

User Behavior Analytics (UBA) relies on machine learning to transform millions of events into the handful of users that are performing risky behavior right now. In essence, UBA is about the machine telling the security analyst where to focus. Threat hunting is a complementary technique that enables analysts to query the event data to find users that match a specific set of criteria. Threat Hunting is about the analyst telling the machine to find the users that fit X, Y, and Z parameters.

Exabeam is the only security intelligence vendor to provide both powerful UBA capabilities and market-leading threat hunting functionality, now available through Exabeam Threat Hunter.

Query, Pivot, and Drill Down on Session Data

The Exabeam platform uses Stateful User Tracking™ to connect individual user activities into a session data model. Threat Hunter allows security professionals to query the platform to find all users whose sessions contain specific activities or attributes, or any combination of activities or attributes. For example, an analyst might first ask for all user sessions where the user logged into the VPN from a foreign country for the first time. The analyst can then trim the results by asking for users who then accessed a server for the first time, and then later the anti-malware software flagged a problem on that server. While each of these activities is independent of the others, the ability to combine them in a simple, point-and-click search provides significant power to even a junior analyst.

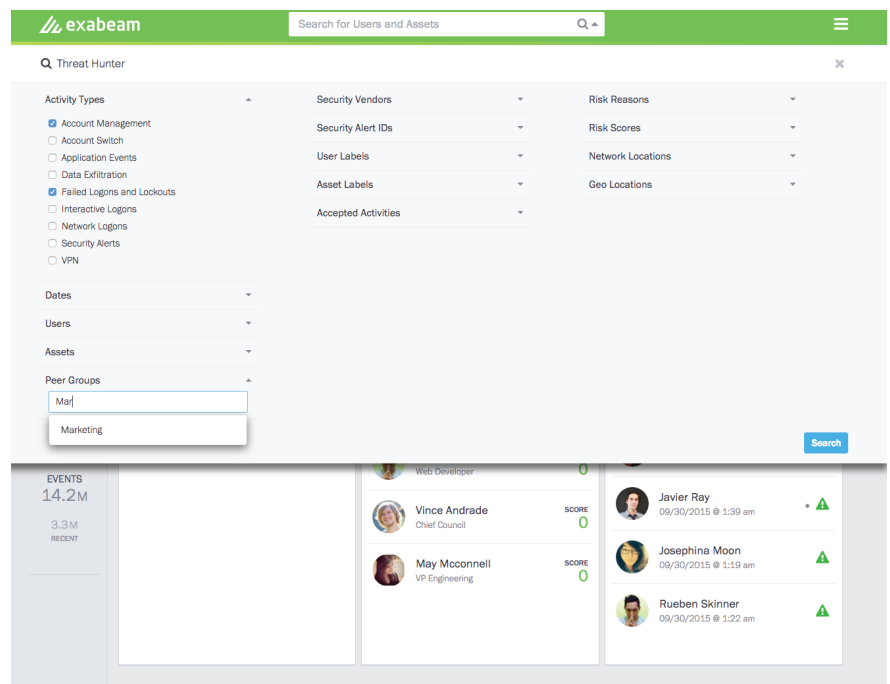
Pull on Threads, Find Hidden Threats

While the UBA engine is designed to find users who have performed multiple activities that, together, add up to an elevated risk score, Threat Hunter gives analysts the tools to “pull on threads” to track activity that is deliberately kept under the radar. Threat hunting can be very effective after UBA is used to detect an attack. Where UBA can identify a specific attack, Threat Hunter can proactively search for groupings of activities that are similar to aspects of that attack. As a result, Threat Hunter customers are more effective at responding to all aspects of a cyber attack.

Proactive Security Intelligence

In the example shown here, an analyst uses Threat Hunter to clean up after a malware outbreak in the marketing department that allowed hackers to penetrate the network. The analyst begins by hunting for all sessions where any user in Marketing performed account management (i.e. new account creation or privilege escalation) and also had a failed logon.

The analyst doesn't need to understand the structure of the applicable logs, nor the search language of the underlying log management system. She simply clicks a few fields and hits “Search.”



