

Exabeam Advanced Analytics User Guide

Exabeam Security Operations Platform - Cloud-Delivered
Release Only

July 17, 2024

Exabeam

1051 E. Hillsdale Blvd, 4th Floor
Foster City, CA 94404

650.209.8599

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com

Disclaimer: Ensure that you are viewing the most up-to-date version
of this guide by visiting the Exabeam Documentation Portal.

Copyright

All content in this document, including text, graphics, logos, icons, images, and video clips, is the exclusive property of Exabeam or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this document is the exclusive property of Exabeam and is also protected by U.S. and international copyright laws. The content in this document may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this document is strictly prohibited.

Copyright ©2024 Exabeam, Inc. All Rights Reserved.

Trademarks

Exabeam, the Exabeam logo, Threat Hunter, Smarter SIEM, Smart Timelines and Security Management Platform are service marks, trademarks or registered marks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. The marks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

Patents

Exabeam owns, and reserves all rights for, patents for Exabeam products and services, which may be protected under registered patents as well as patents pending.

Other Policies

For information regarding Exabeam's treatment of personally identifiable information, please review Exabeam's current privacy policy at www.exabeam.com/privacy.

Table of Contents

What is Exabeam?	5
Exabeam's Role	5
Get to Know Exabeam Terminology	5
Get to Know Exabeam Use Cases	6
How Exabeam Works	7
Build a Baseline for Each User and Asset Using Training	8
Confidence in Assessing Events	9
Role-Based Access Control	9
Mask Data in the Advanced Analytics UI	10
Data Masking Fields	10
Obfuscate PII When Exporting Logs	10
Mask Data in Search & Threat Hunter Functionality	10
Unmask Data with Clear-Text Permissions	10
Welcome to the Advanced Analytics Homepage	11
High-Level Counters on the Advanced Analytics Homepage	12
About the Notable Users List	13
Watchlists	13
Asset Watchlists	14
Out-of-the-Box Watchlists	14
Customizable Watchlists	14
Configure Role-based Access Control for Watchlists	15
Account Lockouts List on the Advanced Analytics Homepage	15
Navigate to Other Pages, Sign Out, or Change Password from the Advanced Analytics Homepage	16
Bookmark Sessions	16
Get to Know a User Profile	17
1 General Information	18
2 Data Insights	18
3 Active Incident(s)	19
4 User Risk Trend	19
5 Risk Reasons	20
Get to Know the User Timeline Page	23
Examine Events by Category with the User Session Summary	25
About the User Session Timeline	27
Filter User Timelines	28
View Activity Summary on a Specific Day	28
Get to Know the Daily Timeline	29
View and Understand an Account Lockout Sequence	30
Get to Know the Account Lockout Sequence Timeline	31
Accepting a Session or Sequence	32
Entity Analytics	37
Get Started with the Asset Page	38
About the Asset Directory Information Page	38
Get to Know the Asset Risk Trend Page	39
Get to Know the Asset Risk Reasons Page	40

About the Asset Timeline Page	41
Get to Know the Asset Session Summary Page	43
Get to Know the Asset Session Timeline	44
Filter Asset Timelines	45
Accept a Session, Export Events, Create Incidents, and Load Search Parameters From the Asset Timeline	45
Get Started With the Threat Hunter Page	46
Navigate to the Threat Hunter Page	46
Search in the Threat Hunter Page	46
Threat Hunter Support for Entity Analytics	46
Save Search Criteria	47
Managing Saved Searches	47
View Pre-Configured Searches Using the Exabeam Search Library	49
Search for Assets Associated With an IP Address	51
Search Histograms Using the Data Insights Page	52
Types of Histograms	52
Table Histogram	52
Time of Week	53
Cluster Histogram	53
Map Histogram	54
About the Session Data Insights Panel and Page	55
Navigate to the Session Data Insights Page via the More Insights Button	55
Monitor Exabeam Processes Using the System Health Page	57
Health Check	57
Configure Alerts for Worker Node Lag	58
Disaster Recovery Health Alerts	58
Alerts for Storage Use	58
System Optimization	58
Critical Alerts, Warnings, and Error Messages	59
Contact Technical Support	60
Licensing Options	60

What is Exabeam?

What is Exabeam?

The Exabeam Security Management Platform provides end-to-end detection, User Event Behavioral Analytics, and SOAR.

Exabeam builds a layer of intelligence from the logs collected in an environment either through a SIEM platform or directly ingested via Syslog. Through this integration, an analyst can see the events within the attack chain to more effectively and quickly remediate the risk.

If you are a security response personnel or analyst, get started with Exabeam and learn how you can use Exabeam to investigate suspicious events.

You will understand:

- How Exabeam works
- Exabeam Use Cases
- The pages of the Exabeam interface

For Advanced Analytics, the latest versions of the following browsers are supported:

- Chrome
- Internet Explorer
- Firefox
- Safari

Please consult the *Exabeam Administration Guide* for further information on installation and operation.

Exabeam's Role

Get to Know Exabeam Terminology

The following terms are frequently used in the Exabeam UI.

- An **analyst** is the operator of Exabeam.
- An **incident** is an unusual occurrence that may indicate a threat to an organization's security and which a security analyst is investigating.
- **Users** are people that Exabeam is monitoring in an organization. These users can be employees, contractors, partners, service accounts, and so on.
- **Events** are the constituents of a session, sequence, or feed. For example, logging onto a VPN is an event, and logging onto a computer is an event. Although events constitute a logical session, it is also true that Exabeam links each event to a user or asset.
- **Event details** contribute to the baseline and are monitored for anomalies during regular operation. For example, user activities can result in a user being marked as notable or an asset becoming compromised.

- **Assets** are computer devices such as servers, workstations, and printers.
- **User Session** represents all the events that Exabeam attributes to an individual user in a timeframe (after 5 hours of user inactivity or 24 hours of maximum duration, Exabeam closes the user session). Typically, user sessions are one day of activity, but there can be multiple user sessions in a day. Exabeam collects event logs that relate to the user's assets and activities and defines these as a logical user session. A user session is a logical container that Exabeam creates and, therefore, is not a session the way an analyst may typically think of a session.
- **Asset Session** represents all the events that Exabeam attributes to an individual asset in a timeframe. Asset Sessions are similar to User Sessions in that they are a logical container of event logs related to the asset's activities, however an Asset Session lasts for one 24-hour period, from midnight UTC to midnight UTC.
- **Daily Feeds** are similar to User Sessions in that they are a logical container of event logs. However, unlike user sessions they represent a single day. They are high-volume feeds that are processed outside of a user session but their risk scores will be added to a user's session score. Examples of daily feeds are proxy logs, endpoint logs, and DHCP logs.
- **Lockout Sequence** refers to all of the account lockout related events that Exabeam attributes to an individual user in a timeframe. A sequence begins with an account change, a failed logon event, or a lockout event and all additional account lockout related events are added to the sequence until a period of inactivity has been reached. The sequence is analyzed and marked as risky if the activities in the sequence are identified as anomalous and cross a risk threshold.
- A **Queue** is a group of users assigned to incidents. This is based on how your organization's resources are arranged, such as analyst groups designated in Tier1, Tier2, etc. Queues contain Incidents and analysts are Queue Members who are notified when new Incidents are added to the Queue.

Get to Know Exabeam Use Cases

To make the best use of Exabeam, it's helpful to understand the out-of-the-box use cases we support.

External Compromise: Attackers gain entry into an environment by compromising the credentials of valid users. They move laterally within the environment looking for sensitive information. Compromised credentials present a significant threat to organizations due to the difficulty of differentiating between normal and risky behavior. Using machine learning and data analysis, Exabeam assembles all activities from a variety of log sources into an easy-to-understand timeline for each user within an organization and assigns a risk score to their behavior. An example includes an attacker who uses a valid credential to create a new account and then uses that account to access many assets, contacts a domain that is generated by a Domain Generation Algorithm (DGA) and ex-filtrates critical database records to a C&C server.

Insider Threat: Exabeam helps in identifying rogue insiders within the environment. It's easy for these attacks to go undetected because insiders in the environment know where the sensitive data is and they will not trigger the same types of anomalies as an external attacker taking control of an environment using stolen credentials. Exabeam also incorporates log sources from Cloud Applications into its analytics engine and detects insider threats within the data center and on the cloud. Customers want to analyze the physical presence of their employees along with their IT activities. Exabeam will stitch physical presence into user sessions and identify anomalies across

them. For example, points would be added to a session the first time a user accesses a building. This allows for cross-referencing of IT behaviors with physical behaviors for a higher level of visibility. Other scenarios include, data access outside of the job scope or a privileged insider accessing compensation records of an employee.

Data Loss Prevention (DLP): DLP solutions are widely-deployed as a means of finding sensitive data and detecting the movement of that data to the outside world. Exabeam brings unique UBA capabilities to DLP by ingesting and analyzing non-authentication events and identifying anomalous behavior around data exfiltration. Many corporate PCs contain endpoint security software that logs the use of thumb drives in USB ports. Exabeam can use this log data to identify risky operations such as the first time a user saves files to a USB drive or when a user is copying files that are outside of that user's normal behavior. Other scenarios would be: an employee taking high net-worth client information when they leave; a terminated employee badging into a building; an employee accessing a CEO mailbox.

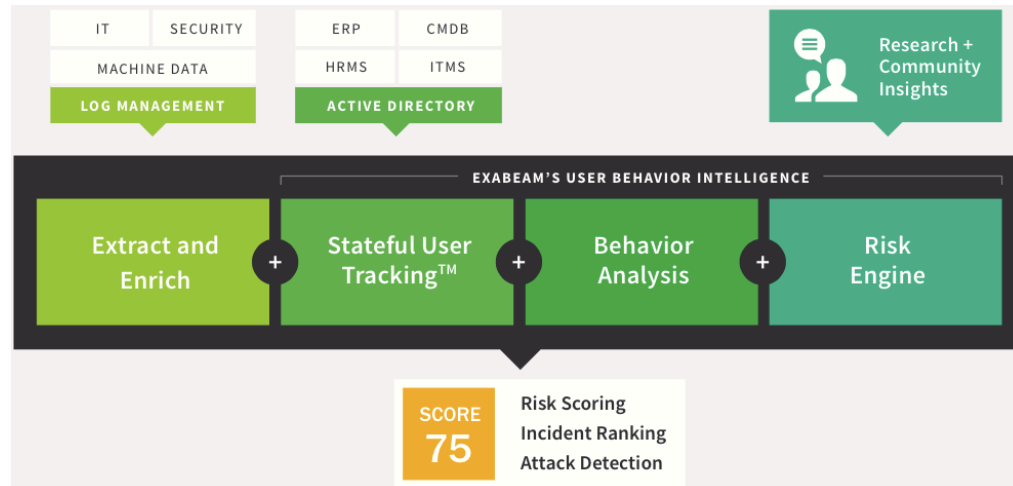
Alert Prioritization: As IT environments grow in scale and complexity, Security Operations teams often struggle to keep up with the resulting increase of monitoring alerts. Since alerts are a critical early warning system, finding a way to reduce false positives and prioritize alerts becomes a critical success factor. Exabeam's machine learning technology addresses rapidly growing data volumes by automatically identifying anything that is amiss without the time and labor required to configure and maintain alert rules or thresholds. We take alerts from other security vendors, such as FireEye or Palo Alto Networks and Exabeam's Stateful User Tracking associates an alert from any of the third party products into a user session and is able to present the activities of the user before and after the alert.

Another example would be alerts related to an organization's Account Lockout policy. While they serve an important security purpose, they also place a strain on already short-staffed IT teams. By analyzing the events around account lockouts and presenting the information in a timeline, Exabeam accelerates efficiency and reduces the resources consumed by these investigations.

How Exabeam Works

Exabeam assigns a risk score to users and their IT environment sessions by combining user behavior intelligence and fact-based information. In a single session, Exabeam may report risk related to abnormal access to an asset, a security alert received from a 3rd party system, a new user being created from a new network location, and changes to the access privilege of the user. Asset criticality and threat intelligence information can also be factored into the risk analysis.

The following major components work together to produce a risk score:



- **Extract and Enrich** – Exabeam draws from the organization’s log management system and enriches the logs with identity, asset, and network information. For example, Exabeam links to Microsoft Active Directory to discover the department and roles of the users in the organization. Exabeam also uses machine learning to categorize users and assets to further enrich the contextual information. For example, Exabeam can detect certain users as service accounts based on their behavior.
- **Stateful User Tracking** – While reading logs, Exabeam follows user sessions by tracking the state of the users’ presence within the IT environment. Sessions represent the activities performed by the users from the moment they enter the environment until they log off or remain idle for a period.
- **Behavior Analysis** – Behavior Analysis is where Exabeam detects anomalies. Exabeam continuously maintains a baseline of normal behaviors for each user in the environment and each group, e.g. Department. New activities are then compared to the baseline and reported as anomalies if they are deemed inconsistent.
- **Risk Engine** – The Risk Engine combines data science and security expertise to quantify the risk of the anomalies. It also adds risk according to fact-based information, such as privilege levels, security alerts or threat intelligence and produces a risk score.

Build a Baseline for Each User and Asset Using Training

To build a baseline, Exabeam extensively profiles the people, asset usage, and sessions (Exabeam’s word for profiling or base-lining is training). In a typical deployment, Exabeam starts by examining 90 days of an organization’s logs. After the initial baseline analysis is done, Exabeam starts scoring the sessions. Note the following:

- In most cases during initial deployment, Exabeam uses the data from the previous 30 days as if it were scoring during that time. The purpose is to analyze a month of data and paint a meaningful picture for the analyst without waiting 30 days to create a picture.
- Training does not stop. Exabeam continuously adjusts the profiles as the users and the IT environment changes.

When Exabeam categorizes behavior as anomalous, it does so based on rules and models that it applies to users, assets, peer groups, and the organization as a whole. In the case of an employee

who exhibits suspicious behavior or a security device that posts an alert, Exabeam will display events that are not normal for that user or asset. However we don't display only abnormal events. We also display normal events so that the Analyst can have the full picture and can understand what led to the anomalous event. For example, behind the suspicious behavior could be VPN requests from countries never before seen or remote logons to assets or network zones that never have been accessed.

Confidence in Assessing Events

Before evaluating a specific event, Exabeam must have confidence in the basis of its evaluation of that event. In Exabeam's case, this basis means enough quantity and consistency of data for each user and their attributes. If Exabeam lacks enough data for a specific type of event, it does not evaluate the rule for that event even as it evaluates other rules during the session. However, note that the confidence factor is not taken into account for the first time a rule is triggered.

The confidence in each user's profile is built during the initial baseline development as well as on an ongoing basis as new events arrive. In contrast, some behaviors might require Exabeam to take more time to establish confidence. For example, if a user's job involves irregular foreign travel, establishing confidence in a profile of VPN sessions from foreign countries takes longer.

An example of profiling that might never lead to confidence in one area of behavior is a behavior that changes every day. The only predictable thing about this behavior is that it changes daily. For example, if an ISP starts a policy of assigning a different IP address every day, Exabeam cannot establish a histogram that applies to that behavior. An organization can accept this because if the new IP address were part of an attack, many other rules would be triggered. Put another way, a new IP address every day does not automatically indicate a threat. The total score for all anomalies during a session indicates attacks.

Analysts also have an option for choosing certain behaviors to accept, as the Sessions chapter describes. After sufficient examination of a session, an analyst can manually add the session's events to a user's profile so that those events stop triggering the applicable rules.

Role-Based Access Control

Access to configuration, data views, actions, and analysis in Advanced Analytics is restricted based on user-assigned roles. Roles are functional groups you configure and adjust based on your organization's task structure.

For example, you may have two tiers of security analysts along with a group of auditors who all need access to Advanced Analytics. The three groups do not have equal level of privileges to view, run tasks, or adjust system configurations. You may have roles named SA1, SA2, and Auditor. While users in the SA1 and SA2 roles are allowed to view notable users, those in the Auditor role may not. A SA1 user may make a copy of URLs from a suspicious session and sends it them to a user in SA2 who can see the information in clear text. Another SA1 user will not be able to see that same information if the role excludes viewing data that is masked due to privacy policies.

Users are assigned a role in their profile. More than one role can be assigned, but be aware of tasks with conflicting privileges. In the case of conflicting privileges, we combine the privileges and give all explicitly allowed permissions between them.

What is Exabeam?

