Splunk Threat Timeline Instructions

Splunk Enterprise Installation and Setup:

In order to run the application, you will need to install Splunk Enterprise.

Open your preferred web-browser.

Search and go to the official Splunk site – which you can access using the following link:

https://www.splunk.com/

Create an account with Splunk.

Once the account is created, navigate to the "Products" tab located at the top of the Splunk site's web-page. and select "Splunk Enterprise". This will bring you to the information about the Splunk Enterprise application's abilities.

From the Splunk Enterprise page, there will be an icon labeled "Free Trial" that is next to another button labeled "Take a Guided Tour" - click the "Free Trial".

This step will potentially ask you to create an account for Splunk – if this happens, in the upper right-hand corner there is an icon next to the "Free Splunk" button that is shaped like a person, click the person icon and select "Log In". Follow the steps and input the information you made in the Splunk account creation. This step will officially log you into Splunk and will allow access to the products offered by Splunk. Use the above steps to navigate back to the "Free Trial" option.

By clicking the “Free Trial” option, it should bring you to a screen that has several options for downloading in accordance with your operating system with the options being Linux, Windows, and Mac. This instruction manual will only cover Windows operating system downloads, but there are instructions for other operating system downloads here: https://docs.splunk.com/Documentation/Splunk/9.1.2/SearchTutorial/InstallSplunk

[Go through the windows Installation process and initial Splunk set up.]

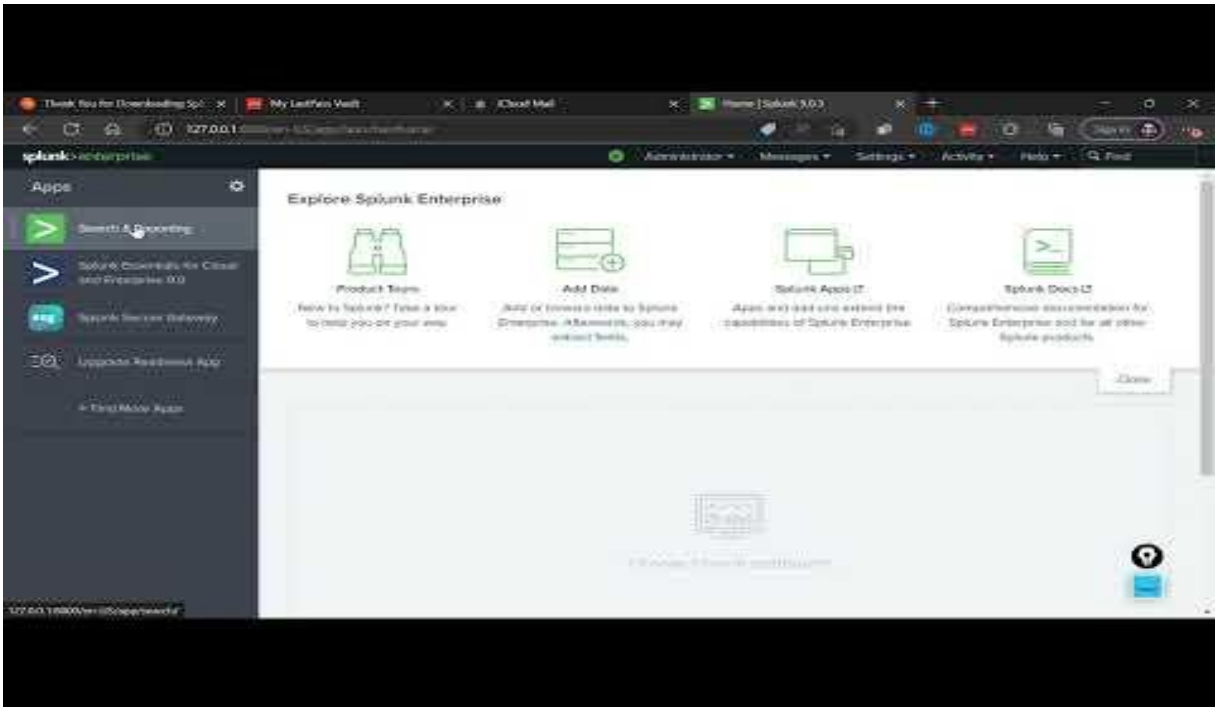
If additional help is needed, the following links on the official Splunk documentation might help:

https://docs.splunk.com/Documentation/Splunk/9.1.2/SearchTutorial/InstallSplunk

https://docs.splunk.com/Documentation/Splunk/9.1.2/Installation/Chooseyourplatform

