

Synapse Bootcamp - Module 23

Stories - Exercises

Stories - Exercises	1
Objectives	1
Exercises	3
Creating a Story	3
Exercise 1	3
Part 1 - Create the Story	3
Part 2 - Add Elements from the Palette	6
Part 3 - Add Data from the Research Tool (Tabular Mode)	12
Part 4 - Add Additional Data from the Research Tool (Force Graph Mode)	16
Part 5 - Preview Your Story	20
Part 6 - Practice Adding and Resolving Comments	20

Objectives

In these exercises you will:

- Create a report in Synapse's Stories Tool and populate basic data
- Capture data from Synapse's Research Tool and add it to your Story
- Use data from different Research Tool Display Modes to convey your findings
- Add comments to a Story
- Resolve comments in a Story

Note: We are constantly updating Synapse and its Power-Ups! We do our best to make sure our course documents (slides, exercises, and answer keys) are up-to-date. However, you may notice small differences (such as between a screen capture in the documents and the appearance of your current instance of Synapse).

If something is unclear or if you identify an error, please reach out to us so we can assist!

Exercises

- This exercise uses the **Research Tool** with the **Storm Mode Selector** set to **Storm mode**.
- Some example queries may wrap due to length.

Creating a Story

Exercise 1

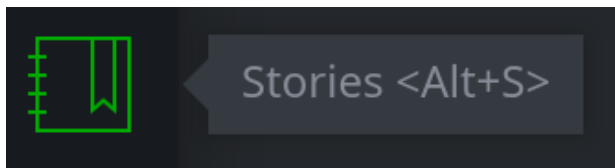
Objective:

- Use Synapse's Stories Tool to create a report containing data and communicating analytical findings.

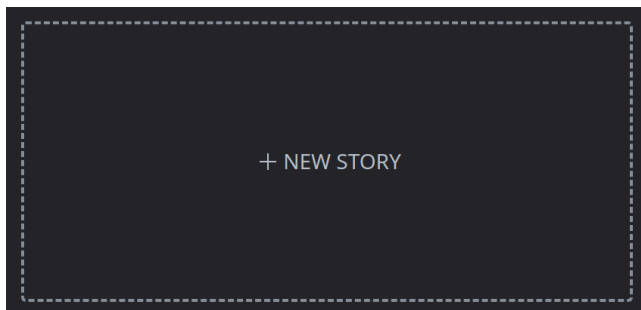
You recently identified a new spear phishing attack. You have attributed the attack and related indicators to a new threat cluster "T96". You want to create a Story to report your findings.

Part 1 - Create the Story

- From the **Toolbar**, select the **Stories Tool**:

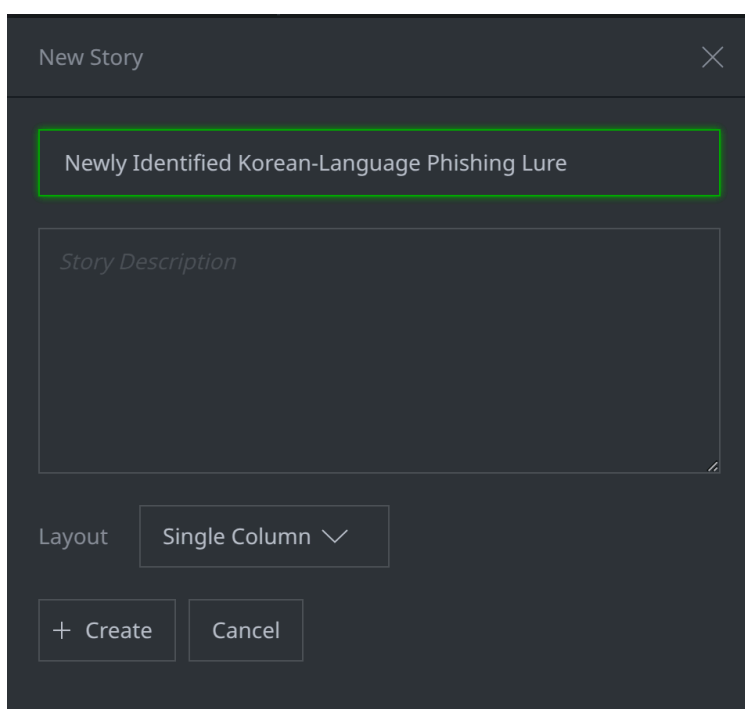


- In the **Stories Tool**, click on the **+ New Story** card to create a new Story:



- In the **New Story** input form, in the *Story Title* field, enter the following:

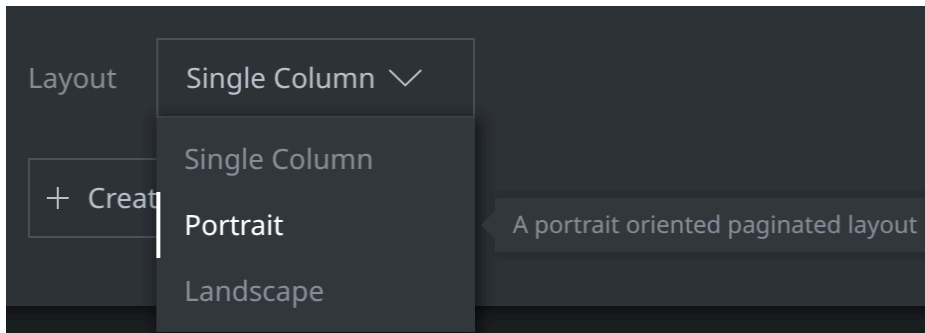
Newly Identified Korean-Language Phishing Lure

A dark gray modal window titled "New Story" with a close button (X) in the top right corner. Inside the modal, there is a text input field containing the text "Newly Identified Korean-Language Phishing Lure", which is highlighted with a green rectangular border. Below this field is a larger text area labeled "Story Description" in a lighter gray font. At the bottom left, there is a "Layout" label and a dropdown menu currently showing "Single Column" with a downward arrow. At the bottom, there are two buttons: "+ Create" and "Cancel".

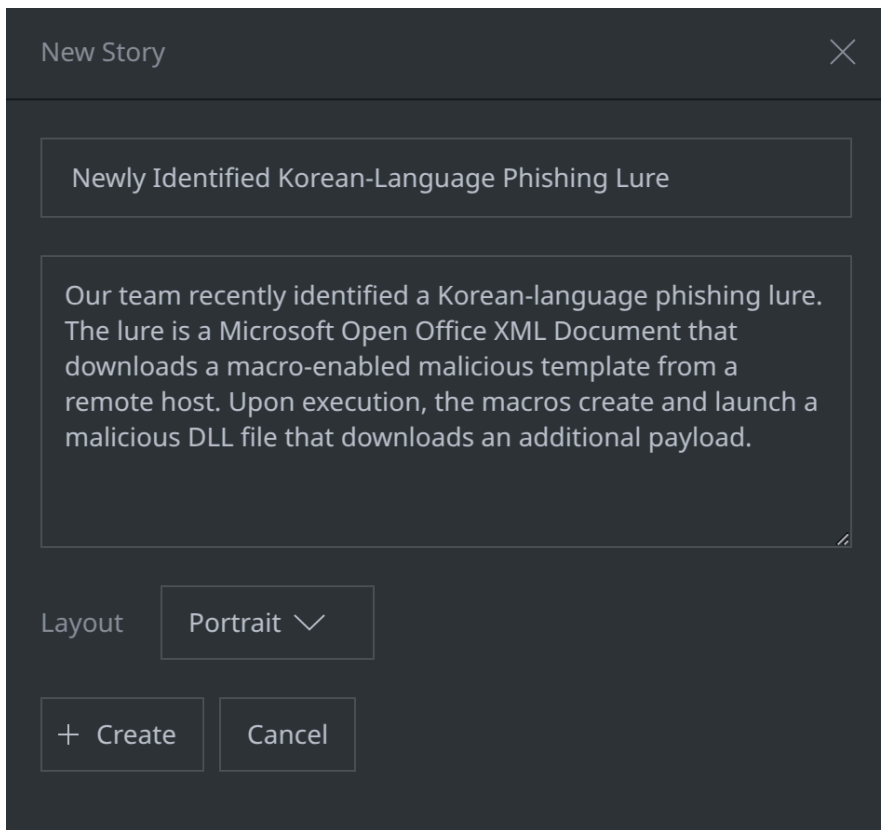
In the *Story Description* field, enter the following:

Our team recently identified a Korean-language phishing lure. The lure is a Microsoft Open Office XML Document that downloads a macro-enabled malicious template from a remote host. Upon execution, the macros create and launch a malicious DLL file that downloads an additional payload.

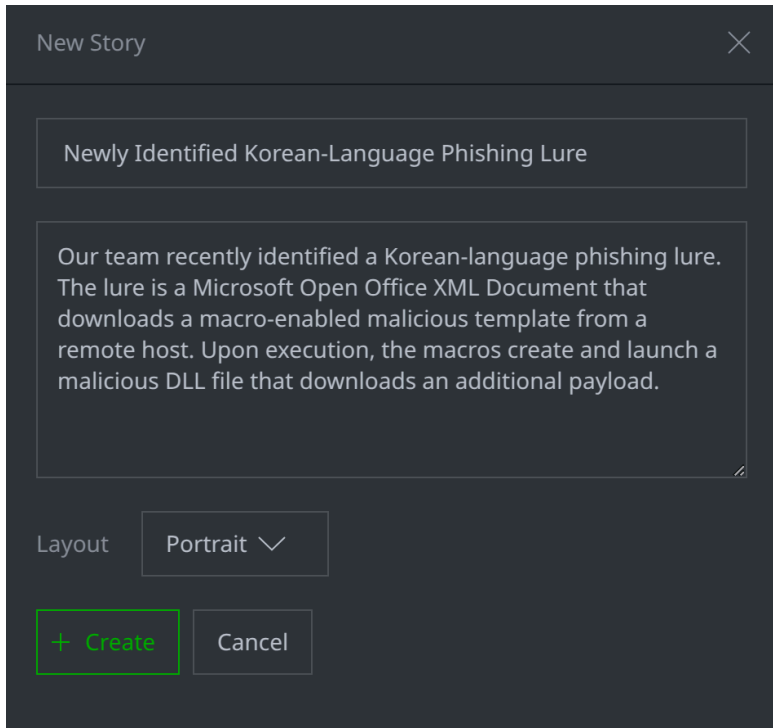
Use the dropdown menu to change the Layout from **Single Column** to **Portrait**:



Your **New Story** dialog should look like this:



- Click the + **Create** button to create the Story:

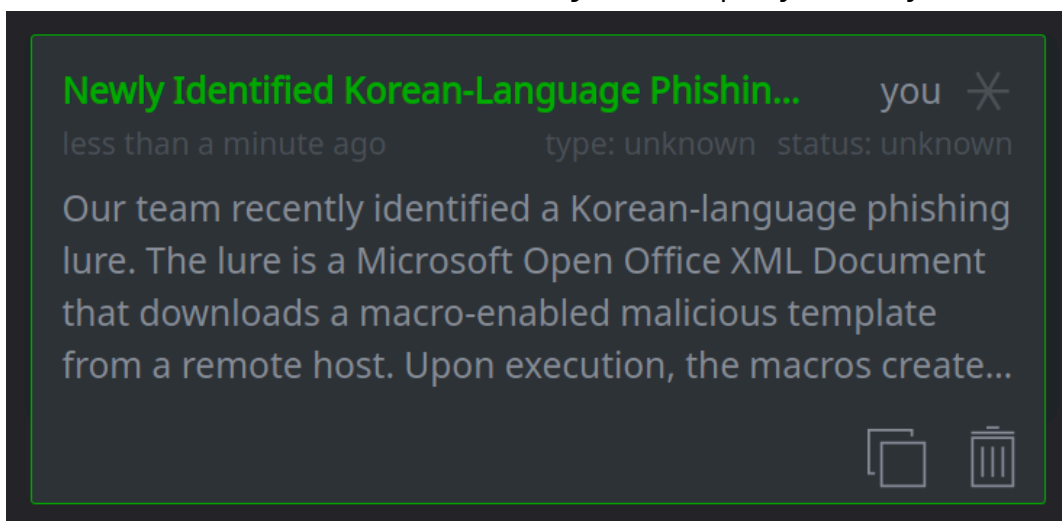


Question 1: After you create the Story, what is displayed in the Stories Tool?

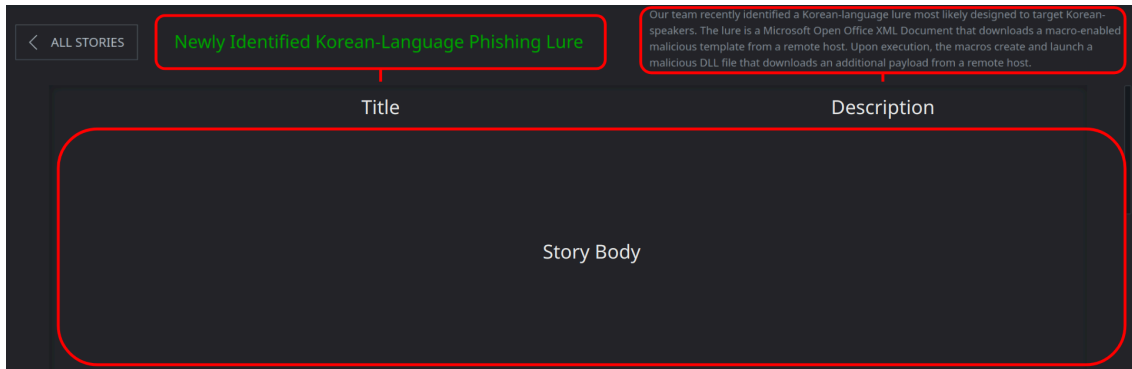
Part 2 - Add Elements from the Palette

Add the Story Title and Description

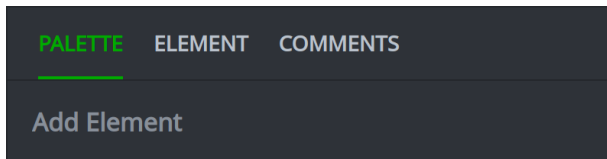
- In the **Stories Tool**, click on the new **Story card** to open your Story:



