Vertex

Synapse Bootcamp - Module 14

Modeling Data Manually - Exercises

Objectives

In these exercises you will learn:

- How to manually model data in Synapse based on real world information.

> **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

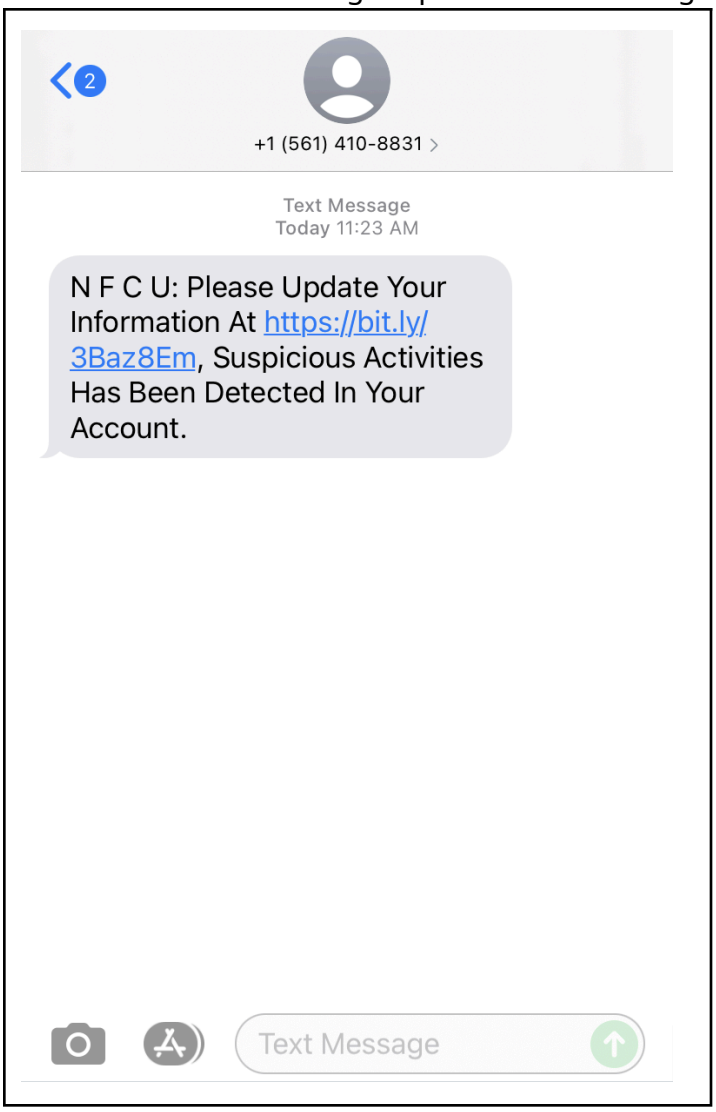
Modeling Data Manually

Exercise 1

Objective:

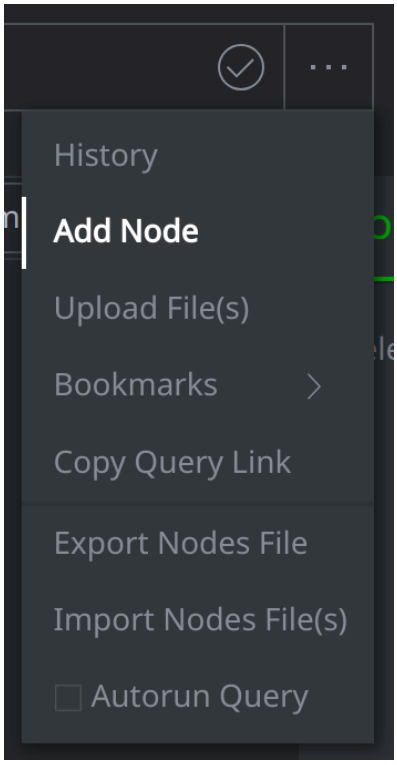
- **Use real world data to model an SMS-based phishing attack.**

You received the following suspicious SMS message:

