Due to the processes involved it is anticipated that you will need to take an hour to complete the entirety of this process. This may take longer than that to complete but there are points where you can stop and continue later. Please budget your time accordingly.

If you need assistance or an error occurred in the testing of this product, please contact us at: danae.oconnor@ucdenver.edu or noah.warren@ucdenver.edu.

Splunk Enterprise Installation:

Overview:

This is an installation guide for Splunk Enterprise as well as for inserting a static table of data in order to fully utilize the "Threat Timeline" Splunk Enterprise visualization product.

If you already have an up-to-date installation of Splunk Enterprise, you may skip these instructions and head directly to the section labeled **"Threat Timeline Installation and Use"**.

Safety:

The sign-up process for Splunk and Splunk Enterprise requires an email, password, and some personal information. Do not share this information with anyone else to prevent security risks.

Required:

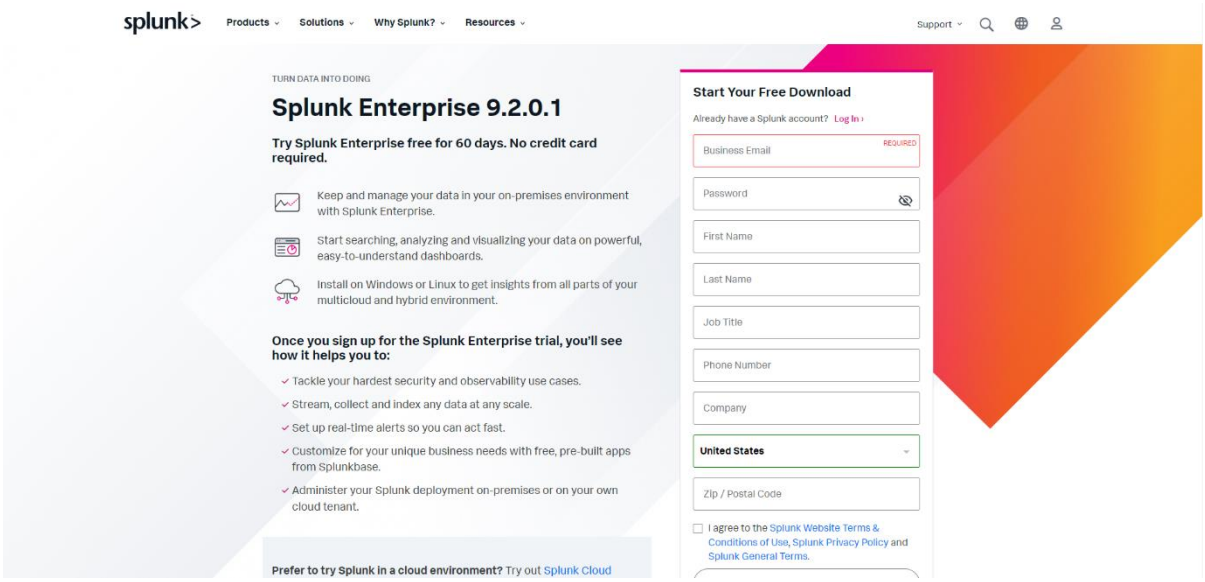
- A computer system that has an operating system of Linux, Windows, or Mac that can run Splunk Enterprise. More specific information can be found here: https://docs.splunk.com/Documentation/Splunk/9.2.0/Installation/Systemrequirements

Steps:

1. Open your preferred web-browser.
2. Navigate to the Splunk Enterprise free trial download site. You can access it using the following link:

   https://www.splunk.com/en_us/download/splunk-enterprise.html

3. You should see a screen like this:

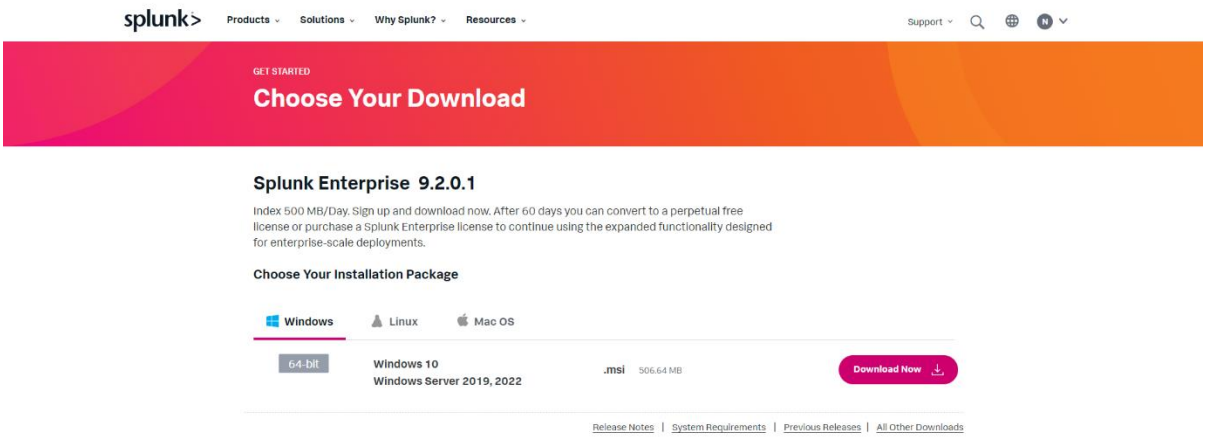


   If you already have an account with Splunk, you can click the “Log In” option next to “Already have a Splunk account”.

   Otherwise, you will need to fill out the information in the required boxes on the right-hand side of the screen as well as agree to the Splunk terms and conditions by clicking the checkbox below the required boxes.

   Make sure you write down your Splunk Login information. You will need this later to log into Splunk Enterprise and use the application.

4. Once you have created your Splunk account, you will be brought to a page that looks like this:



You'll notice there are various installation options dependent on whether you have Windows, Linux, or Mac. Choose the option appropriate for your machine's operating system and choose "Download Now".

5. After downloading, run the obtained file and follow the onscreen prompts to install Splunk Enterprise. If the Splunk Enterprise download prompt asks for another username and password for set-up – write this information down as it will be used to log you into Splunk Enterprise.

   If you require additional help more information can be found at: https://docs.splunk.com/Documentation/Splunk/9.1.2/SearchTutorial/InstallSplunk

This is a point where you can stop and come back later.

Threat Timeline Installation and Use

Overview:

This is a guide on the installation procedures and the use of the Threat Timeline Splunk Enterprise visualization. The visualization will let you see the cyber-threats from a csv file that is within Splunk in an organized manner by having the data represented by tactics used for the cyber-attacks.

Safety:

The sign-in process for Splunk Enterprise requires your Splunk username and password. Do not share this information with anyone else to prevent security risks.

Required:

You already have an account set up with Splunk.

Splunk Enterprise has been installed for your device.

You have the Threat_Timeline.tar.gz file from the email you received from us.

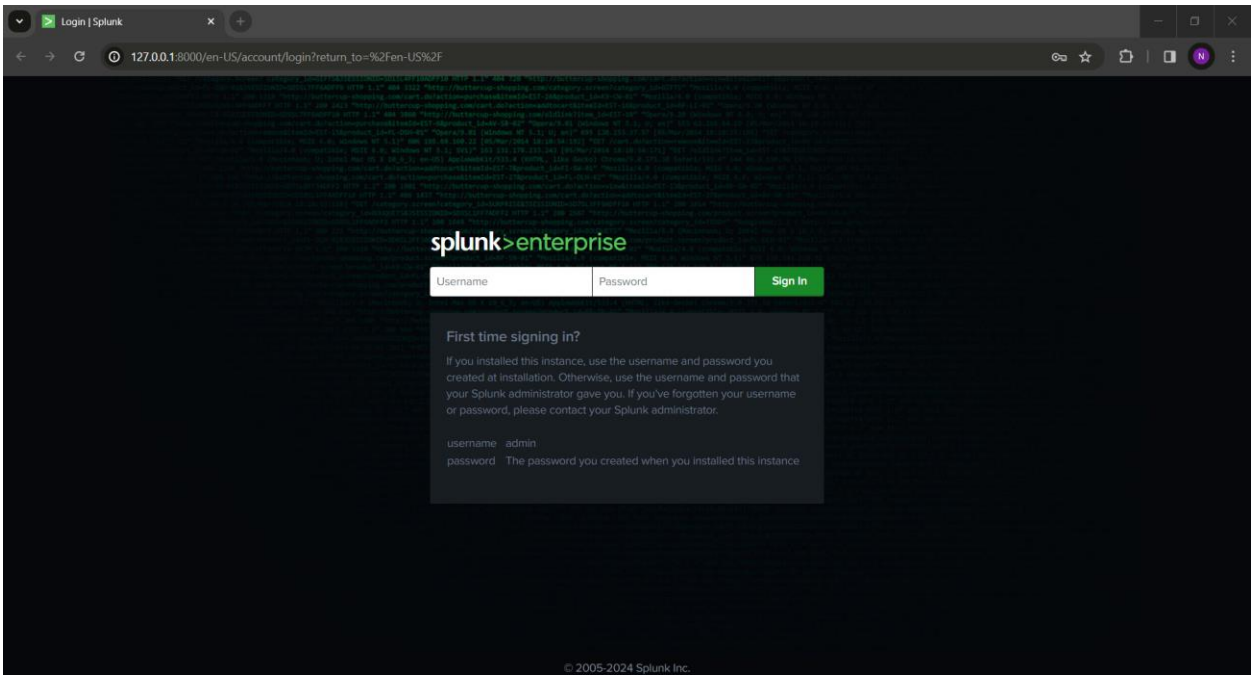
You have the sparse.csv and the dense.csv files from the email you received from us.

An input lookup file, with the required data fields already in Splunk Enterprise.

Steps:

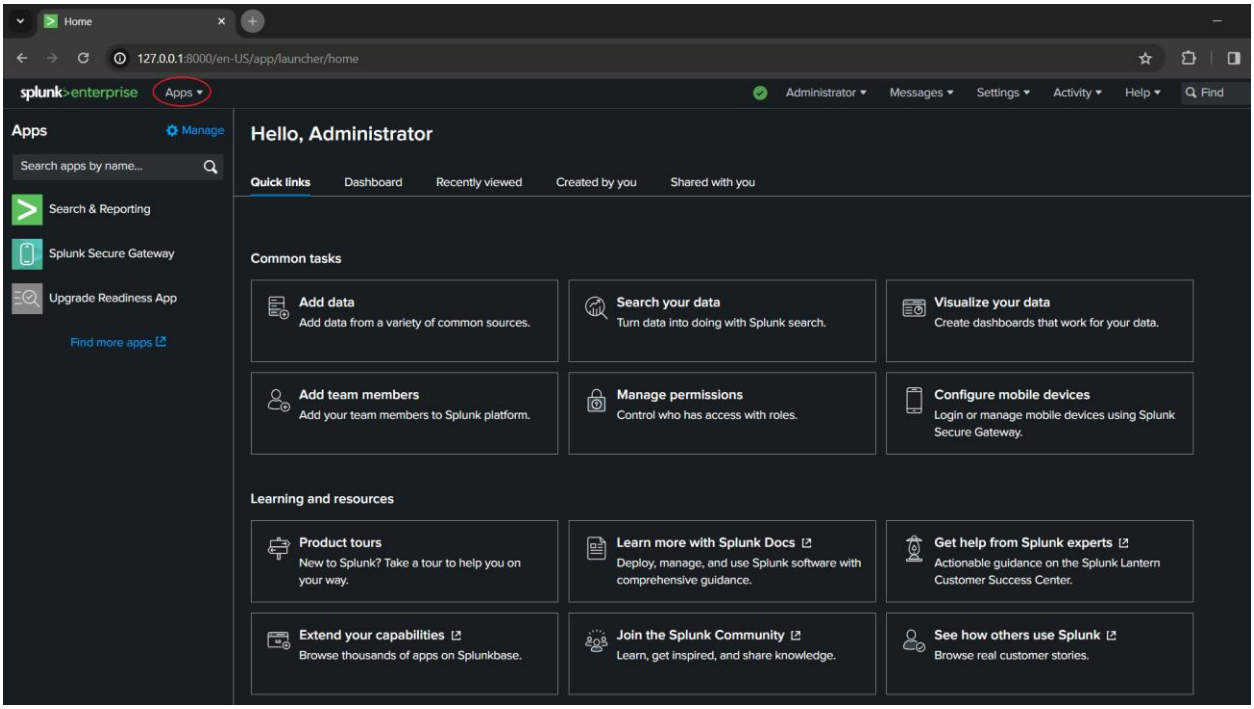
Installation of the Application:

