



Exabeam Expedition Step-by-Step Login Instructions

1. Open the Exabeam Expedition UI: <https://ctf-0-event.exalabs.io/>
2. Scroll down and open the Exabeam interface(s) you will be using in a separate tab. Your host will specify Advanced Analytics, Data Lake, or both. Return to the CTF UI when done.

Advanced Analytics

Data Lake

3. On the CTF UI, select “Register” in the top right corner.

 Register  Login

4. Create a Username (Make It Fun...But Clean!), enter your Email Address and create a Password.

User Name

Email

Password

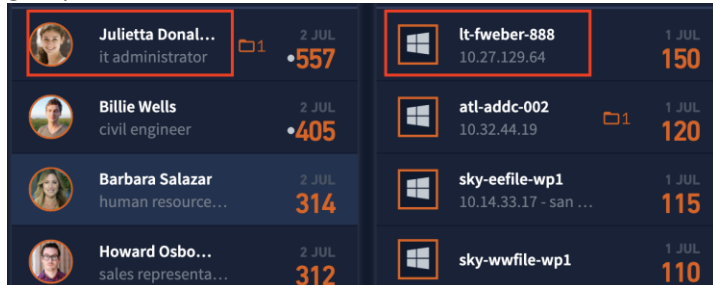
5. Select “Join Team”. Your host will provide your team logins and Exabeam UI logins when we are ready to begin.









Exabeam Expedition UI Walkthrough

Advanced Analytics - 4 workflows.

Workflow 1: Watchlist > User/Asset > Timeline

1. Click on User/Asset names to view their Context Page. This includes things like their department, manager, peer groups, user risk trend, and risk reasons.

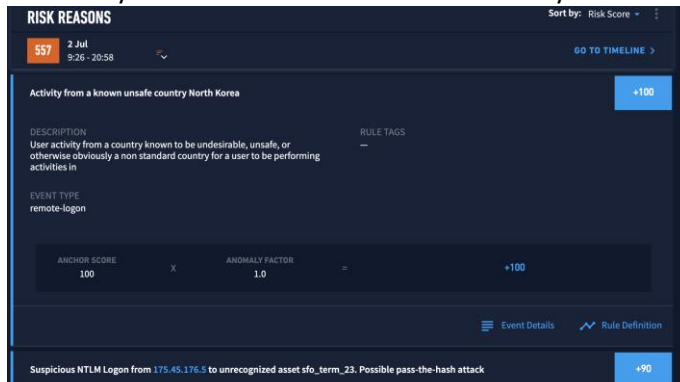


 Julietta Donal... it administrator 2 JUL •557	 lt-fweber-888 10.27.129.64 1 JUL 150
 Billie Wells civil engineer 2 JUL •405	 atl-addc-002 10.32.44.19 1 JUL 120
 Barbara Salazar human resource... 2 JUL 314	 sky-eefile-wp1 10.14.33.17 - san ... 1 JUL 115
 Howard Osbo... sales representa... 2 JUL 312	 sky-wwfile-wp1 1 JUL 110

2. Scrolling down on this page reveals the **User Risk Trend** to easily view what their risk looks like over a period of time. Clicking on any dot (session) will update how many rules, events, alerts, accounts, etc were triggered/touched that day.



3. Clicking on a dot (session) will also update the Risk Reasons below the risk trend graph. By default, this view shows all the risk reasons from the selected day in highest to lowest risk. It's a great way to get a quick idea of what risky events occurred on the selected day. Events can be expanded for more information.



RISK REASONS Sort by: Risk Score

2 Jul 9:26 - 20:58

Activity from a known unsafe country North Korea +100

DESCRIPTION: User activity from a country known to be undesirable, unsafe, or otherwise obviously a non standard country for a user to be performing activities in