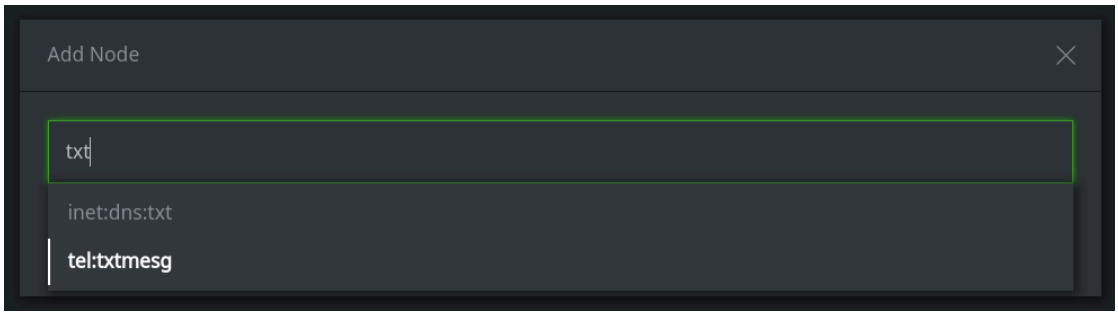


Synapse represents a mobile text message as a **`tel:txtmesg`** node.

- In the **Research Tool**, click the **Storm Query Bar Menu** (the three dots (**...**) or "meatball" menu) and select **Add Node:**



- In the **Add Node** dialog, start typing **txt** in the *Form* field to find forms that contain this string:



  Select **tel:txtmesg** from the dropdown list.

- Using information from the **screenshot** above, enter information into the **Add Node** input form to create the **`tel:txtmesg`** node. (**Note** that a **`tel:txtmesg`** is a guid form.)

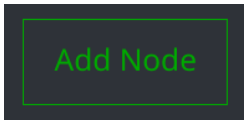
You should be able to fill in the following fields:

Field	Data
tel:txtmesg	*
from	The sending telephone number
svctype	The kind of message (e.g., SMS)
text	The content of the message (included **below** if you want to copy / paste)
time	The date / time the SMS was received ("today" at 11:23 AM)
to	The primary telephone number receiving the message (in this example, **you** received the SMS!)

Message text:

N F C U: Please Update Your Information At https://bit.ly/3Baz8Em, Suspicious Activities Has Been Detected In Your Account.

- When you have finished filling in the fields, click the **Add Node** button to create the node:



Question 1: What does your new **`tel:txtmesg`** node look like?

Exercise 2

Objective:

- **Use real world data to represent contact information for a company.**

Siemens is one of the many companies reportedly targeted by the "Winnti" group. You want to:

- verify that we have an organization node (**`ou:org`**) for Siemens, and
- create a contact (**`ps:contact`** node) to represent the company's global headquarters.

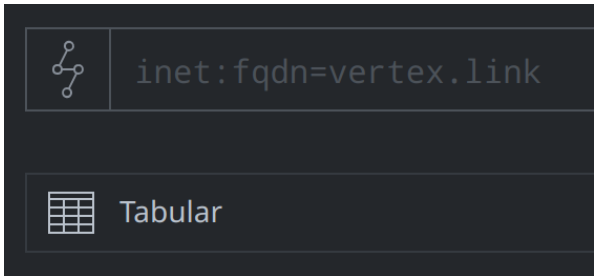
Part 1

First we will create the organization (**`ou:org`**) node.

- In your **web browser,** open the Siemens legal page listing their corporate headquarters information:

  `https://www.siemens.com/global/en/general/legal.html`

- In the **Research Tool,** ensure your **Storm Query Bar** is in **Storm mode** and your display mode is set to **Tabular:**



We will use the **`gen.ou.org`** command to create the node (or find an existing one). The command takes the **company name** as a parameter.

- Enter the following query into the Query Bar and press **enter** to run the command:

```
gen.ou.org siemens
```

Question 1: What happened? Did the command create a **new** node, or lift an existing node? How can you tell?

Part 2

Now we want to add a **`ps:contact`** node for Siemens' headquarters. We will use the **`gen.ou.org.hq`** command to create the contact (or find an existing one). This command also takes the **company name** as a parameter.

- Enter the following into the **Query Bar** and press **enter** to run the command:

```
gen.ou.org.hq siemens
```

Question 2: What happened? Did the command create a **new** node, or lift an existing node? How can you tell?

Use the information from the **Siemens website** to edit the **`ps:contact`** properties and add information for Siemens' **corporate headquarters.**

Hint: It may be easiest to make the changes using the **ALL PROPS** tab in the **Details Panel**.