1. Open Splunk Enterprise. You will be brought to a login screen that looks like this:

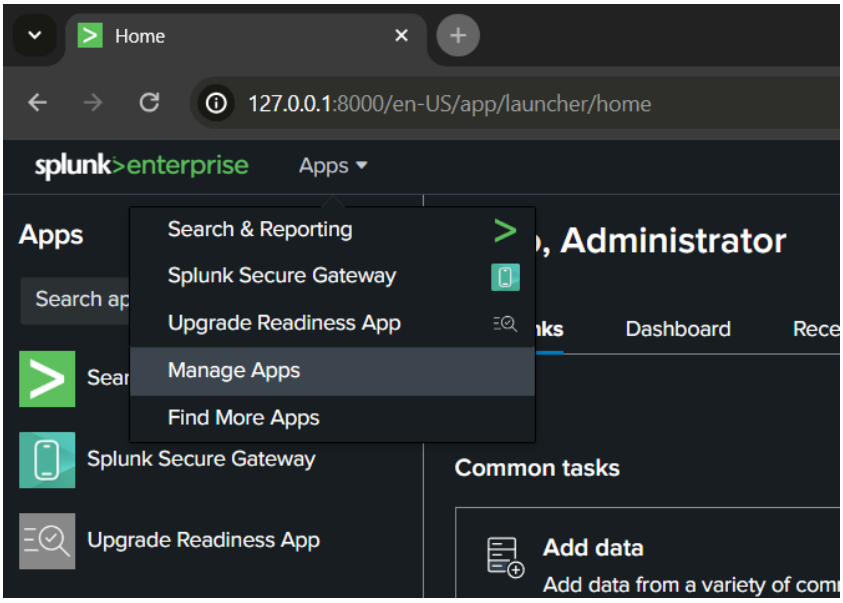


Enter the username and password you registered with when installing your Splunk Enterprise application and click the “Sign In” button to Log in.

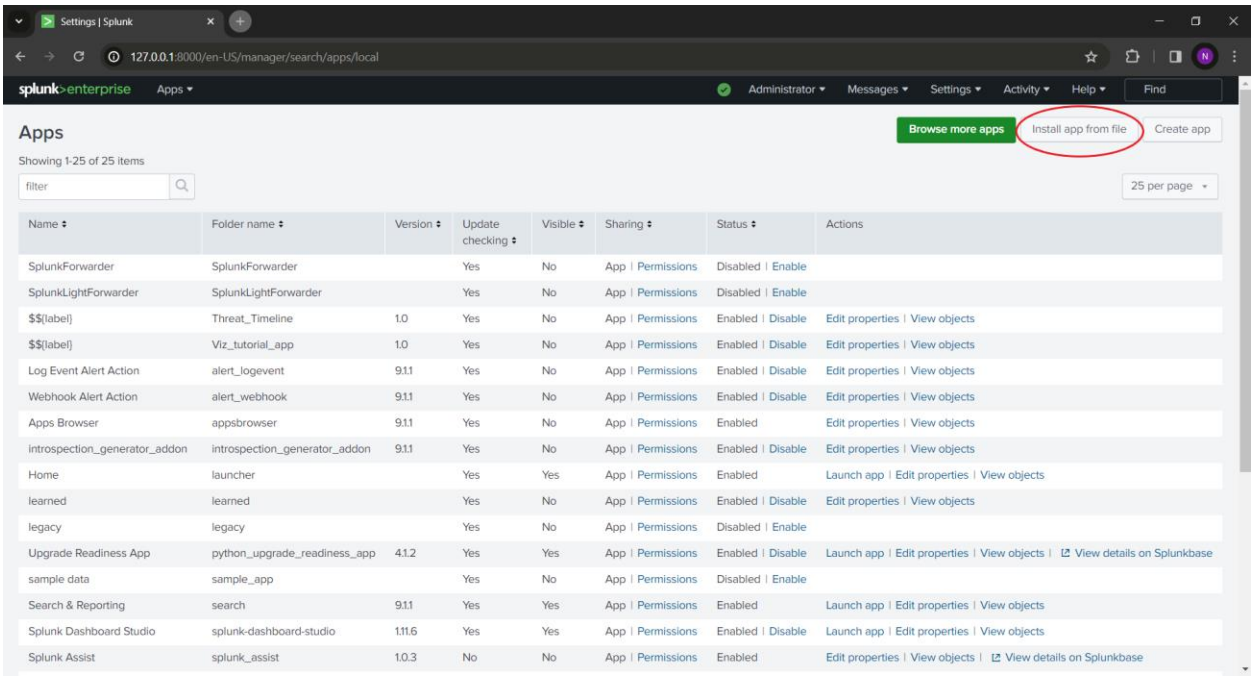
2. Once you have logged in, you will be brought to Splunk Enterprise’s Home Page. From here, click on “Apps” selection next to the Splunk Enterprise logo in the top-left corner.



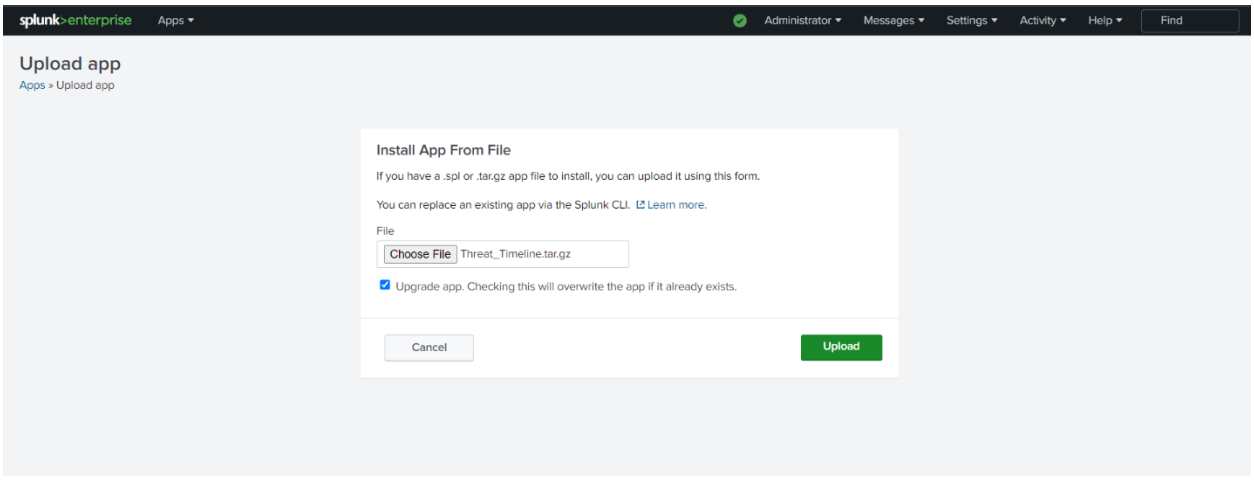
3. From the “Apps” dropdown menu, select “Manage Apps”



4. Click on the “Install app from file” button next to the “Browse more apps” button in the top right corner of the screen.



5. Click on the file selection tool that should say either “Browse…” or “Choose File…” in the prompt, navigate to the Threat_Timeline.tar.gz file and select the file.
6. With the file selected, click on “Open” in the bottom right of the file selector window.
7. Under the file selection, click the box labeled “Upgrade app.” Your screen should now look like below:



8. Click on the green "Upload” button of the prompt.

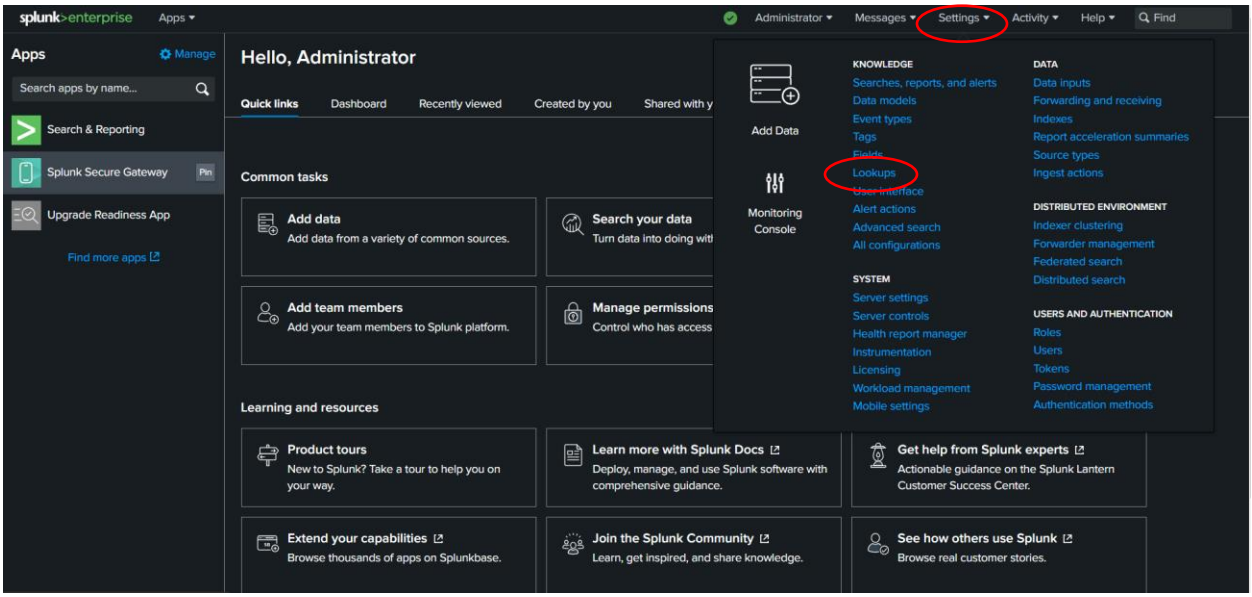
Splunk will now install the Threat Timeline application into your Splunk Enterprise installation.