When a user tries to access a view, menu, or execute a task outside the designated role, an error message is presented advising the user does not have sufficient privileges.

For information on how to configure access restrictions, see [Universal Role-Based Access](#) in the Advanced Analytics Administration Guide.

Mask Data in the Advanced Analytics UI

Exabeam supports Data Masking to meet the data privacy directives of enterprise organizations.

It ensures that personal data cannot be read, copied, modified, or removed without authorization during processing or use. With data masking enabled the only SOC analysts that will be able to see clear text PII will be those administrators that are assigned to the Data Privacy Officer role. All other administrators will see disguised information:

Data Masking can be enabled via a configurable setting. It is turned off by default. Please see the *Administration Guide* for more information on how to enable the feature.

Data Masking Fields

The data masking fields are individually configurable. For example, the administrator is able to decide to only mask username, photo, and contact information. In such a case, all the other fields are available in an unmasked form for any analyst. The user name, photo, and contact information can only be seen in a clear text form for those users whose roles have the "View clear text PII data" permission.

See the section *Configure Data Masking Fields* in the *Administration Guide* for more details.

Obfuscate PII When Exporting Logs

When exporting logs from the session timeline or Threat Hunter, all fields that are configured to be obfuscated are shown in a masked form when the logs are downloaded.

Mask Data in Search & Threat Hunter Functionality

The Search & Threat Hunter functionality work with data masking enabled. An analyst is able to provide a masked value and find matching results. For example, if a User Name is masked as **DondU8** then any search for **DondU8** will return results for that same user, with all configured fields masked.

Unmask Data with Clear-Text Permissions

The session URLs of masked users can be sent to administrators with clear-text permissions. For example, a Tier 1 Analyst (a data masked role) views a suspicious user, then copies the URL of the specific session for that user and sends it to a Data Privacy Officer (a clear-text role). When opening the URL, the Data Privacy Officer is able to view that user's information in clear-text.

Welcome to the Advanced Analytics Homepage

The home page alerts the analysts to items that require investigation.

Some panels are unique to products you've purchased and installed. **My Incidents** and **Incidents in My Queue** panels as well as **Folder** icon in the **Notable Users** panel are only available when Case Management is deployed. Notable Assets is available when Entity Analytics is deployed.

The screenshot shows the Exabeam Advanced Analytics homepage. At the top, there is a green navigation bar with the Exabeam logo and the word 'ANALYTICS'. To the right of the logo are navigation links: HOME, INCIDENTS, METRICS, and PLAYBOOKS. There are also icons for search, a plus sign, a bell, and a hamburger menu.

Below the navigation bar is a summary section with five panels, each showing a metric and its total:

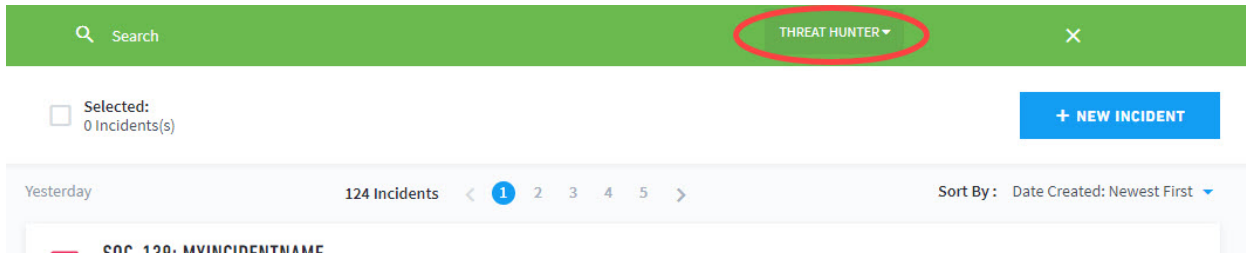
- USERS:** 22 (7.9K TOTAL)
- ASSETS:** 1.1K (1.7K TOTAL)
- SESSIONS:** 772 (827 TOTAL)
- EVENTS:** 85K (339.2K TOTAL)
- ANOMALIES:** 1.8K (2.1K TOTAL)

The main content area is divided into several panels:

- MY INCIDENTS (11):** A list of incidents with details like 'Incident from Exabeam Advanced Analyt...', 'NOTABLE USER: BARBARA SALAZAR', 'SYMANTEC MALWARE ALERT: UNRECOG...', 'Barbara Salazar Phishing Incident', and 'NOTABLE USER: GARY HARDIN'. Each incident has a severity level (MED, HIGH) and a status (NEW).
- INCIDENTS IN MY QUEUES (19):** A list of incidents in queues, including 'Incident from Exabeam A...', 'NOTABLE ASSET: SKY-WW...', 'NOTABLE ASSET: SKY-EEF...', 'NOTABLE USER: BILLIE W...', and 'Malware incident flagged...'. Each incident has a severity level (HIGH), a status (RESOLVED, NEW), and a tier (Tier 1, Tier 2, Tier 3).
- NOTABLE USERS:** A list of users with their names, roles, and counts. For example, Julietta Donaldson (IT Administrator) has 326 incidents, Howard Osborne (Sales Represent...) has 295, Sherri Lee (Sales Represent...) has 270, and Barbara Salazar (Human Resourc...) has 264.
- NOTABLE ASSETS:** A list of assets with their names, IP addresses, and counts. For example, sky-wwfile-wp1 (10.55.44.33) has 125 incidents, sky-eefile-wp1 (10.14.33.177 - sa...) has 120, and att-addc-002 (10.32.44.19) has 110.
- ACCOUNT LOCKOUTS:** A list of users with their names, roles, and lockout counts. For example, Mario Erickson (05/01/2018 @ 2:...), Jim Coleman (05/01/2018 @ 1:...), and others.
- Executive Users:** A list of executive users with their names, roles, and counts. For example, Andrew Bautista (VP Sales) has 0, Chelsea Mayo (VP Business Dev...) has 0, Emely Blanchard (CEO) has 0, and Emery Santiago (VP Council) has 0.

The home page presents the following:

- **Search Field** for locating information. Users can perform a basic search in using username, asset name, a specific security alert using the event ID, or incident (when Case Management has been installed; for more information on Case Management, see chapter *Case Management*).
- **Threat Hunter** is an advanced search function which allows for searches across a variety of dimensions. Clicking on the triangle inside the search box opens the Threat Hunter menu.

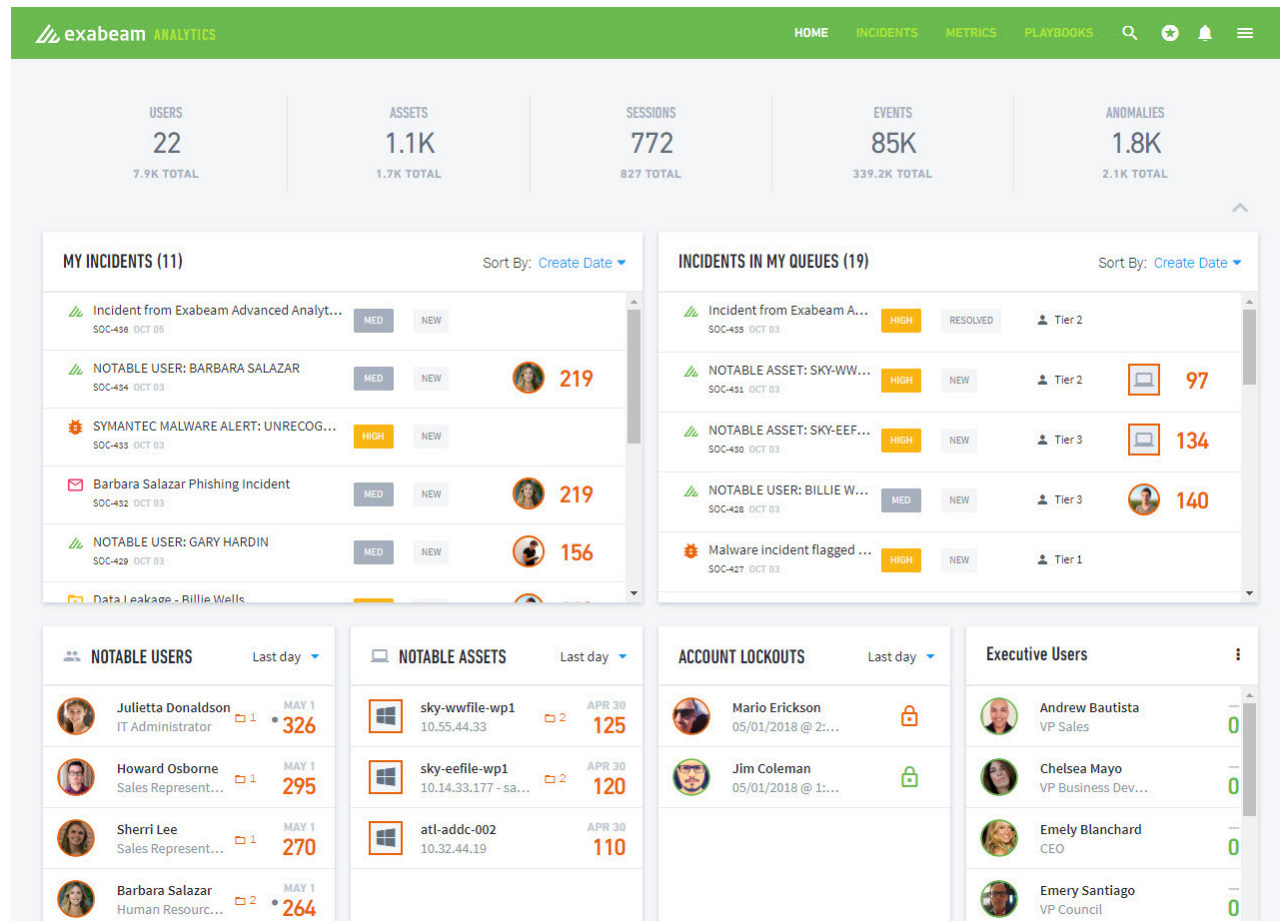


- **Proactive Health Checks** that will alert administrators when:
 - Any of the core Exabeam services are not running.
 - There is insufficient disk storage space to store the logs or events.
 - Exabeam has not been fetching logs from the SIEM for a configurable amount of time.
- **High-level counters** for key metrics that Exabeam monitors.
- **My Incidents** An incident is an unusual event that may indicate a threat to an organization's security that is or was being investigated. The list consists of active, closed, or newly created incidents. This feature is available when Case Management has been installed. For more information on Case Management, see chapter *Case Management*.
- **My Queues** A group of users designated to handle assigned incidents is known as a queue. Incidents assigned to the queues you are associated with are listed. This feature is available when Case Management has been installed. For more information on Case Management, see chapter *Case Management*.
- **Notable Users** where notable means the user had a session score that met or exceeded the configured threshold (default is 90).
- **Notable Assets** where notable means the asset had a session score that met or exceeded the configured threshold (default is 90). This feature is available when Entity Analytics has been installed. For more information on Entity Analytics, see the *Advance Analytics Administration Guide* chapter *Entity Analytics*. contact your Technical Account Manager.
- **Account Lockouts** is a list of users that have an account lockout event in the Session Timeline.
- **Multiple Watchlists** Watchlist Users are lists of users or assets the analyst wants to keep an eye on.
- Next to some usernames and risk scores there is a small dot. This indicates that there is a comment from an analyst on that User Page or Timeline (Commenting on a User, Asset, or Session).
- Within Notable Users and Watchlist Users analysts can **click on the username or score**. Clicking the username opens the **User** Page, clicking the score opens that specific session on the user's **Timeline** Page.
- **Clicking on the username in Account Lockouts** opens the User Page, while clicking the lockout symbol opens that specific Lockout Sequence on the user's Timeline Page.

High-Level Counters on the Advanced Analytics Homepage

Along the top of the home page is a row of counters for the environment that Exabeam is monitoring. The counters are for users, assets, sessions, events, and anomalies. Each counter

shows totals for the organization and recent counts (during regular operation, recent means the past 30 days). Take the following image, for example:



The organization has 7.9K employees and 22 have been active recently. These counters refresh automatically every 5 minutes.

About the Notable Users List

The **Notable Users** list shows the highest scoring session for users whose highest score is at least 90. Only the highest scoring session for a user is represented in the **Notable Users** list. Even if a user has many sessions with a score of 90 or above, his or her name appears in this list only once.

Clicking the caron at the top right activates a drop-down list for selecting the timeframe for that list: last day, last 2 days, last 3 days, last week, last 1 month, or last 3 month.

Watchlists

The users that are on watchlists are users that the analyst may want to keep an eye on for a time. For example, if an employee's computer was infected with malware and needed to be monitored to ensure the remediation was effective or if an employee has been given termination notice. Watchlists provide quick visibility into any sessions started by these sets of users, their latest risk scores, any assets they touched, and abnormal activities of which they were a part.

There are two types of watchlists - those that are created out-of-the-box by Exabeam and those that are created by an analyst. Users cannot be added or removed from watchlists generated by Exabeam, though the watchlists themselves can be deleted. Analysts can also create their own watchlists (see "Customizing Watchlists"). Users can be added using a search expression or by importing a list of usernames from a CSV file. They can be removed the same way, or deleted automatically after a configurable period of time.

Asset Watchlists

Analysts can create asset watchlists on the homepage.

Similar to user-based watchlists, assets can be added to a watchlist based on any of the following criteria:

- Asset Name
- Asset Label
- CSV
- IP Address

Analysts can create user watchlists or asset watchlists but not a watchlist composed of both users and assets. Asset watchlists created by analysts can have a maximum of 100 assets, and can be edited and deleted. When creating an asset watchlist, analysts can determine how long a given asset will remain on the list (Figure 1-2). For example, if a 30-day limit is set then every asset added to that watchlist will be automatically removed 30 days after it is added.

Assets can also be added to an existing asset watchlist from the timeline.

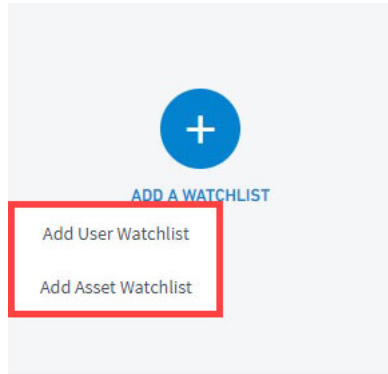
Out-of-the-Box Watchlists

By default, Exabeam will create the following Watchlist categories: Executive Users and Service Accounts. These Watchlists are automatically populated by Exabeam and therefore cannot be configured to add or remove individual users. However, the Watchlists themselves can be deleted. When deleted, the users are removed from the Watchlist and the Watchlist is removed from the dashboard.

- **Executive Users:** Users that are identified as executives during the setup process are automatically added to the Executive Users Watchlist. When executives are added or deleted, these changes are automatically reflected in the Watchlist.
- **Service Accounts:** Users that are identified as service accounts are automatically added to the Service Accounts Watchlist. When service accounts are added or deleted, these changes are automatically reflected in the Watchlist.

Customizable Watchlists

Analysts can create their own watchlists - these can be username-based, CSV-based, user label-based, or peer group-based. To create a custom watchlist, click **Add A Watchlist** at the bottom of the home page, and then select the type of watchlist you wish to create.



The customizable watchlists can be edited by clicking the vertical ellipsis icon in the upper right corner of each watchlist panel. Watchlist can be edited in the following ways:

- **Add User** – Add users by username, by uploading a CSV file, by user label, or by peer group. You can also set a timeframe, after which the user(s) will be removed from the watchlist. This timeframe is per user, not per watchlist. Users can also be added individually from the User Page.
- **Add Asset** – Add assets by asset name, by uploading a CSV file, or by IP address.
- **Remove User** – Remove users either individually or by uploading a CSV file.
- **Remove Asset** – Remove assets either individually, by uploading a CSV file, or by IP address.
- **Edit Watchlist:** – This option allows the analyst to edit the name or description of the watchlist.
- **Delete Watchlist** – The watchlist will be permanently deleted.

Configure Role-based Access Control for Watchlists

When you create a new watchlist or edit an existing watchlist, you can configure permissions to view and manage them according to user roles.

Choose from one of the following options:

- **Public** – Allow all users in your organization to view the watchlist.
- **Based on Role** – Allow specific users to either view or view and edit the watchlist.
- **Only Me** – Deny access (view and edit) to all users in your organization.