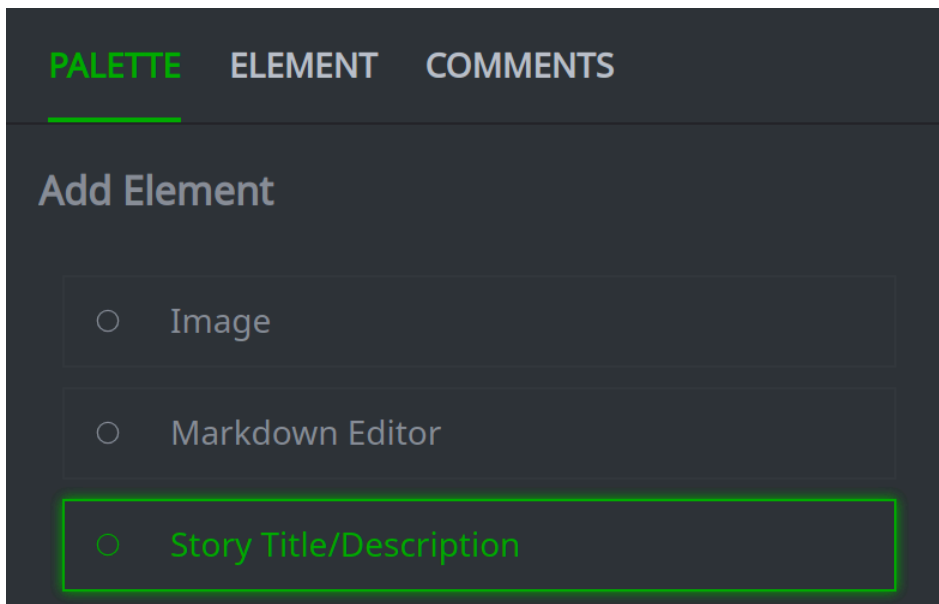
Note that the **title** and **description** you provided are visible at the top, but the **Story body** is blank:



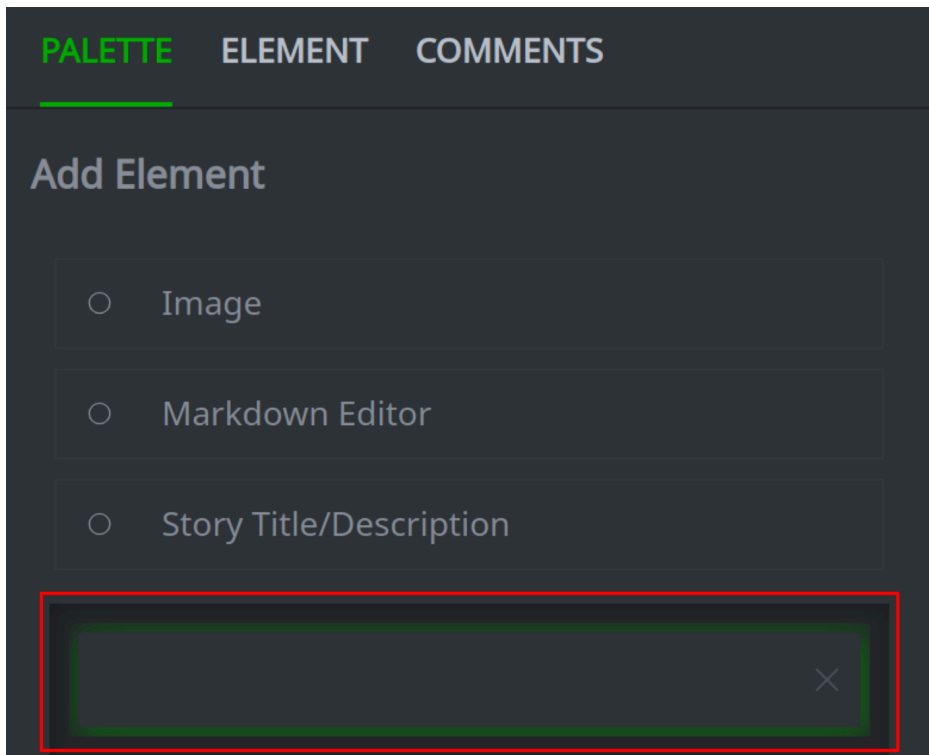
- In the **Stories Details Panel**, select the **PALETTE** tab:



- From the **Add Element** menu, click **Story Title/Description** to add this element to your clipboard:

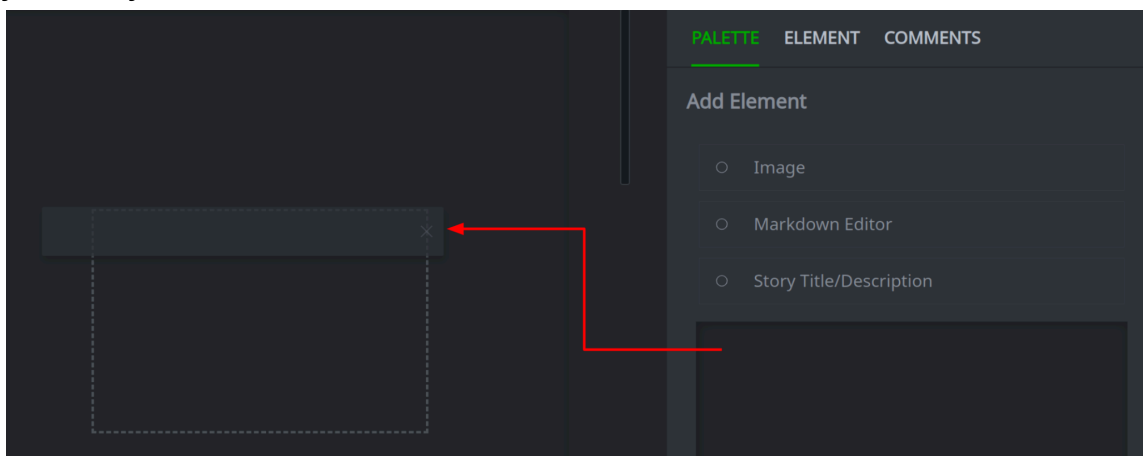


You should see a **gray rectangle** in your **Palette Clipboard**:

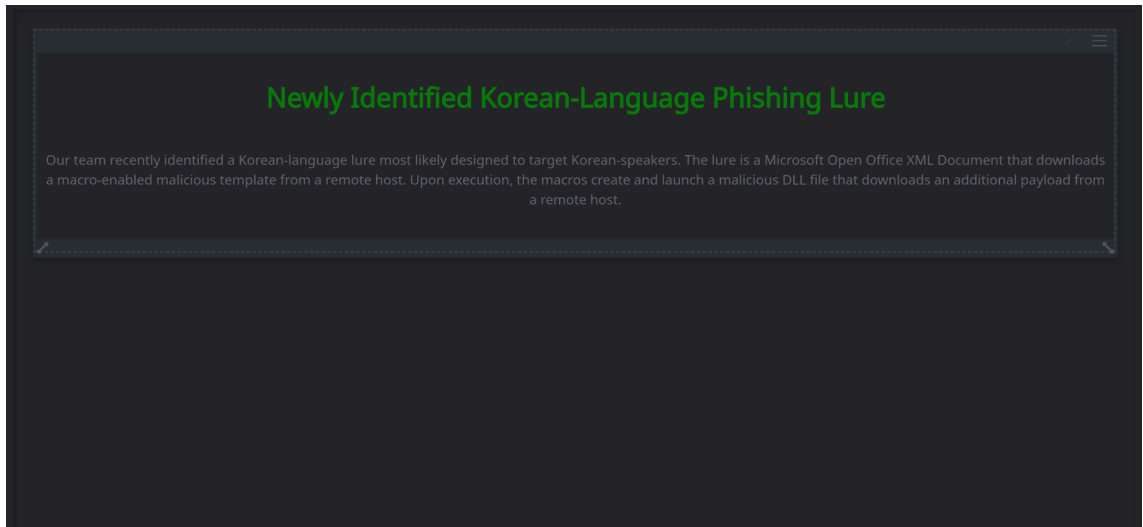


Tip: the rectangle briefly has a faint green outline (see above) and then fades to gray.

