexibility to run on existing SIEM, log management, or data lake tools, bolstering defenses against sophisticated attacks.

The Exabeam Security Operations Platform offers both integrated and standalone UEBA solutions. Exabeam Fusion provides modern SIEM using data lake technology. Exabeam Security Analytics and Exabeam Security Investigation offer flexible integrations, upgrading defenses against elusive threats. All three solutions baseline normal behavior, highlight anomalies, and assign risk scores to notable events. In addition, they provide the following UEBA capabilities:

Rule and signature-free incident detection — Exabeam uses advanced analytics to detect abnormal and risky activity, eliminating the need for predefined correlation rules or threat patterns. It delivers meaningful alerts with minimal setup and tuning, reducing false alarms.

Automatic timelines for security incidents — Exabeam consolidates related security events into a timeline, revealing incidents across users, IP addresses, and IT systems.

Dynamic peer groupings — Exabeam not only performs behavioral baselining of individual entities, but also dynamically groups similar entities, like users from the same department or IoT devices of the same class. This enables the analysis of normal collective behavior across the entire group and identifies individuals exhibiting risky behavior.

Lateral movement detection — Exabeam tracks attackers moving through a network with different IP addresses, credentials and machines to locate sensitive data or key assets. By consolidating data from multiple sources, it connects the dots, offering a comprehensive view of the attacker's journey through the network.

Explore Exabeam Solutions

Key features of the Exabeam Security Operations Platform include rule-free incident detection, automated timelines for security incidents, dynamic peer groupings, and lateral movement detection.

Whether replacing a legacy SIEM or augmenting an existing one, Exabeam provides modular solutions for overall security operations success.

Get started: [Exabeam Security Log Management](#)

SIEM replacement: [Exabeam SIEM](#) and Exabeam Fusion

SIEM augmentation: [Exabeam Security Analytics](#) and [Exabeam Security Investigation](#)

Exabeam, the Exabeam logo, New-Scale SIEM, Detect. Defend. Defeat., Exabeam Fusion, Smart Timelines, Security Operations Platform, and XDR Alliance are service marks, trademarks, or registered marks of Exabeam, Inc. in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2023 Exabeam, Inc. All rights reserved.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation, and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.

 **exabeam®**
**Detect
Defend
Defeat™**

Get a demo →

Speak with an Expert →

Join a CTF →