An additional Windows Installation Video:

https://www.youtube.com/watch?v=GtikcQfKb04



Current Implementation Process – Manual:

Make sure that Splunk Enterprise is installed on your device.

In addition, because we currently don't have an app item in a traditional sense the following is a more manual approach that is currently essential. Hopefully in the future this process will be simplified greatly.

Additional Splunk Setup %SPLUNK_HOME% Variable – Windows OS Specifically:

Creating the %SPLUNK_HOME% variable:

First %SPLUNK_HOME% variable. This acts as the applications contact between the installation folder of the Splunk Enterprise application and the Splunk folders on the system.

To set up the SPLUNK_HOME variable for windows, you will need to open the command prompt.

Once you have command prompt open, enter in the following command:

setx SPLUNK_HOME "[File path to the Splunk installation folder]"

For example, with the default file installation folder, the command should be:

setx SPLUNK_HOME "C:\\\"Program Files\" \\Splunk"

The extra slashes are necessary to allow for strings which encapsulate spaces to be correctly read in the file path, such as “Program Files”. In addition, the double slashes between directories are needed in order for the application to properly read the file path.

App Installation:

Configuration File and App File Configuration:

There is a file titled "web.conf" this is a configuration file that allows for the Splunk Enterprise application to actually read the Splunk files on the system - especially modified ones. This file will need to be placed in: "Splunk/etc/system/local" file directory.

In order to get our application onto your system, you will need either the provided zip folder or the file from our GitHub labeled as "Threat_Timeline". This file download may take some

time, if you wish you can go to the “Data Input into Splunk” step of this document while waiting for this process.

You can get the files from this link: https://github.com/noahw18/Kaiser-Permanente-Cybersecurity-Project

You need to place the file into the “Splunk/ect/apps” file directory. If you are using the zip file - make sure that the Threat_Timeline isn't hiding in another file folder named Threat_Timeline, this will cause issues with installing the application.

The **correct** file structure should be: "Splunk/etc/apps/Threat_Timeline/<app directory structure>"

The file structure should **NOT** be: "Splunk/etc/apps/Threat_Timeline/Threat_Timeline/<app directory structure>"

Data input into Splunk:

This step can be done in tandem with the Threat_Timeline download if you wish. You can also skip this step if there is acceptable data is already in Splunk Enterprise. Acceptable data will mean data that has attack data that has the fields of: title, tactic, technique, technique ID, description, and time with the tactic, technique, technique ID, and description being that of MITRE ATT&CK database’s formats.

In order to see if the app is available on Splunk - some data will need to be loaded to see if the visualization appears.

In the gitHub for this application there is a csv file labeled "miniCU_total.csv" which will be the tester data for the application for right now. This contains some data that has tactics, titles, times, tactic ids, and descriptions.

In the Splunk Enterprise webpage go to "Settings" and under the "Knowledge" section click on "lookups". In the lookups page click the item that says, "lookup table files". Once on that page click the "New Lookup Table file" button in the upper right corner in order to add a new lookup table into Splunk which is a static table that Splunk can be used to display.

Follow the prompts to add in the miniCU_total.csv file. When this is complete the lookup table will automatically be set to private, but it needs to be global in order for the rest of the Splunk system to see it. If needed navigate back to the “lookup table files” area from the previous steps. Once here navigate to the file that was set for the miniCU_total.csv file and click the option labeled "permissions". In the permissions screen select the option that all apps can see the file and that the various roles can Read it by selecting the "Read" check box next to "Everyone".