- In the **Palette Clipboard**, click and drag the **Story Title/Description** element onto your Story:



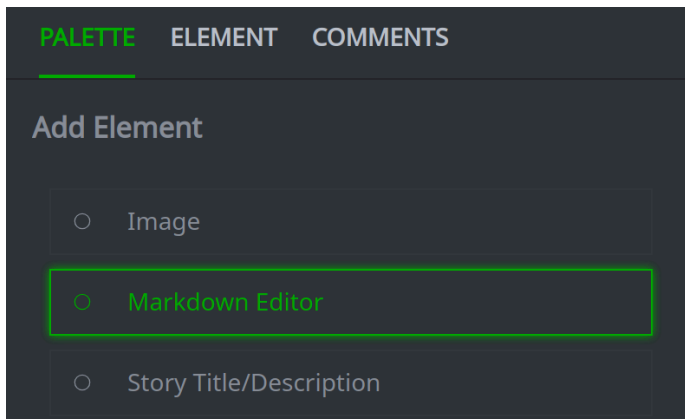
- **Resize** the element to position it across the top of your Story layout:



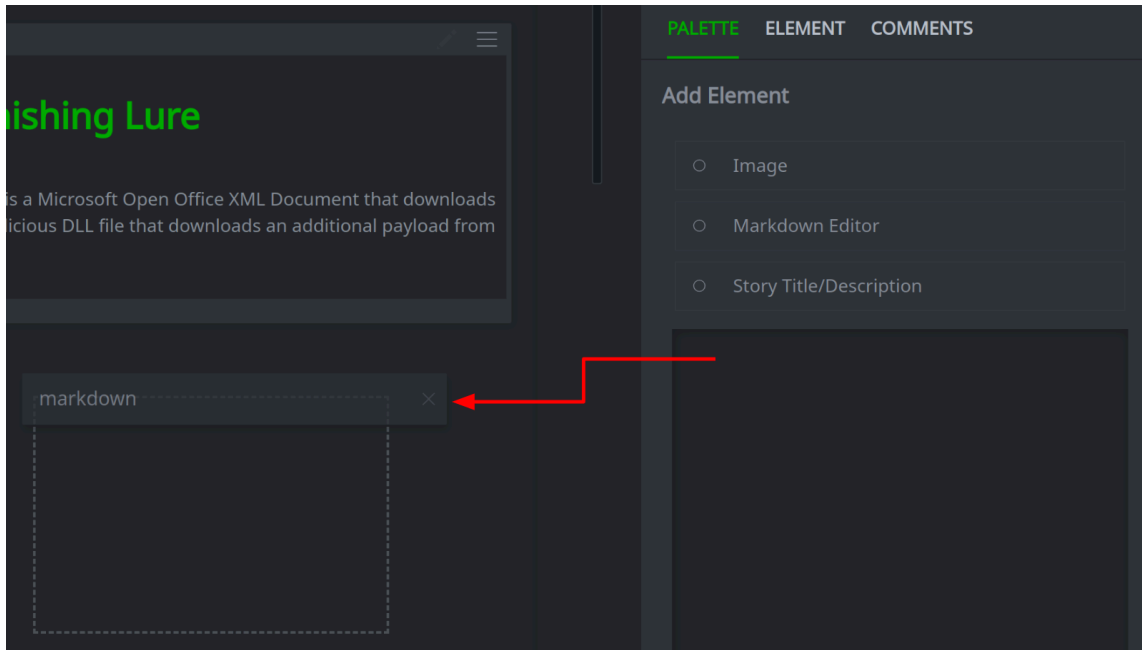
Question 2: What information is visible in the element once you place it in your Story?

Add a Summary

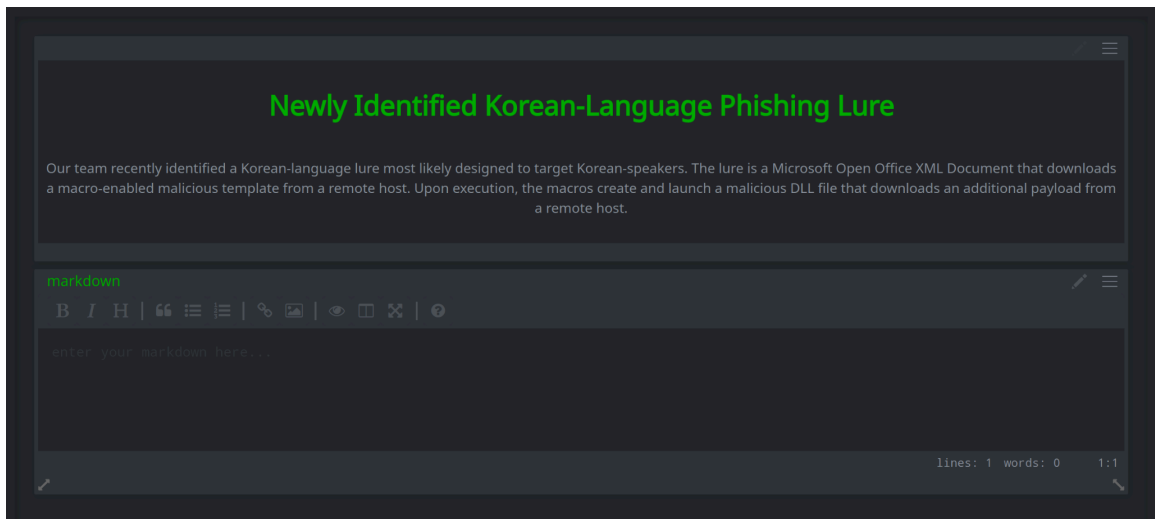
- In the **Stories Detail Panel**, on the **PALETTE** tab, click **Markdown Editor** to add this element to your Palette Clipboard:



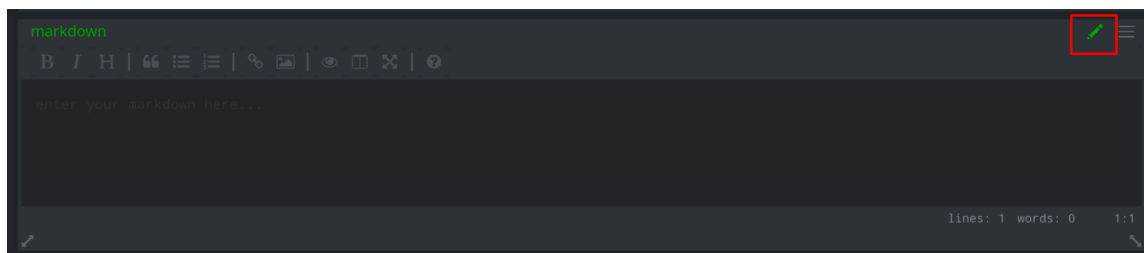
- **Click and drag** the **Markdown Editor** element from the **Palette Clipboard** onto your Story body:



- **Resize** the **Markdown Editor** element so that it extends the width of the Story layout:



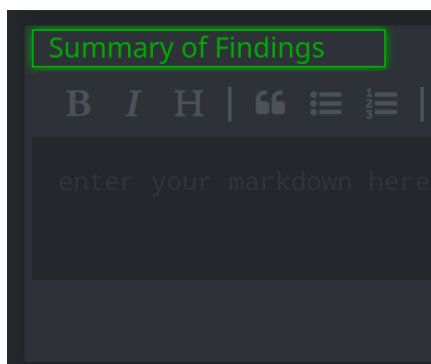
- Click the **edit** icon in the upper right corner of the **markdown** element to edit this element:



Question 3: How does the appearance of the **markdown** element change?

- In your **Story** body, **double-click** the title of the **markdown** element. Change the title to the following text and press **Enter** to save your changes:

Summary of Findings

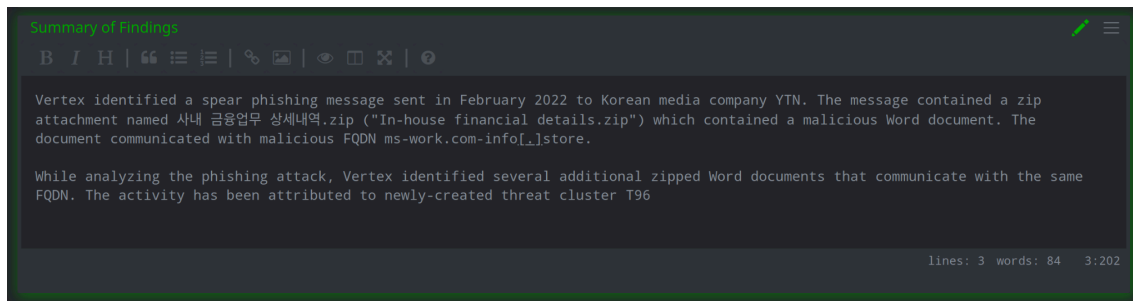


- In your Story body, in the **markdown** box, paste the following text:

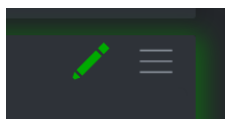
Vertex identified a spear phishing message sent in February 2022 to Korean media company YTN. The message contained a zip attachment named 사내 금융업무 상세내역.zip ("In-house financial details.zip") which contained a malicious Word document. The document communicated with malicious FQDN ms-work.com-info[.]store.

While analyzing the phishing attack, Vertex identified several additional zipped Word documents that communicate with the same FQDN. The activity has been attributed to the newly-created threat cluster T96.

Resize the element if necessary so you can see all of the text:

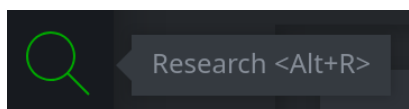


- Click the **edit** icon in the upper right corner of the element to stop editing:

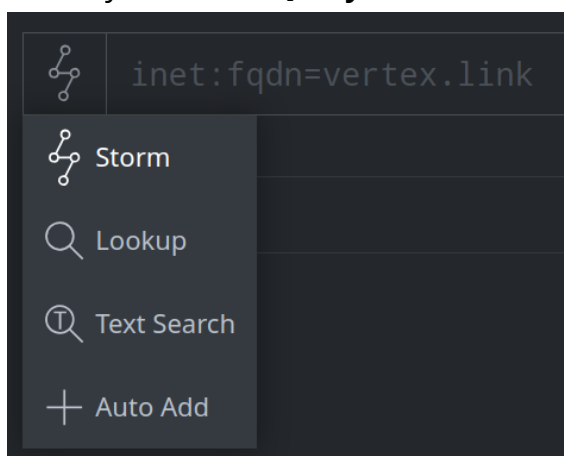


Part 3 - Add Data from the Research Tool (Tabular Mode)

- From the **Toolbar**, select the **Research Tool**:



- Ensure your **Storm Query Bar** is in **Storm mode**:

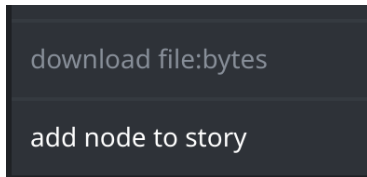


Add the Lure Document

- In the **Storm Query Bar**, run the following query to lift the **file:bytes** node for the lure document:

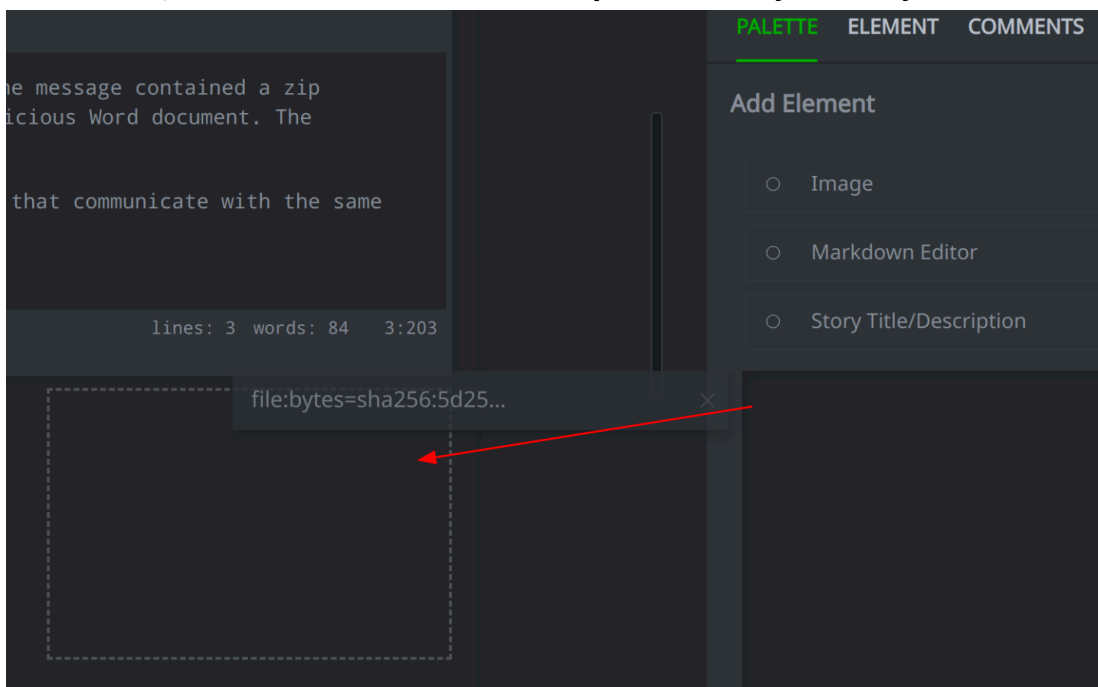
```
file:bytes=5d25e53b59bd2dcf234c6819f8cd294efe6d943d04625b9d575002362794e74a
```

- In the **Results Panel**, right-click the **file:bytes** node and select **add node to story** from the context menu:



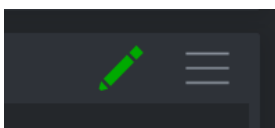
Question 4: What happens when you select **add node to story**?

