Lab Review

Exabeam User Behavior Analytics

Date: March 2016 **Author:** Tony Palmer, Senior Lab Analyst

Abstract: This ESG Lab review documents hands-on testing of the Exabeam User Behavior Analytics (UBA) platform. Testing focused on how Exabeam's Stateful User Tracking technology enables organizations to detect attacks quickly and easily without agents or taps, and empowers SOC analysts to be more timely and effective in response to threats and attacks.

The Challenges

The threat landscape has grown more dangerous for critical infrastructure organizations over the last several years. Nearly one-third (31%) of organizations surveyed by ESG believe that the threat landscape is much worse today than it was two years ago, while another 36% say that the threat landscape has grown somewhat worse.[1] It is interesting to note that ESG asked this same question in its 2010 research project, and it produced strikingly similar results—68% of respondents said that the threat landscape was worse in 2010 compared with 2008.[2] Clearly, the threat landscape is getting more hazardous on an annual basis with no relief in sight.

These beliefs represent more than just opinion, as many of these same organizations report facing constant cyber-attacks. A majority (68%) of surveyed organizations reported experiencing a security incident over the past two years, ranging from generic attacks brought in by users' systems, targeted attacks, and data breaches due to lost/stolen equipment to insider attacks.[3]

Traditional security systems were designed to attempt to find attacks by searching for known signatures or exploits at a single location during a single point in time, with organizations attempting to consolidate security by leveraging a SIEM solution to collect log, syslog, and netflow data from perimeter security and point solutions. Traditional security information and event management (SIEM) solutions can present thousands of events per hour to IT security staff for manual analysis. This is how many security compromises in the real world evade detection.

What is needed is an approach that can leverage the huge amount of log data generated by all the users, servers, apps, and devices across an organization's IT ecosystem and provide organizations with the context they need to secure and manage operations in the modern IT environment.

[1] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.
[2] Source: ESG Research Report, *Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure*, November 2010.
[3] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.

The Solution: Exabeam User Behavior Analytics

The Exabeam security intelligence platform is designed to provide deep context by combining statistical analysis and baseline profiling with analytics leveraging Exabeam's security domain expertise to create what it calls Stateful User Tracking capabilities. Stateful User Tracking connects individual user events into activity sessions, creating a distinctive session data model that ties together users' activities as they use different account credentials, change devices, and connect from different IP addresses. The resulting detailed timeline tells a security story about each session. This enables Exabeam to quickly and accurately identify anomalous behaviors, enabling accurate threat detection and accelerated response.

ESG Lab Tested

First, ESG Lab examined the installation process, connecting to an Exabeam appliance set to factory configuration, which had been connected to the lab network and powered on. Installation was very straightforward, requiring just four major areas of configuration: Log Management, LDAP import, assets and network, and accounts and groups.

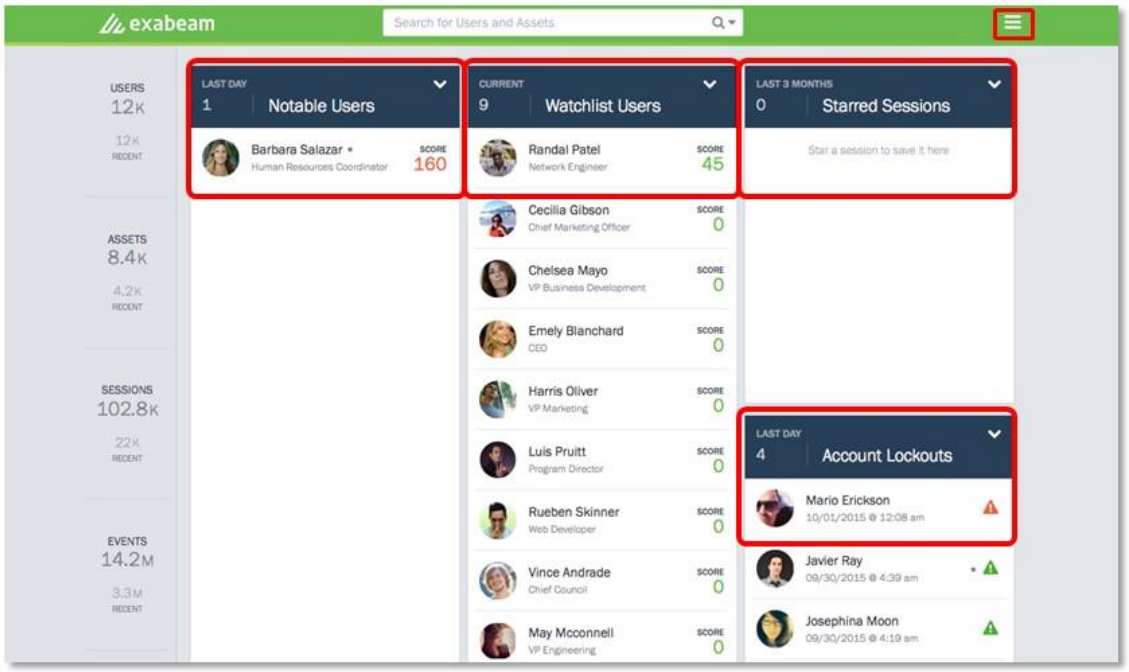
Exabeam attaches to SIEM servers or Log Management Systems (LMS) including HP ArcSight, McAfee ESM, IBM QRadar, RSA Security Analytics, and Splunk. LDAP, and, optionally, syslog, for systems that don't pass their logs to an LMS system, are also supported.

ESG Lab connected Exabeam to a local Splunk server by entering the IP address, username, and password. Once connected, log feed types to be fetched from the Splunk server were selected. Exabeam provides default search queries for each log feed type and allows organizations to edit the queries or create custom queries.

In day to day operation, Exabeam collects logs, parses the raw data into messages, and passes the messages to the Exabeam event builder, which assembles the sessions. As part of the installation process, organizations can select a small set of data to process, to confirm that the queries are collecting the expected data correctly. With all the required information gathered before beginning the installation—IP addresses, login credentials, log feed types, asset lists, etc., the entire process took a total of 10 minutes.

