Vertex

Synapse Bootcamp - Module 14

Modeling Data Manually - Answer Key

Answer Key

Modeling Data Manually

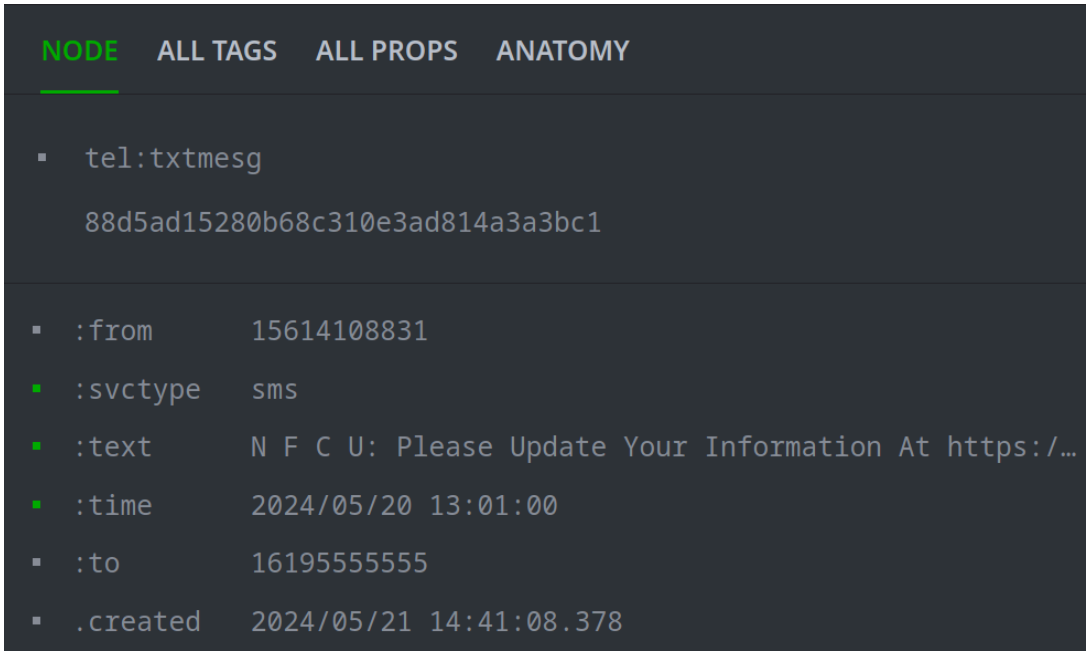
Exercise 1 Answer

Objective:

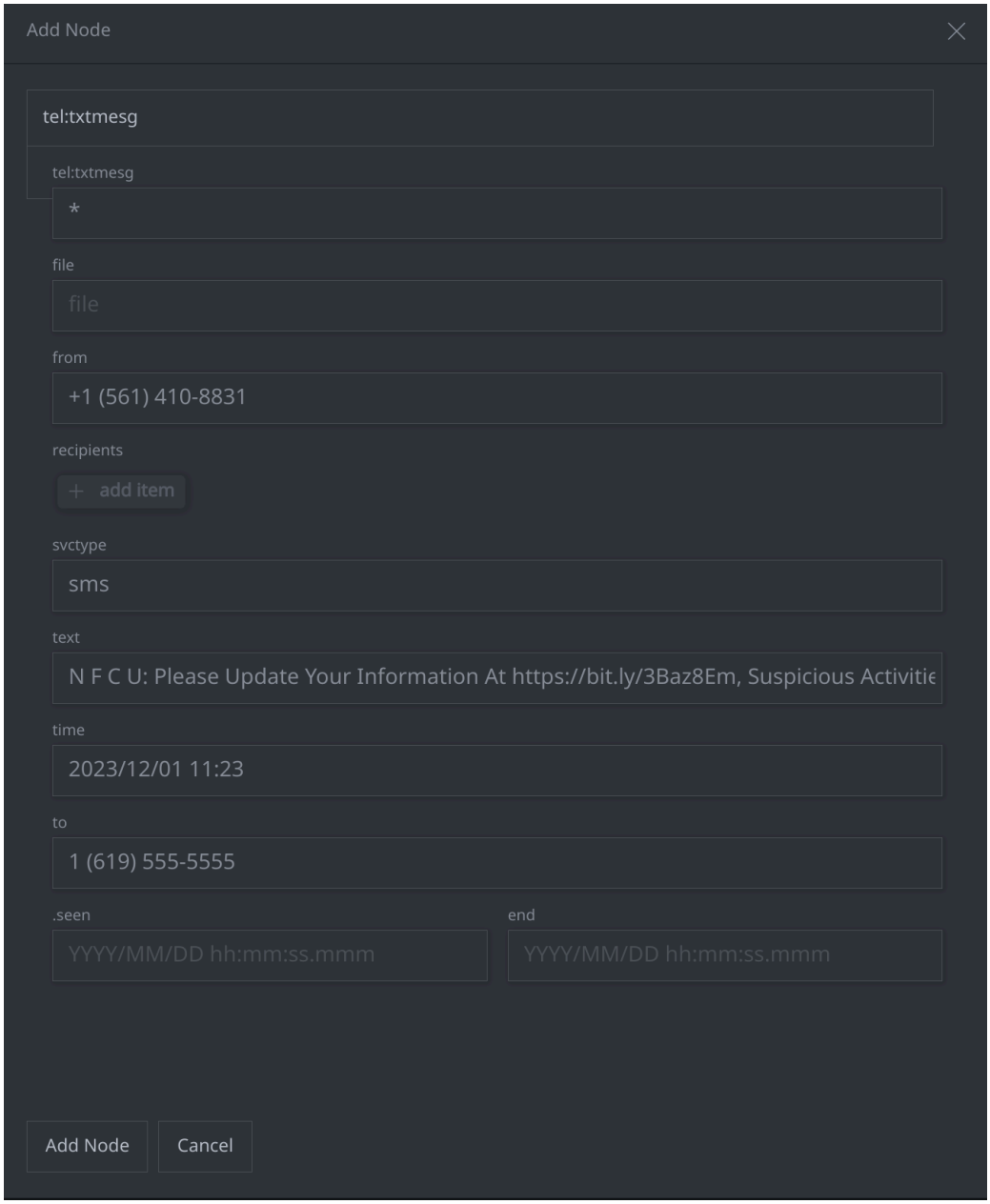
- **Use real world data to model an SMS-based phishing attack.**

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

- Your completed node should look similar to the following:



When you fill in the **Add Node** dialog, it should look similar to the following:



When creating nodes, the **Add Node** dialog helps by showing you available properties and providing hints (tooltips) for the type of data to fill in.

Because secondary properties are all **optional,** you can always create the node and add or edit properties later in the Research Tool.

Exercise 2 Answer

Objective:

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

Part 1

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

- Synapse displays an **`ou:org`** node for Siemens:

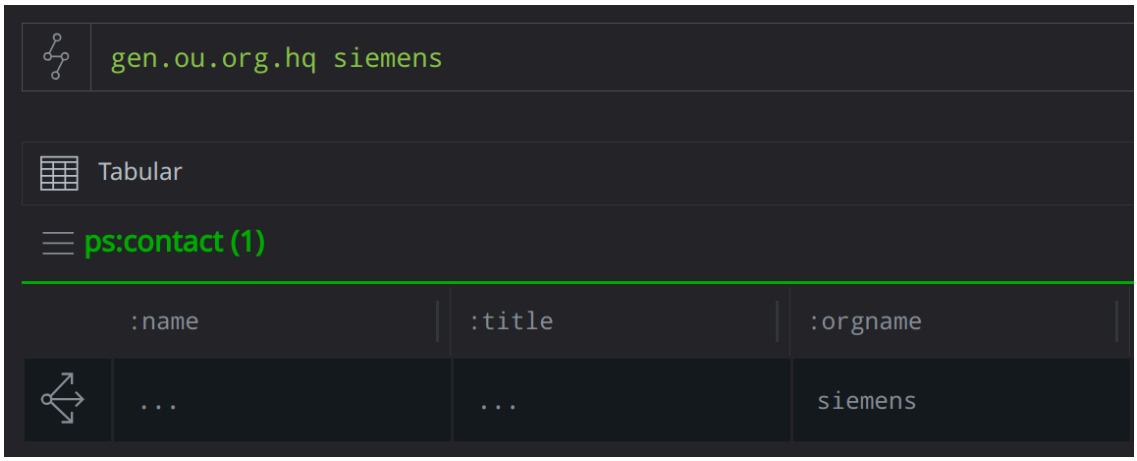
- Synapse returned an **existing** node - the command used the name you provided (**siemens**) to find the node.