- In the **Stories Tool**, from the **Stories Detail Panel**, **PALLETTE** tab, click and drag the **file:bytes** node from the **Palette Clipboard** onto your Story:



Resize the element if necessary so you can view the contents.

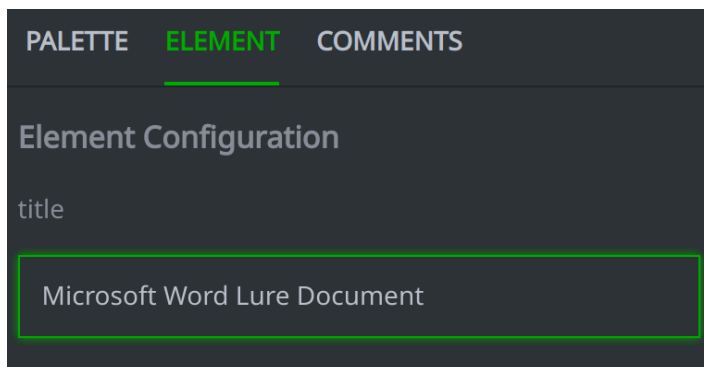
- Click the **Edit** icon on the element to enable editing.



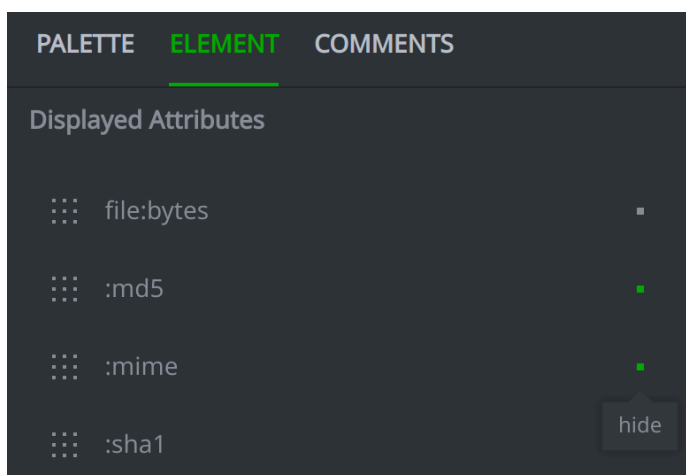
Question 5: What happens when you select the **Edit** icon? Which tab does Synapse display in the Stories Detail Panel?

- In the **Stories Detail Panel**, **ELEMENT** tab, change the **title** of the element to the following:

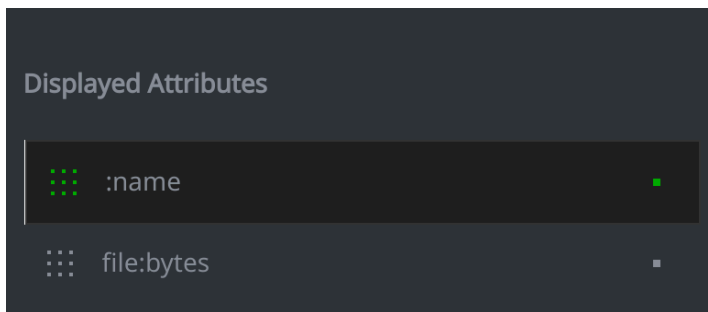
Microsoft Word Lure Document



- On the **ELEMENT** tab, under **Displayed Attributes**, use the **toggle** dots to the **right** of the properties so that **only** the following properties are selected:
 - **:md5**
 - **:mime**
 - **:name**
 - **:sha1**
 - **:sha256**
 - **:size**

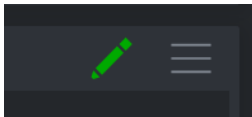


- Under **Displayed Attributes**, use the grid of dots to the **left** of each property to **click and drag** the displayed properties so they are listed in the following order:
 - **:name**
 - **:size**
 - **:mime**
 - **:md5**
 - **:sha1**
 - **:sha256**

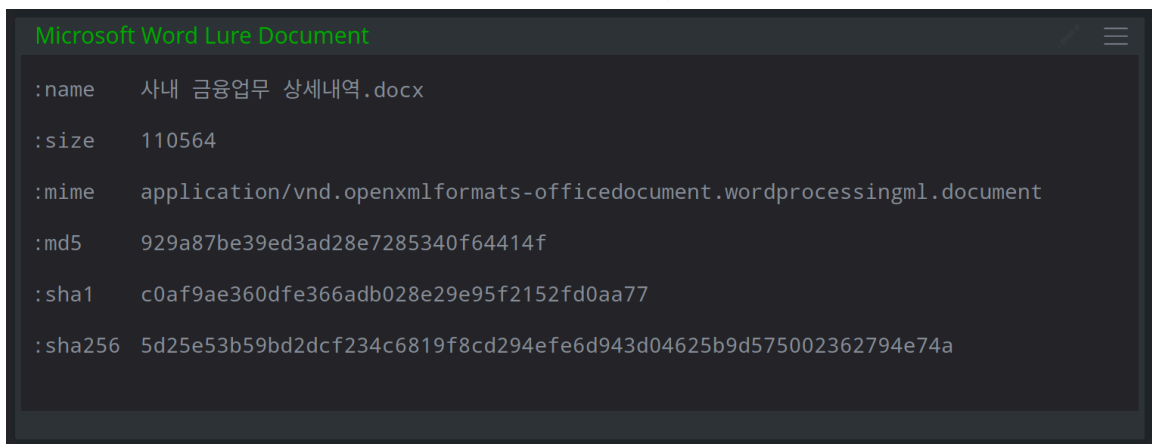


In your **Story body**, **resize** the element if necessary.

- When you are finished with your changes, click the **edit** icon in the upper right corner to stop editing:

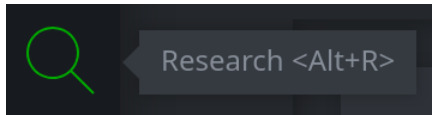


Your element should look similar to the following:

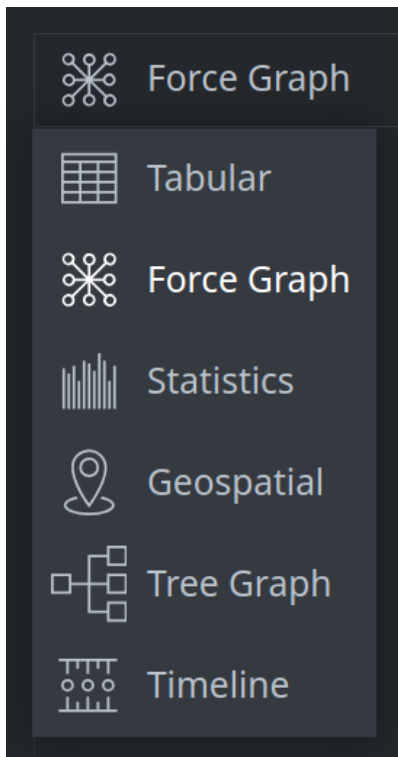


Part 4 - Add Additional Data from the Research Tool (Force Graph Mode)