The screenshot displays the Exabeam Threat Hunter interface. At the top, there is a search bar labeled "Search for Users and Assets" and a search icon. Below this, the "Threat Hunter" section is active, showing a list of filters. The "Activity Types" filter is expanded, showing options like "Account Management", "Account Switch", "Application Events", "Data Exfiltration", "Failed Logons and Lockouts", "Interactive Logons", "Network Logons", "Security Alerts", and "VPN". The "Dates", "Users", and "Assets" filters are also visible. The "Peer Groups" filter is set to "Marketing". The "Security Vendors", "Security Alert IDs", "User Labels", "Asset Labels", and "Accepted Activities" filters are also present. The "Risk Reasons", "Risk Scores", "Network Locations", and "Geo Locations" filters are also visible. A "Search" button is located at the bottom right of the filter section. Below the filters, the results are displayed in a grid. The first column shows "EVENTS" with a count of "14.2M" and "3.3M RECENT". The second column shows a list of users with their names, titles, and risk scores. The third column shows a list of users with their names, dates, and risk scores. The users listed are: Vince Andrade (Chief Council), May Mcconnell (VP Engineering), Javier Ray (09/30/2015 @ 1:39 am), Josephina Moon (09/30/2015 @ 1:19 am), and Rueben Skinner (09/30/2015 @ 1:22 am). Each user has a risk score of 0 and a green triangle icon next to their name.

Filter and Drill Down

The analyst filters the result set further by adding a parameter where the event type equals “Account password was changed.” Threat Hunter responds with a list of all users, within the default time period, who are in the marketing department and had credentials that were used to perform account management, had a failed logon, and then changed the account password.

Near the top of the list we see one user, Angella French, who has been flagged by Exabeam UBA as having unusual account lockout activity.

The analyst clicks on Angella, and Exabeam displays detailed information about her identity and the events associated with this lockout.

We see a very high number of failed logons across thirteen different systems. As account lockouts can be a strong signal of a compromised account and a hacker impersonating a valid internal user, this is worth further investigation. The analyst now has an additional candidate for malware infection and account takeover within the Marketing department, and can respond accordingly.

Works With Any Log or SIEM System

Exabeam UBA and Threat Hunter include pre-built integrations with all leading log management products, including:

- IBM QRadar
- Splunk
- HP ArcSight
- McAfee ESM
- RSA Security Analytics

In addition, Threat Hunter and UBA can integrate with any log system via syslog forwarding. Additional feeds from products such as Data Loss Prevention, endpoint security, cloud security, and others can be easily integrated and used in threat hunting.

The screenshot shows a search results page in Exabeam. The search filters are: Activity Types: Account Management, Failed Logons and Lockouts; Peer Groups: Marketing; Event Types: Account password was changed. The results table lists several users:

User	Reasons	Events	Alerts	Accounts	Assets	Locations	Score
Candida Sellers (Marketing Strategist)	7	242	0	1	14	0	12
Angella French (Web Developer)	11	1.6K	0	0	13	0	7
Deloris Luna (Marketing Strategist)	2	93	0	1	9	0	7
Junior Key (Marketing Strategist)	6	106	0	1	15	0	7
Quiana Melendez (Marketing Coordinator)	4	260	0	0	8	0	7
Candida Sellers (Marketing Strategist)	5	91	0	0	9	0	7

The screenshot shows the user profile for Angella French (Web Developer, Marketing, 1,408 contacts). The main section is titled "Logon Failures and Lockouts" and displays the following statistics:

- Reasons: 11
- Failed Logons: 1.6K
- Updates: 0
- Lockouts: 0
- Assets: 13
- Locations: 0

Below these statistics, there are sections for "Account Changes", "Assets", and "Failure Reasons". The "Assets" section lists sources and destinations. The "Failure Reasons" section lists "BAD USER NAME OR PASSWORD" (1551) and "ACCOUNT PASSWORD EXPIRED" (59). A timeline of events is shown below, including:

- 3:22AM - 7:58AM: 6 x Failed logon. Failed logon due to bad credentials. Failed logon to an asset at:ldap-014 that this user has previously never logged on to. User failed to logon to a top failed logon asset at:ldap-014.
- 3:06AM - 4:23AM: 56 x Failed logon. Abnormal for user to fail logon to this asset dr-k2 48-642. Failed logons had multiple reasons.
- 4:30AM - 4:30AM

On the right side, there is a "Data Insights" panel showing workstations, assets, zones, and countries.

For more information, please contact Exabeam at info@exabeam.com