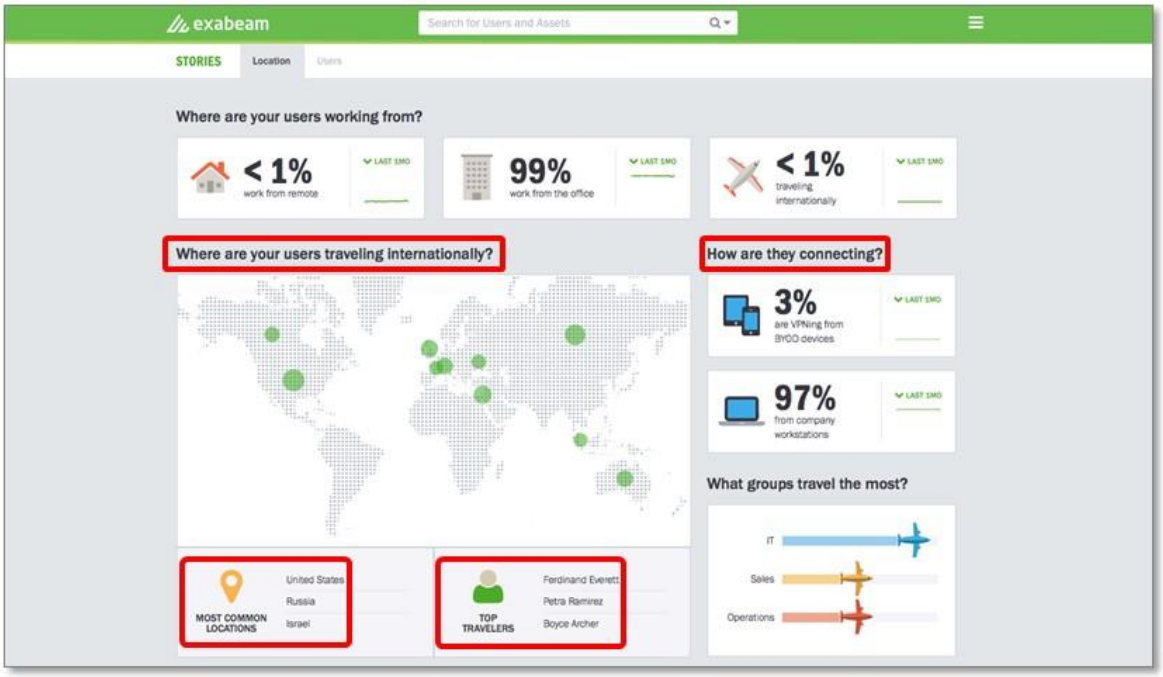
Once complete, ESG Lab switched to a system that had been running and collecting data for some time, as shown in Figure 1. The first screen a security analyst sees when they log in to Exabeam shows summary statistics listed on the left, including users, assets, sessions, and events. Details about users are listed in categories in the center: ***Notable Users*** is where you'll find the users with the highest risk scores. ***Account Lockouts*** lists users who have been locked out of their accounts. ***Watchlist Users*** and ***Starred Sessions*** list users and sessions that have been flagged by an analyst.

FIGURE 1. The Exabeam Dashboard



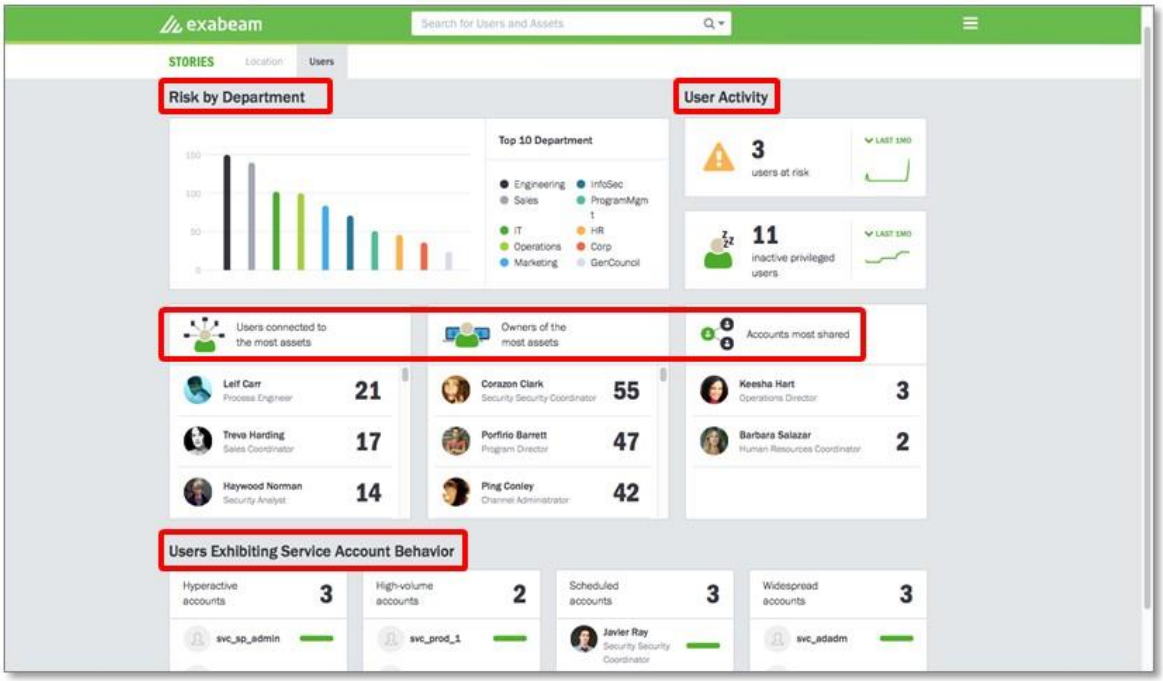
Before examining users and events in detail, ESG Lab clicked on the "hamburger" icon at the top right to examine the high level visualizations of data provided by Exabeam. The ***Location*** view provides location-centric information, including where users are connecting from, where they are traveling and how they're connecting to corporate networks and assets.