- From the **Toolbar**, select the **Research Tool**:

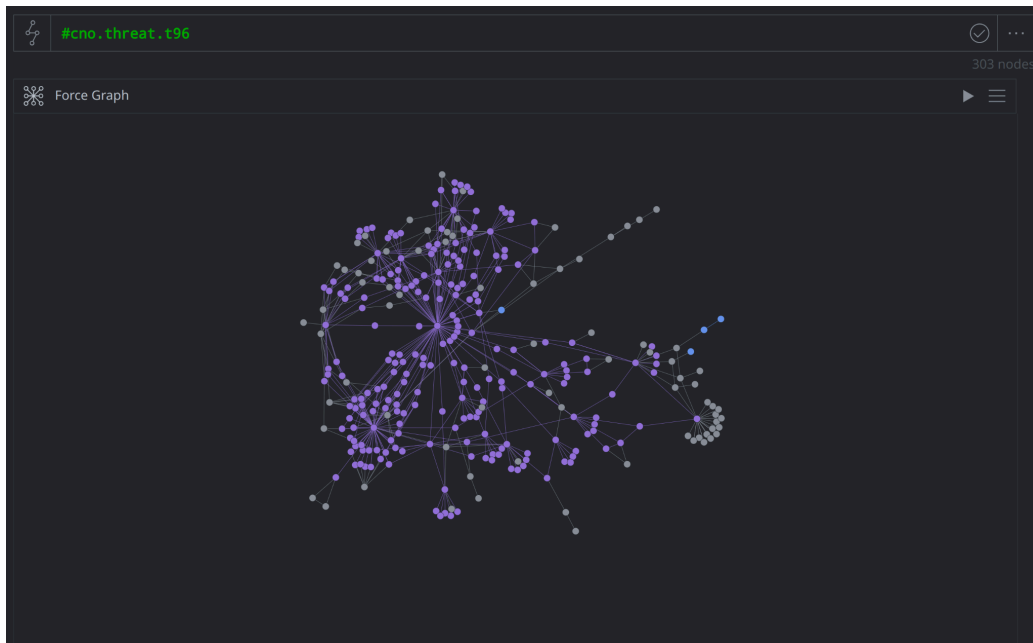


- Click the **Display Mode Selector** and choose **Force Graph** as your display mode:



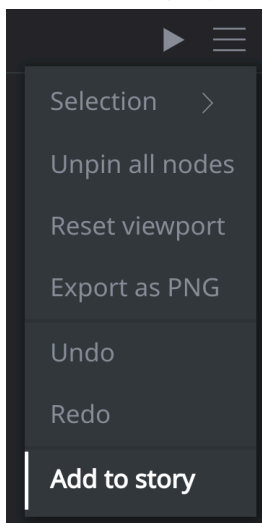
- Enter the following into the **Storm Query Bar** and press **Enter** run the query:

```
#cno.threat.t96
```

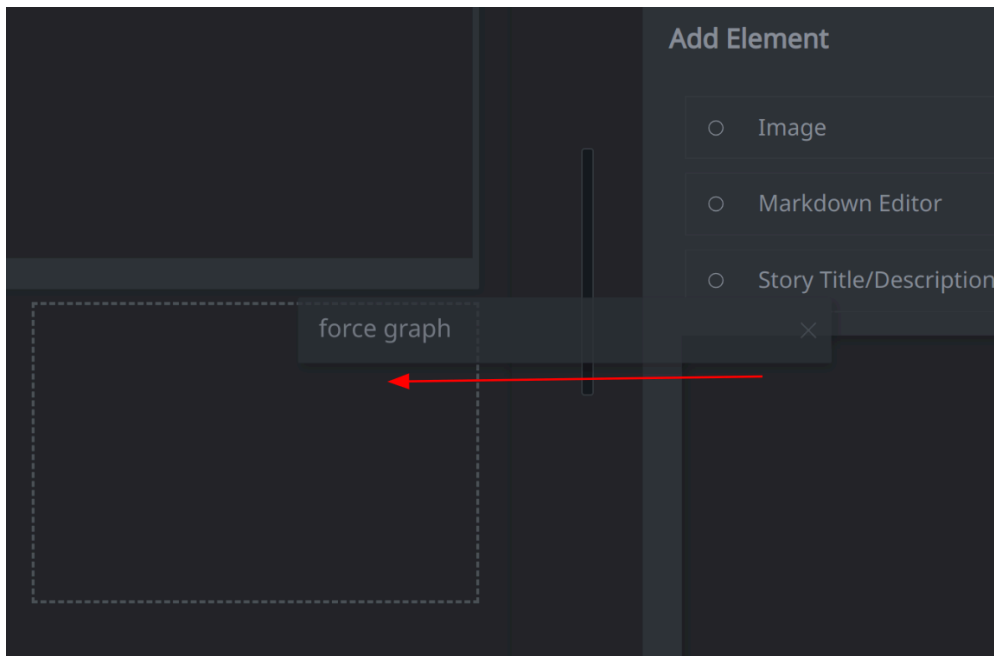
This query lifts all the nodes that are associated with threat cluster T96, which we created based on our research into the phishing attack.

- Click the display mode **hamburger menu** and select **Add to story**:

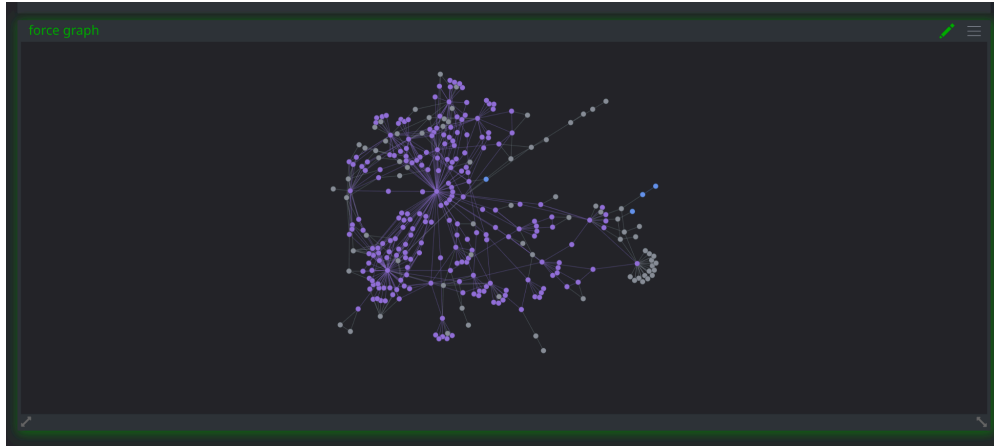


Note that Synapse returns you to the **Stories Tool**.