You should be able to set the following properties on the **`ps:contact`** node:

Property	Data
address	The listed street address (as a single string). **Werner-von-Siemens-Straße 1, 80333 Munich, Germany** (**Note:** if you copy/paste from the web site, you may need to remove line breaks.)
asof	The last known date that the contact data was **current.** For a company's official website, it is reasonable to assume that the contact data is current as of **now.** (Some contact data may include a **last modified** or **last updated** field.)
email	The email address listed in the contact data.
loc	A dotted geolocation string for the location.
orgfqdn	The company's main FQDN zone (i.e., **siemens.com**).
phone	The phone number associated with the location / contact data.
phone:fax	The fax number associated with the location / contact data.
url	The URL for the company / contact data.

Question 3: What does your new **`ps:contact`** node look like?

Exercise 3

Objective:

- **Use public reporting to represent basic information about a compromise.**

QuoIntelligence published an article on the WINNTI threat group. The article listed several companies reportedly compromised by WINNTI. You want to capture this information using a `risk:compromise` node.

- In your **web browser,** view QuoIntelligence's report:

  https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/

- The relevant paragraph appears in the **Introduction,** along with an infographic:

  In the last year, researchers and journalists have publicly disclosed that the Winnti group targeted and eventually compromised Henkel (2014), BASF (2015), Bayer (2018) and Roche (2019). This most recent previously unreported German chemical company is yet another German chemical company targeted by Winnti since 2015. Prior to our analysis this attack activity was not publicly reported.

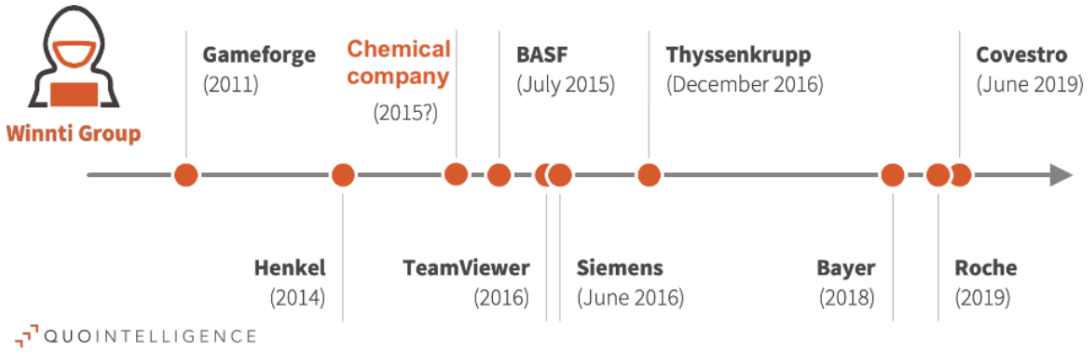


Figure 1: Timeline of attacks located in Germany and attributed to Winnti

We will use **Siemens (June 2016)** as an example to model a `risk:compromise` node.

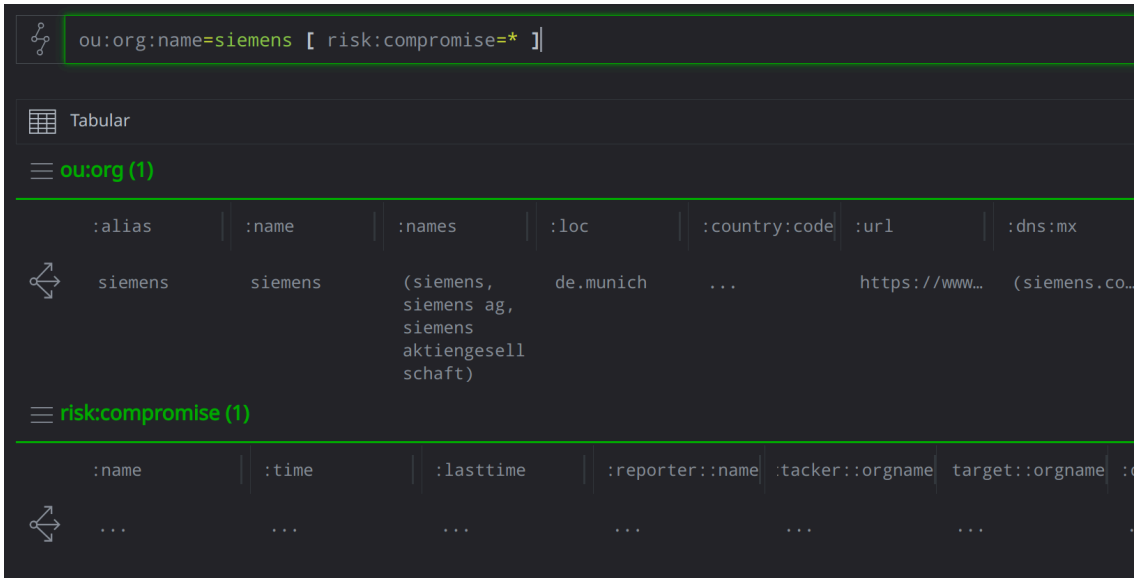
- Enter the following into the **Storm Query Bar** and press **Enter** to lift the `ou:org` node for Siemens:

```
ou:org:name=siemens
```