FIGURE 2. Exabeam Visualization—Location



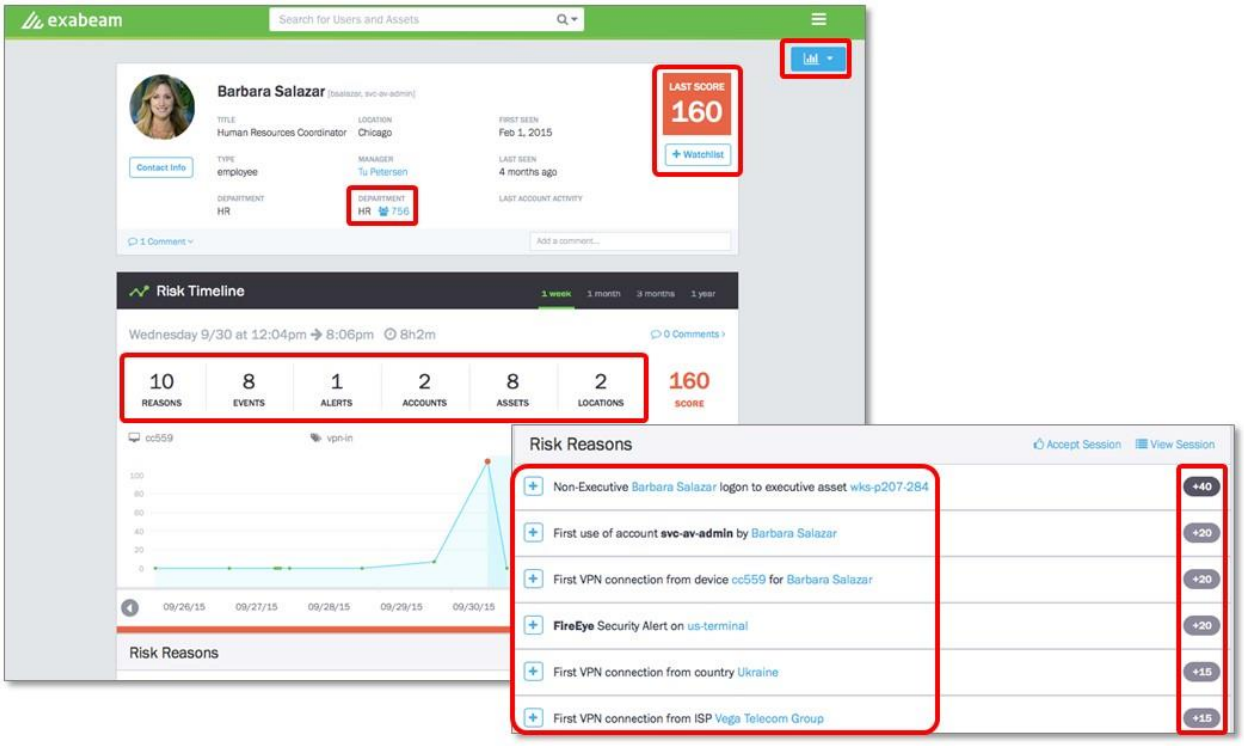
Next, ESG Lab clicked on ***Users*** and examined a user-centric look at the IT ecosystem, which included high level risk analysis of the entire user population, as seen in Figure 3. Activities are broken out into several categories, which provides an information-rich view of the organization, in the context of potentially risky activities.

FIGURE 3. Exabeam Visualization—Users



Next, ESG Lab returned to the main screen and clicked on Barbara Salazar under ***Notable Users,*** as seen in Figure 1. As seen in Figure 4, this user has a risk score of 160 which is the highest in the company. The ***Risk Timeline*** shows that over the course of the last week, her score went from near zero to 160 overnight, indicating a serious anomaly. It's interesting to note that Exabeam carries over risk from session to session, to alert IT to "slow and low" attacks, where the bad actor tries to stay under the radar by spreading their activities out over longer periods of time.