- In the **Stories Tool**, from the **Stories Detail Panel**, **PALLETTE** tab, **click and drag** the **force graph** element from the **Palette Clipboard** onto the Story:

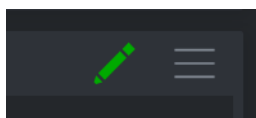


Resize the element to fit within the Story grid:



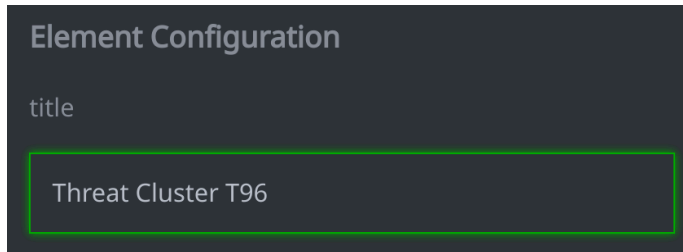
Note: you can adjust the **zoom** of the force graph (so the graph fits within the size of the overall element) using edit mode, below.

- Click on the **edit** icon in the upper right corner of the element:

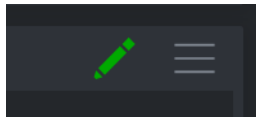


- In the **Stories Detail Panel**, **ELEMENT** tab, change the element **title** to:

Threat Cluster T96



- With the **edit** icon enabled:
 - Use your mouse wheel to adjust the **zoom** of the force graph so that it is sized the way you like.
 - **Click and hold** to drag the image so it is centered, if necessary.
 - If you need to reset or refresh the element, click the **hamburger menu** and select **Refresh Query**.
- When you are finished with your changes, click the **edit** icon in the upper right corner to stop editing:

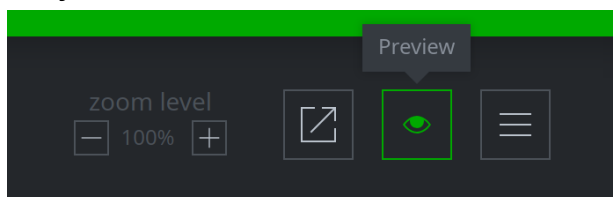


Your element should look similar to the following:



Part 5 - Preview Your Story

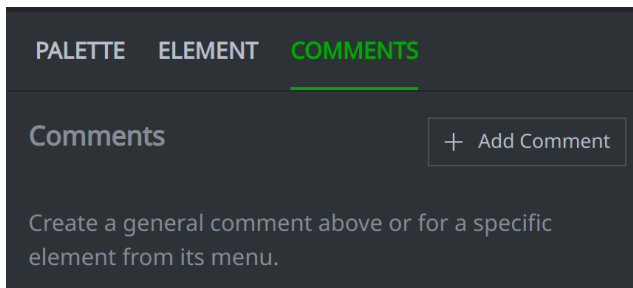
- In the **Stories Tool**, in the **Stories Task Bar**, click the **Preview** icon to see how your Story looks so far:



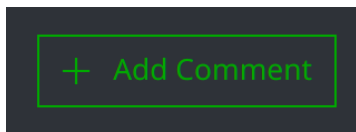
Question 7: How does the Story change when in Preview mode?

Part 6 - Practice Adding and Resolving Comments

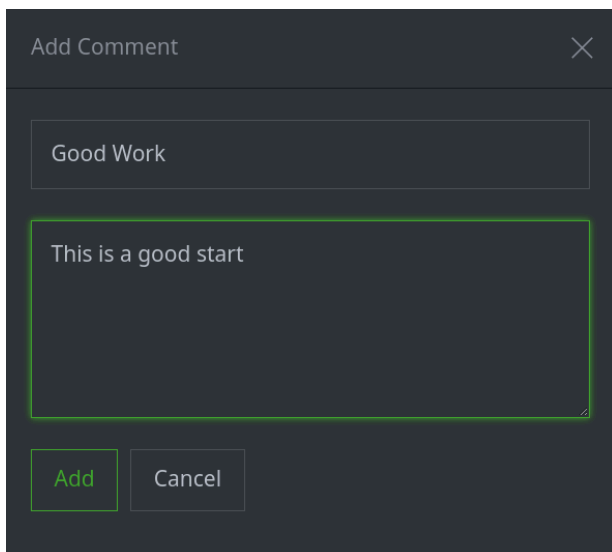
- In the **Stories Tool**, in the **Stories Detail Panel**, click the **COMMENTS** tab:



- Click the **+ Add Comment** button to create a comment:

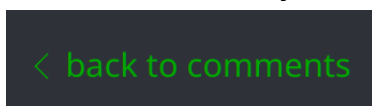


- In the **Add Comment** input form, enter:
 - **Good Work** in the *Subject* field
 - **This is a good start** in the *Message* field
- Click **Add** to add the comment:

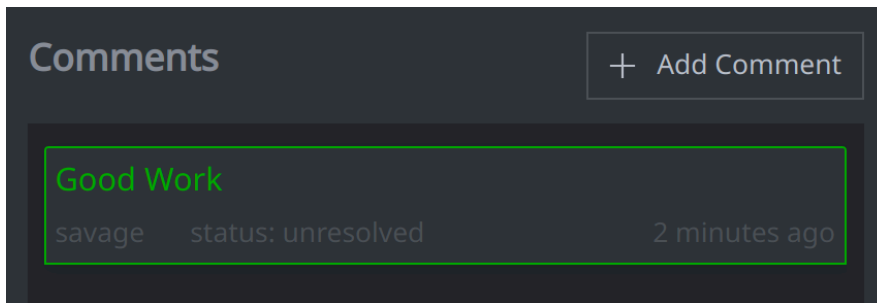


Question 8: What happens when you add the comment?

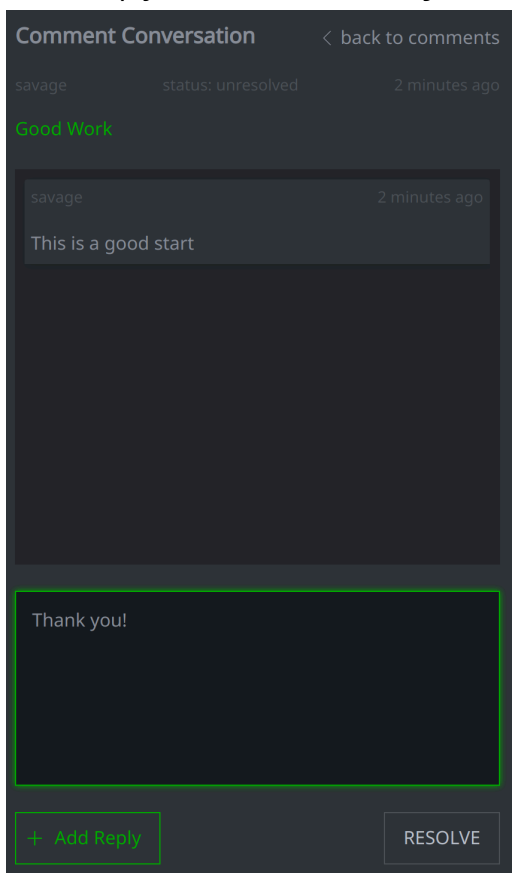
- In the **Comment Conversation** dialog, click **< back to comments**. This will display all the comments in your Story.



- **Click** on the comment you just created to open it:



- In the *Reply* field, enter **Thank you!** :



Click the **+Add Reply** button to add your response to the comment.

- Click the **Resolve** button to resolve the comment.



Question 7: What happens when you resolve the comment?