Picking **Based on Role** lets you select the watchlist's permissions, which are based on user roles.

Revise the watchlist permissions at any time by locating a watchlist on the homepage and clicking **Edit Watchlist** and then clicking the **permissions** dropdown menu.

Account Lockouts List on the Advanced Analytics Homepage

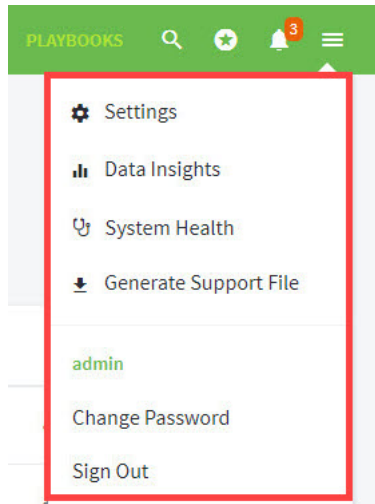
Account Lockouts is a list of users who have been locked out of their account within the timeframe selected. Clicking the caron at the top right activates a drop-down list for selecting the timeframe for that list: last day, last 2 days, last 3 days, last week, last 1 month, or last 3 months. The account lockouts that Exabeam has deemed risky are at the top.

The account lockouts that Exabeam has deemed risky are at the top.

Navigate to Other Pages, Sign Out, or Change Password from the Advanced Analytics Homepage

The **admin** drop-down menu can be found in the upper-right corner of any page. From there you can navigate to the **Settings**, **Data Insights**, or **System Health** pages, and visit **Starred Session Users** without returning to the homepage. The Admin Panel also offers the option to logout or to change your password. At the bottom right is where the current Exabeam build number is located.

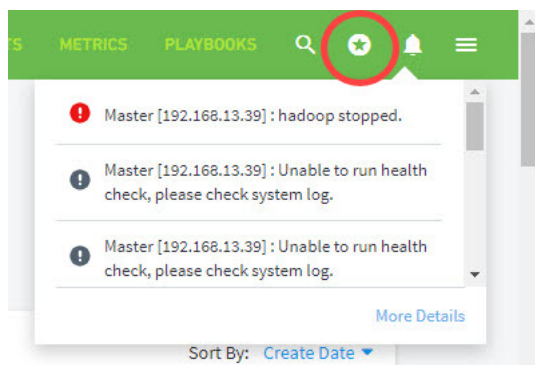
The information available in the admin panel is primarily for administrators or Exabeam customer support, but it does give access to models not available elsewhere.



Bookmark Sessions

Starred Sessions is a list of selected sessions that an analyst keeps. The list is a mini-bookmark of sessions that an analyst might want to revisit or show to other analysts. Clicking an employee name in this area opens the same Risk Timeline area.

A starred session remains in this list regardless of time. An analyst can add or remove the session from the list by visiting the Session Timeline Page.



Get to Know a User Profile

Each user in your organization has a profile that contains important security information about them. This section breaks down a profile into its components to help you learn about the information and functionality available in profiles.

From the **Home** page, under **Notable Users, Account Lockouts, Executive Users,** or a custom watchlist, select a user's name to navigate to their profile.

The screenshot displays the user profile for Fredric Weber, a web developer in the Atlanta office. The profile includes a risk score of 24, department of marketing, and manager Harris Oliver. It also shows incident details, a user risk trend graph, and a list of risk reasons.

1 Profile Overview: Shows user name, photo, department, manager, top peer group, and risk score (24). Includes buttons for Watchlist and 0 comments.

2 Incident Details: Lists active incidents under investigation. Includes incident name, priority, status, and assignee.

Incident	Priority	Status	Assignee
fweber: Notable AA Session SOC-8 19 JAN	HIGH	INPROGRESS	tier3-analyst
Test SOC-19 7 OCT	MEDIUM	NEW	tier1-analyst

3 User Risk Trend: A line graph showing risk score over time. Includes a table of metrics.

Metric	Value
RULES	19
EVENTS	27
ALERTS	2
ACCOUNTS	1
ASSETS	19
ZONES	3
SCORE	203

4 Risk Reasons: A list of reasons contributing to the user's risk score, sorted by risk score.

Reason	Risk Score
10 x First access to asset	+100
2 x Security Alert on asset accessed by this user during VPN session	+80
2 x First security alert name for user	+20
First access to srv_246g_stage for group Harris Oliver	+3

5 Summary/Action: A small box with a bar chart icon and a dropdown arrow.

1 General Information

The screenshot shows a user profile for Fredric Weber. The profile includes a profile picture, a 'Watchlist' button, and a 'RISK SCORE' of 24. The user's details are as follows:

DEPARTMENT	MANAGER	TOP PEER GROUP
marketing	Harris Oliver	107 +19 more groups

FIRST SEEN	LAST SEEN	LAST ACTIVITY	EMPLOYEE TYPE	LAST PASSWORD RESET
1 Jun 2020	3 Jul 2020	Account is active	employee	—

0 COMMENTS

View general information about the user.

1 Review the user's full name, job title, and location, and other identifying labels like **executive** or **privileged**. You also see information like:

- **First seen:** Date when Exabeam first detected the the user in the IT environment.
- **Last seen:** Date the user last logged in to a device or network; the user's most recent login event.
- **Department:** Corporate department the user works in.
- **Manager:** Full name of the user's manager. Click to navigate to the manager's user profile.
- **Top peer group:** The peer group the user is most strongly associated with, as defined by a factor of group cohesiveness.
- **Last activity:** Whether the user's account is active, disabled, locked out, or deleted.
- **Employee type:** Type of employee, as defined in the user_employee_type context table; for example, full-time, part-time, or contractor.
- **Last password reset :** Last date and time Advanced Analytics detected that the user reset their password.

2 To reveal the user's contact information, click the phone  icon on the user's profile picture.

3 To add or remove the user from an existing watchlist on the **Home** page, click the **Watchlist** button.

4 View the risk score from the user's most recent session.

5 Write comments and notes about the user and view how many comments have been written.

2 Data Insights

View the user's top five workstations and assets they use, zones and countries they connect from, and times they are active and inactive.

Under each section, hover over each item to to view the number of times the user:

- **Workstation** – Logged onto this workstation.

- **Assets** – Logged onto this asset.
- **Zones** – Accessed this network zone.
- **Countries** – Connected to this country using a VPN.
- **Time of Week** – Was active during this period.

To view more data about the user, click **MORE INSIGHTS**.

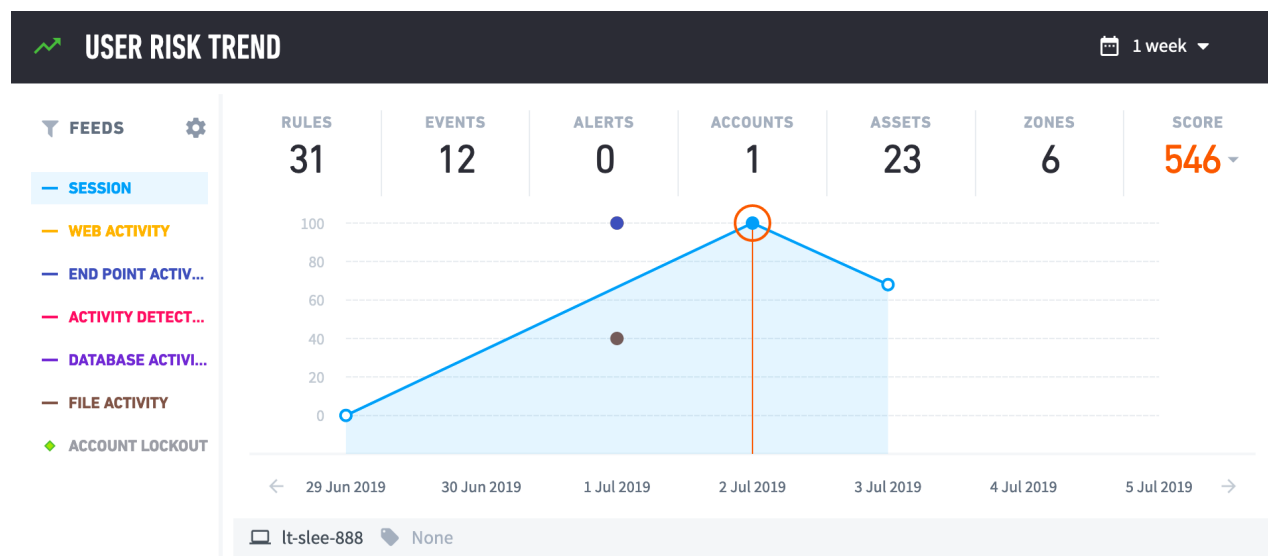
3 Active Incident(s)

View all active Case Manager incidents for which this user is an entity. Review the date the incidents were created and their priority, status, and assignee.

- To navigate to an incident in Case Manager, click the incident's name.
- To view this list of incidents in Case Manager, click **View all incidents**.

4 User Risk Trend

View a graph of the user's risk score over a time frame you select.



You can view risk scores over a time frame of one week, one month, three months, or one year. To view the risk score from a specific day, click the calendar icon. The graph highlights that day within the time frame you selected.

The y-axis shows the risk score out of 100. The x-axis shows dates in a time frame. To move forward or backward in this time frame, click the left and right arrows.

Depending on time frame, each data point represents something different. If you select one week or one month, each data point represents a user session. If you select three months or one year, each data point represents the user session with the highest risk score in a given week. When you select a data point, the graph switches to the one week time frame.

To view the risk scores for specific types of user activity, you can view different feeds:

- **Session:** All user activity, starting from the time they log in until the time they log out, in a 24 hour period.
- **Web activity:** The user accessed a website, domain, or other web activity.
- **End point activity:** The user accessed an endpoint, or other endpoint activity.
- **Activity detected by external sources:** Any unusual activity as detected by the Change in Daily Activity algorithm, if enabled.
- **Database activity:** The user logged onto a database or other database activity.
- **File activity:** The user read a file, wrote to a file, or other file activity.
- **Account lockout:** The user was locked out of their account or failed to log in.

These feeds correspond to log feeds you configured. To view a feed, click **Feeds**.

Each data point is highlighted in green, yellow, or red. Green indicates that the session was not risky. Yellow indicates that the session was risky. Red indicates that the session was highly risky.

As you move along the data points, the counters at the top of the graph changes. These counters summarize what happened in the user session; for example, how many events in the session were notable, how many third party alerts the session triggered, how many assets or accounts were involved, and more. The counters vary based on the feed you select.

When you select a data point, you reveal the **Risk Reasons**. If you view the **Account lockout** feed, selecting a data point reveals information about the user's account, like any changes, assets they use, and reasons for why the lockout was risky.

5 Risk Reasons

When you select a data point in **User Risk Trend**, you reveal the **Risk Reasons**. It lists the events that contributed to the data point's risk score.

RISK REASONS		Sort by: Risk Score ▾
546	2 Jul 8:44 - 20:05	GO TO TIMELINE >
2 x A Suspicious command that deletes shadow copies has been executed for process		+180
Email from competition domain klenergy.com		+90
User attempted to connect to domain iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com associated to WannaCry Ransomware		+90
A Suspicious command that disables recovery mode has been executed for process bcdedit.exe		+40
2 x Abnormal execution of process in this organization		+30
A file sales_opportunities.csv.WCRY has been written and is suspected of Ransomware on host		+20
6 x First execution of process for user		+18
4 x First execution of process in this organization		+12
First file access activity for the organization from network zone new york office		+10
First file access from network zone new york office		+10

You can sort the events by:

- **Risk score** – Highest to lowest risk score.
- **Date** – Earliest to latest time of day the event occurred.
- **Log feed** – Type of activity, as corresponding to a log feed.

To view the session's Smart Timeline™, click **GO TO TIMELINE**.

If you view the **Account lockout** feed, each event is labelled with an arrow. A down arrow indicates that the event reduced the user's risk score, usually that the user was locked out of their own workstation. An up arrow indicates that the the event increased the user's risk score; for example, the user failed to log in from an unusual location.

To view further information about an event, click to open it.

RISK REASONS Sort by: Risk Score ⌵ ⋮


405 2 Jul 9:19 - 22:50 ⌵ [GO TO TIMELINE >](#)

- 4 x Over 5MB of data emailed to personal email domain. +160
- 6 x Abnormally large outbound email for user +60
- First email to/from United States for the organization +25**
 - 1** DESCRIPTION: First email sent or received from this country for the organization
 - 2** EVENT TYPE: dlp-email-alert-out
 - 3** CONFIDENCE: 100%
 - 4** RULE TAGS: Exfiltration Over Alternative ...
 - 5** ANCHOR SCORE: 25
 - 6** ANOMALY FACTOR: 1.0
 - 7** =
 - 8** +25
 - [Event Details](#) [Rule Definition](#) [Data Insight](#)
- First email to/from United States for the user +25

- 1** Description of the event.
- 2** Type of event.
- 3** Level of confidence Exabeam has in the model that triggered the risk rule (not applicable to fact-based rules).
- 4** Tagged MITRE tactics or techniques that the event is associated with. Click the tag to view a description and navigate directly to the MITRE ATT&CK™ database to learn more.
- 5** Formula for calculating the event's total risk score, which is based on two variables: the anchor score and anomaly factor.
 - The anchor score is determined by the specific rule that was triggered.
 - The anomaly factor measures the degree to which the the action was anomalous for the user. The number is calculated in part by the shape of the user's histogram, how often a rule is triggered, and the size of the user's peer group.
 - The total risk score is the anchor score multiplied by the anomaly factor.
- 6** **Event Details** links to further contextual data about the event.

NOTE

When a Risk Reason includes more than one of the same event type, you can access Event Details by moving your pointer over an event and clicking the link on the right.

EVENT TYPE	CONFIDENCE	DATE	DESCRIPTION	ANCHOR SCORE	ANOMALY FACTOR		Event Details
remote-access	Not applicable	2 Jul 10:19:00	First access to asset: il-ips-wp1	10	X	1.0	= +10 
		2 Jul 10:45:00	First access to asset: us-apps-wd1	10	X	1.0	= +10

[Rule Definition](#)

7 Rule Definition links to information about the rule that triggered the event.

8 Data Insights links to information about the model. The link appears only if the triggered rule is associated with a histogram model.

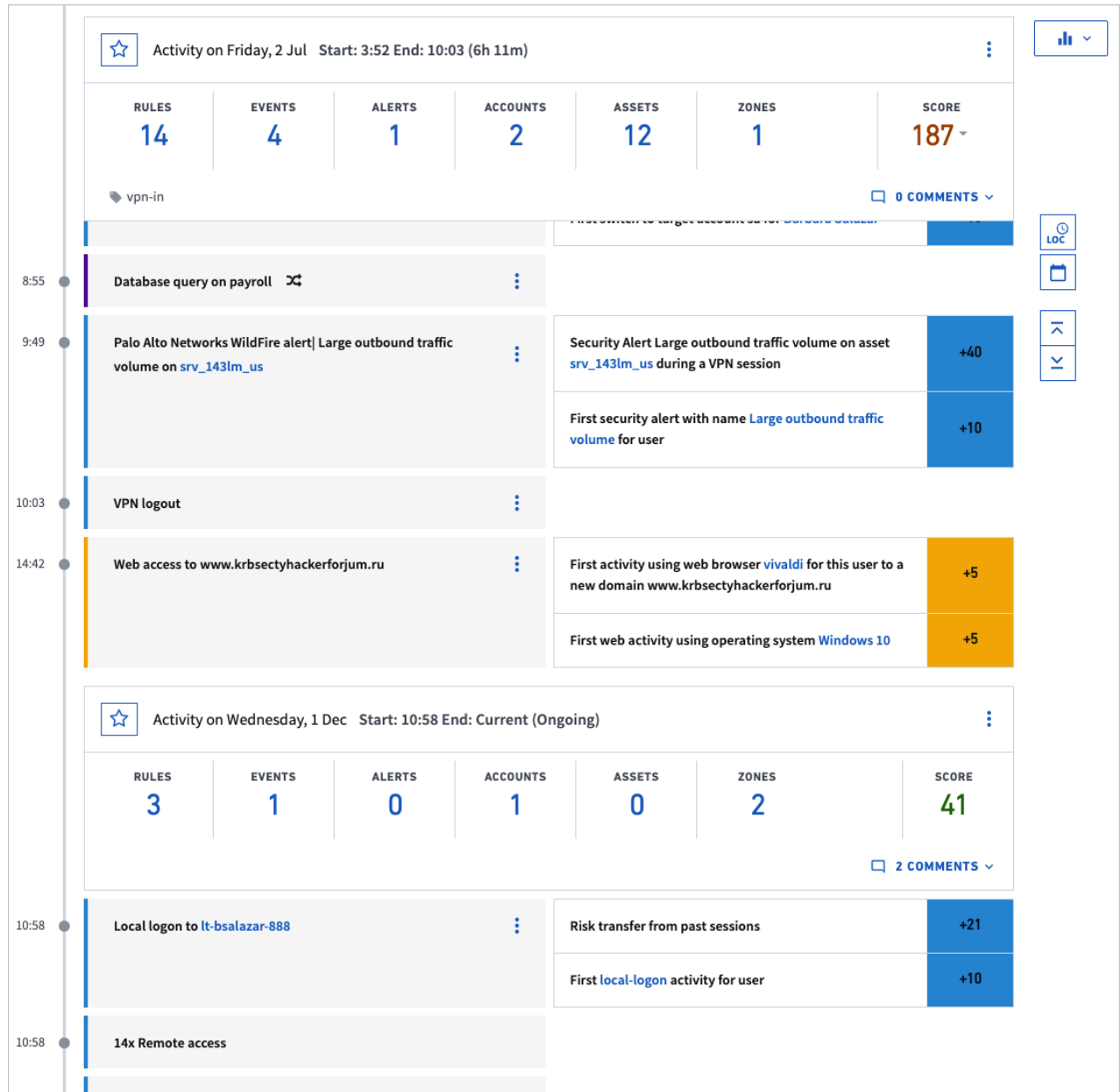
NOTE

When a Risk Reason includes more than one of the same event type, you can access Data Insight by moving your pointer over an event and clicking the link on the right.