FIGURE 4. Investigating a User

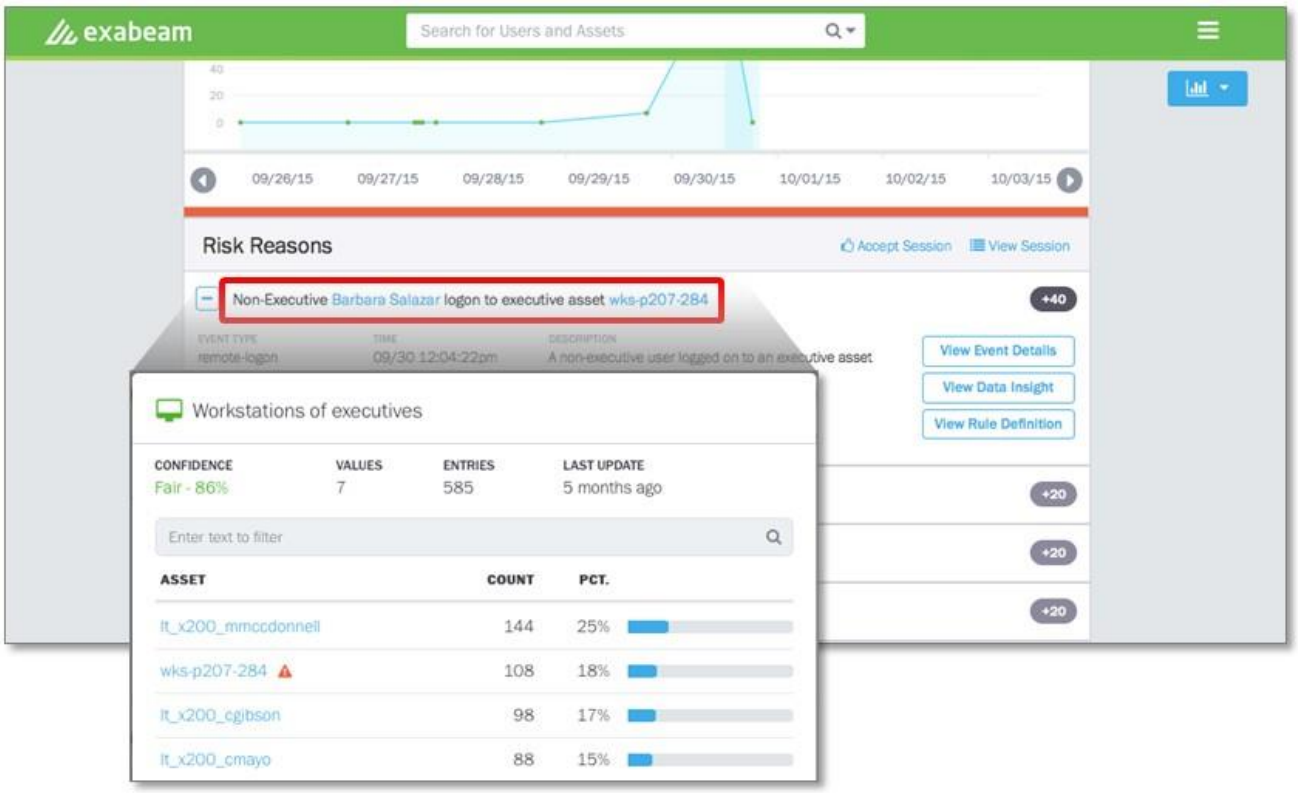


Scrolling down below the timeline revealed the ***Risk Reasons***, which are the specific events that contributed to the score, ranked by contribution to the score, with the riskiest behaviors first. While this user is part of the HR department, they logged into an executive's workstation, used a service admin account for the first time, logged in via VPN from a country they've never visited before, and triggered a FireEye alert.

To compare this user to her peers, ESG Lab clicked on ***Department.*** This showed that this user is indeed an anomaly, with the highest risk score in the HR department by far.

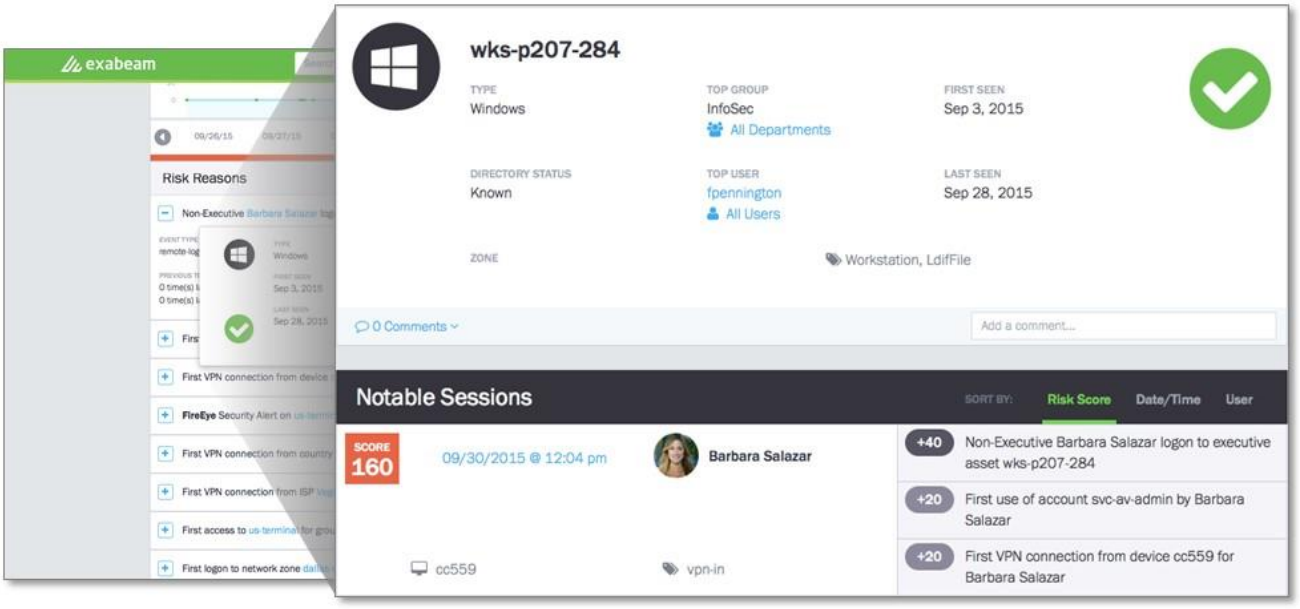
ESG Lab clicked on the plus sign to expand the most significant risk reason, a non-executive logging into an executive asset. From here it was a single click to pivot to the executive workstation list, which shows that this workstation is the only one involved in a risky event.

FIGURE 5. Viewing Executive Workstations



Next, ESG Lab clicked on the asset "wks-p207-284" to get information about it, shown in Figure 6.