9. Click on the “splunk>enterprise” logo in the top left corner to return to the Home page.

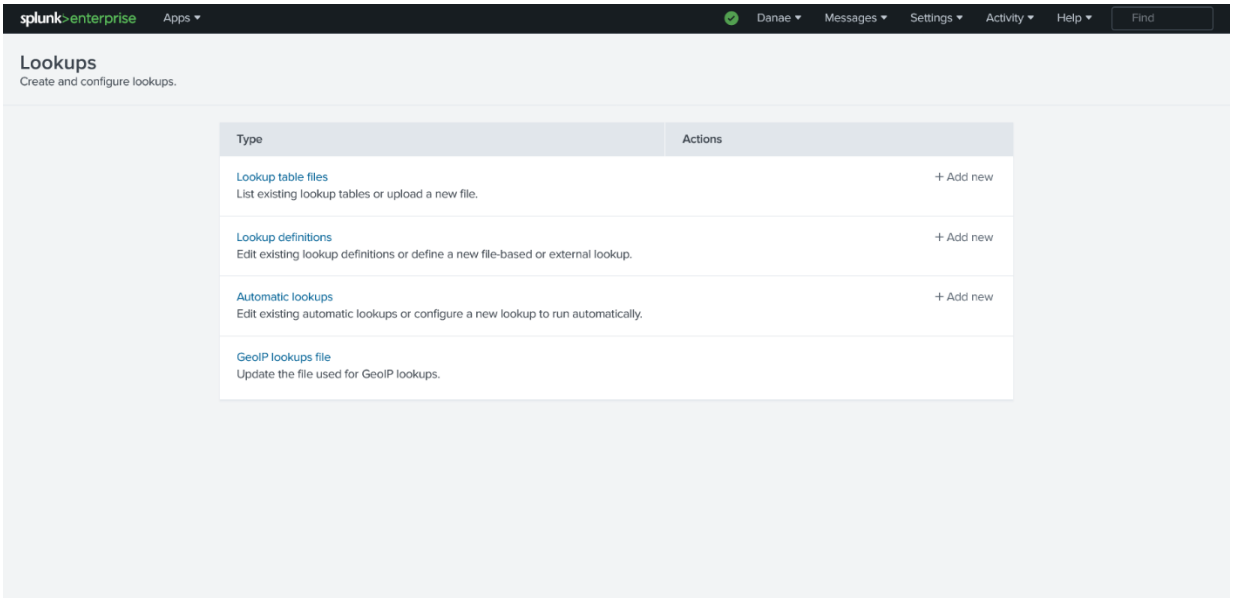
Putting data into Splunk:

In order to properly use this application, you will need to have valid data for the application to use. This data is cyber-attack information that contains the following: a title, a technique ID, a technique name, a description of the technique, and a time of the cyber-attack. This data needs to be in Splunk before the application can be used properly. Two datasets have been provided, follow the instructions below to import them into Splunk

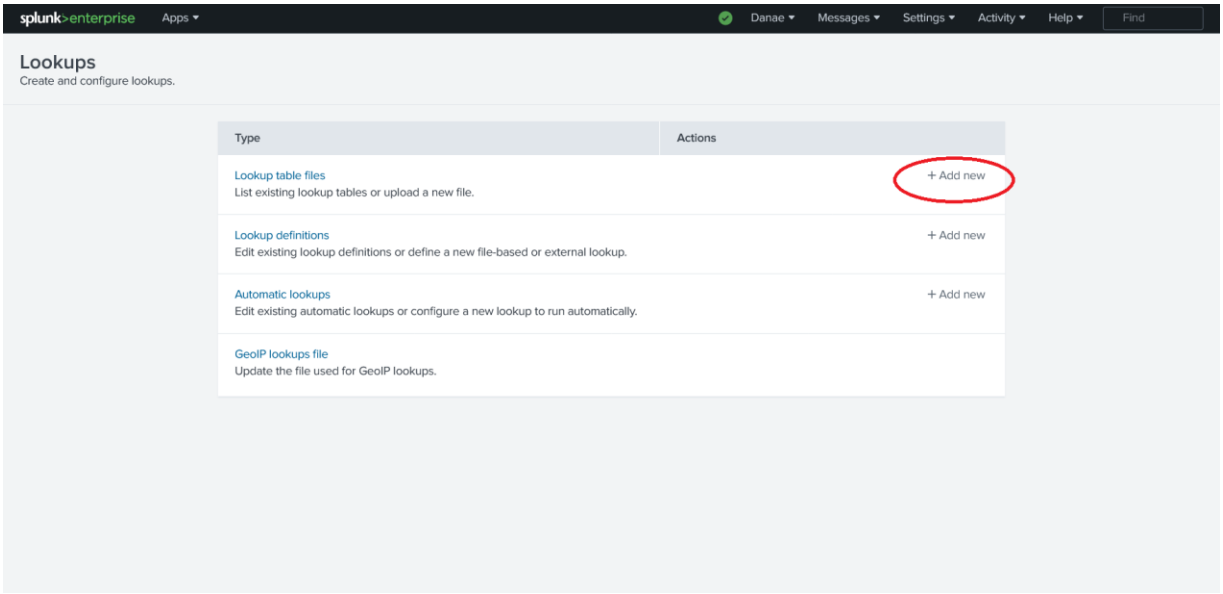
1. Click the “settings” on the upper right-hand corner of the screen. This will bring up a drop-down menu.
2. Click on the “Lookups” setting on the left-hand side of the drop-down menu underneath the “Knowledge” section.



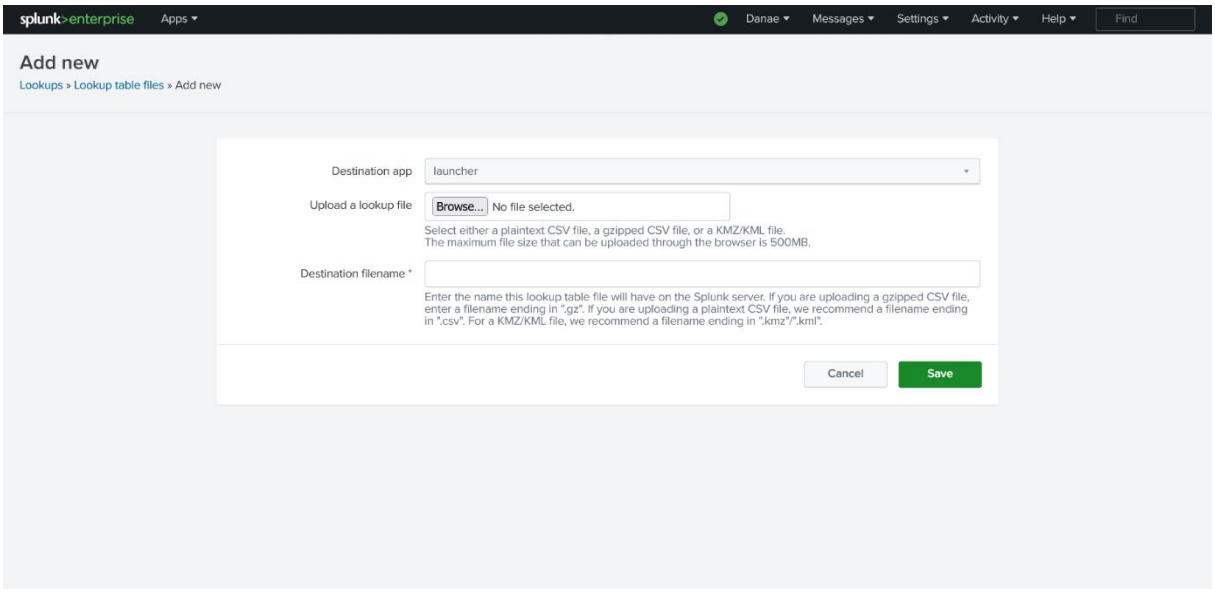
Once clicked, you should be brought to a screen that looks like this:



3. Click the “Add new” on the “Look up table files” selection – the top selection.

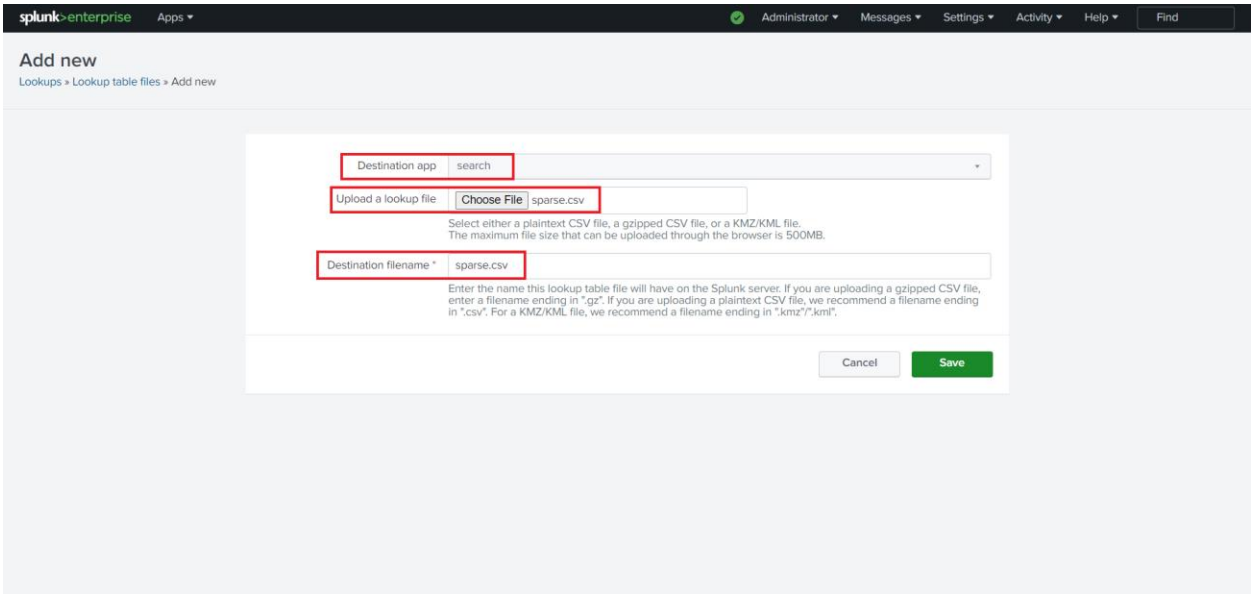


You should now be in the File adding prompt which looks like this:



4. In the dropdown menu next to “Destination app” choose search. This will ensure the added file is visible to the search application which is required later to submit a query.
5. Click on the “Browse…” or “Choose file…” in the prompt to select a file.
6. Click on the “sparse.csv” file that was given to you.
7. With the file selected, click on “Open” in the bottom right of the file selector window. This will bring you back to the selection prompt.
8. Click on the “Destination Filename” box and type in “sparse.csv”. This will make the sparse.csv file being inputted into Splunk Enterprise have the name of “sparse.csv” for later usage in the instruction.

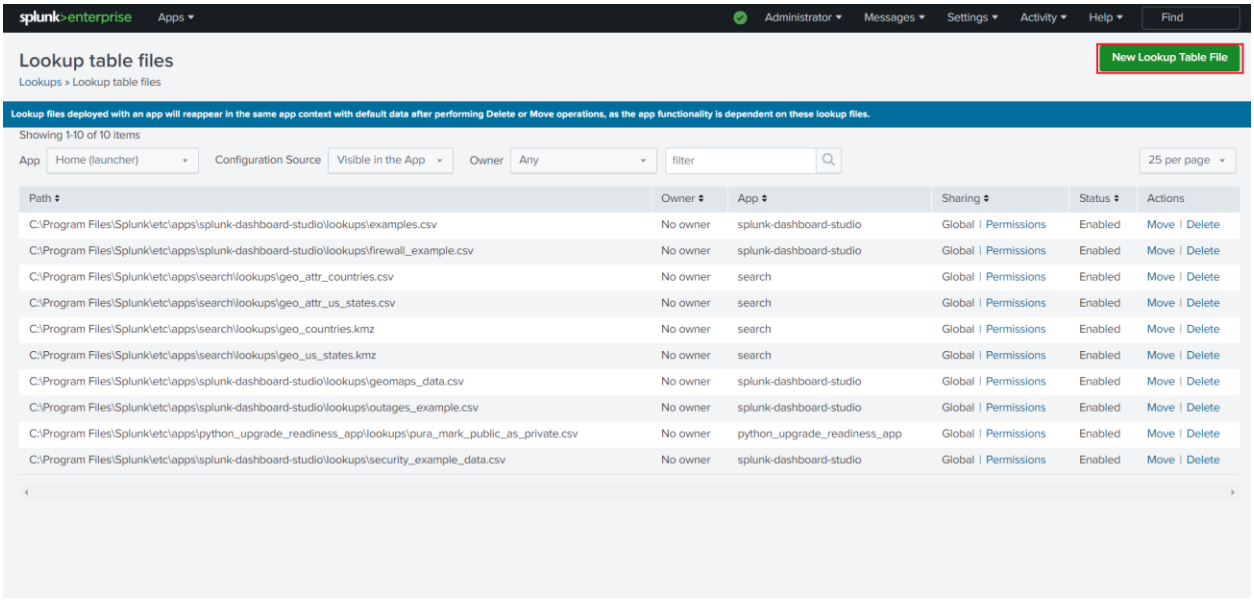
   Before continuing, make sure all of the fields look exactly like the following image:



9. Click on the “Save” button in the prompt to finalize the file upload.

This will send you to the Lookup tables you have in your Splunk Enterprise system.