	CONFIDENCE	DESCRIPTION	ANCHOR SCORE	ANOMALY FACTOR		Data Insight
1:00	Not applicable	First access to asset: l-web-wp1	10	X	1.0	= +10 
6:00		First access to asset: us-apps-dev1	10	X	1.0	= +10
2:00		First access to asset: srv_246g_stage	10	X	1.0	= +10

Get to Know the User Timeline Page

This section describes the contents and capabilities of the User Session Timeline page.



Analysts can access a user's Timeline by clicking on the user risk score on the homepage, selecting **Go to Timeline** from the user page, or from user search results in **Threat Hunter**.

The **Session Timeline** Page displays all the events in chronological order during the session, so the analyst can see all events before and after a security, anomalous, or lockout event. Seeing the whole timeline helps the analyst see, for example, whether a hacker started the session from outside the network or the legitimate user started the session on-site (the **Risk Timeline** in the **User** Page shows only anomalies). The timeline includes all events in that session, whether high, low, or no risk. There are three logical containers of information that are displayed on the timeline: **Daily Summary**, **Sessions**, and **Account Lockout Sequences**.

By default, the timeline page will only show sessions and events within sessions. Daily Summary and Feeds are turned off. However, clicking the **filter** icon at the upper-left corner of the **Session** Page opens a calendar and filters. The analyst can choose to display all events or only those events that were anomalous. They can also choose to display lockouts, sessions, feeds, or all. In the calendar any date with a color is a day for which Exabeam has data - black numbers are inactive days, green are days within a normal range, and red are days with a high risk score. The analyst can choose the date of a different session for the same user and filter how they see the timeline.

Account Lockout Sequences appear within the **Timeline** when the **Show Lockouts** filter is selected. It is also turned on by default when the analyst is clicking on notable lockouts from the home page. They contain their own Sequence Summary, followed by the events in that sequence.

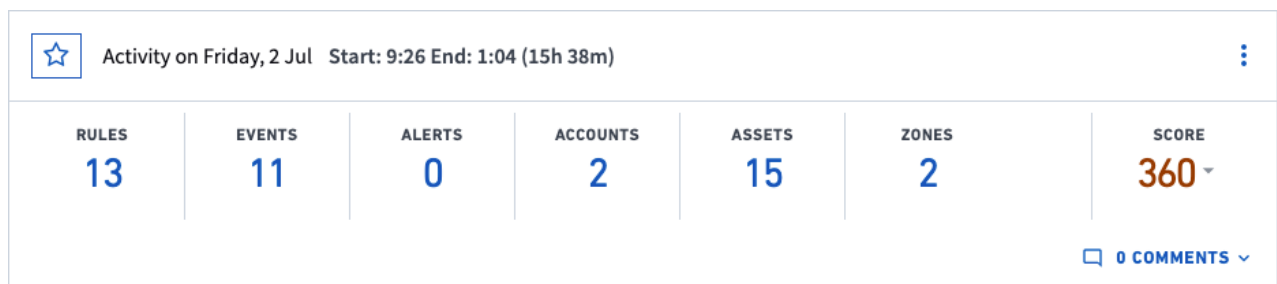
Feeds appear within the **Timeline** under the heading **Daily Summary** when any feed is selected in the filter.

Analysts can move back and forth to other sessions for a particular user to see whether the current threat is a sudden change or has been a gradual development. The image above shows the **Session Summary**, which is the upper part of the **Session Timeline** Page and illustrates how to go to the previous session. At the bottom of the timeline, the analyst can go to the next timeline if one exists.

The list of events can be very long, so the session summary provides a mechanism for the analyst to jump to items of interest.

Examine Events by Category with the User Session Summary

This section defines the counters that make up the session summary. The counters are for categories that an analyst might want to examine in detail. These are interactive and all-inclusive: they represent all events whether the events are benign, anomalous, or threatening.



The session summary expedites research. A session can have many thousands of events, but instead of scrolling through many screens to locate the risk-associated events, the analyst can click a counter to see a popup with all the events for that category. Clicking on an item in the popup shifts the timeline to that specific event. The choice of which count to click first can depend on previous steps, but analysts frequently start with a security event.

Details of the counters are as follows:

- **Reasons:** Reasons are details about anomalies or risks. To see the anomalies that contributed to a non-zero risk score, the analyst can click the Reasons counter. Anomalies that also were security threats are in the Security Events counter.
- **Events:** Events are the constituent activities of a session. For example, logging onto a VPN is an event, logging onto an account is an event, and sending a document to a printer is an event.
- **Alerts** – Security alert events are threats of malicious activity.
- **Accounts:** Users can access different facilities with different sets of logon credentials. Each set of credentials represents an account. This list shows all accounts but does not indicate a first-time use of an account or another anomaly. A first-time use will be in Reasons.
- **Assets:** An asset can be a server, workstation, a local host computer of any type, a printer, and so on.
- **Locations:** Locations are network zones rather than a necessarily physical place. Network zones are internal network locations. Exabeam and an organization collaborate to define zones during the set-up process. Zones can be cities, business units, buildings, or even specific rooms. For example, "Atlanta" can refer to a network zone in a city rather than the city (all according to an organization's preference).
- **Score:** This is the total risk score for this session.

Near the bottom of the session summary is a **tag** icon. This icon is a label for the nature of the VPN that started the session (if applicable). In the current release, this label is informational only. The possible labels are:

- **VPN-in** means the user started the session by logging onto a VPN to get inside the IT environment.
- **VPN-within** means the user started the session from a local workstation but then started a VPN, for example, to a more secure part of the enterprise.
- **VPN-out** means the user logged onto a VPN to the outside of the local network. This scenario is the least likely.

At the bottom right is the option to query Splunk Logs, Export Events, and Accept Session. Before accepting a session be sure to read [Accepting a Session](#) on page 1.

If your SIEM is Splunk, then clicking **Splunk Logs** opens a new window where you can search for events within Splunk, with the appropriate query parameters set. This is helpful if an analyst wants to gather additional details regarding the user by looking within the SIEM during investigations.

Clicking the **Export Events** link exports all the events in a user session to a CSV file that the user can save locally; default file name is `Exabeam_<username>_<sessionid>_<riskscore>`. The CSV contains a list of all events and key details. Columns titled `time`, `session_id`, `Event_id`, `event type`, `host source`, `user`, and `account` are populated for every file. The columns following those are dependent on the information available (i.e. `dest_host`, `domain`, etc.). Under `risk_reason` the rules that were triggered are listed; if more than one rule was triggered then semicolons separate them.

About the User Session Timeline

This section describes the information elements in the **User Session Timeline**.

Details for an event are on the left side of the timeline regardless of whether the event was an anomaly or a security risk. If an event also has a risk score, the details of the risk are on the right side of the timeline.

8:55	VPN login from Unknown		
10:00	Process execution: winlogon.exe	A Windows program executable was started in a suspicious folder.	+10
10:09	Process execution: conhost.exe		
12:21	Process execution: barbarian.jar	First execution of process barbarian.jar	+3
12:21	CrowdStrike Falcon alert Trojan.Generic on lt-fweber-888	Security Alert Trojan.Generic on asset lt-fweber-888 during a VPN session	+40
		First security alert with name Trojan.Generic for user	+10
12:32	Process execution: vssadmin.exe	A Suspicious command that deletes shadow copies has been executed for process vssadmin.exe	+90
		First execution of process vssadmin.exe	+3
12:36	Process execution: bcdedit.exe	A Suspicious command that disables recovery mode has been executed for process bcdedit.exe	+40
		Bcdedit executable was used to delete boot configuration data.	+10
		First execution of process bcdedit.exe	+3

The risk from **Sequences and Daily Feeds** can be transferred to the session. For example, Exabeam could have found that the user’s web activities included going to a malicious domain, which resulted in a risk score. This score will be transferred to the user’s session. If the malicious web activity happened outside of a session (i.e. during a time period where there was not an open session) the score will be transferred to the user’s next session.

When the session timeline is opened, by default the events that earned points are expanded. We collapse events of the same type that have no score, in which case the page displays something like, “3x Remote access,” as in the center of the image above.

The image also shows a session started about 5:45PM, with three risk transfers from web activities (clicking on any of those highlighted web activities links will take you to the relevant Daily Summary where they occurred) and ten points added to the session because of the abnormal session start time.

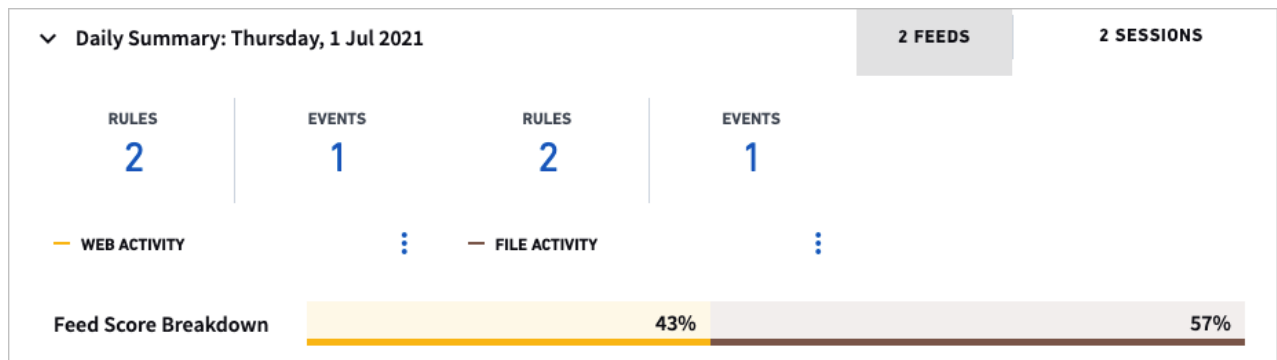
Filter User Timelines

The drop-down **Filter** panel can be accessed to the left of the timeline. An analyst can choose to see all events, or only those with anomalies. They can also choose to see any combination of session and feeds. When loading the timeline page from the homepage the default selections are **All Events** and **Session Activity** turned on; **Web Activity** and **Account Lockout** are off.

The calendar at the bottom makes it easy to jump to a different day. The days are color coded to signpost when there was a high-risk session - red indicates a high-risk session, green indicates a low-risk session.

View Activity Summary on a Specific Day

The **Daily Summary** and **Timeline** only appear when at least one of the feeds filters are turned on.



A **Feed** here refers to events that happen outside of the logical container of a session. They are often high volume feeds and processed in parallel to session and lockout sequences. These can be application logs, web access logs, DHCP, etc. Feeds are measured in a different timeframe to sessions - they are 24 hours. If a feed begins at 5pm on 01/10/16 then it will end at 5pm on 01/11/16. Anomalies within daily feeds will be assigned a risk score and that score is transferred to the nearest session that begins after the feed. You will also notice the **Feed Score Breakdown** at the bottom of the **Daily Summary**. This is an at-a-glance bar graph that breaks down what percentage of each feed comprises the Daily Summary. This is color-coded to match the color of each feed in the timeline.

The **Daily Summary** provides a look at what happened in a 24-hour period. This is different from the session view because sessions are bound by the time a user logs in, to when the user logs out. The **Daily Summary** is a way to look only at what happened on a specific day.

At the top of the **Daily summary** heading are tabs on the right which allow you to select if you want to see a summary of the day's feeds or a summary of the day's session and lockout events that also occurred in that same day. In the image above, the **Feed** tab is selected. This informs the analyst of all the feed activity that happened during the day; in this case the user had 2 feeds, one with 160 web activity events for which there was 0 risk reasons, and one with 273 DHCP events for which there was 1 risk reason. Clicking on the reason will open a pop-up window that explains what the event was and how many points were added to the session because of it.

▼ Daily Summary: Thursday, 1 Jul 2021
2 FEEDS
2 SESSIONS

SCORE

150

SESSION:

Friday, 2 Jul at 10:48

GO TO SESSION >

SCORE

42

SESSION:

Wednesday, 1 Dec at 11:01

GO TO SESSION >

If the analyst were to select the **Session & Lockout** tab, as in the above image, she would see that there was 1 Lockout Event and one Session that began during that day. Because there is no logout event the session did not end during that same day, however. You can jump to the lockout or session header by clicking **Go to Lockout** or **Go to Session**.

Get to Know the Daily Timeline

This section describes the information elements present in the Daily Timeline.

12:00AM

12:00AM

12:00AM

> Web access to proxy-36.sg1.dailymotion.com

- > First activity using this web browser [AppleCoreMedia](#) for the organization +5
- > First activity using web browser [AppleCoreMedia](#) for this user to a new domain proxy-36.sg1.dailymotion.com +5
- > First activity using this web browser [AppleCoreMedia](#) for the peer group NA +3

▼ Web access to scores.espn.go.com

TIME	HOST	METHOD
12:00:00AM	10.1.254	GET
DEST. DOMAIN	URL	QUERY
scores.espn.go.com	/nfl/caster/snapshot	?sessionl...p=96880&rand=1447045618003
SOURCE IP	SOURCE_ZONE	PROXY_ACTION
10.2.130		OBSERVED
OS	BROWSER/APP	PROXY_FILTER
Windows	Trident	TCP_MISS
DEST. IP	CATEGORY	
	Sports/Recreation	

DESCRIPTION

This is the first time Exabeam has seen anyone in the organization utilizing this browser. An organization typically uses a standard set of software and deviation from this standard is rare. This event is notable because it indicates that a user has introduced software previously unseen in this organization, or an application is masking its behavior. [View Rule Definition](#)

RULE TYPE	EVENT TYPE	CONFIDENCE
web	web-activity-allowed	Not applicable

- > First activity using web browser [Trident](#) for this user to a new domain scores.espn.go.com +5
- > First web activity using operating system [Windows](#) for the organization +5
- > First web activity using operating system [Windows](#) for the peer group NA +5
- > First web activity using operating system [Windows](#) +5
- > First activity using this web browser [Trident](#) for the peer group NA +3

> 2 x Web Activity

The **Daily Summary** and **Daily Timeline** only appear when one or more of the feeds filters are turned on; the **Daily Timeline** will show all of the feeds that are selected in the filter. For example,

in the image above, the **Web Access** filter is turned on, and so all of the Web Access events are present in the Daily Timeline.

The event itself is on the left side of the timeline, and if the event was assigned a risk score then the details of the rule(s) triggered are to the right. We collapse events of the same type that have no risk score. Clicking a caret will open further details. In the image above, six rules were triggered by the Web Access to scores.espn.go.com event, five of those rules were assigned a risk score of 5 points and one a score of 3 points, totaling 28 risk scores for that one event.