- **Modify** your query to use a Storm edit operation to create a new `risk:compromise` node, and press **Enter** to run the query:

```
ou:org:name=siemens [ risk:compromise=* ]
```

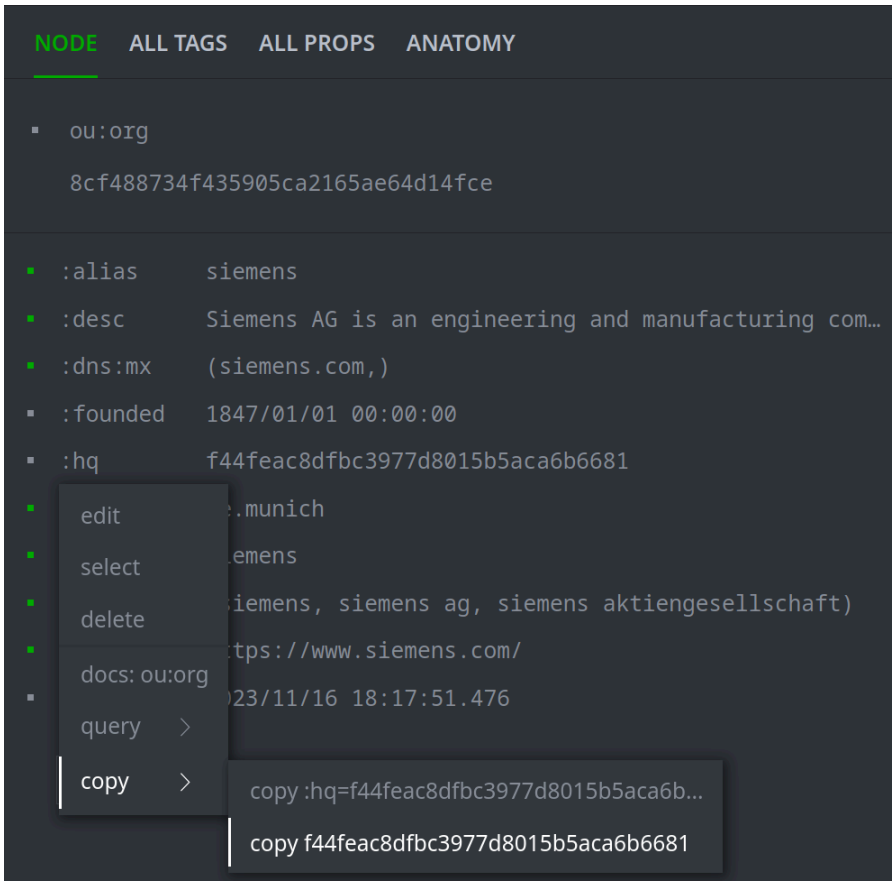
You should see **both** nodes in your **Results Panel:**



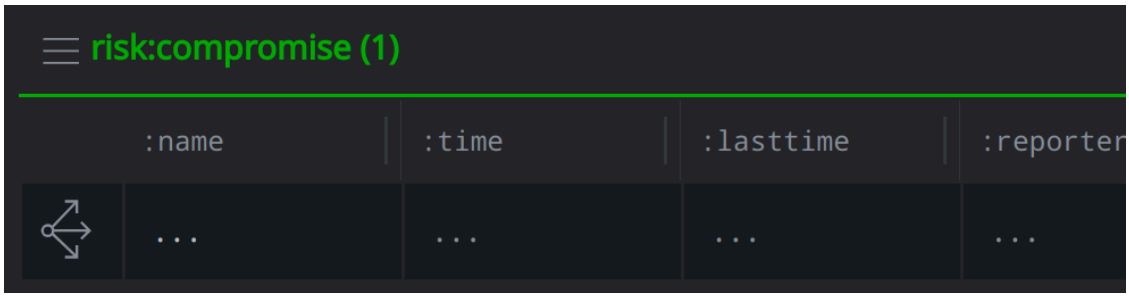
First we will set Siemens as the **target** of the compromise. The target will be the **`ps:contact`** associated with the Siemens' **`ou:org`** node (i.e., the **`ou:org:hq`** property).