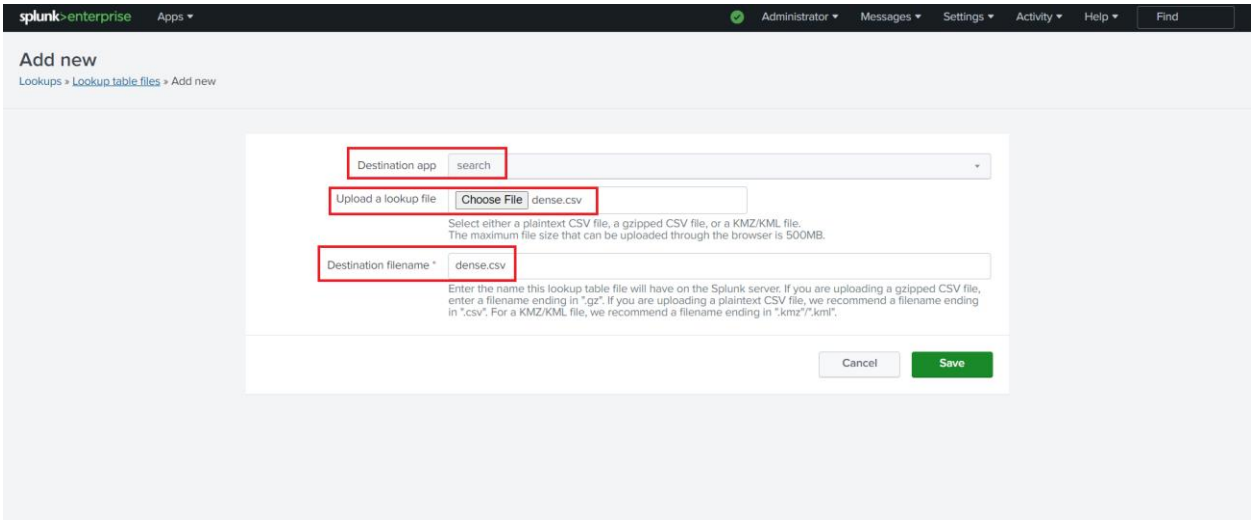
10. Click on the green button labeled “New Lookup Table File” in the upper right-hand corner of the screen. This will bring you back to the file prompt.



The following steps are repeated from above, but for the dense.csv file.

11. In the dropdown menu next to “Destination app” choose search. This will ensure that the added file is visible to the search application that is required later to submit a query.
12. Click on the “Browse…” of “Choose file…” in the prompt to select a file.
13. Navigate and click on the “dense.csv” file that was given to you.
14. With the file selected, click on “Open” in the bottom right of the file selector window. This will bring you back to the selection prompt.
15. Click on the “Destination Filename” box and type in “dense.csv”. This will make the dense.csv file being inputted into Splunk Enterprise have the name of “dense.csv” for later usage in the instruction.

    Before continuing, make sure all the fields look exactly like the following image:



16. Click on the “Save” button in the prompt to finalize the file upload.

The data for testing and using the application has now been added. To navigate back to the home page, click the “splunk>enterprise” logo in the upper left corner of the screen.

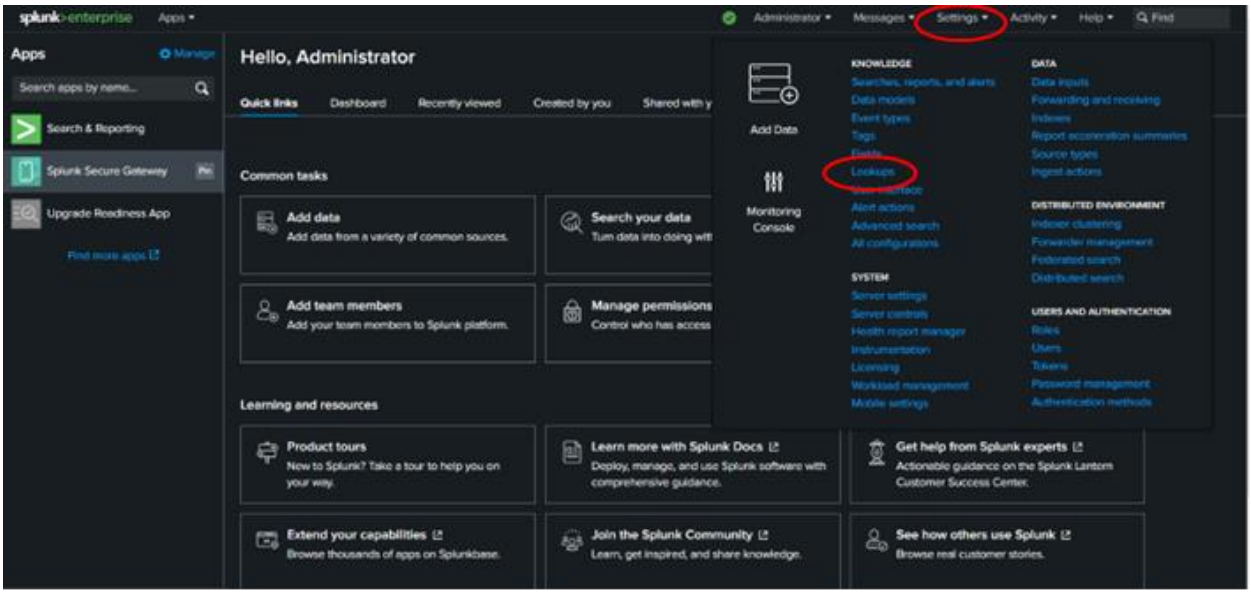
This is a point where you can stop and come back later.

Troubleshooting Issues with the Datasets:

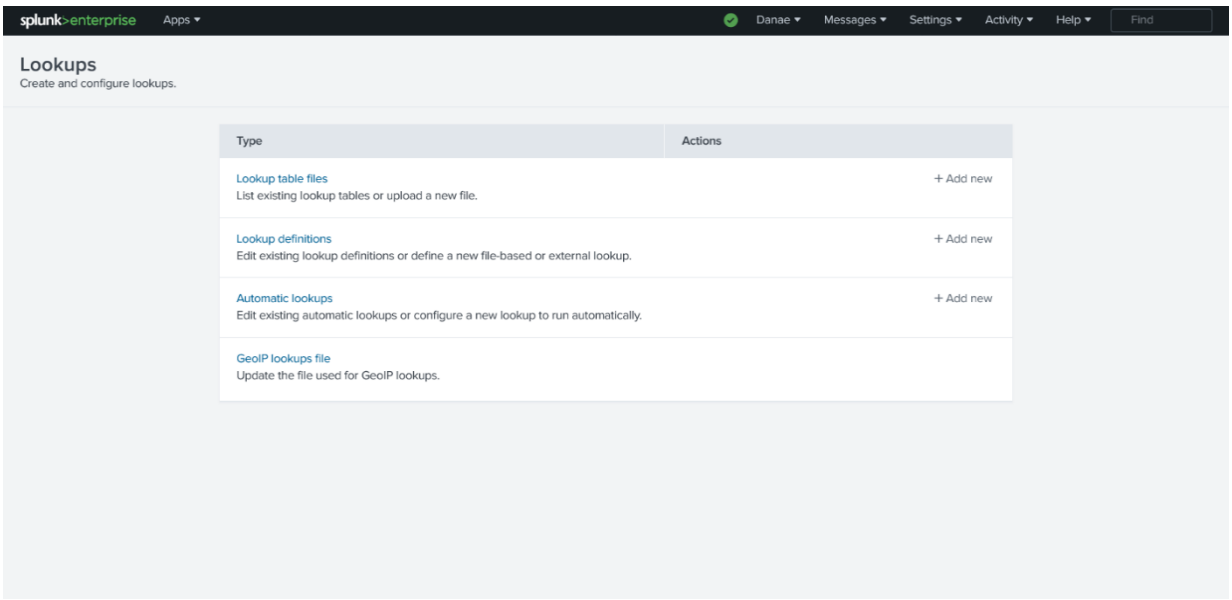
This section may be skipped, assuming there are no issues with making queries on the datasets.

If you receive a message when attempting a query on sparse.csv or dense.csv, there may have been an issue when uploading the dataset. This can be mitigated by reuploading the datasets.

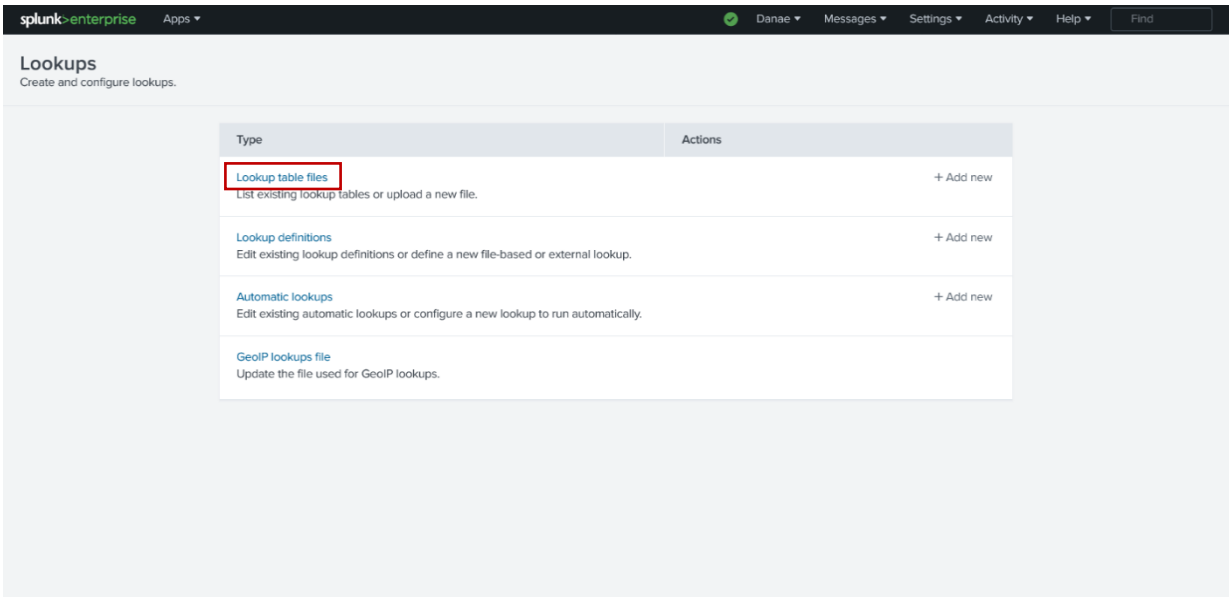
1. Navigate back to the Splunk home page by clicking on the Splunk Enterprise logo in the top left corner of your screen.
2. Click the “settings” on the upper right-hand corner of the screen. This will bring up a drop-down menu.
3. Click on the “Lookups” setting on the left-hand side of the drop-down menu underneath the “Knowledge” section.