  You can tell this is an existing node because:
  - Many node properties are already set. If Synapse had created a **new** node, only the **`:name`** property would be set.
  - The node has a **`.created`** timestamp of **2023/11/16 18:17:51.476,** which shows when it was created in Synapse.

Part 2

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

- Synapse displays a **`ps:contact`** node for Siemens:

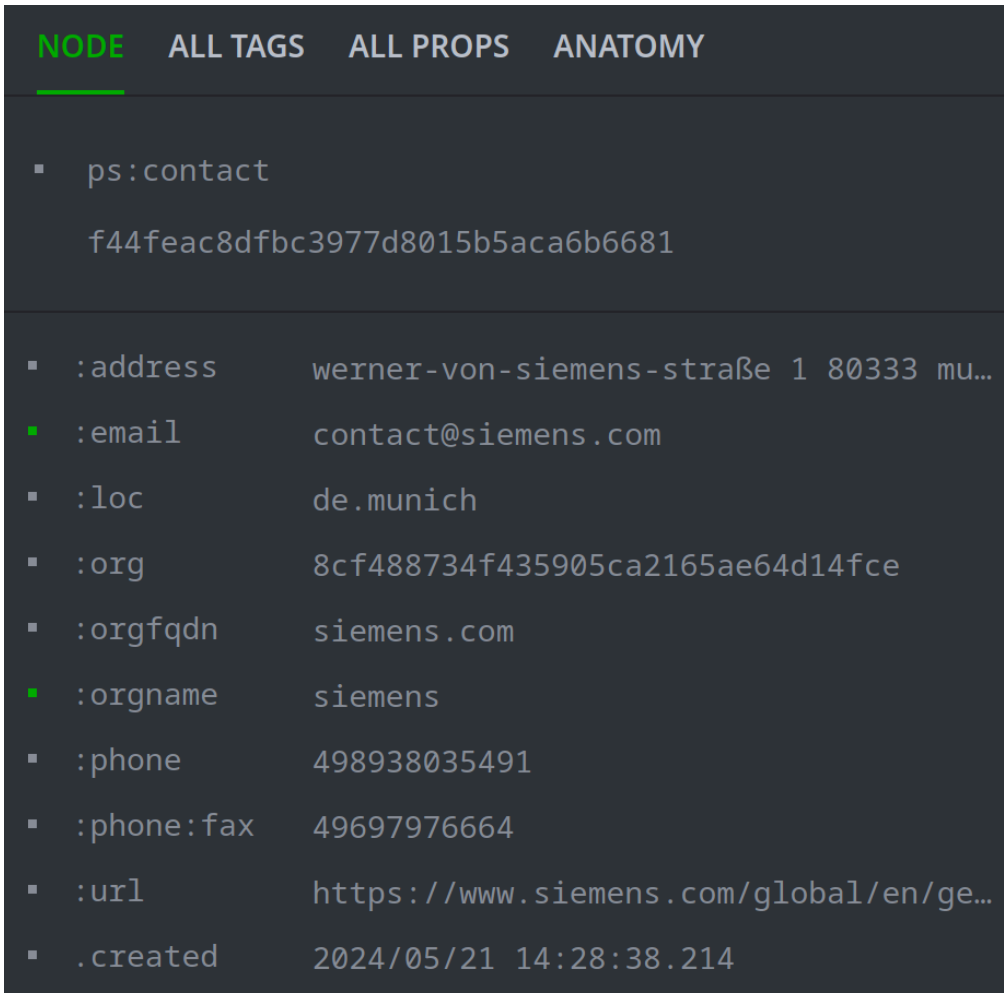


- Synapse returned a **new** node. If the **`ou:org`** for the name **siemens** does not have its **`:hq`** property set, the command creates a new contact.

  You can tell this is a new node because:
  - Only the **`:orgname`** (and **`:org`**) properties are set. Synapse automatically links the contact and the organization (**`ou:org`**).
  - The **`.created`** time for the node should be the current date and time. This shows the node was just added.