FIGURE 6. Asset Details

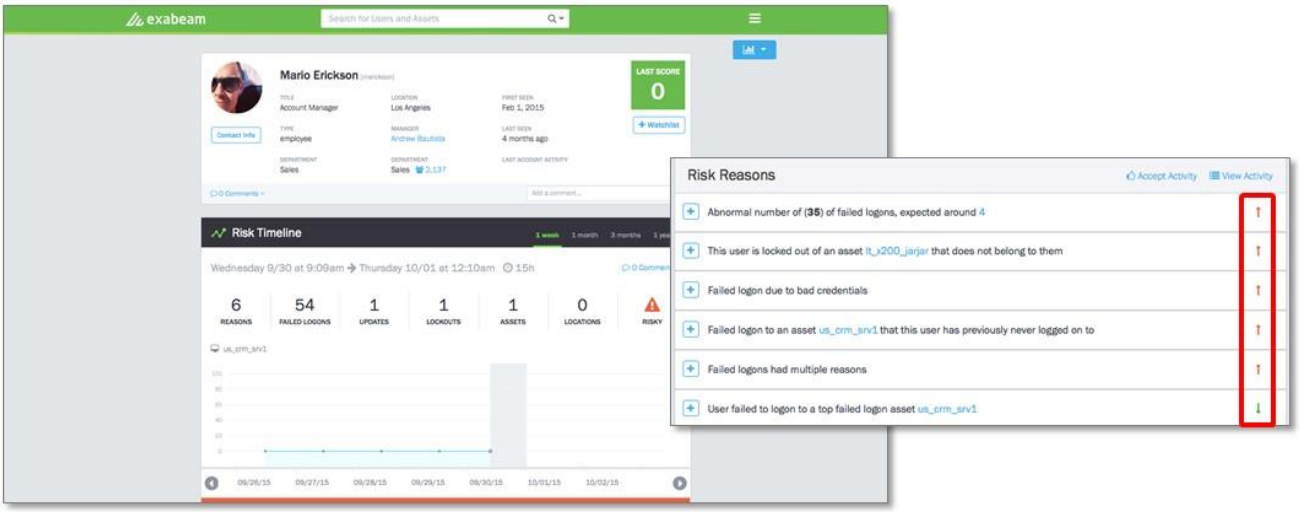


Finally, ESG Lab clicked on the ***Get Details*** button to view more information about the asset. It's interesting to note that the asset view also links back to any incidents that it is involved in, giving analysts wider visibility into potential incidents.

In less than five minutes, ESG Lab was able to identify a user whose identity had been compromised and was being used to attempt to remotely log in to an executive's laptop and acquire data. All of these insights were built from the millions of lines of raw log data collected and analyzed by Exabeam from numerous different feeds.

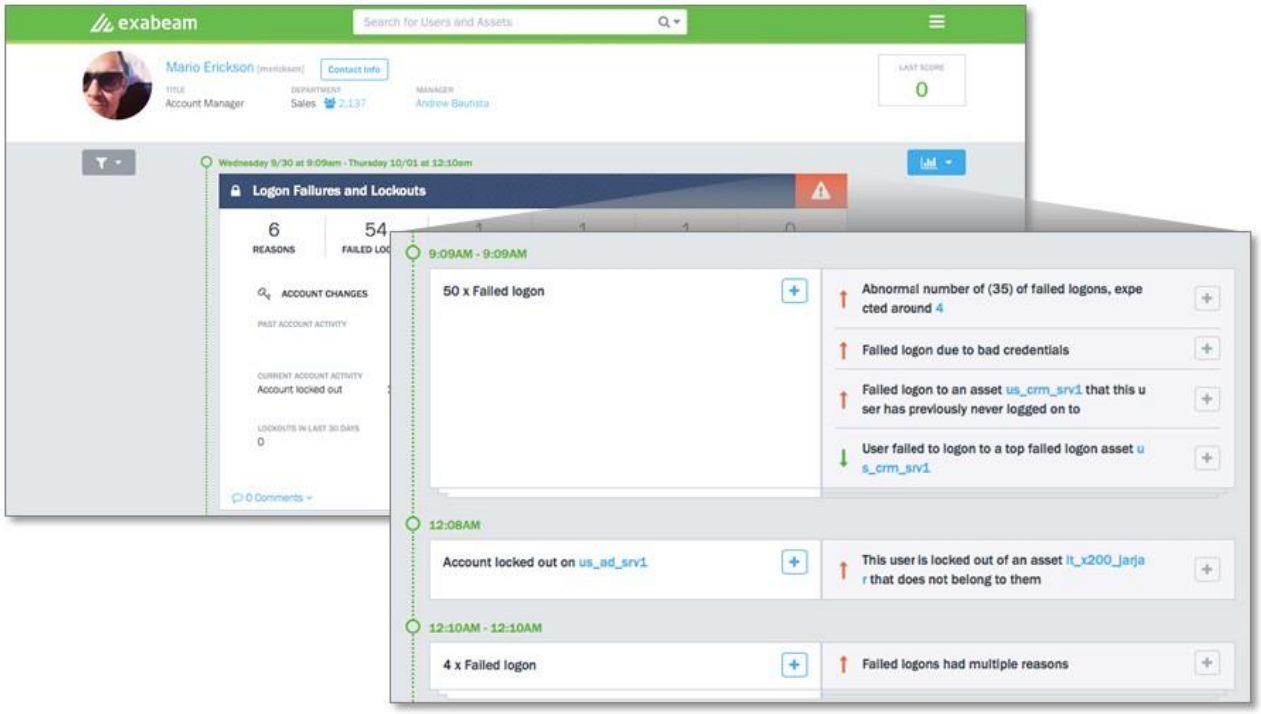
Next, ESG Lab took a look at a user exhibiting excessive account lockout activity. In this case, the risk timeline shows the user at zero risk. As seen in Figure 7, scrolling down to ***Risk Reasons*** shows that arrows rather than risk score are shown on the right hand side. This is because even though the user is exhibiting behaviors that could be potentially risky, their account is locked out and they are not currently accessing any assets.

FIGURE 7. Account Lockout—Risk Timeline



With a click, the warning triangle brought up the lockout event timeline. The timeline shows a listing of all lockout events with detailed explanations of the risk level of each event. Explanations can include the number of logon attempts, whether a user has ever logged on to that asset, whether the asset belongs to them, and whether the asset is one that frequently experiences failed logons, e.g., a server with a quick password reset cycle and strong password security requirements.