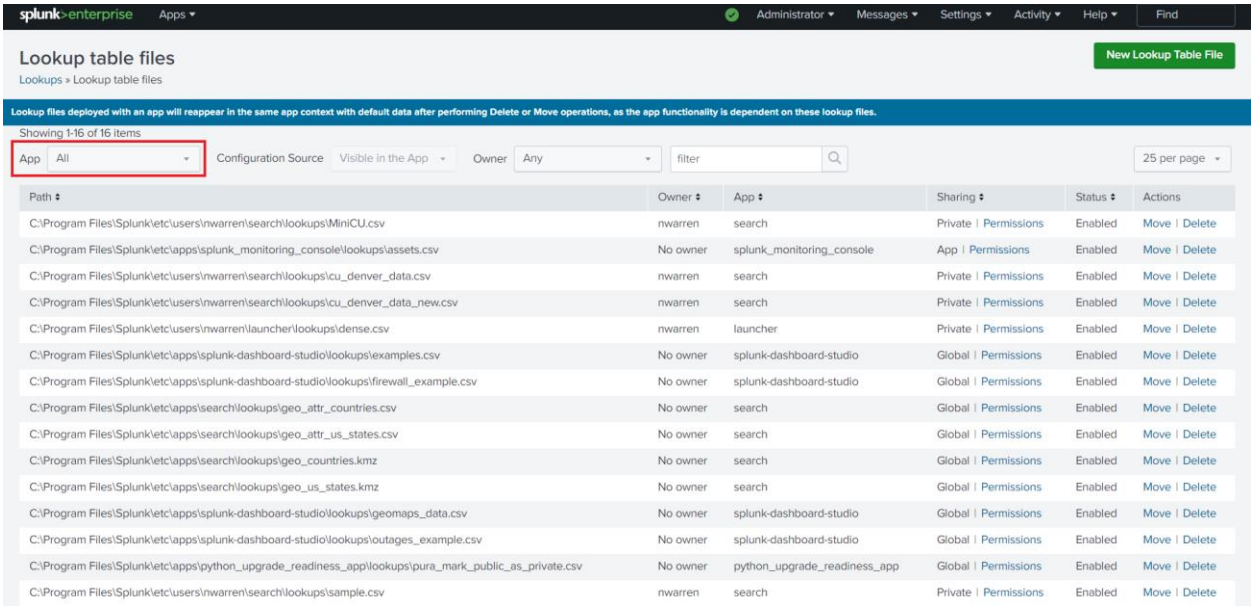
Once clicked, you should be brought to a screen that looks like this:



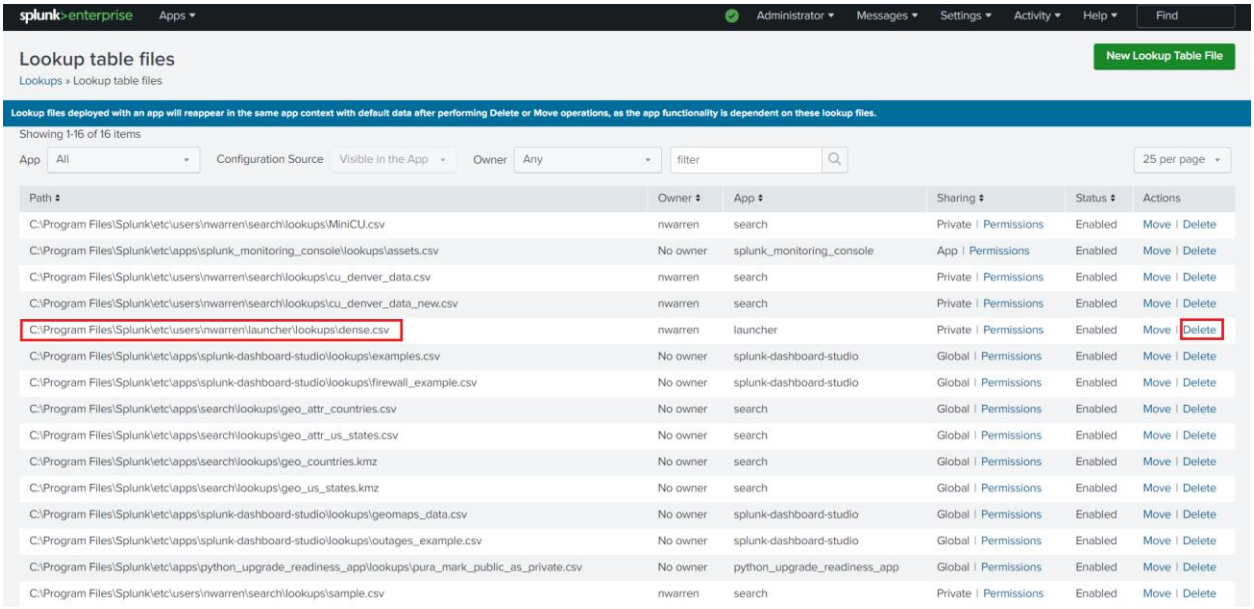
4. Before you can reupload the datasets, you must manually delete the current ones from your Splunk Enterprise installation. To do this, you must first navigate to “Lookup table files”



5. This will bring you to a screen containing all of the lookup table files visible to your installation of Splunk. Navigate to the box labeled as “App” and ensure that “All” is selected. If it is not, use the dropdown menu to change it to “All”



6. From here, you need to find the file path corresponding to sparse.csv and/or dense.csv. Once you find it, you will need to choose “Delete” under the column labeled as “actions” to remove the file.



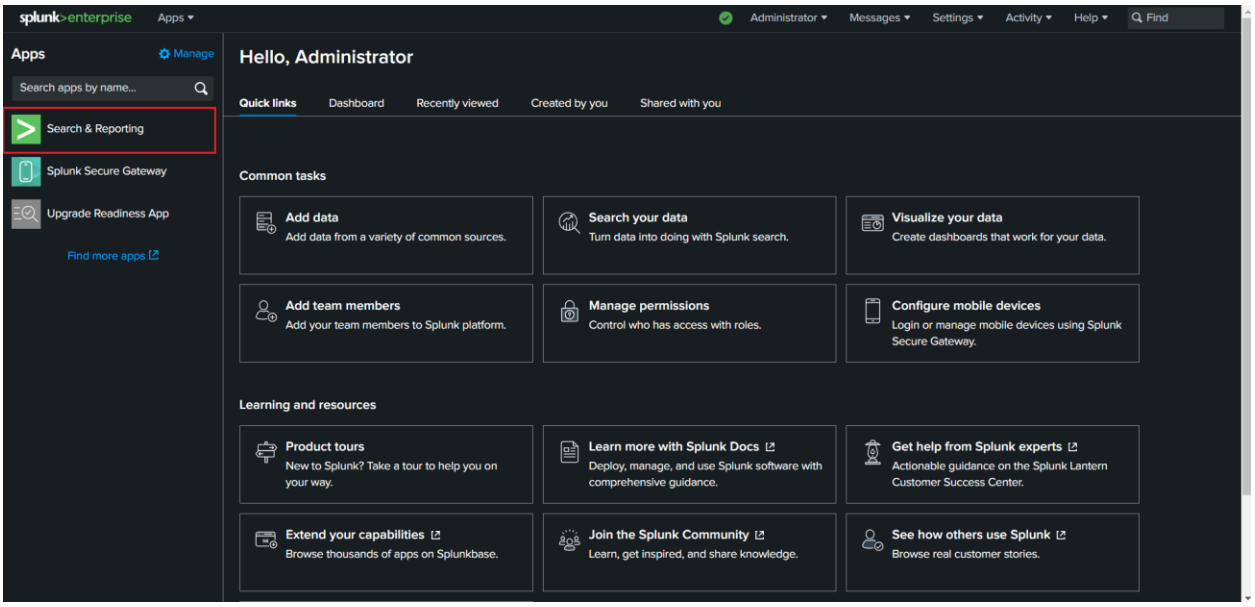
7. On the popup that says, “Are you sure you want to delete?” click “Yes”
8. Repeat the above steps for all lookup table files that have issues and return to the “Putting data into Splunk” section to reupload the data.

Using the Threat Timeline Application:

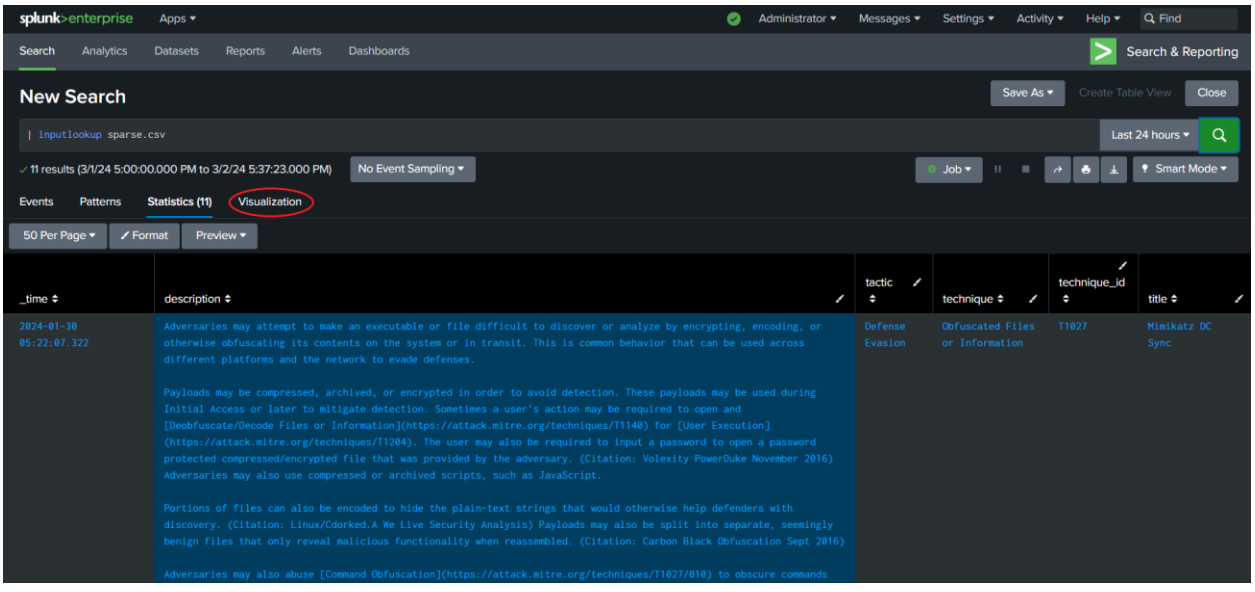
Before beginning the following section, make sure you have opened the response form that was sent to you by email. Please fill out the corresponding questions in the form as you complete each step. Also, one of the form’s questions will ask you the total time it took you to complete these instructions, so please note when you began going through the following section.

ADD IN LINK TO SURVEY

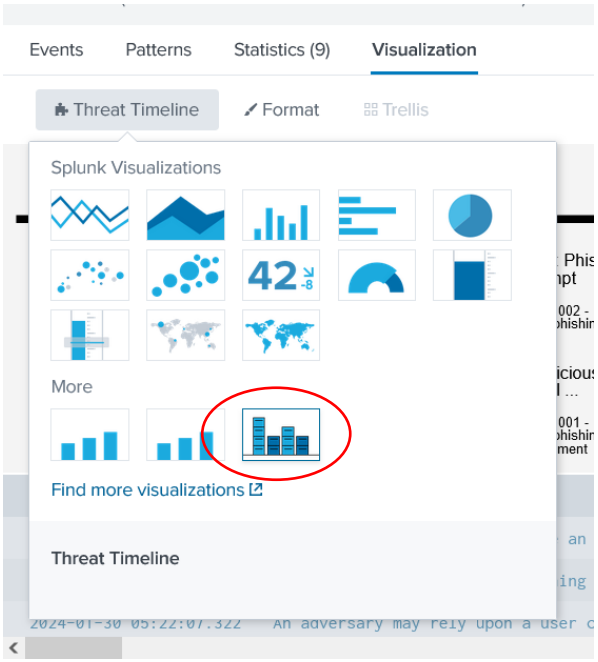
1. From the Splunk home page, select “Search & Reporting” from the left-hand side bar.



2. In the search bar, type in "| inputlookup sparse.csv" in the "Search & Reporting" screen. This is your query.
3. Either hit "Enter" on your keyboard while the search bar is selected or click on the green "magnifying glass" icon on the right side of the search bar to initiate your query.
4. Click the "Visualization" tab underneath the search bar.



5. Click on the button that says "Column Chart" next to the button labeled "Format" to bring up a pop-up menu to change the visualization.
6. Click on the icon with four bars with lines in the boxes in the "More" section of the visualization selection. The title of the icon will be "Threat Timeline" at the bottom of the visualization selection.



You should now be in the Threat Timeline visualization in the "Tactic View" where your query is sorted according to the different attack tactics used.

Question #1: Did the visualization window update when you selected the Threat Timeline visualization?