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

- Your **`ps:contact`** should look similar to the following:

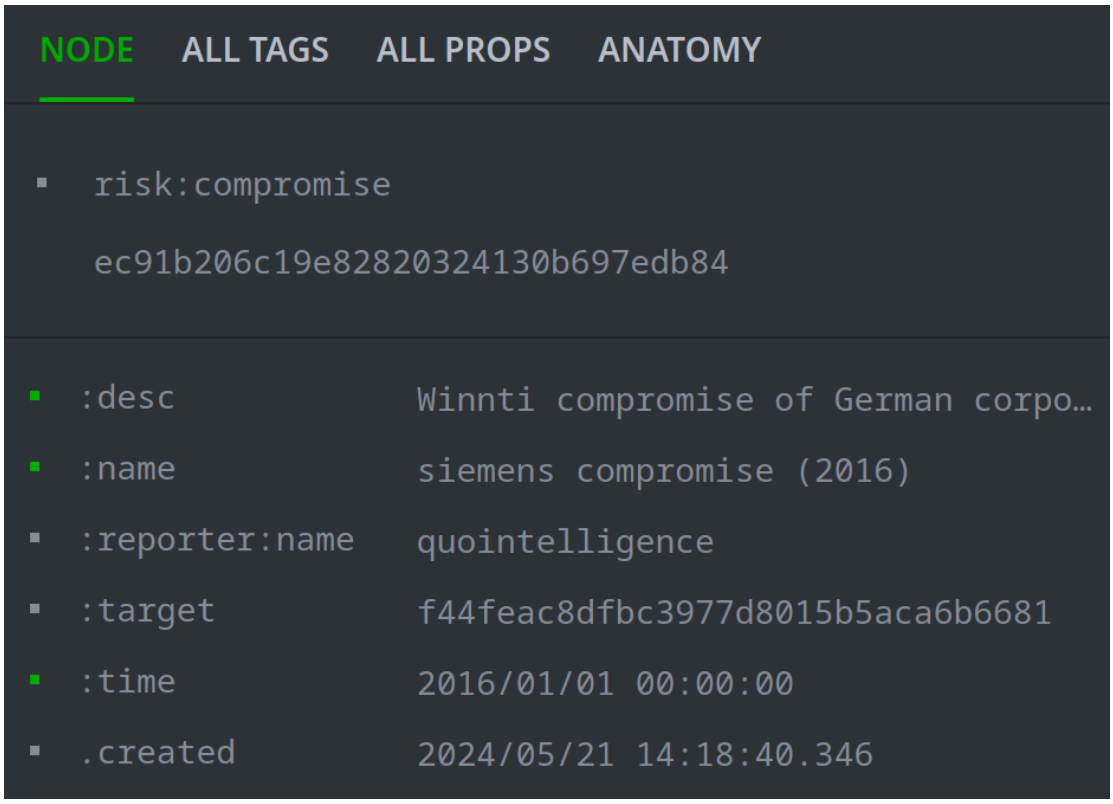


Exercise 3 Answer

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

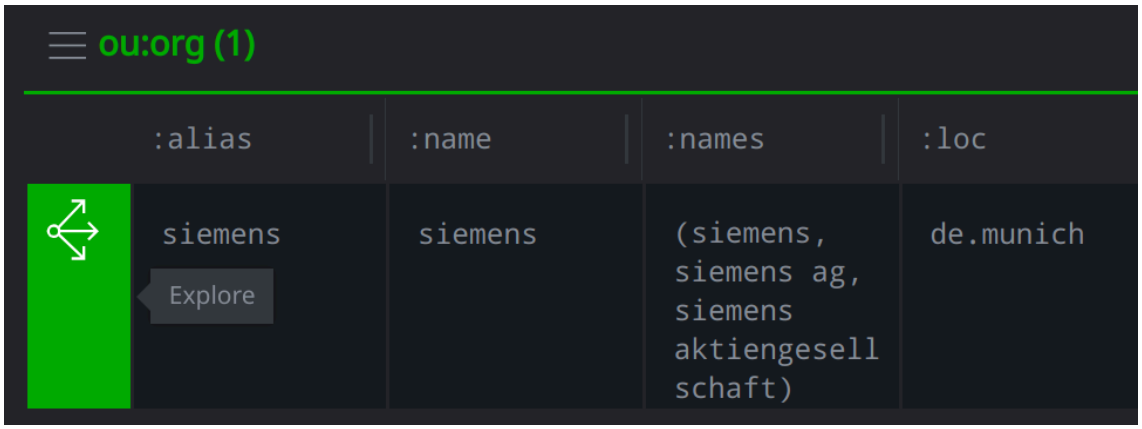
Question 1: What does your **`risk:compromise`** node look like?