FIGURE 8. The Lockout Event Timeline



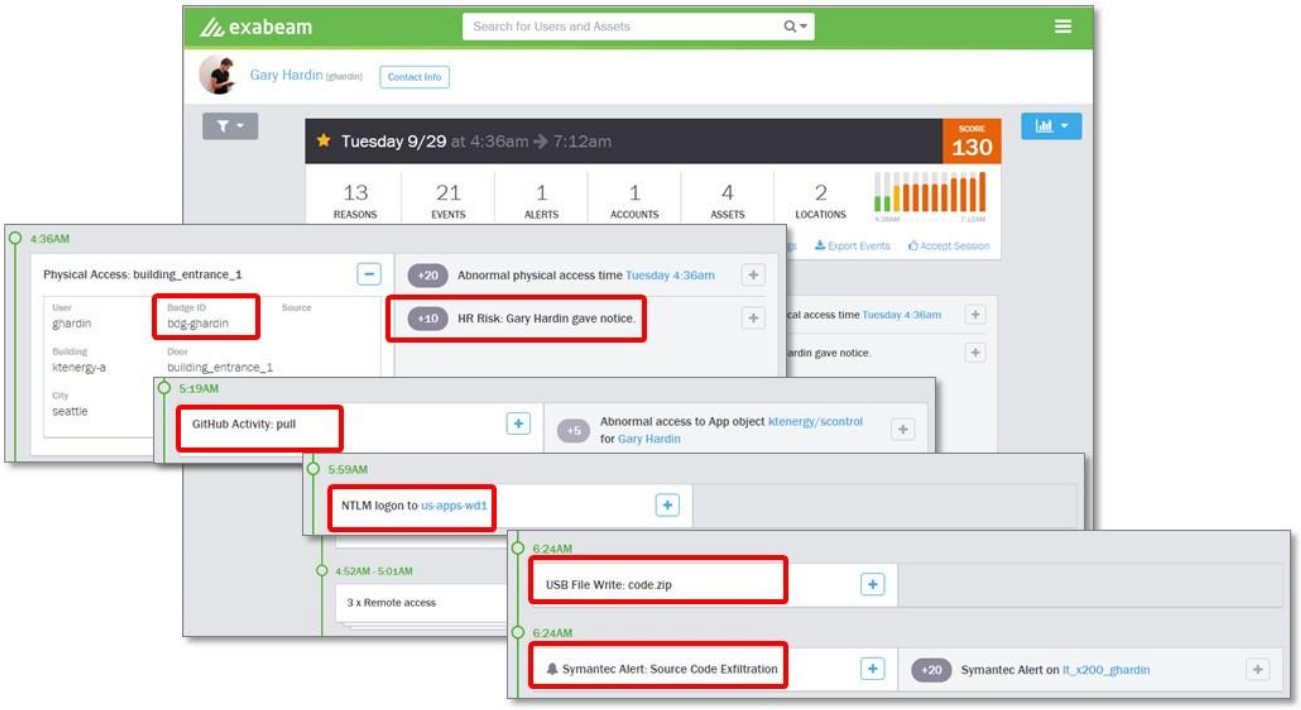
Analysts can expand the timeline to interleave session data with lockout data. This is an important capability, as it can provide additional context when analysts are investigating an incident.

Moving Beyond Access

The Exabeam platform can be extended to support new use cases and new types of data in the field with no code updates. This is accomplished by adding new content in the form of context data such as HR data, CMDB asset data, DLP data, or endpoint data along with data feeds such as new types of logs, network data, proxy data, etc., then adding new logic to describe how to model and assign risk scores. Exabeam's stated goal is to ship the platform with pre-built content for access analytics on log data because access use cases and log data are accessible for any organization and can offer fast time to value while providing organizations with the tools needed to add use cases specific to their business.

ESG Lab looked at a use case for a software company using code checkout data from Github, physical building access data, and HR data in addition to the network and security feeds examined earlier. Figure 9 shows a user with an elevated risk score. Examining the events in the session shows that his physical badge was used to enter the building at an abnormal time, he's recently given notice to HR, has checked out source code from Github and copied it to a USB drive.

FIGURE 9. Expanding Exabeam Beyond Access



While a security alert was generated to indicate a source code exfiltration, Exabeam was able to add context and build a timeline showing exactly where the user was and what they were doing every step of the way.

Threat Hunter

Finally, ESG Lab took a look at Threat Hunter, the newest addition to the Exabeam platform. Threat Hunter enables advanced querying of the security data processed within the Exabeam UBA platform. With Threat Hunter, security professionals can search across multiple dimensions of user activity to find sessions with unusual behaviors to proactively detect and respond to attacks already within their networks.