In the visualization window, you should see groups of text corresponding to each tactic category. Each of these represents a specific cyber-attack from the dataset you were provided. For each attack, there should be three things. A title, which is represented with larger text, a technique ID, which begins with "T" followed by numbers, and a technique name, which is separated from the technique ID by a dash. These three items make up a "card preview" and will be referred to as such from now on. Locate the column labeled as "Initial Access."

Question #2: For the column labeled as "Initial Access" are the titles, technique ID's and techniques present for each card?

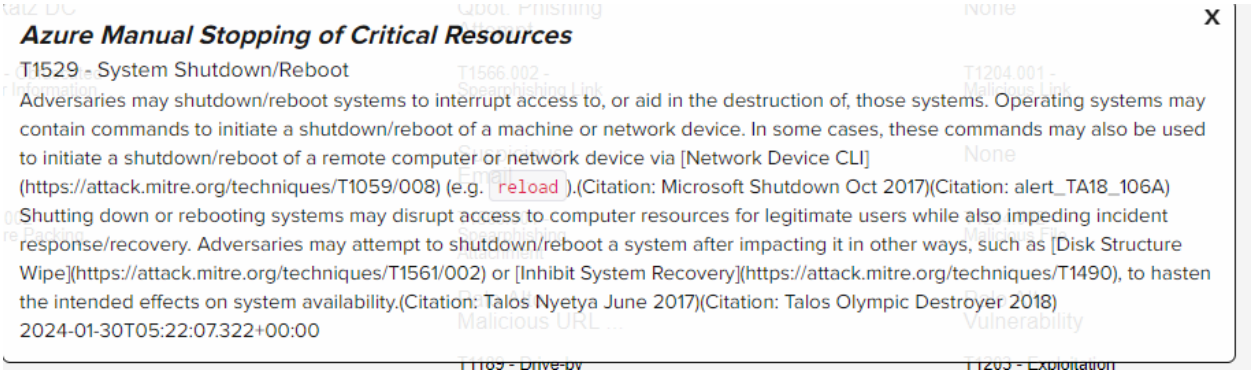
Question #3: Is the first card preview in "Initial Access" labeled as "Qbot: Phishing Attempt"?

7. Click on any card preview to bring up an expanded view of the card containing its full information.

Question #4: When you click on the card preview, does another window pop up?

Each expanded card view should contain the same title, technique ID, and technique as the card preview you selected, as well as a description of the technique and a timestamp.

For reference, here is what an expanded view of a card should look like:



Question #5: Are all the listed items present on the card? (The title, technique ID, technique, a description, and timestamp)

8. Without attempting to close the current window, click on another card preview.

   Question #6: When you clicked on another card preview, did the information in the pop-up window change to display the information for the new card?

9. Click the “X” in the top right of the expanded card to close it.

   Question #7: When you clicked on the “X”, did the expanded card close correctly, returning you to the original view?

10. Now, we’re going to try out a dataset with more items. Navigate back to the search bar, and type the following query:
    "| inputlookup dense.csv”

11. Push “enter” on your keyboard while the search bar is selected or click the green magnifying glass to submit the new query.

    Question #8: Did the view change to have more card previews?

If the view did not change, click the refresh button on your browser.

Question #9: Did you have to push the refresh button to view more card previews?

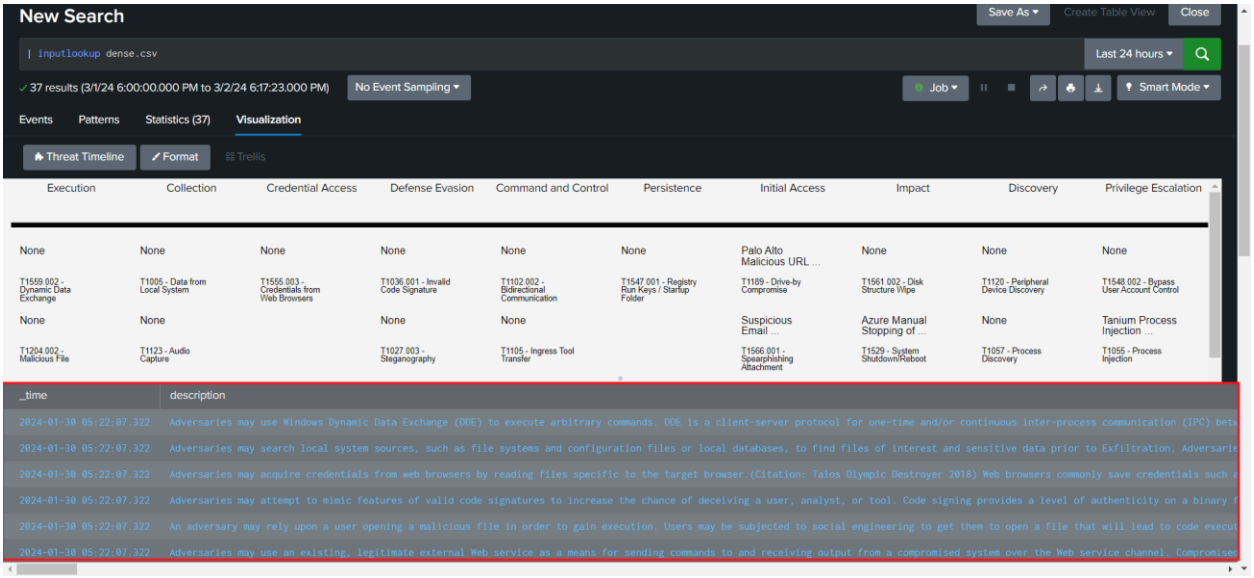
Like before, you should see groups of text corresponding to each tactic category. There should be more tactic categories than before.

Question #10: How many tactic categories (columns) are listed at the top of the screen?

12. Locate the tactic category labeled as “Initial Access”.

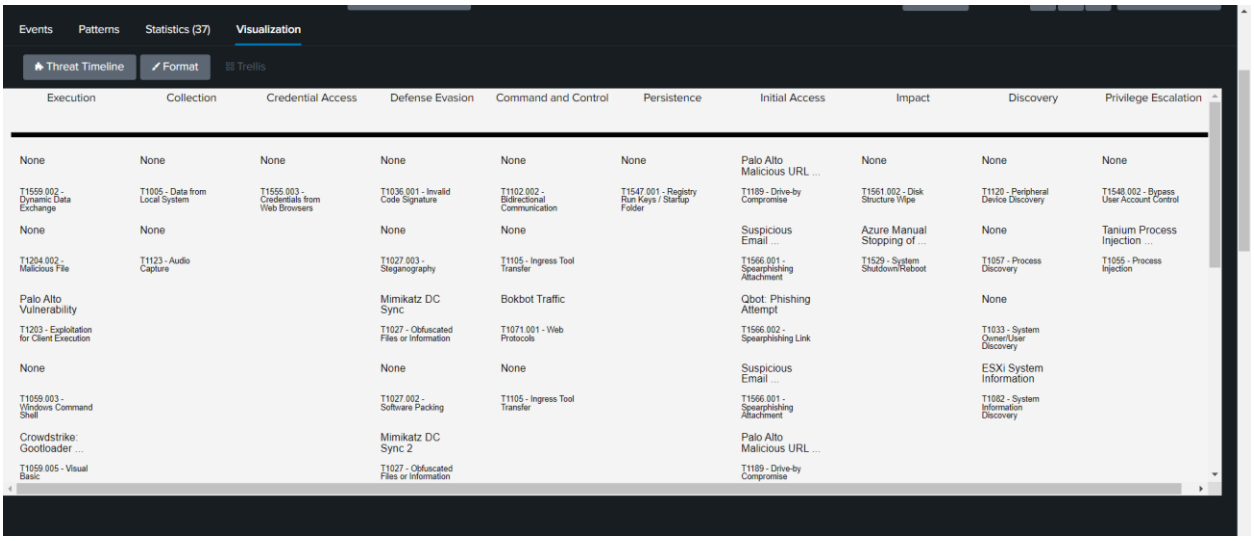
Question #11: Does the first card preview in this column contain the technique ID and technique name “T1189 – Drive-by Compromise”?

13. On your screen, there should be a box containing information from the dataset. You may need to use the far right scroll bar of your browser’s window to scroll down and see it. You should be able to grab the top edge of this box and drag it up or down. The box looks like this:



Question #12: Were you able to successfully move the box up and down?

14. Use the mouse to drag this box out of the way until you can view the full visualization window. You may need to use the furthest right scroll bar of your browser’s window to move the screen down. Your screen should look like below:



15. Navigate to the right side of the visualization window. You should see two scrollbars like in the image above. Use your mouse to move the scrollbar that is closest to the text up and down.
    Question #13: When you interacted with the scrollbar, did the visualization window move up and down?

16. Navigate to the bottom of the visualization window. You should see another scrollbar, this one horizontal. Use your mouse to navigate the scrollbar to the left and right.

    Question #14: When you interacted with the horizontal scrollbar, did the visualization window move from left to right?

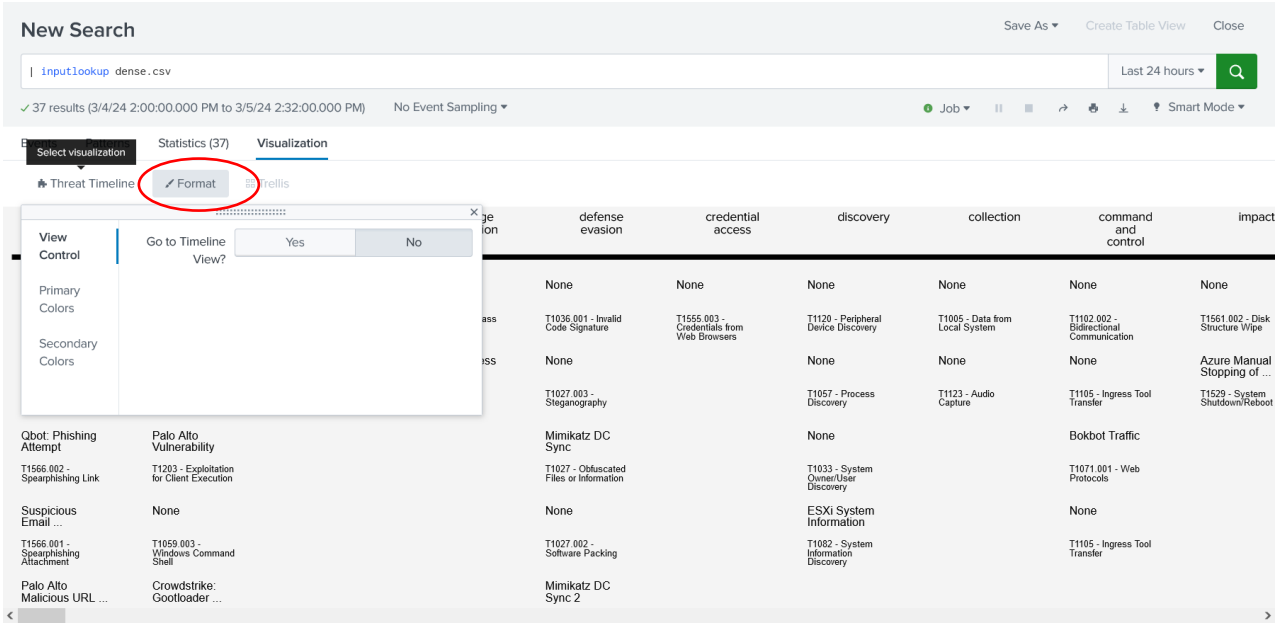
This concludes the Tactic view test and instructions! Thank you for your time.

Question #15: How long did it take you to complete the testing? (Using the Threat Timeline Application set of instructions.)

If you need assistance or an error occurred in the testing of this product, please contact us at: danae.oconnor@ucdenver.edu or noah.warren@ucdenver.edu.