Visualization Itself:

Both “Data Input into Splunk” and the “Configuration File and App File Configuration” steps must be completed before continuing with this step.

Close your web-browser containing the Splunk Enterprise application if you are using it.

You will want to restart your Splunk Enterprise application.

For Windows OS – to restart the Splunk application, click the search bar of the computer and type “Services”. This will pull up a window that contains all the services on the device – this list is in alphabetical order. Scroll down to the “Splunkd Service”. Select the “Splunkd Service” and right click it, there will be a drop down menu that appears. In this menu click the “stop” selection and wait for it to properly stop. Once it is done the “Splunkd Service” will have a blank in the status column. With this complete, select “Splunkd Service”, right click to get to the drop-down menu and click the “start” option. This will start the Splunk application again. Once it is started the “Splunkd Service” will have a “running” status.

Open the Splunk Enterprise application again and log in.

With this complete you should have data to call to as well as the app installed. In order to check and see if it worked, click the "Apps" button next to the Splunk Enterprise logo and go to “Search & Reporting”. In the search bar type in the command:

| inputlookup <lookup_TableFileName.extension>

For example, using the miniCU_total.csv as the name of our lookup table:

| inputlookup miniCU_total.csv

Hit enter or click the green spy-glass icon that is on the search bar, in order to commit the search.

Once the search is done, click the "visualizations" button that shows up underneath the search bar – the default visualization is a "Column Chart". Click the button titled "Column Chart" and from the pop-up, in the "More" section click "Threat Timeline". This is our visualization.

As we understand it, this should be the last step and should allow for the Splunk Enterprise application to see our application and it should be ready to use.

Instructions for Using the Application:

Visualization & It's Views:

Now that you have successfully installed the application, we will see how we can utilize the application. If you had to complete the final step above and ran the command "npm run build" from the Threat_Timeline directory, you may need to change the URL after logging into Splunk from "http://[your_IP_address]:[port_number]/en-US/app/launcher/home" to "http://[your_IP_address]:[port_number]/e en-US/debug/refresh". Then, you will need to hit the refresh button that appears and wait for the page to finish loading. From here, you can close this page and open Splunk once again from your search bar to see the changes.

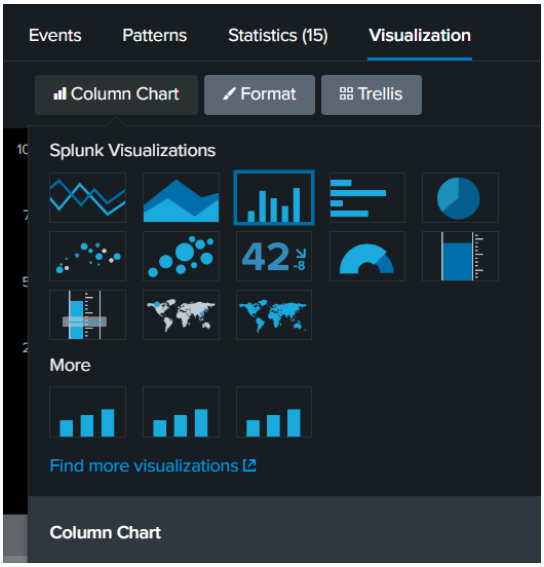
As mentioned above, in order to import the dataset from our lookup table, we will need to use the following command from within Splunk's Search and Reporting application:

| inputlookup <lookup_TableFileName.extension>

For the file we have provided, the correct file name and extension will be:

| inputlookup miniCU_total.csv)

Once we run this search from the Search Bar, we will see our data in table form in Splunk. From here, we want to select the Visualization Tab under the search bar. By default, this will bring up the "Column Chart" visualization. In order to access our visualization, you will need to click on the tab below visualization that says "Column Chart". Once you do this, you will see a list of Splunk visualizations to choose from that looks something like this:

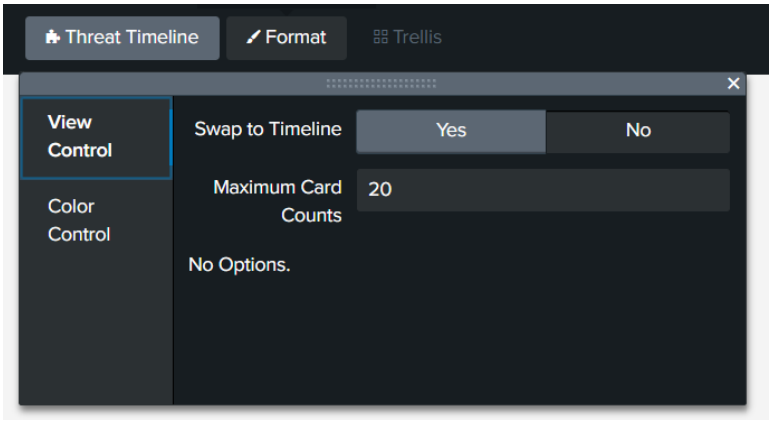


Under the “More” section, you will see a chart with 3 lines. When you hover over it, it should say “Threat Timeline”. This is our application. Click on it to select it as the visualization.

Once you select the visualization, you will see the threat timeline under the options and below it will be the data in table form, like we saw for the “Column Chart” Visualization. If the data is covering part of the visualization, you can simply drag the list of data so that it rests beneath the chart to see the chart in full. This is done by a small drag option that rests in the center point above the data.

Our default visualization is the “Tactic View”, where the threats from the dataset are sorted based on the attack tactic types they belong to. From this view, you can see the number of threats for each tactic type. Each attack is displayed on the main page with it’s unique title, as well as the technique used for each. For techniques that are longer than three words, the techniques are truncated to include only the first three words of the technique name. If you’d like to see more information, such as the full technique name and id, as well as a description of each tactic, you can hover your mouse cursor over each threat to see the full information as a pop up.

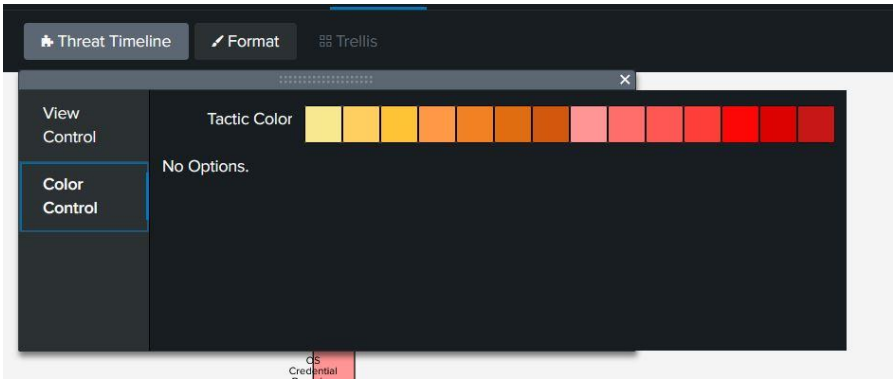
If you’d like to switch to the “Timeline View” to see the attacks in relation to time, you must click on the format menu tab next to the one labeled “Threat Timeline”. Once you click on it, it should look something like this:



To switch to the Timeline View, simply click the button labeled “Yes”. This will change the threats in the dataset to be arranged by time instead of by tactic. The functionality of the Timeline View is similar to the Tactic View, you can still hover over each card to see the full details of each attack, except in this view each threat is in a card format and each card is colored based on the severity of the tactic associated with it.

Color Changing:

If you would wish to change the color of a particular tactic type, you can change the color of a given tactic type by entering into the “Format” menu from above by clicking the “Format” button next to the “Threat Timeline” button. This will by default be in the “View Control” tab for determine the view options. To change the colors, click the “Color Control” menu and it will swap to the Color Control menu. It should look like the following:



Within this menu select the color you wish to change; then select the color you would wish to change it to or enter in the hexcode of your preferred color. With that done click off the prompt tab and the color will be applied.