FIGURE 10. Threat Hunter—Searching for Multiple Risky Behaviors

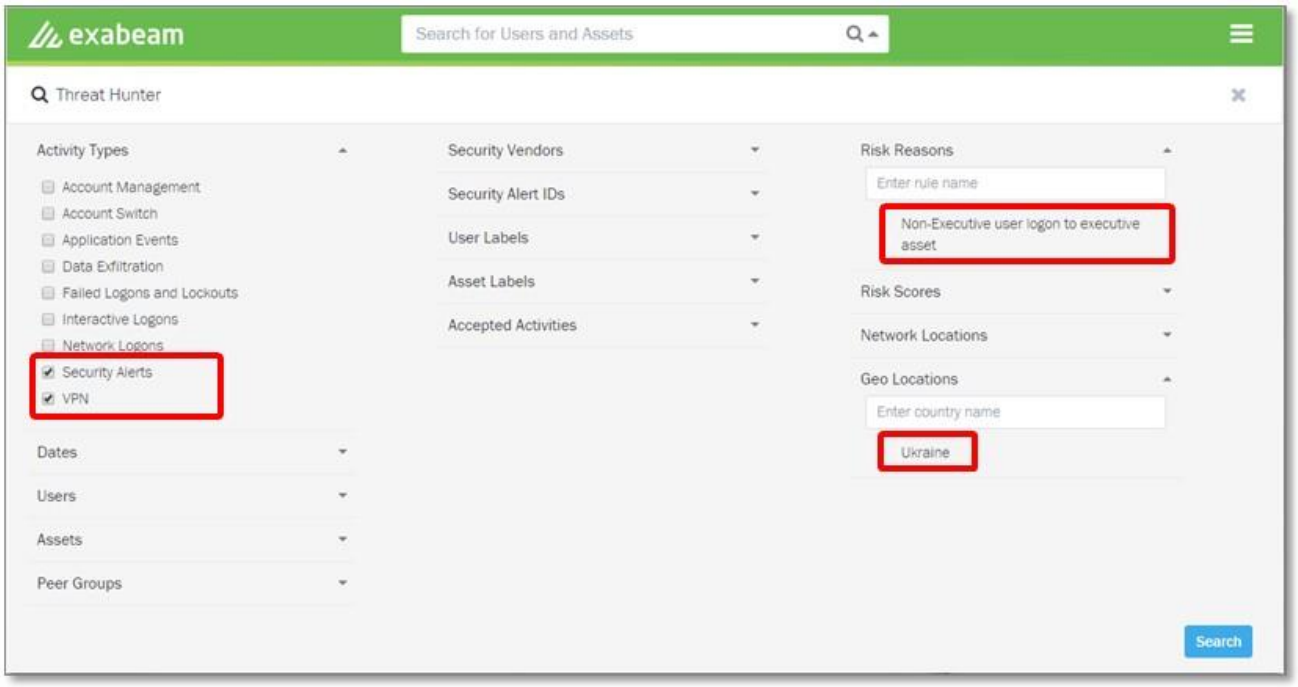
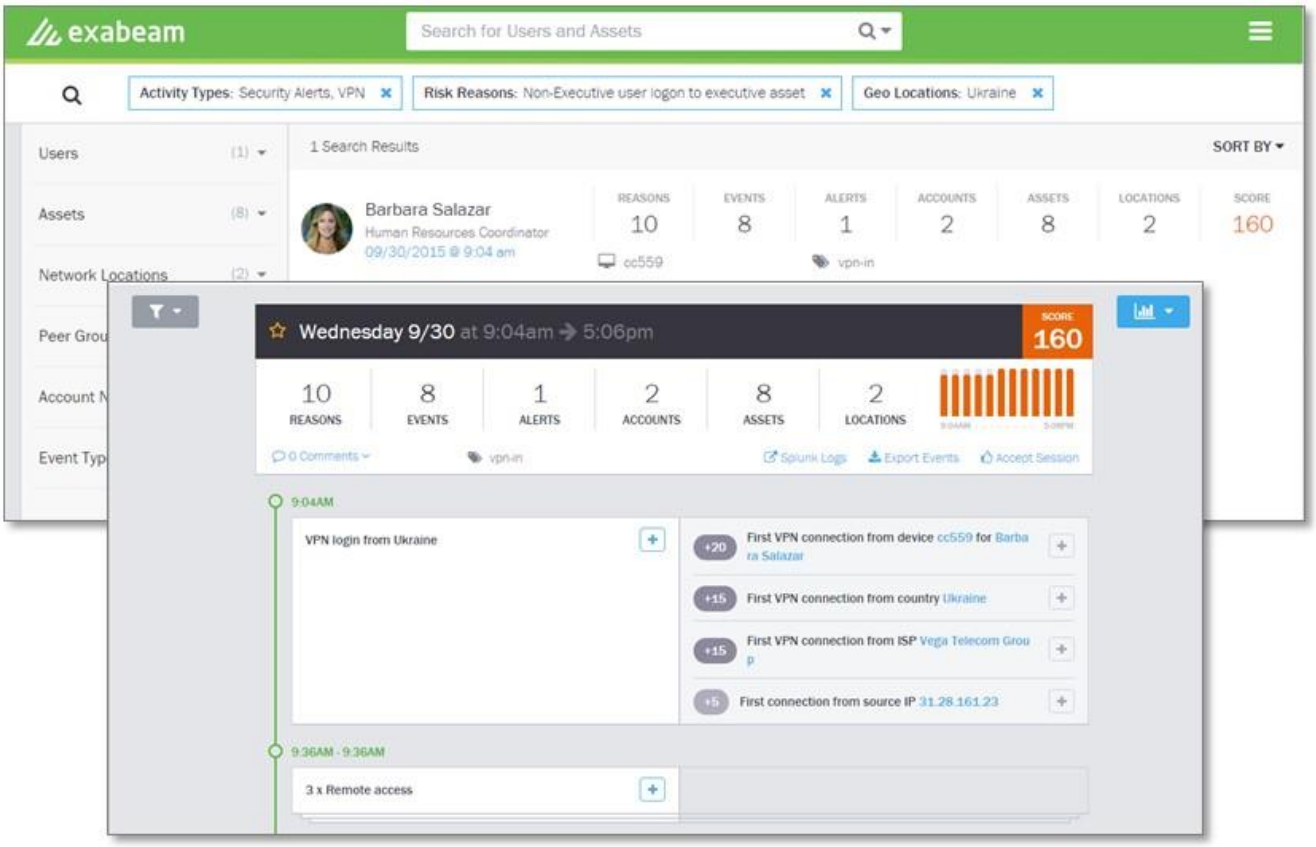


Figure 10 shows ESG Lab searching for users with multiple cross-domain risky behaviors. In this case, the criteria included activity that triggered some kind of security alert, occurring over a VPN, involving a non-executive accessing an executive asset, and originating in the Ukraine. Each criterion is unrelated and reported in different system logs with no easy way to connect them in a search.