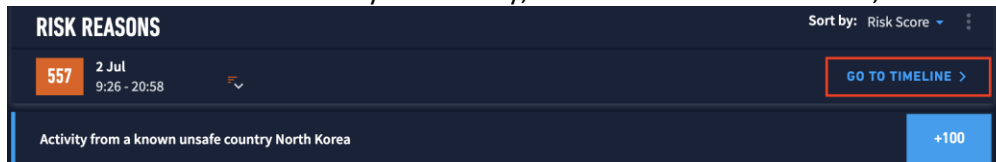
RULE TAGS: -

EVENT TYPE: remote-login

ANCHOR SCORE: 100 X ANOMALY FACTOR: 1.0 = +100

Suspicious NTLM Login from 175.45.176.5 to unrecognized asset sfo_term_23. Possible pass-the-hash attack +90

4. To view all of the user's activity for this day, both normal and anomalous, click on "Go To Timeline"



RISK REASONS Sort by: Risk Score



2 Jul 9:26 - 20:58

GO TO TIMELINE >

Activity from a known unsafe country North Korea +100

5. To go directly to a timeline from the main screen, simply click on a user/asset score.



 Julietta Donal... it administrator 2 JUL •557	 lt-fweber-888 10.27.129.64 1 JUL 150
---	--

6. From a timeline, you can see the user/asset's day in a chronological view showing all activity. On the left side, you will see the event that came into the system. On the right, you will see text and a risk number if the event on the left was risky. If there is no number/text on the right side, it indicates that the corresponding event was

normal. You can click on the text to learn more. Expanding the event on the left will provide some basic information we parsed out. Expanding the risk reason on the right will provide a basic explanation of why the event was risky, rule tags (MITRE techniques), and other useful information.

10:00	Remote access to atl-file-54	First access to atl-file-54 for Julietta Donaldson	+10	Anomalous activity
10:22	Remote access to atl-file-02			Normal activity

- Clicking on a blue hyperlink for an asset name will provide asset details, such as the operating system and top user.
- Clicking on the blue hyperlink for a risk reason will bring up the histogram (model) for this risk reason.

Assets accessed by this user remotely

Models the assets this user has accessed remotely

Model as of 2 Jul 2020	Current Model	
CONFIDENCE Low - 0%	EVENTS 440	
	VALUES 20	
<input type="text" value="Enter text to filter"/>		
ASSET	COUNT	PCT.
tk _s _en_e8b_kt	37	8% <div></div>
tk _s _en_095_kt	36	8% <div></div>
tk _s _en_131_kt	35	8% <div></div>

- Session headers (also available after threat hunting) can be used for a quick view of activity, including what risk reasons fired, or what accounts were touched during this session.

Activity on Thursday, 2 Jul Start: 9:26 End: 20:58 (11h 32m)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES
41	23	0	3	24	4

Remote login to it-jdonaldson-888	jdonaldson	ISP Total Server
Remote access to atl-file-54	jdonaldson-admin	atl-file-54 for Juliet
Remote access to atl-file-02	achen	

Workflow 2: Data Insights

Data Insights for a specific User/Asset

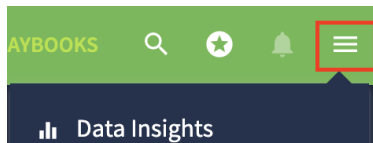


- From a user/asset page or timeline, click the Data Insights button in the top right. This will provide a quick view showing some of the models we have running in the background for this user/asset. Clicking “More Insights” at the bottom will provide a list of all active models by category. Simply expand to view the models inside. For example, the processes a user runs can be found under