View and Understand an Account Lockout Sequence

Analysts can access an Account Lockout Sequence by clicking the warning symbol on the homepage or clicking **View Activity** on the **User** page. By default, the **Show Lockouts** filter will be turned on and the **Show Sessions** filter will be off.

RULES	FAILED LOGONS	UPDATES	LOCKOUTS	ASSETS	ZONES
0	0	1	1	1	0

ACCOUNT CHANGES

PAST ACCOUNT ACTIVITY
Account is active on 29 Jun 2021

CURRENT ACCOUNT ACTIVITY
Account locked out 1

LOCKOUTS IN LAST 30 DAYS
1

ASSETS

SOURCES
lt_x200_nlarson

DESTINATIONS
lt_x200_nlarson

FAILURE REASONS

—

0 COMMENTS

The image above shows the summary for an account lockout sequence in the timeline. To the left of the **Logon Failures and Lockouts** title is a warning icon – orange means Exabeam deems this sequence risky, green means Exabeam sees it as normal. The summary counters at the top give detailed information about the lockout related activities, including:

- **Reasons** – Anomalies or risks that were identified in a lockout sequence. To see the anomalies that contributed to a non-zero risk score, click the Reasons counter.
- **Failed Logons** – The number of times this user has failed to logon in this sequence.
- **Updates** – These represent any changes to the user account within Active Directory, such as a user account disabled or a user account password reset.
- **Lockouts** – The number of times this user has been locked out of an account in this sequence.

- **Assets** – An asset can be a server, workstation, a local host computer of any type, a printer, and so on.
- **Zones** – Zones are network zones rather than a necessarily physical place. Network zones are internal network locations. Exabeam and an organization collaborate to define zones during the set-up process. Zones can be cities, business units, buildings, or even specific rooms. For example, “Atlanta” can refer to a network zone in a city rather than the city (all according to an organization’s preference).



NOTE

As with user sessions, you have the option to Accept Activities in the account lockout sequence. Before Accepting Activities please read the section *Accepting a Session or Sequence*.

Get to Know the Account Lockout Sequence Timeline

This section describes the information elements in an account lockout sequence timeline.

Details for the event itself are on the left side of the timeline and details of the risk – including the rule triggered and how Exabeam has evaluated the event – are on the right side of the timeline. Events of the same type and reason are aggregated, in which case the page displays something like “15 x Account lockout” as in the image below.

Exabeam views account lockout events slightly differently from standard session events. For one, they are not given a score, but a binary rank of either Risky or Normal. In addition, certain lockout related activities increase the risk of the event and some reduce it. For example, if a user fails to logon from an abnormal location, that is a risk increasing activity. Alternatively, if a user has changed their password recently and they are failing to logon to their workstation, that is a risk reducing activity. In the image below, the orange up arrow indicates this is a risk increasing event, while the green down arrow indicates a risk reducing event.

The sum of these scores determines whether Exabeam sees the sequence as risky or normal – if risky the sequence will show an orange warning symbol and appear on the homepage. In addition, if a sequence is risky, 50 points are added to the overall session score.

12:24	NTLM logon to src_k4398_prod			⋮	
13:05	Kerberos logon to src_k4398_prod			⋮	
14:25	Failed to logon to src_k4398_prod			⋮	<p>Failed logon due to bad credentials ↑</p> <hr/> <p>Failed logon to an asset src_k4398_prod that this user has not previously accessed ↑</p>
	TIME	USER	DOMAIN		
	14:25:00	jdonaldson	ktenergy		
	SOURCE HOST	SOURCE IP	SOURCE ZONE		
	lt-jdonaldson-888	10.27.129.64	—		
	DESTINATION HOST	DESTINATION IP	DESTINATION ZONE		
	src_k4398_prod	10.4.44.194	new york office		
	EVENT CODE	RESULT CODE	SOURCE		
	4771	0x18	DC		
	REPORTING HOST	FAILURE REASON			
	src_k4398_prod	Bad user name or password			

Comment on a User, Asset, or Session

An analyst can document the details and progress of an investigation by using text-entry boxes for writing comments. The boxes are available in the **User Page**, **Asset Page**, and **Session Timeline Page**. A comment can explain a change in behavior, such as why a new behavior is acceptable. Comments can be a thread of discussion between analysts.

Accepting a Session or Sequence

Experienced analysts, such as Tier 3 Analysts, can accept behaviors for users and assets so that the behaviors no longer trigger alerts. Accepted behaviors are effectively whitelisted. This action applies only to the particular user or asset associated with the session or sequence, and it is only applied to future events. Sessions and sequences that occurred prior to the date of acceptance are not affected. This feature requires extreme caution because once a behavior is accepted, the action cannot be undone.

Behaviors can be accepted from the User, User Timeline, Asset, and Asset Timeline pages.

WARNING

When behaviors are accepted, they are permanently whitelisted for the associated user or asset. Reverting accepted behaviors is not supported.

Accepting behaviors can undermine security and put your organization at risk. The best practice for eliminating unwanted alerts is through tuning the rules and/or models.

Accept a Partial Session or Sequence

WARNING

When behaviors are accepted, they are permanently whitelisted for the associated user or asset. Reverting accepted behaviors is not supported.

Accepting behaviors can undermine security and put your organization at risk. The best practice for eliminating unwanted alerts is through tuning the rules and/or models.

When analysts do not want to accept the behaviors in an entire session or sequence, they can accept individual behaviors. For example, in a session that includes a First Access to Asset alert and an Account Switch alert, the analyst can accept one of the behaviors without accepting the other.



NOTE

Risk transfers from previous sessions, account lockouts, and feeds cannot be accepted.

For simplicity, the remainder of this section refers only to sessions, but the procedure is also applicable to asset sequences and lockout sequences.

To accept a partial session:

1. On the right side of the Risk Reasons header bar, click the vertical ellipsis icon (⋮), and then click **Accept > Partial**.

The screenshot shows the 'RISK REASONS' section of a user profile. At the top, there is a header bar with 'Sort by: Risk Score' and a vertical ellipsis icon. Below this is a table of risk items. A context menu is open over the 'Accept' button, showing options for 'Partial' and 'Entire'.

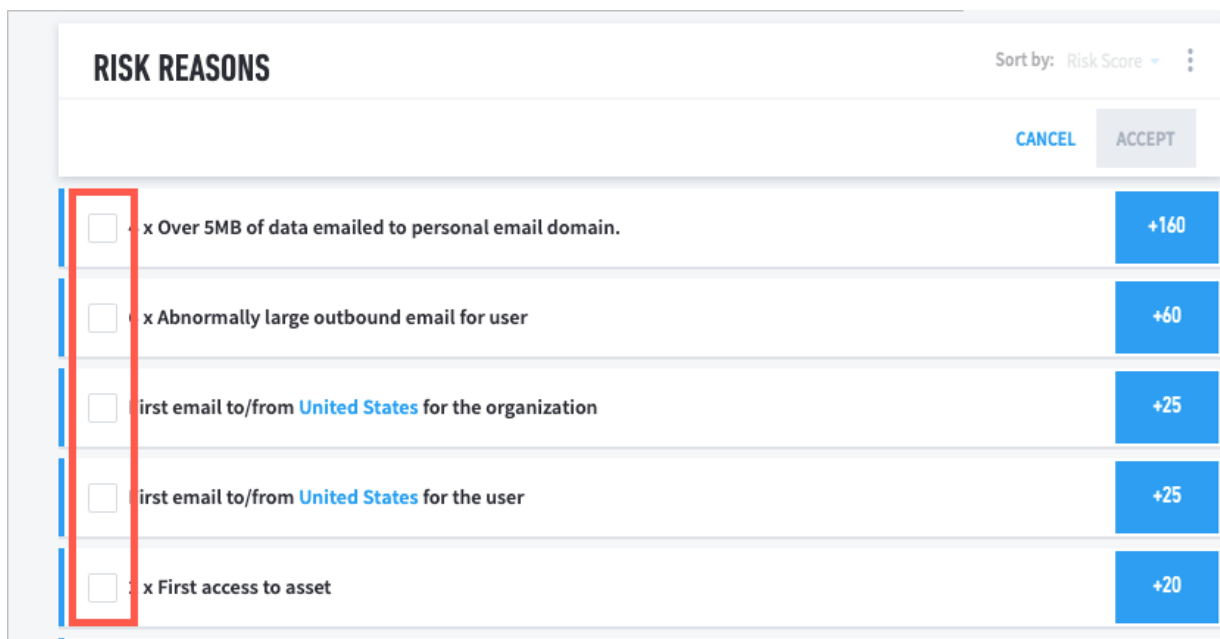
Risk Reason	Risk Score
First time activity from country Ukraine	+40
Credential switch to a privileged or executive account sa	+40
Security Alert Large outbound traffic volume on asset srv_143lm_us during a VPN session	+40
2 x First remote logon to asset	+30



NOTE

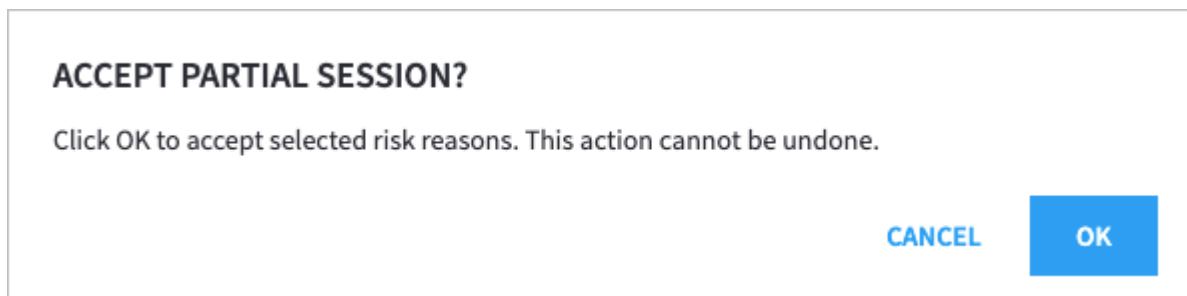
If you do not have permission to accept behaviors, the Accept feature is disabled. The feature is also disabled if all the triggered rules in a session are risk transfers, or if they have already been whitelisted.

Checkboxes appear on the left for each of the individual risk items.



Risk Reason	Score
<input type="checkbox"/> x Over 5MB of data emailed to personal email domain.	+160
<input type="checkbox"/> x Abnormally large outbound email for user	+60
<input type="checkbox"/> First email to/from United States for the organization	+25
<input type="checkbox"/> First email to/from United States for the user	+25
<input type="checkbox"/> x First access to asset	+20

2. Select the checkbox for each of the behaviors that you want to accept.
3. Click **Accept**.
A confirmation dialog box appears.




ACCEPT PARTIAL SESSION?


Click OK to accept selected risk reasons. This action cannot be undone.

CANCEL **OK**

4. To confirm that you want to accept the selected behaviors, click **OK**.

 **NOTE**
This process can be repeated as many times as necessary within the same session.

Accept an Entire Session or Sequence

 **WARNING**
When behaviors are accepted, they are permanently whitelisted for the associated user or asset. Reverting accepted behaviors is not supported.

Accepting behaviors can undermine security and put your organization at risk. The best practice for eliminating unwanted alerts is through tuning the rules and/or models.

WARNING

Accepting the behaviors in an entire session or sequence is not recommended. If you must accept certain behaviors, you can accept them individually. See [Accept a Partial Session or Sequence](#).

NOTE

Risk transfers from previous sessions, account lockouts, and feeds cannot be accepted.

For simplicity, the remainder of this section refers only to sessions, but the procedure is also applicable to asset sequences and lockout sequences.

To accept an entire session:

1. On the right side of the Risk Reasons header bar, click the vertical ellipsis icon (⋮), and then click **Accept > Entire**.

The screenshot shows the 'RISK REASONS' section of a user profile. At the top, there is a summary bar with '314' in an orange box, the date '2 Jul', and a time range '3:52 - 10:03'. Below this is a list of risk events, each with a blue score indicator on the right. A context menu is open over the first event, showing options: 'Sort by: Risk Score', 'Create Incident', 'Accept', 'Partial', and 'Entire'. The 'Accept' option is highlighted, and a sub-menu is visible next to it.

Risk Reason	Score
First time activity from country Ukraine	+40
Credential switch to a privileged or executive account sa	+40
Security Alert Large outbound traffic volume on asset srv_143lm_us during a VPN session	+40
2 x First remote logon to asset	+30

NOTE

If you do not have permission to accept behaviors, the Accept feature is disabled. The feature is also disabled if all the triggered rules in a session are risk transfers, or if they have already been whitelisted.

2. Click **Accept**.
A confirmation dialog box appears.

ACCEPT ENTIRE SESSION?

Click OK to accept this entire session. This action cannot be undone.

Comment (optional):

CANCEL **OK**

3. *(Optional)* In the **Comment** field, provide a summary of the reasons for accepting the session.
4. To confirm that you want to accept the entire session, click **OK**.

Entity Analytics

Entity Analytics offers analytics capabilities for entities beyond users such as hosts and IP addresses within an environment. For our purposes, the words *asset* and *entity* are used interchangeably.

Entity Analytics assigns risk scores on any anomalous activities on Assets in an organization's environment by using machine learning and expert rules. In a single Asset Session, Entity Analytics may report risks related to a machine accessing many new hosts, a malware security alert received from a 3rd party system, and an entity connecting to a host in a new country.

Notable Assets (assets that had an Asset Session score of at least 90) will appear on the homepage next to **Notable Users**.

Entity Analytics creates an Asset Session in cases where logs indicate activities on assets. These can be logs such as Windows authentication, VPN or security alerts that contain events related to users and assets. In addition, asset sessions can be built from logs indicating device to device communication that do not have a user name attached to them, such as firewall, DNS, Netflow or IoT logs. An Asset Session is similar to a User Session in that it is a logical container of events logs. However, unlike User Sessions (which begin when a user logs on and ends when a user logs off) an Asset Session represents a 24-hour window of all activities performed on an asset. Some logs have both asset and user fields and Advanced Analytics creates both a session event and an asset session event out of these.

For example, when a machine is a source of attack and uses multiple identities (user names) in a short amount of time to perform brute force attacks or move laterally within an environment. This type of risk is not elevated by Advanced Analytics as these activities belong to multiple user sessions and a single user did not accumulate enough risk to be identified as anomalous. With Entity Analytics enabled, the entity itself will now have a risk score associated with it. The **Asset Session Timeline** page displays all the events in chronological order during the session, so the analyst can see all events before and after a security, anomalous, or lockout event. Seeing the whole timeline helps the analyst see, for example, whether a hacker started the sequence from outside the network or a legitimate user started the sequence on-site.

Entity Analytics is available as a licensable option and can be added to an existing Advanced Analytics deployment. Please talk to your Technical Account Manager for more information.

Get Started with the Asset Page

Learn about Exabeam analytics and the interactions available during an Asset investigation.

In Advanced Analytics, assets are as crucial to investigations as users. They represent any device on the network with an IP address. Throughout an attack campaign, one or several assets may become compromised; a compromise trail can start at the infection point with a workstation and extend to any server accessed by the attacker. The compromise can spread from one user or asset to others; often this is a result of either cached credentials on the asset getting stolen or malware being executed on the asset to steal the credentials of users logging into it.



NOTE

To ensure accuracy, Asset Session Timelines are updated only when session and non-session data, such as host to IP mappings, have been processed. Data processing may take up to two hours after ingestion.

The Assets page is divided into the following areas:

- **Asset Directory Information:** Contains details about the Asset itself and useful for starting an investigation. This information is typically pulled in from LDAP Server or manually provided by the analyst.
- **Asset Risk Trend:** Shows the risk trend of the asset over time. This graph shows the asset risk analyzed from various log feeds, along with Summary Counters along the top. Below the Summary Counters is a chart that shows different scores over a user-specified window of time. By default, all of the feeds are shown. Time range choices are one week, one month, three months, and one year - these choices are specified in the top right corner.
- **Asset Risk Reasons:** Shows details about the events with non-zero risk scores. The order of the entries is from highest risk score to lowest, though they can also be organized by time. The context for each reason is best investigated in the Timeline Page.

About the Asset Directory Information Page

	fa1_wks_991 10.77.10.163	Workstation	RISK SCORE 0
FIRST SEEN Dec 1st, 2017	LAST SEEN Jan 4th, 2018	LOCATION —	TOP USER Taina Wagner
0 COMMENTS			

The **Asset Directory Information** consists of general asset information, as well as an orange badge at the upper left that shows the number of third-party security alerts that have been triggered on this asset.