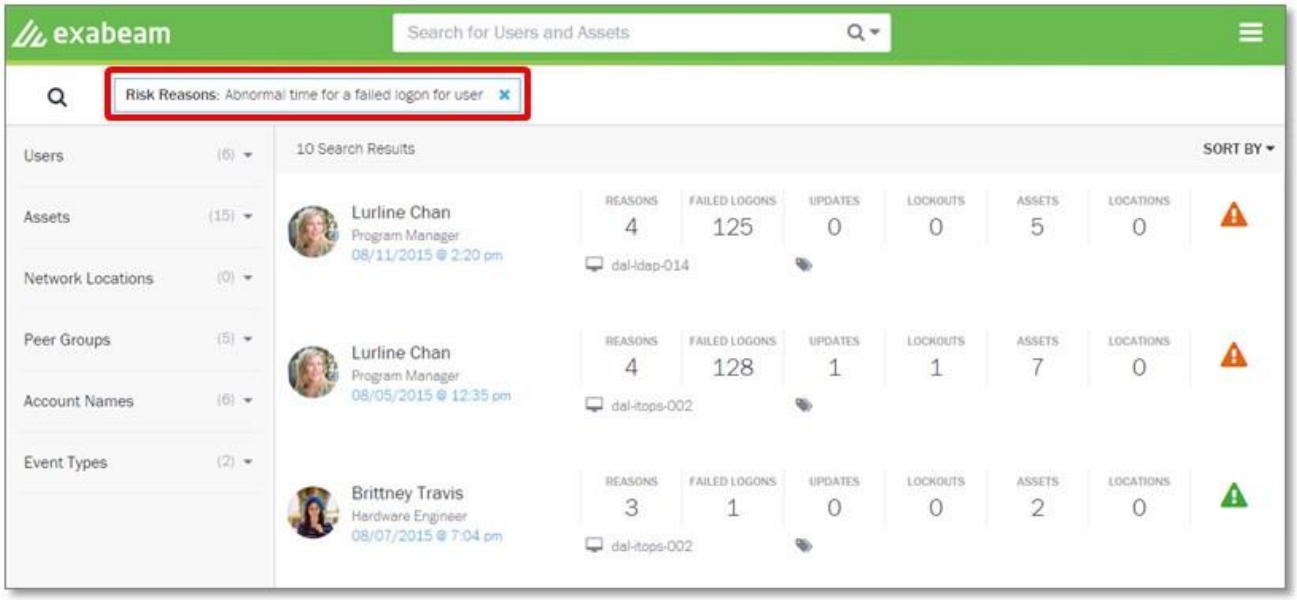
As seen in Figure 11, the search returned one user whose behavior met all those criteria with all the sessions where these criteria were met presented in one place.

FIGURE 11. Threat Hunter—Results



ESG Lab looked at one more example of how an analyst would use Threat Hunter to find a specific behavior (failed logins) within a specific context (at a time that is unusual for a specific user). The results are shown in Figure 12.

FIGURE 12. Threat Hunter—Searching for Contextual Significance



Why This Matters

Information security and business intelligence and data analytics initiatives were the top two most-cited IT priorities in a recent ESG research survey[4] while organizations report that the threat landscape continues to grow more dangerous.[5] The traditional approach is to attempt to consolidate multiple point solutions and system logs using a SIEM or log management solution. Zero-day threats and insider security compromises can evade detection with the traditional SIEM approach, which can present thousands of events per hour—with little to no context—to a security analyst for manual analysis.

What is needed is a solution that can harness the torrent of data collected from security solutions, as well as from servers, workstations, and network devices, and apply statistical analysis to provide organizations with the cross-correlated context they need to secure and manage operations in the modern IT ecosystem.

ESG confirmed the ability of Exabeam User Behavior Analytics to deliver stateful, context-aware visibility and enable analysts to hunt for threats, even as bad actors use different credentials, change locations, and connect from different devices. This enables a security organization to discover, investigate, and manage responses without having to spend inordinate amounts of time and effort sifting through thousands of alerts and log entries.

The Bigger Truth

Security breaches are becoming more common every year. All computing devices in the corporate infrastructure, from smartphones and tablets to laptops, desktops, and application servers, are susceptible. Attacks affect organizations of any size indiscriminately, and the consequences can be devastating to operations, company reputations, and bank accounts. The costs stemming from successful attacks may include not just resuming operations and addressing security gaps, but legal liability and regulatory fines that can be a tremendous burden as well.

This may be why information security has remained at the top of the IT priority list for the last four years, according to ESG research. When asked to consider their organizations' most important IT priorities for 2016, cybersecurity initiatives were the most-often cited, identified by 37% of respondents.[6]

Exabeam User Behavior Analytics is designed to provide context for server and security device log data by combining data science technologies—statistical analysis and baseline profiling—with security analytics to create Stateful User Tracking, which connects individual user events together into activity sessions, creating a session data model that follows users' activities even as they use different account credentials, change devices, and connect from different locations. The resulting detailed timeline enables Exabeam to quickly and accurately identify anomalous behaviors, enabling accurate threat detection and accelerated response.

ESG lab confirmed that the Exabeam platform can be extended to support new use cases and new types of data by simply adding additional content feeds and the logic to model and assign risk scores. The Exabeam platform can show value quickly with pre-built content for access analytics on log data but the solution design is such that data and use cases beyond access analytics are easily added by organizations without having to go back to Exabeam for code updates.

In the opinion of ESG Lab, Exabeam's unique capabilities in User Behavior Analytics provide the real-time and historical analytics—with correlated context—needed for organizations to confidently detect anomalous activity and identify advanced persistent threats. The user interface was straightforward and ESG Lab was able to rapidly identify important

[4] Source: ESG Research Report, *2016 IT Spending Intentions Survey,* to be published.
[5] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.
[6] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, to be published.

events and compromised users, leveraging insight into user behavior across the entire IT spectrum. The ability to search for specific behaviors with precise context with Threat Hunter enables organizations to identify advanced persistent threats as they shift and change behaviors to evade detection from traditional security solutions.

ESG Lab validated that Exabeam User Behavior Analytics Stateful User Tracking technology was able to detect attacks without agents or taps, and can give security analysts the context they need to respond to threats and attacks faster and more effectively. The user interface is polished and uncomplicated, and presents its analyses in an understandable format. Organizations looking to up their game in the fight against advanced persistent threats using the data they are already collecting would do well to take a very close look at Exabeam User Behavior Analytics.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.