- In the **Results Panel, select** the **`ou:org`** node for Siemens:

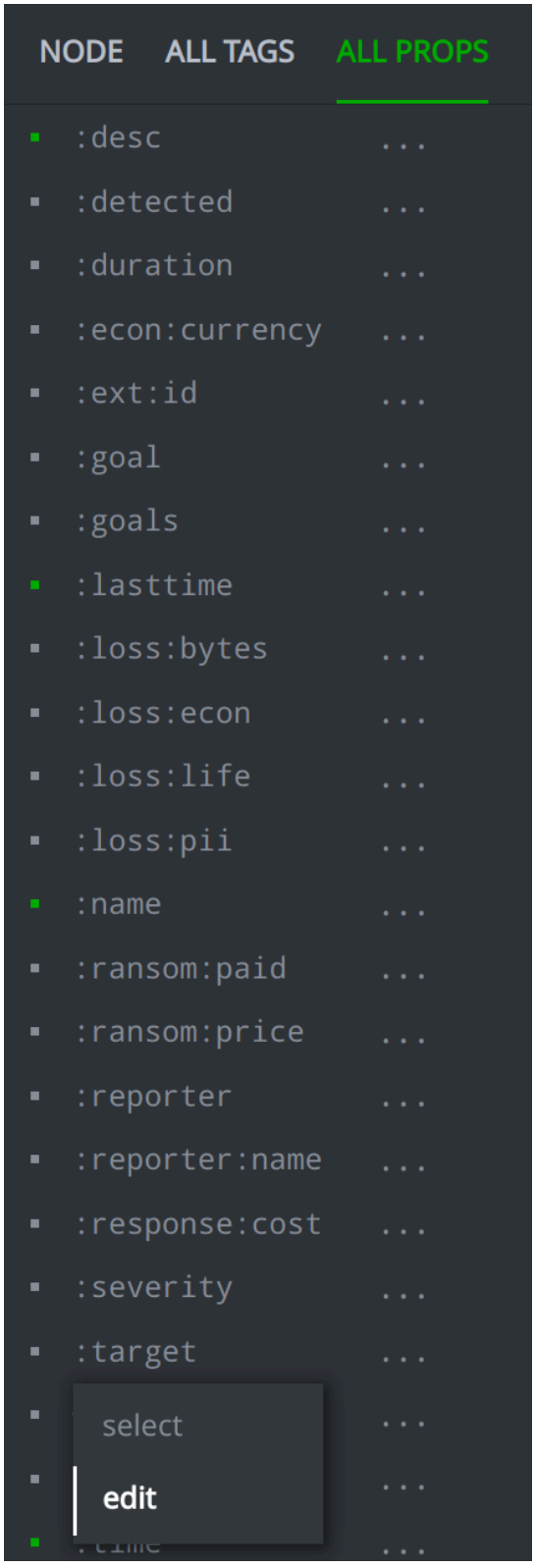
- In the **Details Panel** (**NODE** tab), **click** the **`:hq`** property and select **copy > copy f44feac8dfbc3977d8015b5aca6b6681** from the menu:



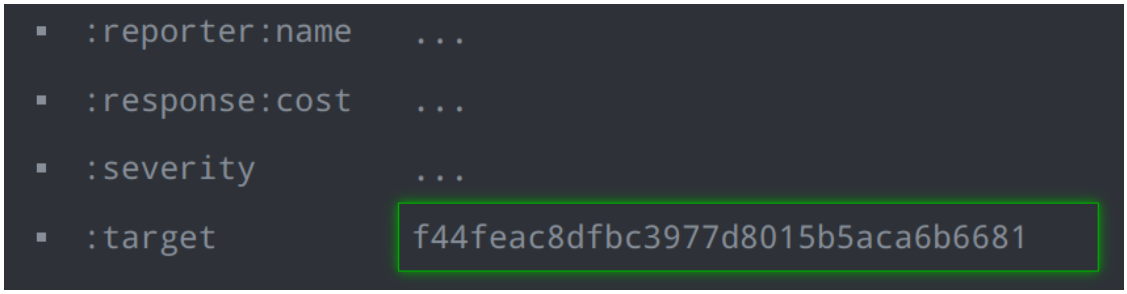
- In the **Results Panel, select** the `risk:compromise` node:



- In the **Details Panel** (**ALL PROPS** tab), click the **`:target`** property and select **edit:**



- **Paste** in the guid you copied from the **`:hq`** property and press **Enter** to save the change:



Now we will set additional properties for the **`risk:compromise`**.

Use the information from the **QuoIntelligence infographic** to edit the **`risk:compromise`** properties and add information.

- Use the **Details Panel** (**ALL PROPS** tab). You should be able to set the following properties using information from QuoIntelligence's report (the graphic is included below):

Property	Data
desc	Description of the compromise
name	Brief name for the compromise
reporter:name	Set to “QuoIntelligence” to indicate the reporter’s name
time	Best known "start time" for the compromise **Note:** use the date/time provided in the infographic.

In the last year, researchers and journalists have publicly disclosed that the Winnti group targeted and eventually compromised Henkel (2014), BASF (2015), Bayer (2018) and Roche (2019). This most recent previously unreported German chemical company is yet another German chemical company targeted by Winnti since 2015. Prior to our analysis this attack activity was not publicly reported.

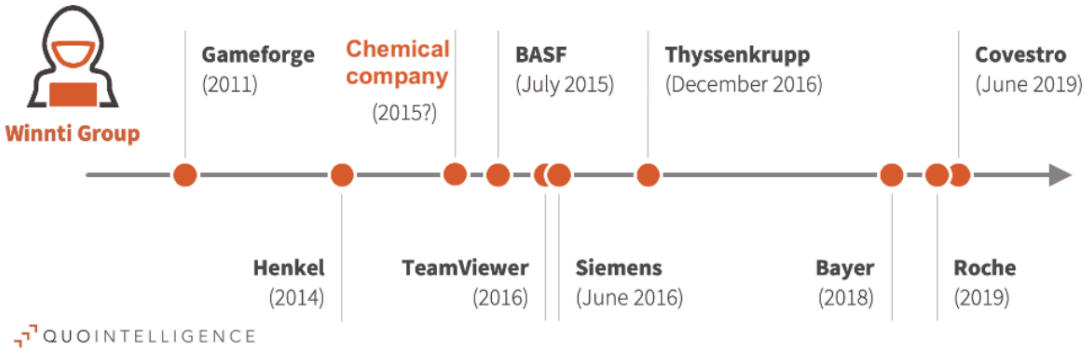
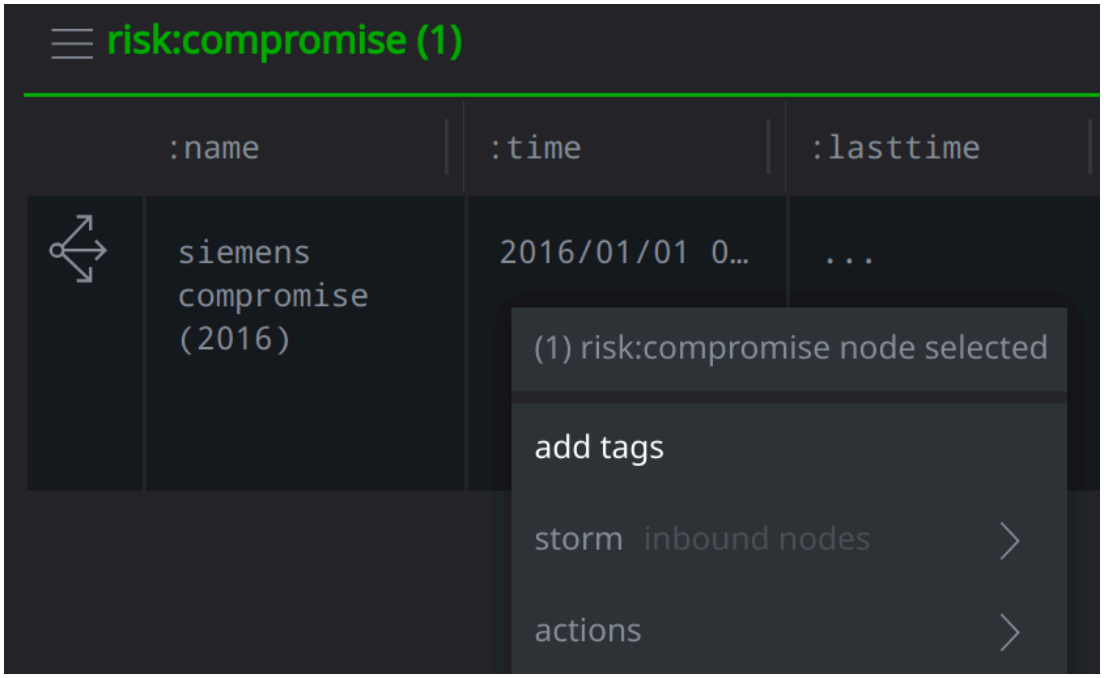