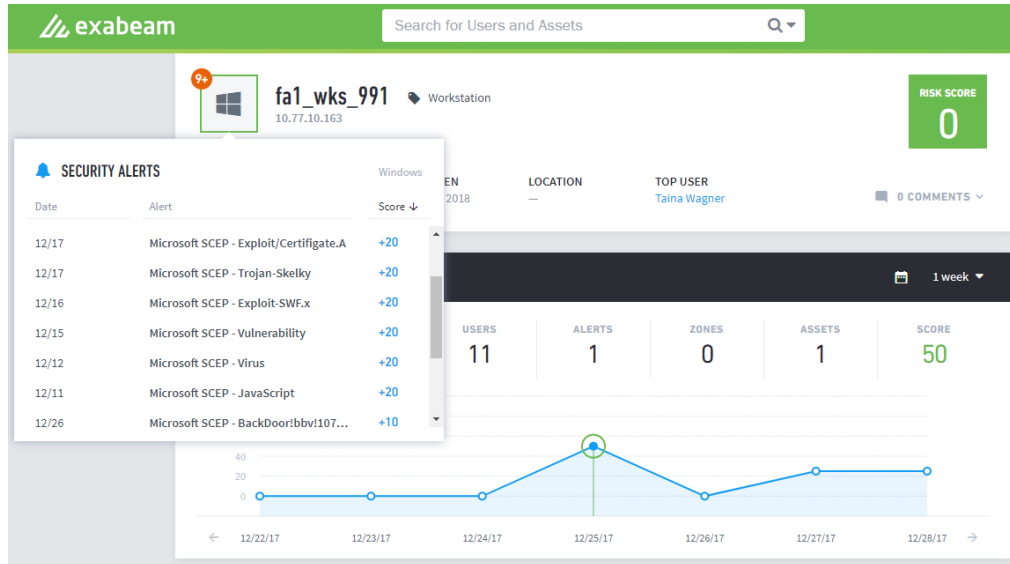
General information consists of:

- IP Address and labels associated with the asset

Get Started with the Asset Page

- First and last-seen dates (first-seen is when Advanced Analytics saw the asset in the IT environment for the first time, last-seen is the date of the most recent sequence where Advanced Analytics detected the asset in the network)
- Location of the asset
- Top User (the user that logs into this asset the most frequently)

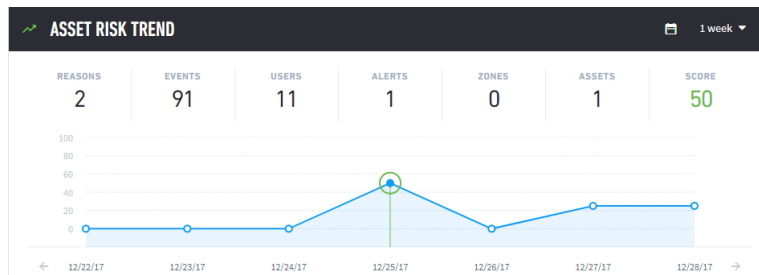
The upper-right corner of the **Directory Information** always shows the asset's most recent sequence score, regardless of which sequence is on-screen.



Advanced Analytics receives security alerts from an organization's security systems through the customer's SIEM, log repository, endpoint security system or malware analysis appliance which may indicate malware is present on a device. Exabeam includes these details in the Security Alerts drop-down list when the icon is clicked and in the Sequence Timeline Page. In the Security Alerts drop-down the event's risk score determines where it appears in the list. In contrast, the Sequence Timeline Page shows the events by their time in the sequence.

The **Comments** icon at lower right opens an area for writing comments. Details about annotation are in *Commenting on a User, Asset, or Session*. In this example, the number of comments on this User is 0.

Get to Know the Asset Risk Trend Page



The interactive **Risk Trend** area in the above image shows **Summary Counters** along the top (these are dynamic and will change depending on your interactions with the graph), a graph of the user's scores over time, detailed risk reasons for the scores, and links for opening more details.

At top right are choices for the timeframe of the data displayed. The period can be one week, one month, three months, or one year. The **calendar** icon will let you choose a specific date. Once the date is selected, the chart moves to that specific week with the day highlighted.

The **Summary counters** are non-interactive and give a quick at-a-glance view of what happened within each sequence or feed. The counters in the asset session summary change depending on the type of trend selected. Values change as the cursor moves over the data points in the graph. Each dot represents the asset session for the day. The **Summary** consists of the numbers of reasons, events, users, alerts, zones, assets, and score. The score is the total risk score attributed to the asset in the timeframe selected.

The **Trend Graph** in the center of the Risk Trend shows the scores for sequences and feeds over the period of the selected time frame (one week in this example). The green dots represent non-risky asset sessions, the yellow dots represent risky asset sessions, the red dots represent very high-risk asset sessions.

Clicking on the dot for the event itself in the graph will populate the **Reasons** area below the graph. When the 1 Year and 3 Months views are chosen, each dot on the graph represents one week; hovering over the dot displays the timeframe it represents as well as the highest score attained by the user in that period. When you select the highest score, the graph will switch to the weekly view for the user.

Immediately below the graph are the dates for the current time frame (whose breadth is selected near the top right of the page). Small arrowheads to the left and right of the dates are for sliding the time window ahead or back.

Get to Know the Asset Risk Reasons Page



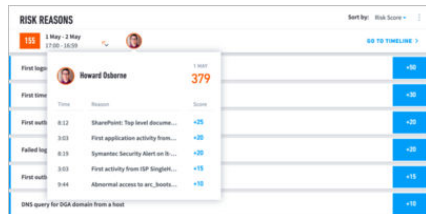
This area contains details about all the reasons for the total score in an Asset Session. There are details for items in the Session summary and links to still more information appears among the reason details.

Analysts can reach the **Asset Risk Timeline** area from the **Notable Assets** section of the **Homepage** or the **Starred Sessions** area.

As in the image above, the title of the reason is to the left, while the score is to the right. By default, the risk reasons are listed by score (highest to lowest), but they can also be sorted by date (earliest first), and log feed type. The total number and values in the reason fields equal the totals in the Asset Session summary.

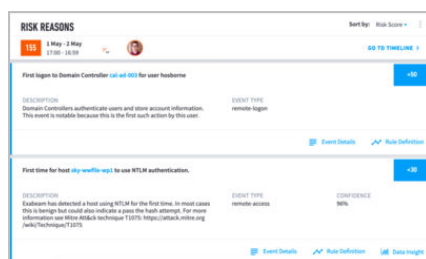
At the top, next to the Session start and end times, you will notice some smiling faces:

Get Started with the Asset Page



These are the users that had high risks scores and interacted with this asset during this Asset Session. The users are organized from highest risk score to lowest, with the top five highest user sessions highlighted. You can click on these users to see a list of their top risk reasons.

When you click on a specific risk it will expand to offer the description of the alert as well as the event type involved:

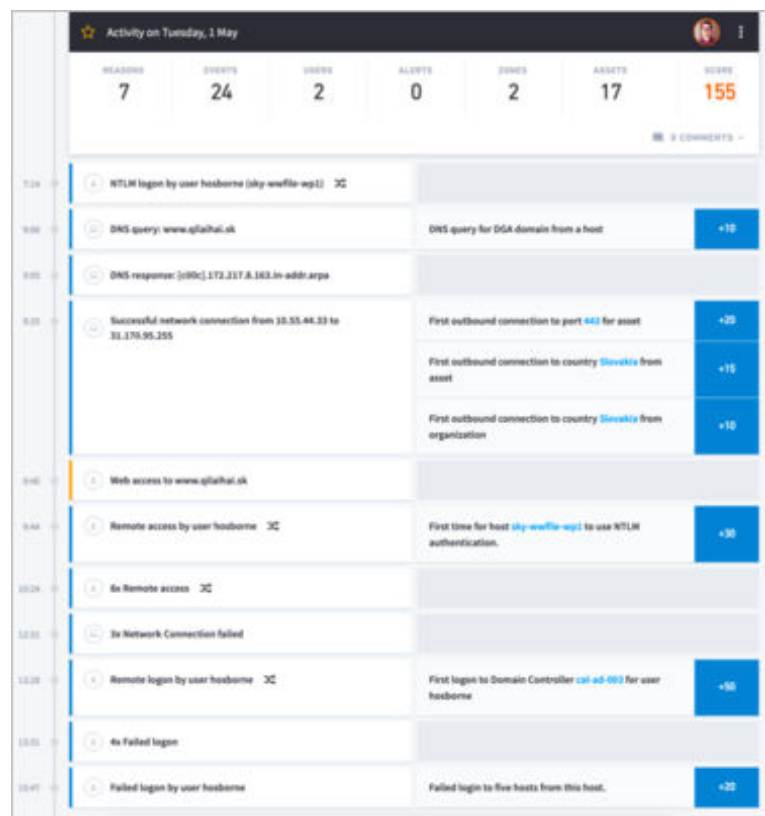


At the top right of the Risk Reasons section, note the **Go To Timeline** link. Clicking this takes you to the **Asset Session Timeline** page for the selected Session.

The vertical ellipsis to the right of the filter is where you can choose to accept the Session. Before doing so, be sure to read [Accepting a Session or Sequence](#).

About the Asset Timeline Page

This section describes the contents and capabilities of the **Asset Session Timeline** Page.



Analysts can access the **Timeline** Page by clicking on the asset score on the homepage or selecting **Go To Timeline** from the **Entity** Page.

The **Session Timeline** Page displays all the events in chronological order during the Session, so the analyst can see all events before and after a security, anomalous, or lockout event. Seeing the whole timeline helps the analyst see, for example, whether a hacker started the Session from outside the network or a legitimate user accessed the asset as part of her normal work on-site (the Entity Risk Trend in the Entity Page shows only anomalies). The timeline includes all events in that Session, whether high, low, or no risk.

NOTE

In order to ensure accuracy, the **Asset Session Timeline** is only updated once session and non-session data, such as host to IP mappings, have been processed. This can take up to two hours.

The timeline page shows all events within Asset Sessions by default. Clicking the filter icon at the upper-left corner opens a number of filter options. The analyst can choose to display User Events, Asset Events, Security Events, or a combination of all three. They can also choose to display any combination of lockouts, sequences, and feeds.

Analysts can move back and forth to other Sessions for a particular asset or user to see whether the current threat is a sudden change or has been a gradual development.

The list of events can be very long, so the Asset Session summary provides a mechanism for the analyst to jump to items of interest.

Get to Know the Asset Session Summary Page

Learn about the counters that make-up the Asset Session Summary.

The counters are for categories that an analyst might want to examine in detail. These are interactive and all-inclusive: they represent all events whether the events are benign, anomalous, or threatening.

The session summary expedites investigation. An asset session can have many thousands of events, but instead of scrolling through many screens to locate the risk-associated events, the analyst can click a counter to see a pop-up with all the events for that category. Clicking on an item in the pop-up shifts the timeline to that specific event. The choice of which count to click first can depend on previous steps, but analysts frequently start with a security event.

Details of the counters are as follows:

- **Reasons** – Reasons are details about anomalies or risks. To see the anomalies that contributed to a non-zero risk score, the analyst can click the Reasons counter. Anomalies that also were security threats are in the Security Events counter.
- **Events** – Events are the constituent activities of a session. For example, logging onto a VPN is an event, logging onto an account is an event, and sending a document to a printer is an event.
- **Users** – Users can access different facilities with different sets of logon credentials. Each set of credentials represents an account. This list shows all accounts but does not indicate a first-time use of an account or another anomaly. A first-time use will be in Reasons.
- **Alerts** – Security alert events are threats of malicious activity.
- **Zones** – Network zones are internal network locations. Exabeam and an organization collaborate to define zones during the set-up process. Zones can be cities, business units, buildings, or even specific rooms. For example, "Atlanta" can refer to a network zone in a city rather than the city (all according to an organization's preference).
- **Assets** – The number of other assets that have connected with this asset during this session. An asset can be a server, workstation, a local host computer of any type, a printer, and so on.
- **Score** – This is the total risk score for this session.

As part of an investigation, an analyst can review the timeline of a risky asset, find users that logged onto the asset at the same time and pivot to the user's timeline. This is important as you investigate threats involving lateral movement and compromised credentials.

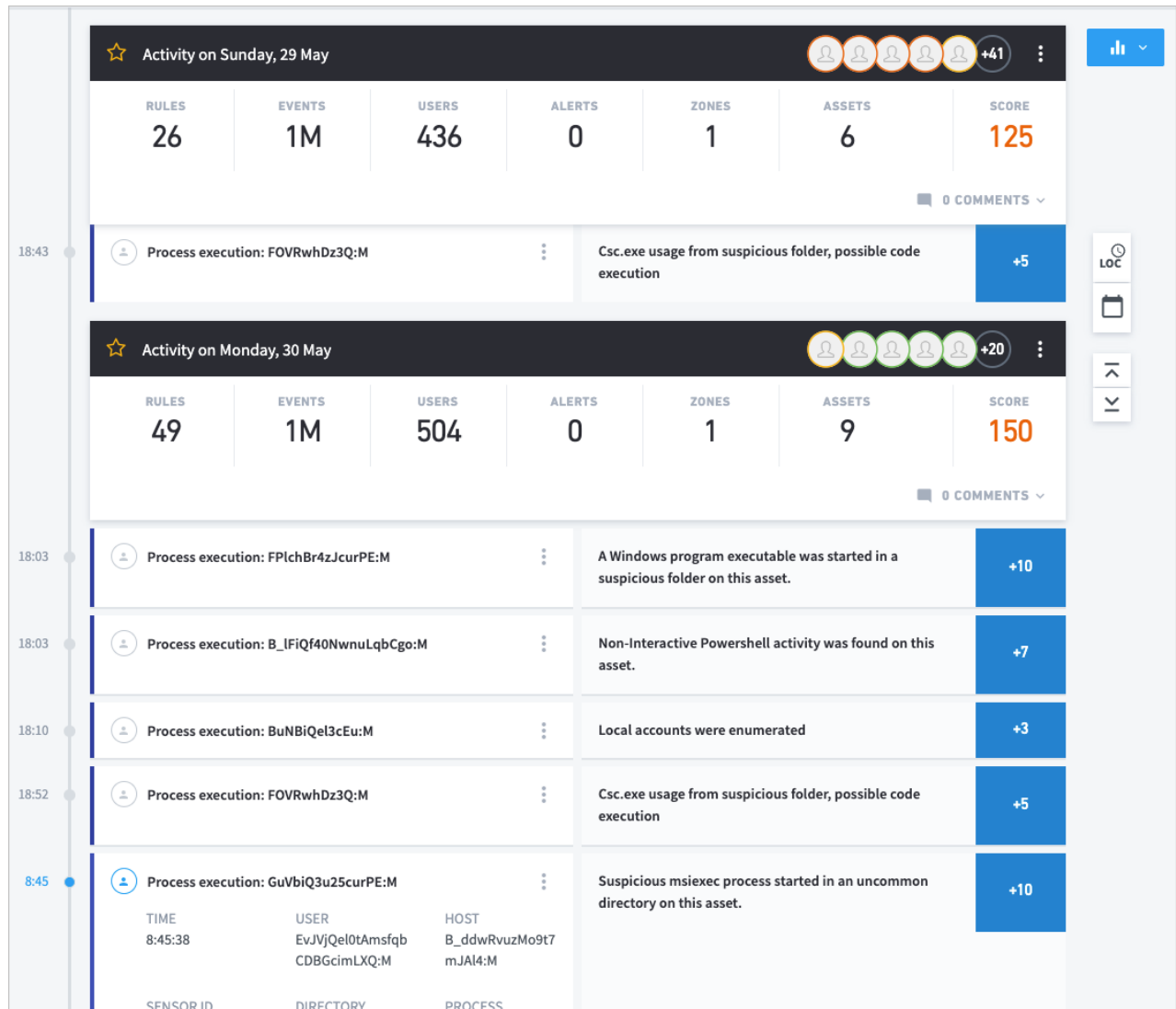
At the bottom right is the option to **Accept** the asset session. Before accepting a session be sure to read *Accepting a Session*.