- Your **`risk:compromise`** node should look similar to the following:

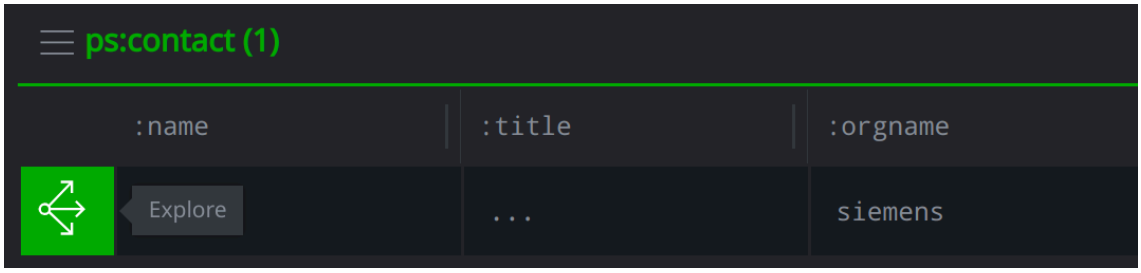


Question 2: Can you use the **Explore** button to navigate from the Siemens **`ou:org`** node, to its **`ps:contact(s)`**, and then from the **`ps:contact`** to the **`risk:compromise`** node?

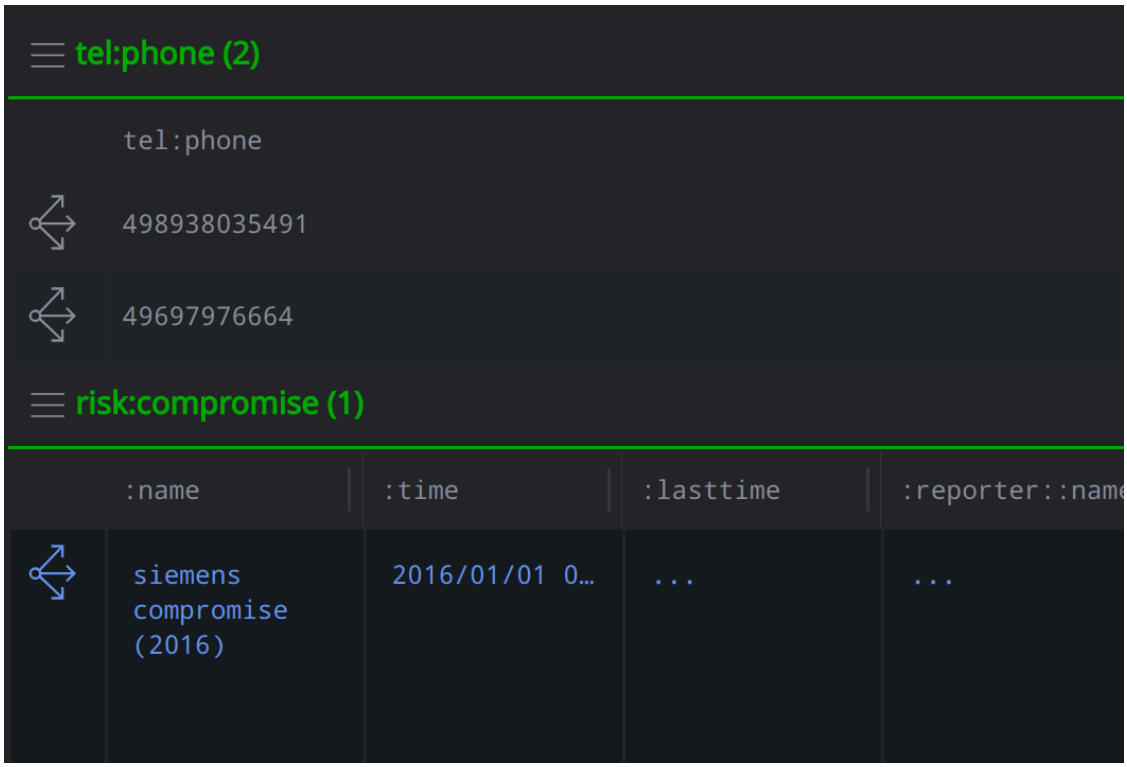
- **Yes.** First **Explore** from the **`ou:org`** node:



Then locate the **`ps:contact`** for Siemens' headquarters and **Explore** from that node:



Then locate the **`risk:compromise`** node in the Results Panel (use **Scroll to Form** if necessary):



> If the nodes are **not** linked, the **`risk:compromise:target`** property may not be set correctly.

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

- **Yes.** The following Storm query will also find the compromise:

```
ou:org:name=siemens -> ps:contact -> risk:compromise | uniq
```