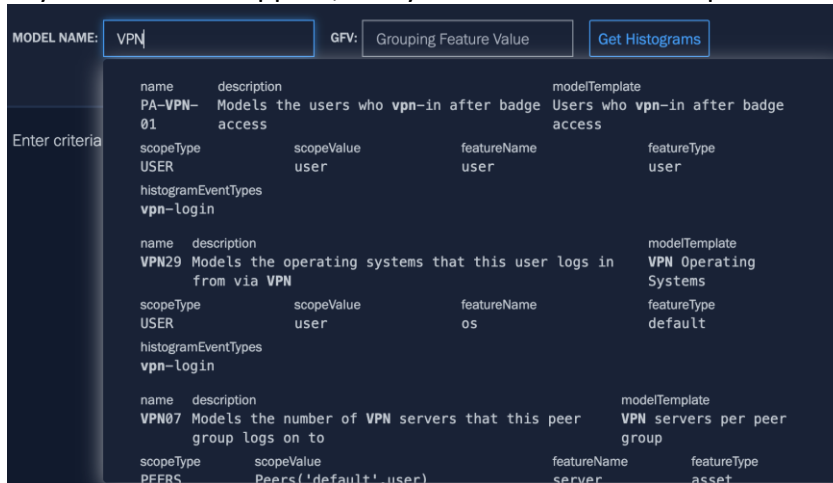
Assets	+
Locations	+
Time	+
VPN	+

Workflow 2: Global Data Insights

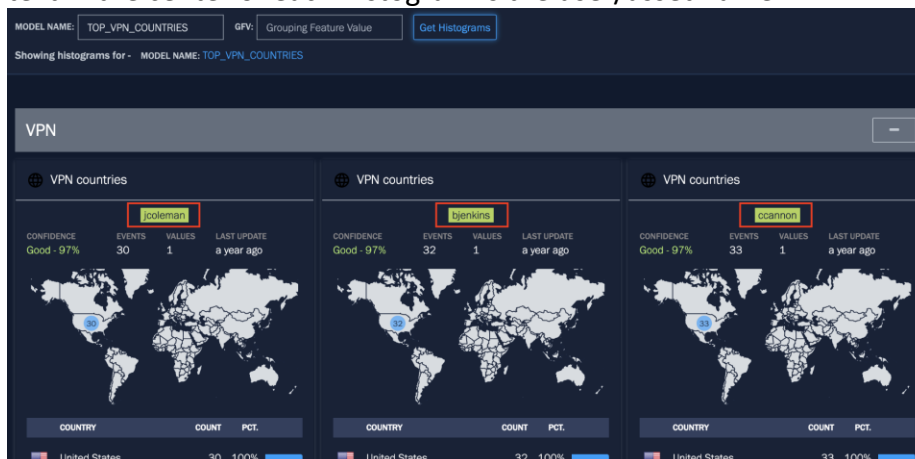
- Click on the Settings button in the top right corner, then select Data Insights.



2. Type a keyword into the Model Name field. Exabeam has type-ahead, so you don't need to memorize the models - you just need an idea of what you are looking for, such as VPN. All models with the keyword VPN will appear, and you can read the descriptions to find the one you are looking for.



3. Click "Get Histograms" to the right. You can now see this model for the entire organization - the green text in the center of each histogram is the user/asset name.



Workflow 3: Basic Search (Magnifying glass)

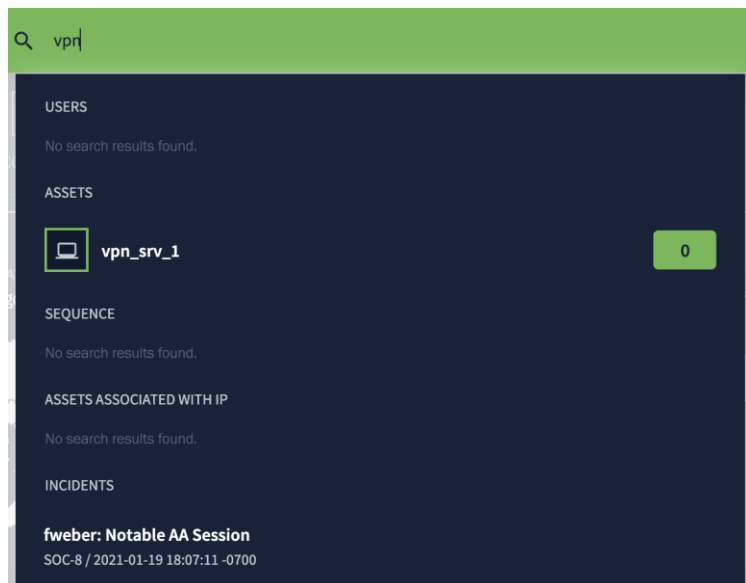
*In this environment, this search will only provide basic context details. To view a user/asset's activity, please click on them from the main page.



1. Click the Magnifying Glass icon.



2. Type your search item into the search bar
3. This search will look for users, assets, IPs, and incidents that match your search. Click on the result you want to view.