From the vertical ellipsis at the top right security analysts can export the events in the session and retrieve the raw logs associated with a session within Exabeam Data Lake. These logs would typically be used to continue the incident response process and forensic work. The analyst can click a link or button in the session page that will open a Log Manager search page pre-configured with a query string that will return all log events related to the current session.

The link in the session page will only appear when the log repository is Data Lake, Splunk, or IBM QRadar.

Get to Know the Asset Session Timeline

This section details the information elements in the Asset Session Timeline.



Details for an event are on the left side of the timeline regardless of whether the event was an anomaly or a security risk. If an event also has a risk score, the details of the risk are on the right side of the timeline. Select any event to see more related details, such as User, Event Code, Destination Host, etc.

When the session timeline is opened, by default the events that earned points are expanded. We collapse events of the same type that have no score, in which case the page displays something like, "3x Remote access."

Similar to risk transfer from one user session to another, for an asset risk can be transferred from one session to the next. Risk can also be transferred from an asset to a user. For example, if a user performs an interactive login to a high-risk asset (risk score of 90 or above), a portion of the risk could be transferred to his user session.

Filter Asset Timelines

The Asset Timeline filters can be accessed to the left of the timeline. An analyst can choose to see events associated with the users of the asset, events associated to the asset itself, security alerts on the asset, or a combination of all three. Additionally, they can choose to see any combination of asset session events, lockout events, and feeds. Analysts must select **Apply Filters** before their selections are applied to the data.

When loading the **Asset Timeline** Page from the **Homepage** the default selections are:

- User Events
- Asset Events
- Security Alerts
- Session

Selecting the **Reset** button at the bottom of the filter will reset to these selections.

Accept a Session, Export Events, Create Incidents, and Load Search Parameters From the Asset Timeline

When reviewing events in the Asset Timeline, click the three dots icon to use available actions, including:

- **Accept** – Accept a portion of or an entire session.
- **Export Events** – Export the session events as a .csv file.

The available actions depend on additional Exabeam modules or log integrations, such as:

- **Create Incident** – Create and send an incident to Incident Responder. This option is only available if your Advanced Analytics deployment has an added Case Manager license.
- **Elasticsearch Logs** – Load the Elasticsearch search parameters and link directly to your Elasticsearch console. This option is only available if your Advanced Analytics deployment has integrated with Elasticsearch.
- **Splunk Logs** – Load the Splunk search parameters and link directly to your Splunk console. This option is only available if your Advanced Analytics deployment has integrated with Splunk.
- **QRadar Logs** – Load the QRadar search parameters and link directly to your QRadar console. This option is only available if your Advanced Analytics deployment has integrated with QRadar.

Get Started With the Threat Hunter Page

Navigate to the Threat Hunter Page

You can navigate to the **Threat Hunter** page by entering an advanced search in the **Search** field at the top of any page. An analyst can click on the triangle located in the search box at the top of the page. This opens an extensive drop-down menu (as in the image below) with three tabs along the left that allow you to navigate between the **Threat Hunter Search Menu**, **Saved Searches**, and the **Search Library**.

Search in the Threat Hunter Page

Within categories, the search is an 'or' function. For example, if you were to select both Symantec Endpoint Protection and FireEye MPS, your results would list all sessions and sequences that contained Symantec Endpoint Protection alerts or FireEye alerts or both. The exception to this is the Activity Types category, where the operation is 'and'.

Across categories, the search is an 'and' function. For example, if you were to enter the dates 07/01/2015 through 07/31/2015 and FireEye MPS as a Security Vendor, you would return a list of sessions that began in the month of July and also included a FireEye alert.

The date field is mandatory for the system to return results. By default, the Last Day is selected for the timeframe that searches for matching results in the last 24 hours. There is no limit to the number of criteria that can be entered in each category - with the exception of Dates, Accepted Activities, and Risk Scores. For example, Barbara Salazar, Luis Pruitt, and Keith Cook can all be entered under Users. This search would return all existing sessions for all three users. Note that User Label and Asset Label searches are case sensitive.

Search results will appear on a new page and can be sorted by

- **Risk Score** (beginning with the highest score and the rest following in descending order)
- **Date** (beginning with the most recent result first and the rest following in descending order)
- **User** (alphabetical by first name)

Results can be further refined with the filters on the left. If multiple containers (session or feeds) match your search, then your results will be shown in tabs. The maximum number of results that will be returned is 10,000 sessions.



NOTE

If the number of results returned exceeds the maximum limit, then the result counts on the left panel will not be accurate since they do not include the extra results over the maximum limit. You must narrow your results by selecting additional filters for the counts to be accurate.

Above the search results, all of the search criteria for the current search are listed. To begin a new search from scratch, click on the triangle in the search box at the top of the page.

Threat Hunter Support for Entity Analytics

Advanced Analytics includes the Asset Sequences in Threat Hunter's search capabilities.

Threat Hunter results encompass both Asset Sessions and User Sessions. For example, if the selected date range is 'Last Day' and the selected Activity Type is 'Security Alerts', then the search results will show all of the User Sessions and Asset Sessions that have had security alerts in the past day.

When search results include both Asset Sequences and User Sessions, the two will be differentiated in separate tabs. By default, the top 100 returned sessions are sorted by risk score.

Under the **Reasons** drop-down panel we have introduced a new icon to help quickly differentiate between User Sessions and Asset Sessions.

Save Search Criteria

Saved Searches are found in the second tab of the **Threat Hunter** drop-down menu.

Saved searches can be shared among other security analysts and engineers without the need for team members to re-create the search independently or from scratch. This allows a threat hunt, that your security team deems important, to be created and then shared and executed quickly.

From the search results page, you have the option to select **Save**, **Save As**, or **Export**. **Save** allows you to save a new search or update an existing saved search; **Save As** will copy an existing saved search and from there you can save any updates with a new name (after saving, this search can be found under the **Threat Hunter > Saved Searches** tab; with the **Export** option you are able to export all of the search results as a CSV file.

Selecting any of the Saved Searches from the **Saved Searches** or **Exabeam Search Library** tab will populate Threat Hunter with that criteria and return results.

For more information on how to configure roles and views, see [Managing Saved Searches](#).

Managing Saved Searches

Threat Hunter searches can be shared with other Advanced Analytics users in particular roles. By default, save searches are **Public**, which does not mean all users can view the search but that those with roles with all of the following search permissions will be able to view saved searches:

- **Manage Search Library**
- **Threat Hunting**
- **View Search Library**

A user who can view and copy a search created by another user, will not be able to edit the original saved search. For more information on configuring user view access, see [Configure User Roles to View Saved Searches](#)

Configure User Roles to Create Shared Saved Searches

Only user roles with all Threat Hunter search permissions can create and save searches that can be shared with other analysts.

1. Go to **Settings > User Management > Roles**.

2. Select the role you want to configure or **Create Role**.
3. Go to the **Search** section and then select **Manage Search Library, Manage Threat Hunter Public searches, Threat Hunting**, and **View Search Library**.
4. Click **Save** to apply the changes.

Configure User Roles to View Saved Searches

User roles, by default, do not have permission to view saved searches. With viewing permission, the user can also create copies of saved searches to make changes to.

1. Go to **Settings > User Management > Roles**.
2. Select the role you want to configure or **Create Role**.
3. Go to the **Search** section and then select **Manage Search Library, Threat Hunting**, and **View Search Library**.
4. Click **Save** to apply the changes.

Configure Which Saved Search to Share

When you have created and saved your search, you can set which saved search you want others to view. By default, your saved searches are **Public**. Users with roles that have all of the following permissions may share saved searches:

- **Manage Search Library**
- **Manage Threat Hunter Public searches**
- **Threat Hunting**
- **View Search Library**

While roles with the following permissions may create **Private** searches and use saved searches made public by others.

- **Manage Search Library**
- **Threat Hunting**
- **View Search Library**

Though your entire saved search collection is shared at first, you can selectively configure which saved search is shared.

1. Click the **Search** icon.
2. Click **Threat Hunter** to expand the menu.
3. Go to the **Save Searches** tab. Two categories are displayed, **Public** and **Only me**, which shows the current share type.
4. Find the saved search you want to configure. Click the **vertical ellipsis** to expand the menu and then select **Edit**.
5. Click to expand the share menu and then select the share type.

6. Click **SAVE** to apply the changes.

Copy a Saved Search

You cannot edit saved searches created by others or found in the Exabeam Search Library. However, you can make a copy of a saved search to reconfigure.

1. Click the **Search** icon.
2. Click **Threat Hunter** to expand the menu.
3. Go to the **Save Searches** or **Library** tab.
4. Find the saved search you want to copy. Click the **vertical ellipsis** to expand the menu and then select **Copy**.
5. Enter a new **Title** for the copied search.
6. Click **SAVE** to apply changes.
7. The copied search is saved as a Public search. To change the share setting, see [Configure Which Saved Search to Share](#).

Delete a Saved Search

Other Advanced Analytics users with view permission to saved searches cannot delete saved searches you created, with exception of those with administrator privileges and those with all the following permissions in their roles:

- **Manage Search Library**
- **Manage Threat Hunter Public searches**
- **Threat Hunting**
- **View Search Library**

1. To delete your saved search, click the **Search** icon.
2. Click **Threat Hunter** to expand the menu.
3. Go to the **Save Searches** tab.
4. Find the saved search you want to delete. Click the **vertical ellipsis** to expand the menu and then select **Delete**.
5. Confirm by clicking **Delete** to remove the search from the library.

View Pre-Configured Searches Using the Exabeam Search Library

The Search Library is the third tab of the **Threat Hunter** drop-down menu and is a collection of pre-configured Exabeam searches.

These cannot be edited or deleted. However, if you would like to customize the Exabeam searches, you can select **Copy** from the item menu and then modify the search criteria.

Exabeam ships with the following out-of-the-box searches:

- **Notable Sessions with Security Alerts**

- This search identifies all security alerts that occurred in the previous 24 hours. This search will help an analyst quickly identify third-party security alerts.
- **Notable Sessions with Account Management**
 - This search identifies risky account management behavior, typically performed by privileged users. This search identifies the following Risk Reasons that occurred in the previous 24 hours:
 - First account management activity from zone
 - First account management activity from asset
 - First account creation activity for peer group
 - First account group management activity for peer group
 - First account management activity for user from asset
 - First account group management activity for peer group
- **Notable VPN Sessions**
 - This search identifies Risky VPN behavior from someone connecting from outside the organization. It identifies the following Risk Reasons that occurred in the previous 24 hours:
 - First VPN connection from country
 - Abnormal VPN connection from country for organization and group
 - Abnormal VPN start time
 - First VPN connection from device for organization
 - VPN connection using a disabled account
 - VPN access by privileged user
 - VPN access by service account
- **Notable Sessions Containing Data Ex-filtration**
 - This search identifies all Data Ex-filtration activities that occurred in the previous 24 hours. These events may be an indication that a user is attempting to appropriate sensitive information.
- **Notable Sessions Containing Executive Assets**
 - This search identifies risky behavior that may indicate someone is attempting to access privileged resources. It identifies the following Risk Reasons that occurred in the previous 24 hours:
 - First VPN connection for service account
 - First access/logon from an asset for a service account
 - Interactive logon using a service account
- **Notable Failed Logons**

- This search identifies all users who had an abnormal number of failed logon activities in the previous 24 hours. Excessive failed logons can be an indication of that credentials may have been compromised or there has been a privilege escalation attempt.

Search for Assets Associated With an IP Address

Exabeam keeps track of the IPs that are assigned to each asset over time. This allows an analyst to perform searches related to IP-asset associations. For example, if an analyst receives a malware alert with an IP and a timestamp from a security product in the SIEM, he can find the specific asset that has this IP address at that point in time. He can then view the user sessions that connected to this asset and even specify only those sessions where the asset was the source or destination.

From the basic search bar, you can enter the IP address of interest, returning a list of all the assets that have been attributed to that IP in the past.

Selecting **View All Assets Associations** at the bottom opens a new pop-up window that contains all of the assets associated with the IP Address, as well as the timeframes during which they were assigned.

Clicking the **View Sessions** icon on the right will take you to the session timeline in which the asset was featured.

Search Histograms Using the Data Insights Page

You can navigate to the Data Insights page from the hamburger menu at the top right corner of the homepage. The **Data Insights** page allows you to search for histograms by Model Name or Grouping Feature Value (GFV). Searching by Model Name produces all the histograms that utilize the specified model. For example, to search for histograms that model remote logons, search 'Remote Logon' and select the desired model.

Searching by GFV yields all histograms that model the specified scope. For example, searching 'Sales' returns all histograms that model the users within the Sales group.

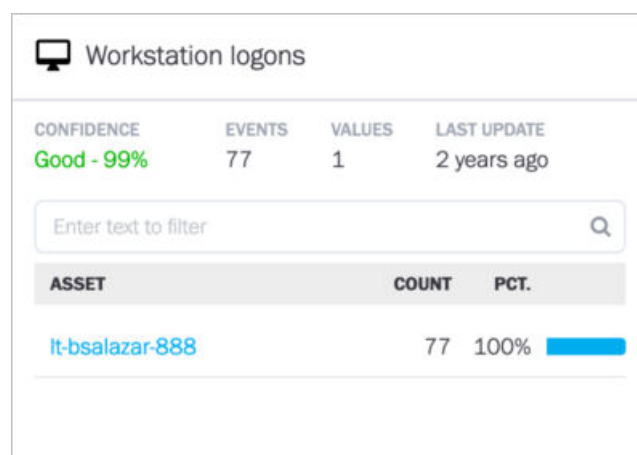
Types of Histograms

Each histogram has one of several possible templates or presentations. This section describes each histogram type. The presentation types are as follows:

- **Table Histogram:** presents a list of values and the number of times they were observed.
- **Time of Week:** shows blocks of time during the day on one axis, plotted against the days of the week.
- **Cluster Histogram:** uses a bar to represent ranges of values that constitute a cluster of events.
- **Map (of the world):** which, for example, can show countries from which a VPN session was started.

Table Histogram

The table histogram view is used to present categorical histograms. Categorical histograms contain lists of non-numerical data, for example, a list of assets or a list of network zones. The example for a table histogram is the Asset-workstations histogram:



This histogram lists all the workstations that User Barbara has logged into.

The top row shows the confidence level Exabeam has for this data (the confidence determines whether Exabeam uses this histogram for anomaly detection; under 80% is not used). The top row also shows a value—one workstation in this case—that Barbara logged into. This number is the

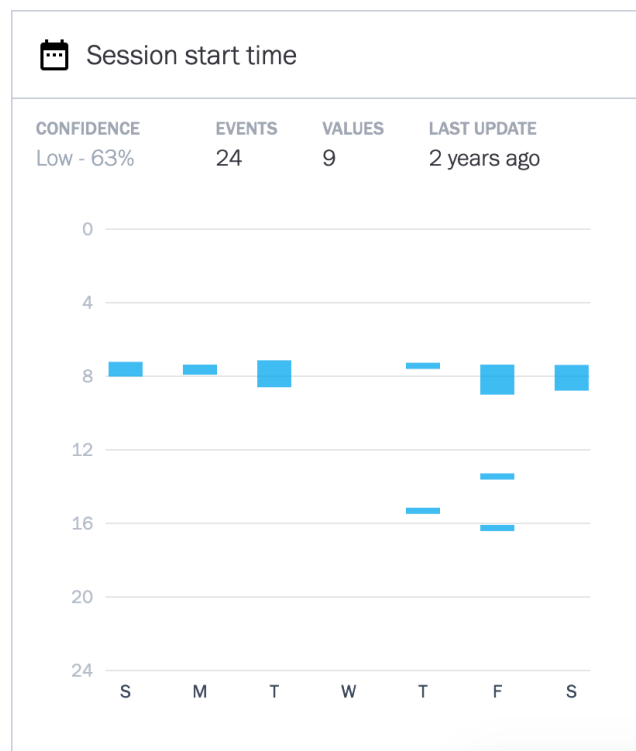
total number of unique assets in the histogram. (In other histograms, the total is for the subject of that histogram.) The Entries value in this example means the total number of times that this user has accessed the asset (77 times). Last Update shows when the histogram was last updated.

The filter box in the next row is for narrowing the scope of the histogram’s display. As representations of all of a user’s activities, histograms potentially can have hundreds of entries.

The lower part of the histogram gives details. It identifies each asset by name, the number of times each workstation was accessed, and the percent of the total accesses that each workstation represents.

Time of Week

This time of week example shows the number of different start times (25) and the total number session start times (52) during the week. The confidence is low, indicating there is not enough information.