---

17. Click on the “Formatter” button next to the “Threat Timeline” button above the visualization under the search bar.



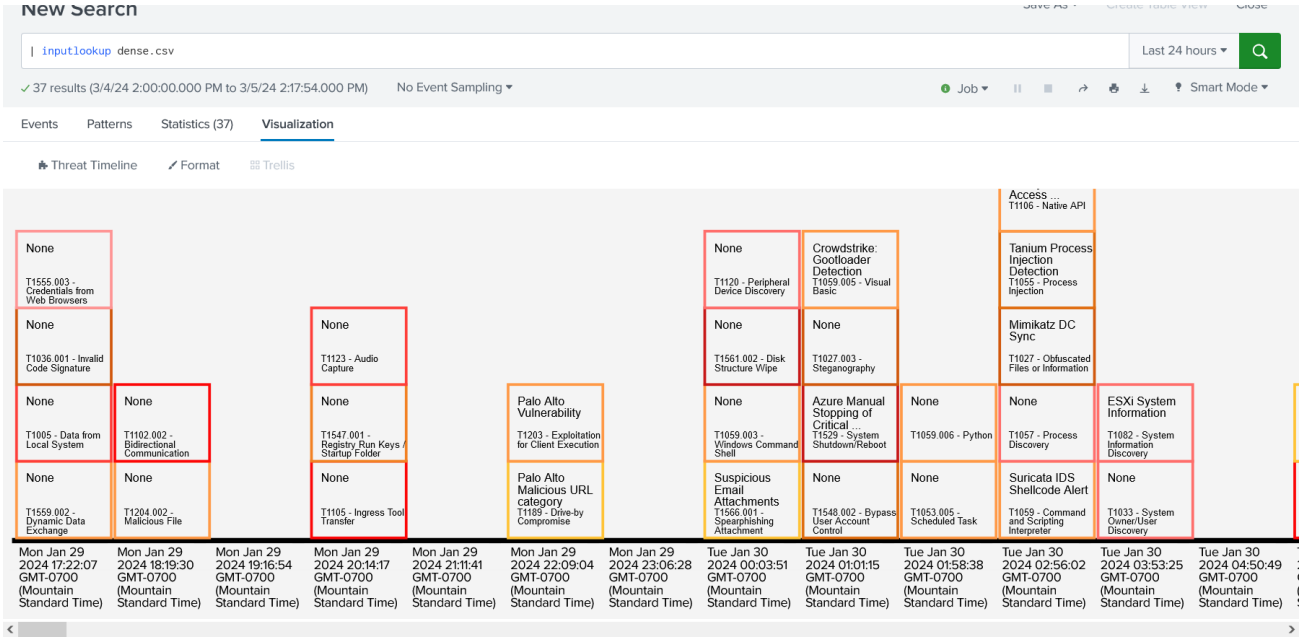
Question #15: Is the first thing that pops up a “Yes/No” selection to go to the Timeline View?

18. Click the “Yes” button.
19. Click on the visualization to reduce the formatter menu.

Question #16: Did the Visualization change?

Click the refresh button of your browser if your view does not change.

The view should now look like this:



Question #17: Are the boxes colored similarly to the picture above?

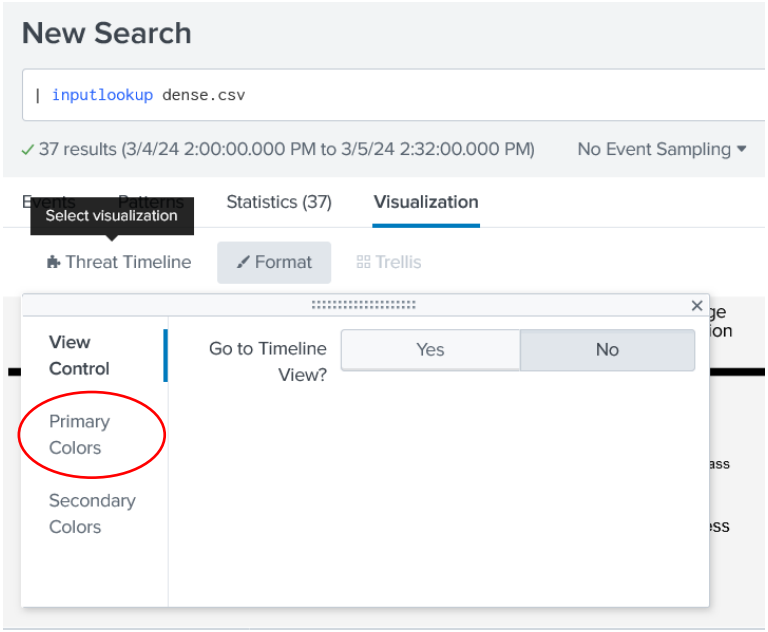
Question #18: Is there any difficulty reading the card previews?

At the bottom of the visualization window are dates.

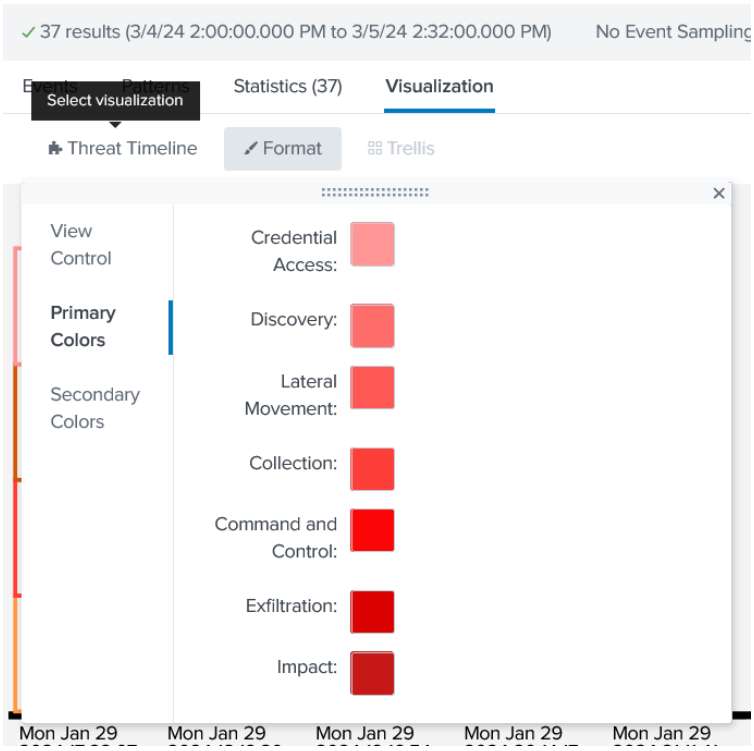
Question #19: Is the first column’s date “Mon Jan 29 2024 17:22:07 GMT-0700"?

Question #20: Is it clear that the content in the first column is placed there, rather than in the second column?

20. Click on the Formatter button to bring up the formatter menu.
21. Click on the button labeled “Primary Colors” on the far left of the formatter menu.



Your formatter should now look like this:



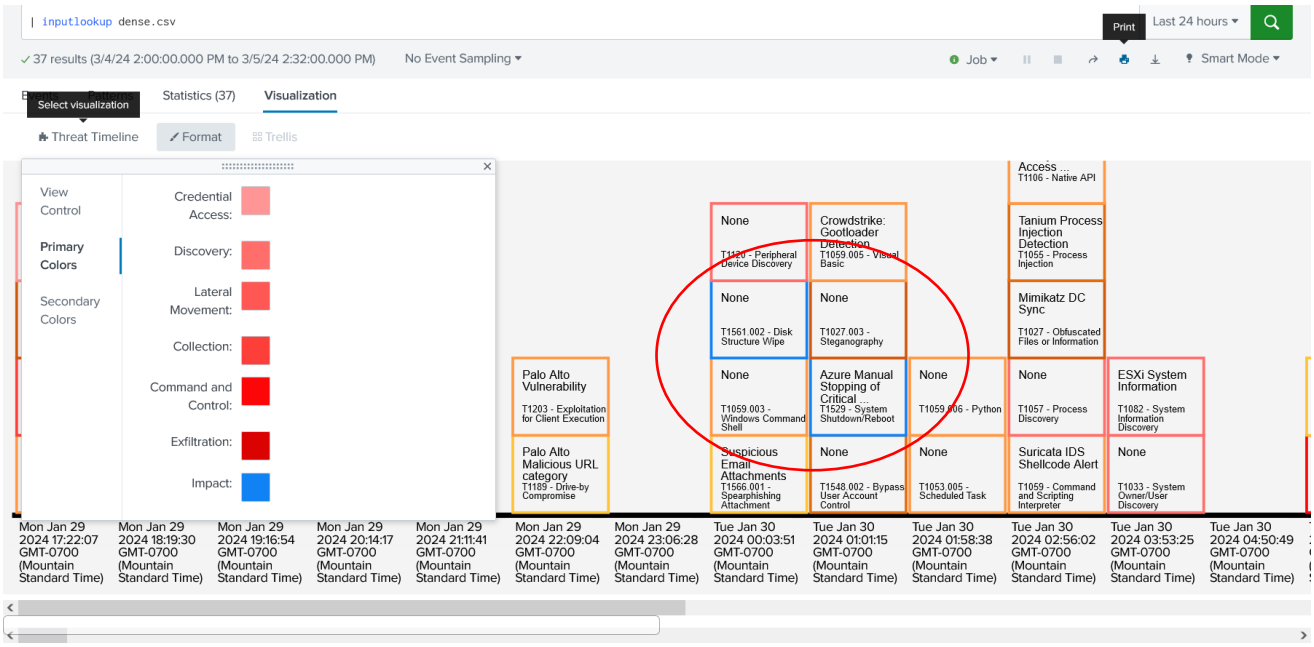
22. Click on the colored box next to “Impact”. This will bring up a color selector.

The color selector should look like this:

Question #21: Did the color formatter appear?

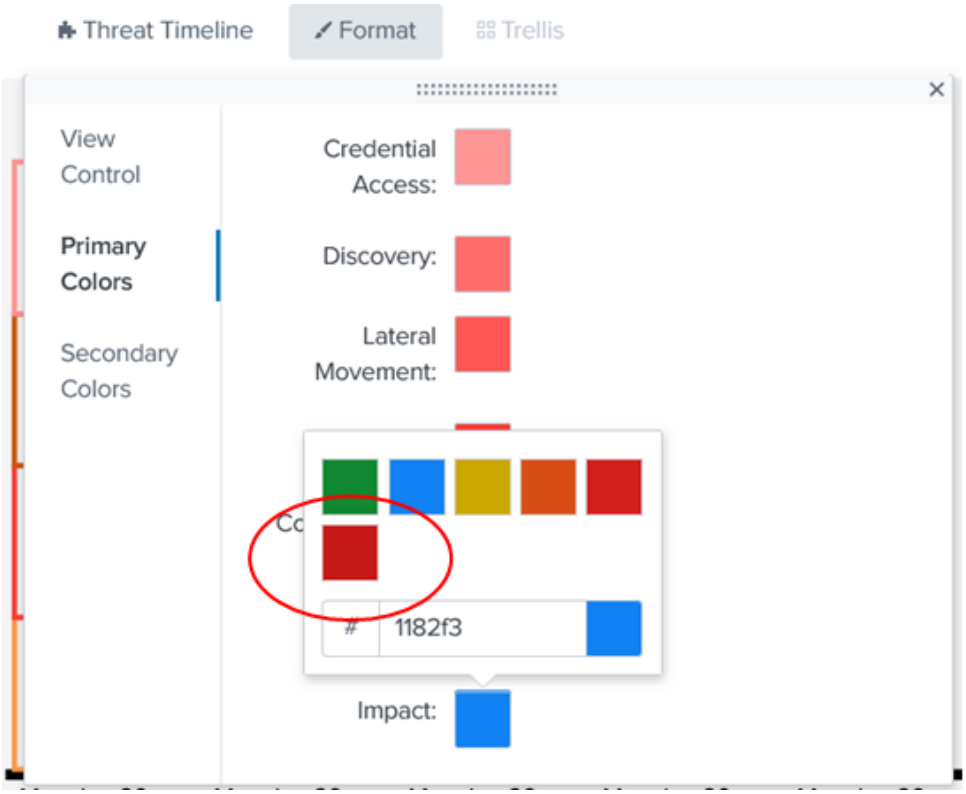
23. Click on the blue color. This changes the color of the cards with that tactic type.