Workflow 4: Threat Hunter

Threat Hunter features a variety of categories to search data with. These all have either a drop-down menu, a selection, or type-ahead for ease of use. In this example, we will use **Reasons** to search our behavior modeling rules. Type in a keyword from the context of the question (vpn, shadow copies, dlp, job search, etc) to view the list of models and find the one that fits the question.

1. Click the Magnifying Glass icon.

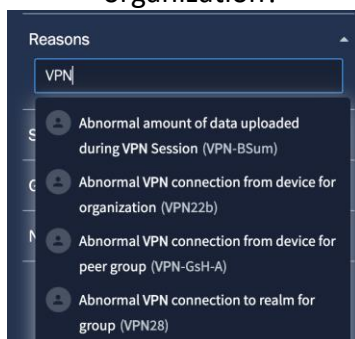


2. Click Threat Hunter

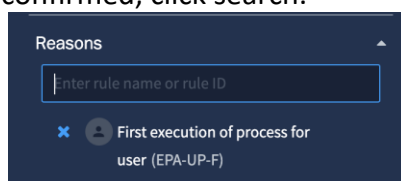


3. Click Reasons and type in a keyword.

- a. Be sure to scroll through the rules and confirm it matches the context of the question. Try to start small and add onto your searches if needed.
- b. Are we looking for a first time or something abnormal? Is it for the user, the peer group, or the organization?



4. Be sure to select the rule you want before clicking search. It should appear below Reasons. Once confirmed, click search.



- Review your results. The summary fields can be used for a quick look at things like the rules and events that fired for your search results. You can also navigate to the timeline of the day that matched your search criteria.

Dates: 06/01/2020 12:00 am - 07/03/2020 12:00 am **Reasons:** First execution of process for user (EPA-UP-F) Save

User Names (4) **Assets** (0) **Network Zones** (2) **Peer Groups** (3) **Account Names** (4) **Event Types** (2) **Rule Tags** (4)

End Point Activity (4 results) We found a total of 4 results for your search **SORT BY**

	RULES	EVENTS	DOMAINS	ZONES	SCORE
Sherri Lee sales representative 1 Jul 2020 @ 18:00	33	13	0	2	302
Fredric Weber web developer 1 Jul 2020 @ 18:00			0	0	159
Gary Hardin software engineer 1 Jul 2020 @ 18:00			0	1	126
Clifton Yu it administrator 30 Jun 2020 @ 18:00			0	1	4

Rule Names Rule Tags

Rule Name	Score
A Suspicious command that deletes shado...	+90
A Suspicious command that deletes shado...	+90
A Suspicious command that disables recov...	+40
Abnormal execution of process vssadmin.e...	+15
Abnormal execution of process bcdedit.exe...	+15
First execution of process bcdedit.exe exec...	+15
First execution of process tor.exe	+3
First execution of process testdisk.exe	+3

Go To Timeline

Example Threat Hunts

There are many categories to use when threat hunting, but the one you will use the most (especially in this event) is **Reasons**. This is where you can search our behavioral rules/models.

Maybe you want to look for a non-executive user that has logged into an executive asset after logging into VPN from China. If I want to do that in my SIEM today I need to break it into a bunch of different searches. I need to..

- Find all the users that VPN'd in from China. Get a list of those user credentials. Copy and paste these somewhere.
- Take each credential and search those VPN logs again to see when the session started and ended. Write the times down next to the users.
- Once I have the users and the timeframes from China, I'm going to search my Windows events for each user and timeframe to see if they accessed an executive asset. I also need to know what my assets and executives are. This simply does not scale well in legacy SIEM.

With Exabeam and Threat Hunter, you can simply select the following to find this information.

Reason: Non-Executive user logon to executive asset(AL-HT-EXEC)

Activity Type: VPN

Geolocation: China

First execution of process

5mb

Shadow copies

job search

CTF Gotchas

Gotchas:

- Please type in any answers that are directories - cut and paste will not work
- Use the main screen to load user/asset data. Searching for data in the basic search bar will not return data due to the way this demo system is architected. Click on Exabeam in the top left to return to the main screen.
- If using Data Lake, set the time frame back to 2 years.