Figure 1: Timeline of attacks located in Germany and attributed to Winnti

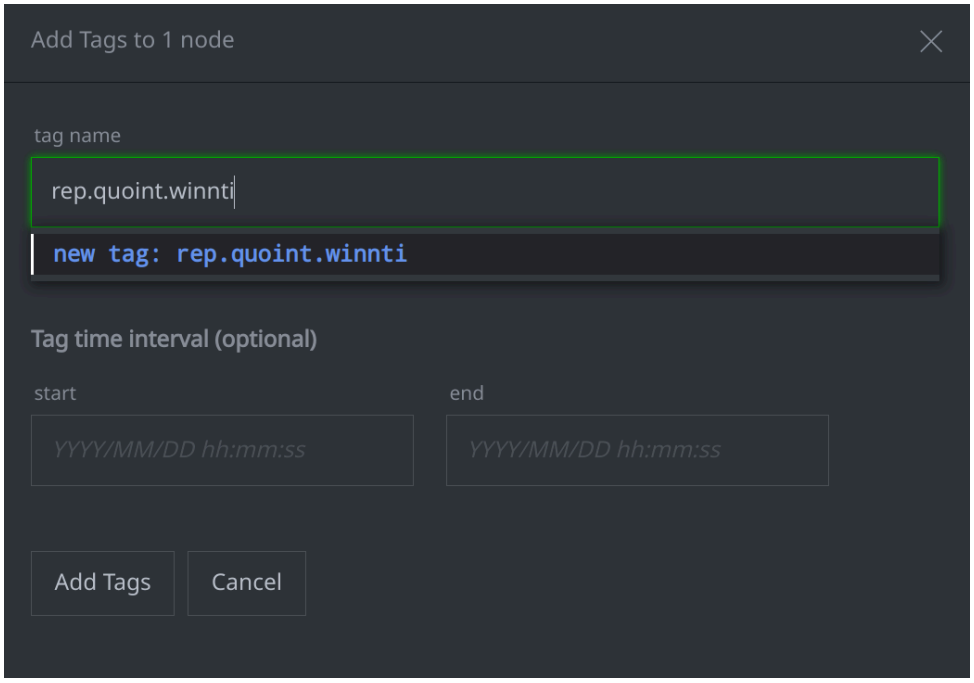
---

Finally, we will **tag** the `risk:compromise` node so we know that QuoIntelligence attributes the compromise to the WINNTI threat group.

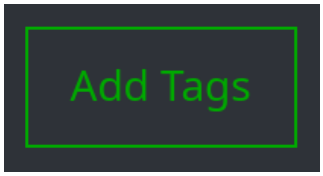
- In the **Results Panel, right-click** the node and select **add tags:**



- In the **Add Tags** dialog, add the tag **rep.quoint.winnti** to show that QuoIntelligence attributes the compromise to the WINNTI group:



Click the **Add Tags** button to apply the tag:



Question 1: What does your **`risk:compromise`** node look like?

Verify that the compromise is now linked to Siemens in Synapse.

- In your **Results Panel,** select the **`ou:org`** node for Siemens:

Question 2: Can you use the **Explore** button to navigate from the Siemens **`ou:org`** node, to its **`ps:contact(s)`**, and then from the **`ps:contact`** to the **`risk:compromise`** node?

Question 3: Is there a Storm query you could use to do this?