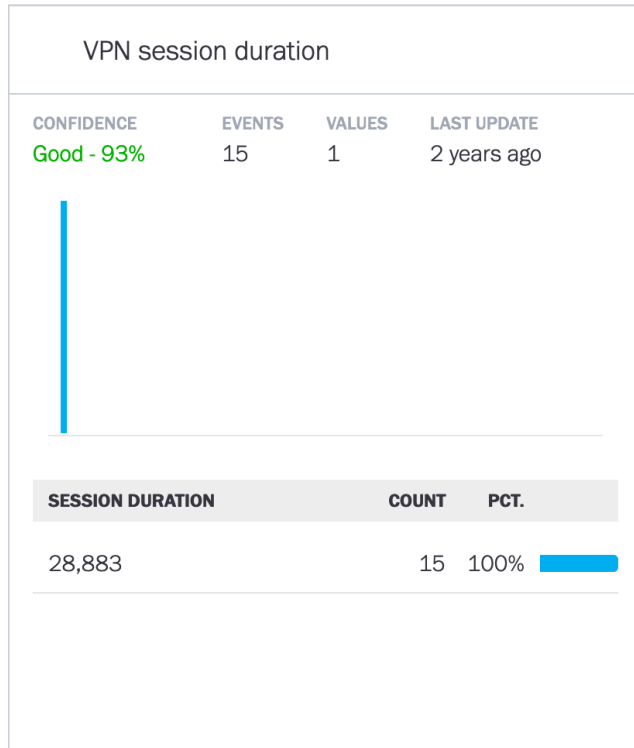
Cluster Histogram

The cluster histogram represents a group of events by a bar, where group is a range of values for an activity. In the example of the start-time histogram in this image, the groups are ranges of hours in which the user starts a session (in another cluster histogram, a group could be the typical set of assets rather than start times). The confidence is high for this histogram, so Exabeam can use it for anomaly detection.

The height of the bars reflects the numbers for session starts in that cluster’s range.

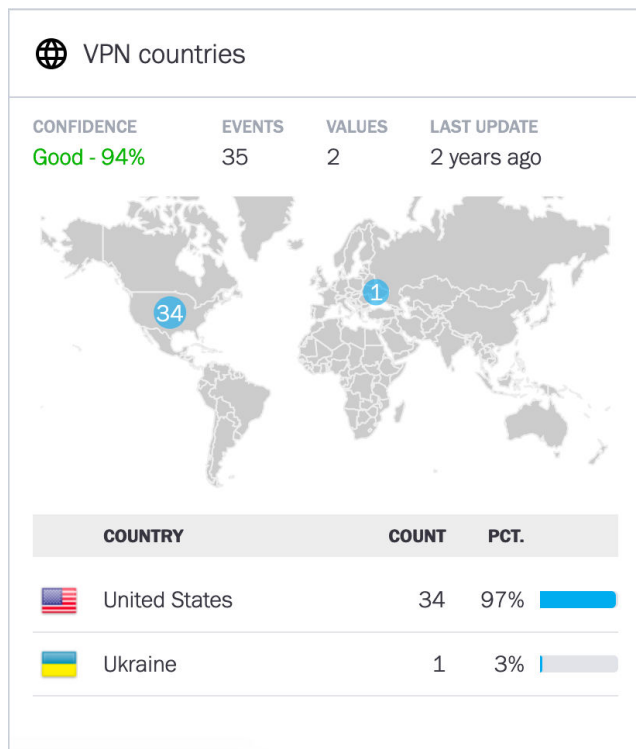
The Values number of 2 means that this user has two different ranges of time that he or she has started all sessions. Visually, the range of each cluster is represented by the width of the bar. The numerical value for the range is represented in the graph but enumerated below the graph.

One range for start times in this example is 5 am – 8 am, and there is a single instance of starting at 1500 hours (3 pm). For 99% of the sessions, the user has started the sessions in the morning hours. The single instance of a 3 pm start is the very small bar at the far right on the horizontal axis.



Map Histogram

The map histogram is a map of the world. In this image, the user has logged onto a VPN from one country, so the Values column shows a 1. The Entries column has 27 to show the number of times this user has logged onto a VPN.



About the Session Data Insights Panel and Page

The **Data Insights** button is in the upper-right corner of a **User Page** or **Session Timeline Page** – selecting it reveals the **Data Insights** drop-down panel:

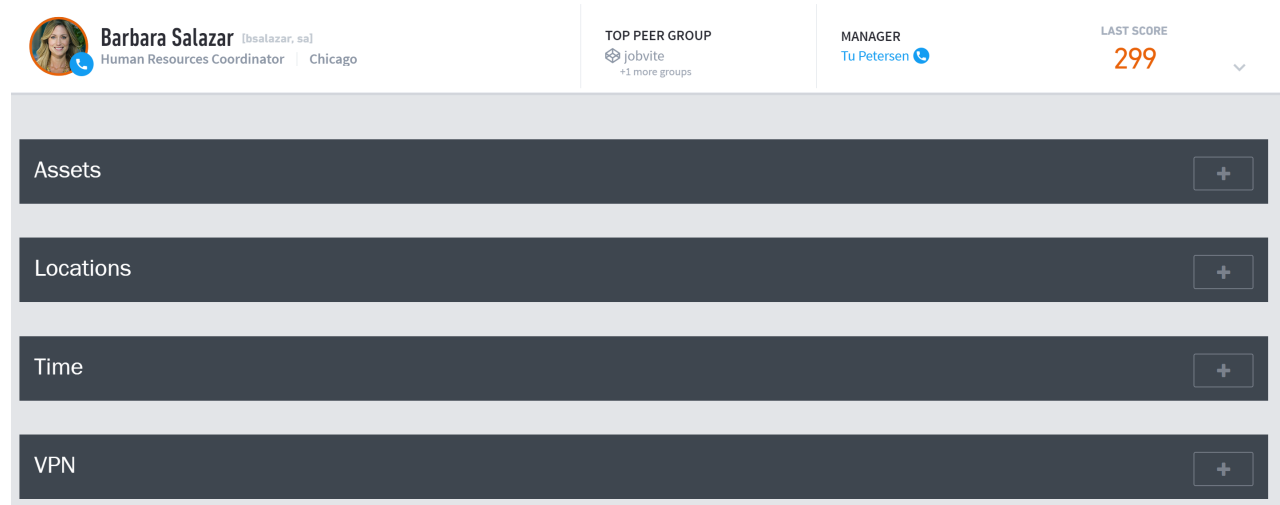
The panel view gives a summary of a user’s workstations, assets, zones, countries, and active/inactive times. Hovering over the **Time of Week** histogram gives more details into the times that the user was active.

Data Insights is a multi-level page that displays histograms (high-level data models) that summarize a user’s activities.

Navigate to the Session Data Insights Page via the More Insights Button

The **More Insights** button at the bottom of the **Session Data Insights** panel gives access to the complete **Data Insights** page of the user. When an analyst clicks **More Insights**, the default display is the Assets category. This image shows the collapsed categories selection rather the default of Assets:

Search Histograms Using the Data Insights Page



The screenshot shows the top section of the Exabeam Data Insights page. On the left, there is a user profile for Barbara Salazar (lbsalazar, sa), Human Resources Coordinator in Chicago. To the right, it shows the user's 'TOP PEER GROUP' as 'jobvite' with '+1 more groups', and their 'MANAGER' as 'Tu Petersen'. A 'LAST SCORE' of 299 is displayed in orange. Below this header, there are four dark grey horizontal bars, each representing a histogram category: 'Assets', 'Locations', 'Time', and 'VPN'. Each bar has a small plus sign icon on the right side, indicating it can be expanded.

The plus or minus sign near the right edge of the Insight choice is for opening or closing the display for that category of histograms.

The histograms in Data Insights fall into the following main categories:

- **Assets** – computers or devices accessed in the user's sessions
- **Locations** – network zones or other geo-location related information
- **Time** – session duration or start and end time histograms
- **VPN** – remote access VPN related models
- **Identities** – secondary accounts and credentials of the user
- **Other Insights** – all other activity for the user

Monitor Exabeam Processes Using the System Health Page

System Health monitors Exabeam's various processes and assists Exabeam engineers with troubleshooting. You can navigate to the **System Health** page from the menu icon at the top right corner of the homepage.

System Health is broken down into two sections: **Health Status** and **System Activity**.

System Activity shows each stage of the Exabeam pipeline and its current status. Expand any section to see more details about the state of a particular procedure.

Health Status is an on-demand assessment of the Exabeam pipeline. It is broken down into three categories:

- **General Health** – General health tests that all of the back-end services are running - database storage, log feeds, snapshots, CPU, and memory.
- **Connectivity** – Checks that Exabeam is able to connect to external systems, such as LDAP and LMS.
- **Log Feeds** – This section reports on the health of the DC, VPN, Security Alerts, Windows Servers, and session management logs.

In all of the above areas GREEN indicates the status is good, YELLOW for a warning, and RED if the system is critical.

If there is a critical status on this page we recommend reaching out to Exabeam support.

Health Check

Advanced Analytics has improved the robustness of health checks by providing visibility on the backend data pipeline. All of the below health checks are configurable, please see the Advanced Analytics Administration Guide for more details.

New proactive health checks include:

- In a multi-node environment processing current logs, when the worker node is lagging more than 6 hours behind the master node, a proactive notification will appear.
- In a multi-node environment processing historical logs, when the worker node is lagging more than 48 hours behind the master node, a proactive notification will appear.
- If an environment has been configured to receive syslog, but has not been receiving them for 1 hour, a proactive notification will appear.

In addition to new health checks, the health notifications are machine parseable and formatted. The format can be defined via configuration (e.g., JSON) and each notification type can have its own format configuration. For example, you can define a different configuration for an email alert versus a syslog notification. Each health check has a clearly defined description of what is being measured, the corresponding value, as well as the alert severity.

Configure Alerts for Worker Node Lag

When processing current or historical logs, an alert will be triggered when the worker node is falling behind the master node. How far behind can be configured in `/opt/exabeam/config/tequila/custom/health.conf`. The parameters are defined below:

- `RTModeTimeLagHours` - During real-time processing the default setting is 6 hours.
- `HistoricalModeTimeLagHours` - During historical processing the default setting is 48 hours.
- `syslogIngestionDelayHour` - If processing syslogs, the default setting is 2 hours.

Disaster Recovery Health Alerts

For organizations that employ a disaster recovery configuration, on-demand and proactive health alerts are provided in the Health Page of Advanced Analytics.

Health Checks:

- Progress of the replication between the primary and secondary clusters.
- Status of the replication service and the most recent timestamp of replication for the different replication components.
- The Disaster Recovery mode that the cluster is running in. Status are: Normal Mode or Failover Mode.

Health Alerts:

- Alert notification to administrators if the replication service is not running.

Alerts for Storage Use

Available on the System Health page, the Storage Usage tab provides details regarding the current data retention settings for your Advanced Analytics deployment. Advanced Analytics sends notifications when available storage capacity dwindles to a critical level. Admins have the option to enable and configure automatic data retention and data purging for both HDFS and MongoDB usage.

For more information on data retention, see [Data Retention in Advanced Analytics](#).

System Optimization

This tab is a single aggregated page for auditing and viewing disabled data types, including:

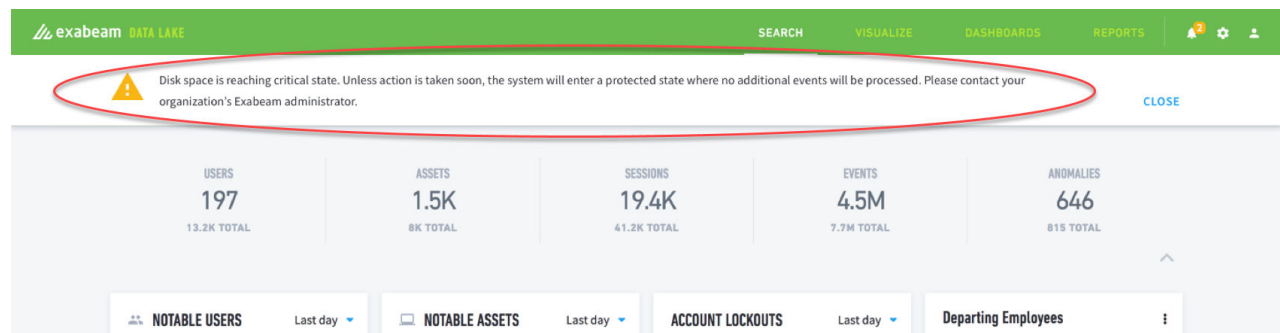
- **Disabled Models** – When a model takes up too much memory, it is disabled and listed here. Re-enabling these models can cause the system to suffer performance issues.
- **Disabled Event Types** – When a high volume user or asset amasses a large number of events of a certain event type, and that event type contributes to a large portion of the overall event count for that user the event type is automatically disabled and listed here.
- **Disabled Parsers** – Advanced Analytics automatically identifies poor parser performance and disables such parsers in order to preserve the system health.

- **System Load Redistribution** – Advanced Analytics automatically identifies overloaded worker nodes, and then takes corrective action by evenly redistributing the load across the cluster.

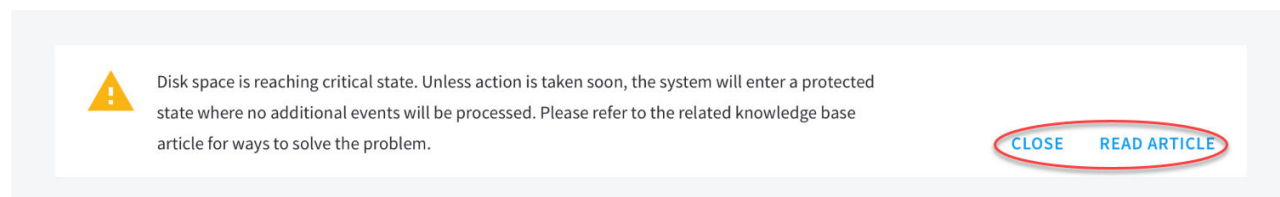
Critical Alerts, Warnings, and Error Messages

Although all notifications appear on the **System Health** page, there are two additional ways the Advanced Analytics UI provides better visibility on critical alerts, warnings, and error messages.

When a critical notification is generated, a banner will appear at the top of the UI. It contains specific information about the source of the warning or error, what the user and/or admin should do to correct the potential problem, and any helpful links to relevant knowledge base articles.

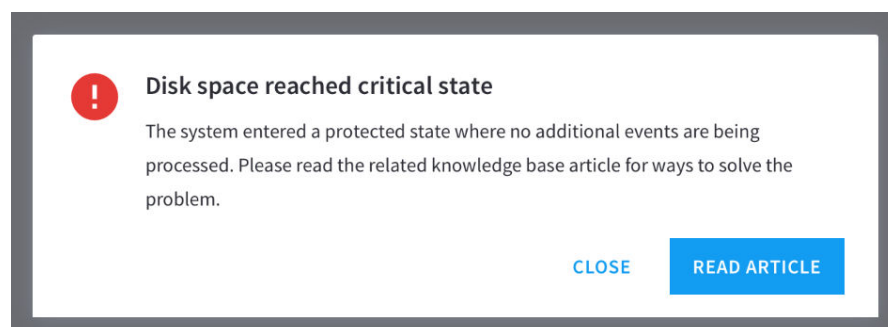


Depending on the level of the warning and user type (either administrator or user), the banner includes buttons to **Close** (i.e., dismiss) the banner and/or read an article containing important information about the message.



Additionally, a message box for critical notifications that require administrator decisions or multiple tasks to fix will appear upon admin login.

These message boxes include buttons to **Close** (i.e., dismiss) the banner and/or read an article containing important information about the message.



Contact Technical Support

To contact Exabeam Customer Support, please open a case via [Community.Exabeam.com](https://community.exabeam.com).

For more detailed troubleshooting, Administrators can also generate an output file for Exabeam Customer Support. For information, refer to the *Advanced Analytics Administration Guide*.

Licensing Options

Exabeam provides customers with two licensing options: Exabeam and Threat Hunter together, or Exabeam alone. In both cases when a license expires (a standard Proof-of-Concept license is for 30 days) the analyst will receive a warning stating that the customer does not have a valid license.

Please see *Licensing* in the *Advanced Analytics Administration Guide* for details on how to apply your license.