Your view should look like the picture below:



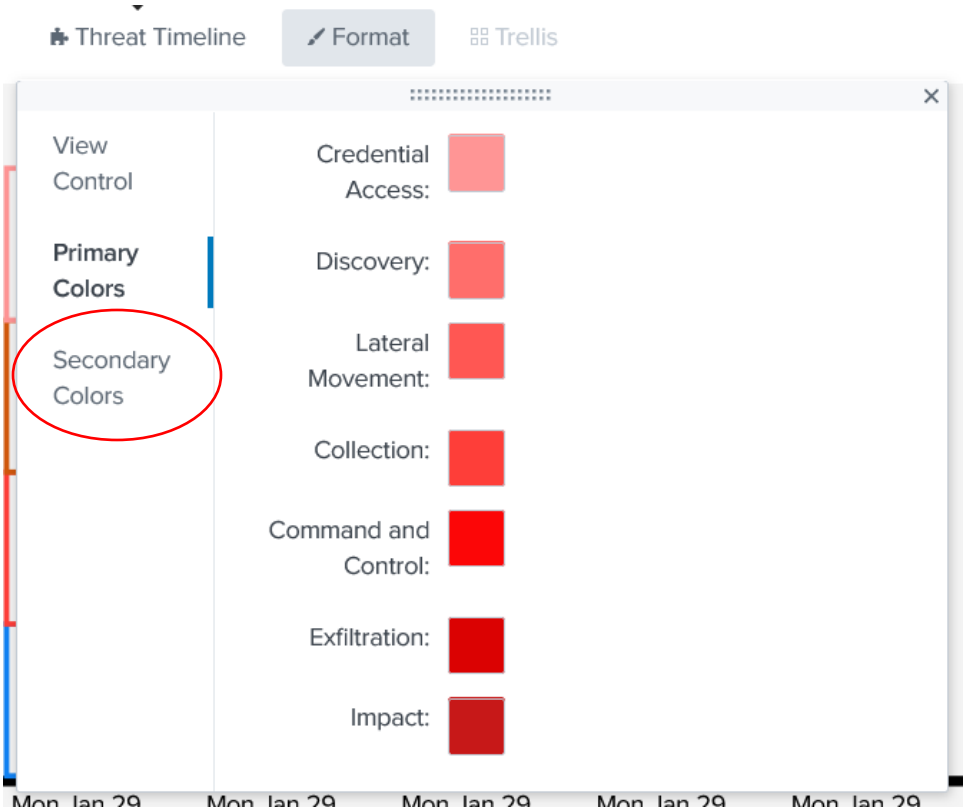
Question #22: Did some of the borders of the card previews change to blue?

24. Click the colored box next to “Impact” in the formatter.
25. Click the red box on the second row of the color selector.



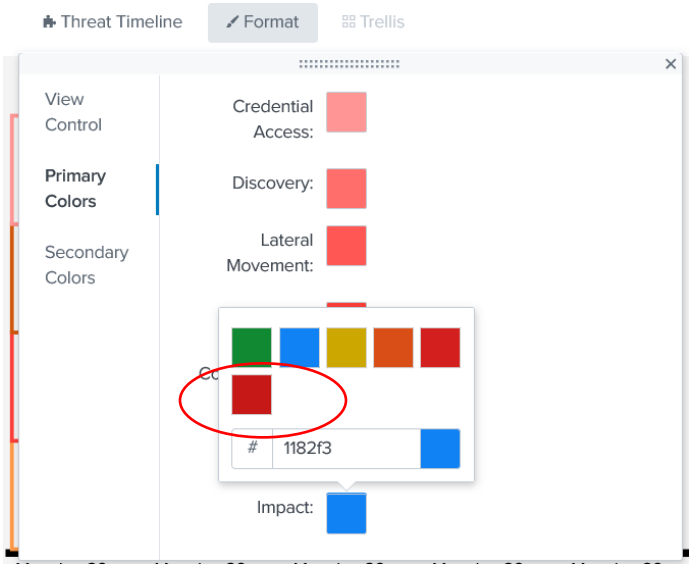
Question #23: Did the card preview’s colors go back to being red?

26. Click on the button labeled “Secondary Colors” on the far left of the formatter.

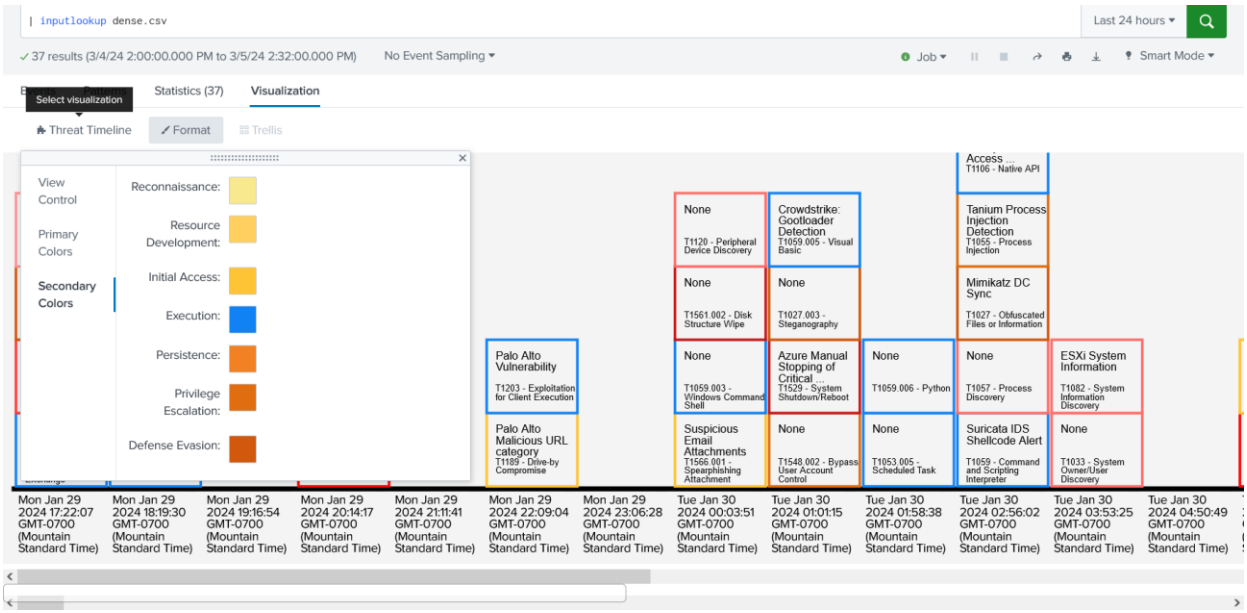


Question #24: Did the colors and labels change?

27. Click on the colored box labeled “Execution”. This will bring up the color selector.
28. Click on the blue box from the color selector.

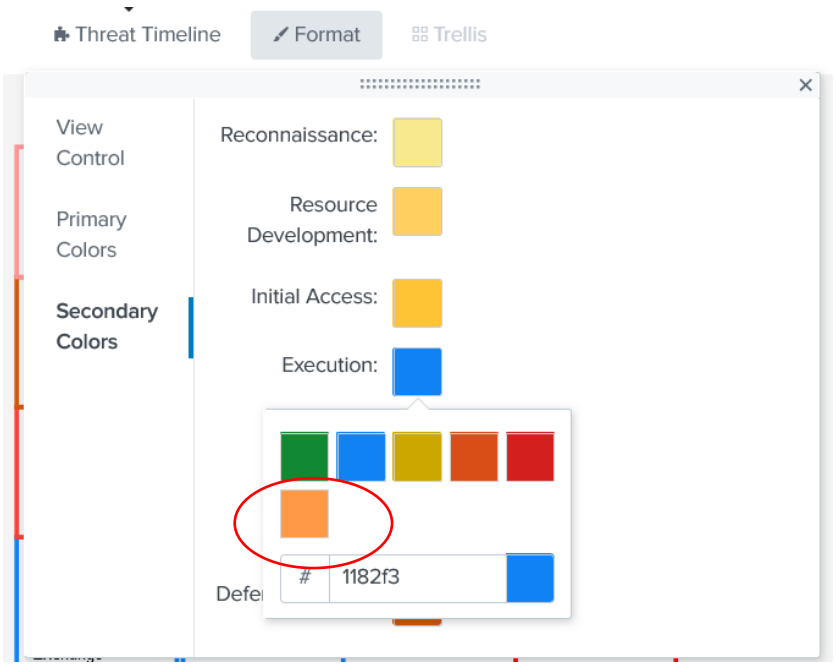


The view should now look like this:



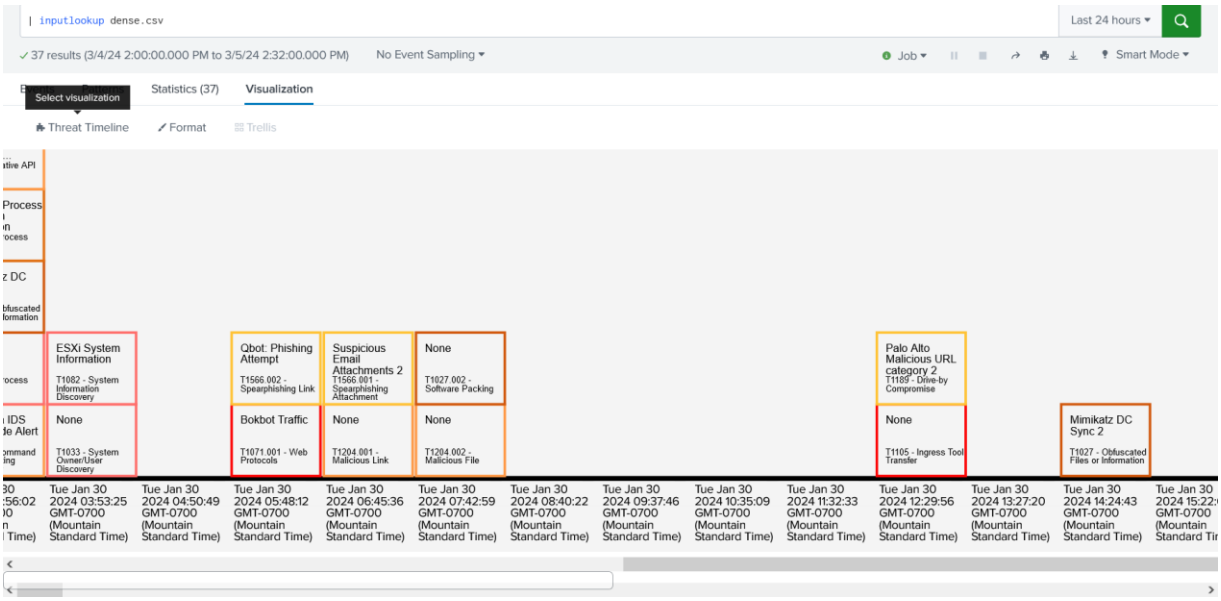
Question #25: Did the colors for the card previews change to blue?

29. Click the colored box next to “Execution”.
30. Click the orange box on the second row of the color selector.



31. Click on the visualization to reduce the formatter.
32. Navigate to the horizontal scroll bar at the bottom of the visualization.
33. Click and drag the horizontal scrollbar to the far right of the visualization window.

Your view should now look like this:



Question #26: Were you able to use the horizontal scroll bar?

Question #27: Is there a card preview titled “Mimikatz DC Sync 2” in the second to last column?

This concludes the Threat View test and instructions! Thank you for your time.

Question #28: How long did it take you to complete the testing? (Using the Threat Timeline Application set of instructions.)

If you need assistance or an error occurred over the testing of this product, please contact us at: danae.oconnor@ucdenver.edu or noah.warren@ucdenver.edu