Threat Hunter Data Sheet

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.

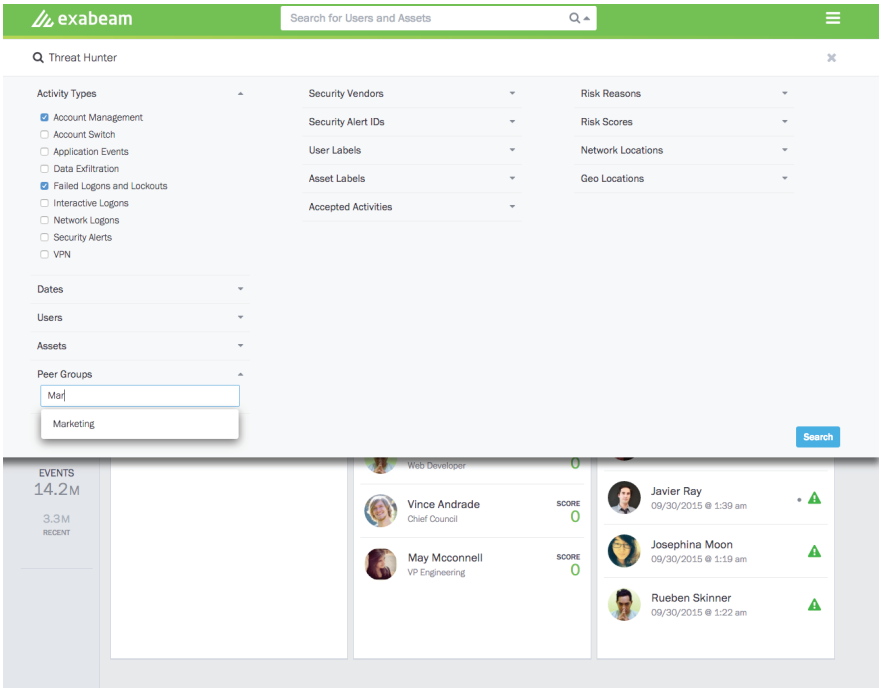
Pull on Threads, Find Hidden Threats

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

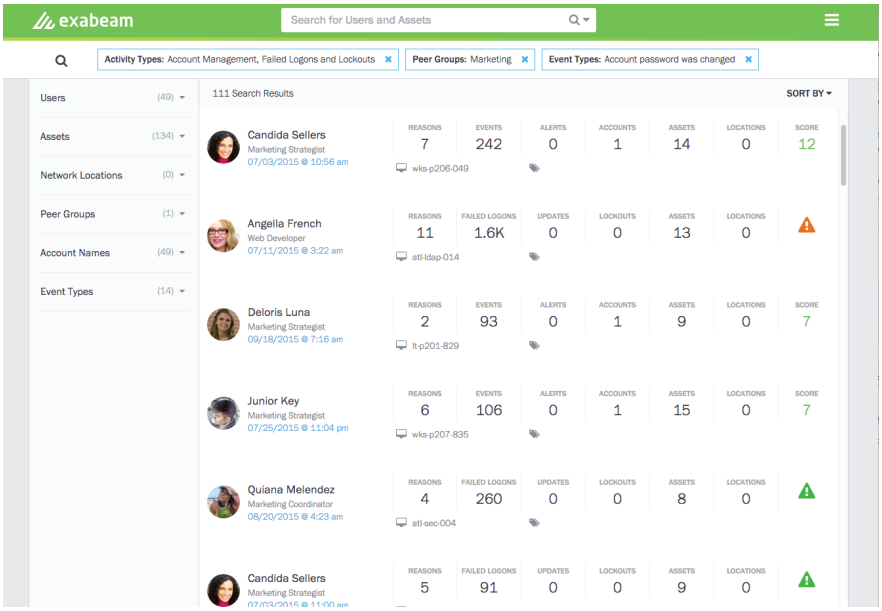
In the example shown here, an analyst uses Threat Hunter to clean up after a malware outbreak in the marketing department that allowed hackers to penetrate the network. The analyst begins by hunting for all sessions where any user in Marketing performed account management (i.e. new account creation or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



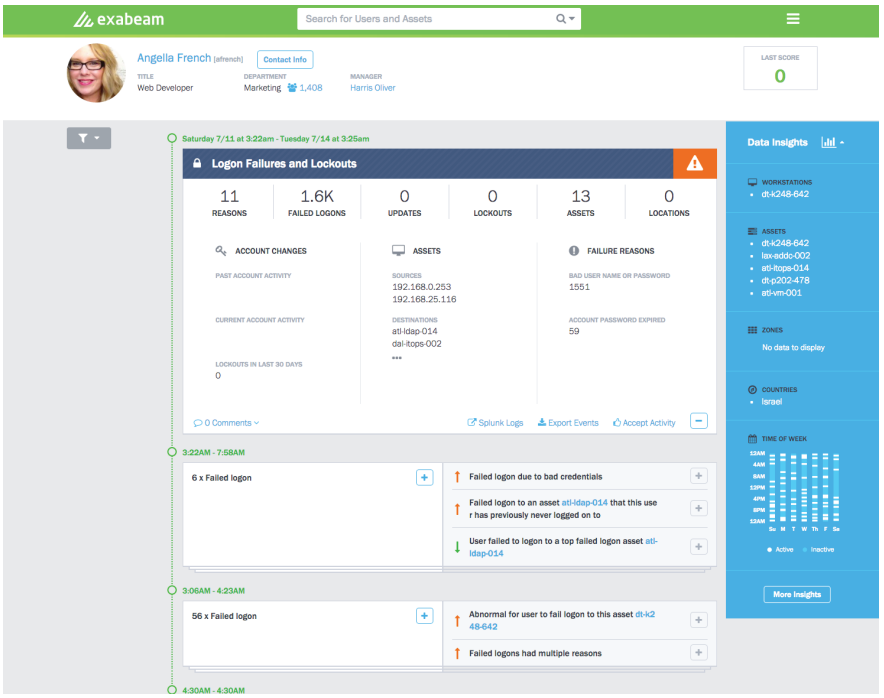
Filter and Drill Down

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.



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.

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