Synapse Bootcamp - Module 12

Modifying Data with Storm - Exercises

Objectives

In these exercises you will learn:

- How to manually add (create) nodes with Storm edit operations
- How to set, modify, and remove node properties with Storm edit operations
- How to add, modify, and remove tags from nodes with Storm edit operations
- How to add light edges using the 'add edges' dialog

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

- All exercises use the **Research Tool** with the **Storm Mode Selector** set to **Storm mode.**
- Some example queries may wrap due to length.

The **Storm Quick Reference** on Edits (included with the supplemental materials provided for this course) may be helpful for this (and future) exercises.

The online **data modification** (i.e., edits) reference includes detailed documentation and examples for all edit operations. It is part of the Storm Reference included with the Synapse User Guide.

Creating Nodes in Storm

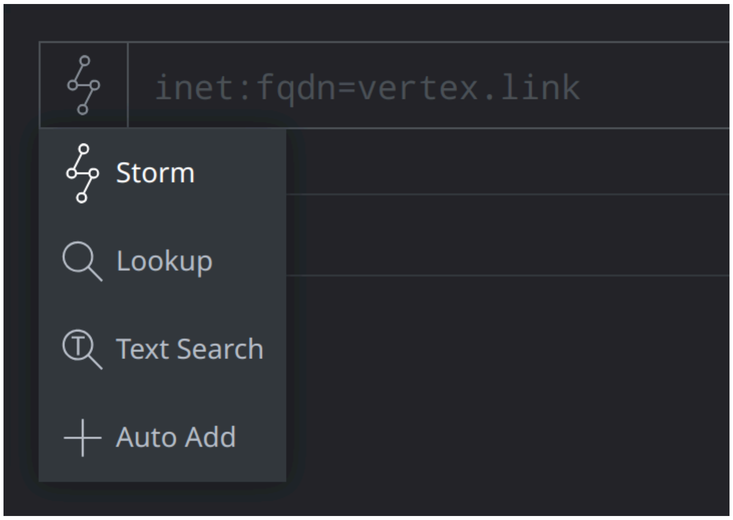
The company QuoIntelligence published a blog describing activity associated with the WINNTI threat group. You have not processed reporting from this company before, so you need to create some data in Synapse to represent this organization before you process the report.

Exercise 1

Objective:

- **Use Storm edit operations to create simple and composite forms.**

- In the **Research Tool,** ensure your **Storm Query Bar** is in **Storm mode:**



```
inet:fqdn=vertex.link
```

- In your **Storm Query Bar,** use Storm edit operations to create nodes for each of the following items. Use an individual Storm query / edit operation to create each node:

Object	Value
A URL (`inet:url`)	`https://quointelligence.eu/`
A phone number (`tel:phone`)	`+49 69 34868044`
An email subject header (`inet:email:header`)	`subject,"Re: Important Software Update!"`

Hint:

- Values that contain **spaces** need to be enclosed in **single or double quotes** when using Storm.
- An email header (`inet:email:header`) is a **composite** form made up of an email header's field name and value.

Question 1: What Storm query did you use to create each node?

Exercise 2

Objective:

- **Use Storm edit operations to create a guid form and set some of its properties.**

- In your **web browser,** open the "about" page for QuoIntelligence:

```
https://quointelligence.eu/about/
```

We want to create an organization (**ou:org**) node to represent QuoIntelligence and set some properties. We will use information from the company's "about" page (contact / location information is at the bottom of the page, under "EU Headquarters").

Property	Value
:name	QuoIntelligence
:loc	de.frankfurt am main
:url	https://quointelligence.eu/

Question 1: What Storm query could you use to create the **ou:org** node and set the listed properties using a single edit operation?

Hint:

- An **ou:org** node is a **guid** node, so you can generate an arbitrary value for its primary property using the asterisk (*****); Synapse will generate a guid for you.
- **Strings** with spaces in them must be enclosed in **single or double quotes.**

Modifying Nodes in Storm

Exercise 3

Objective:

- **Use Storm edit operations to modify an existing node.**

- Enter the following in the **Storm Query Bar** and press **Enter** to run the query to **lift** the **ou:org** node you created for QuoIntelligence:

```
ou:org:name=quointelligence
```

You want to set additional properties for the organization, including its 'alias' (a nickname or "short" name that can be used for easy reference), 'founded' date, and phone number.

Property	Value
:alias	QuoInt
:founded	2020/02
:phone	+49 69 34868044

Question 1: How can you **add** an edit operation to your Storm query to set the above properties for the QuoIntelligence **ou:org** node?

Hint:
- Strings with spaces in them must be enclosed in **single or double quotes.**

Adding and Removing Tags

Exercise 4

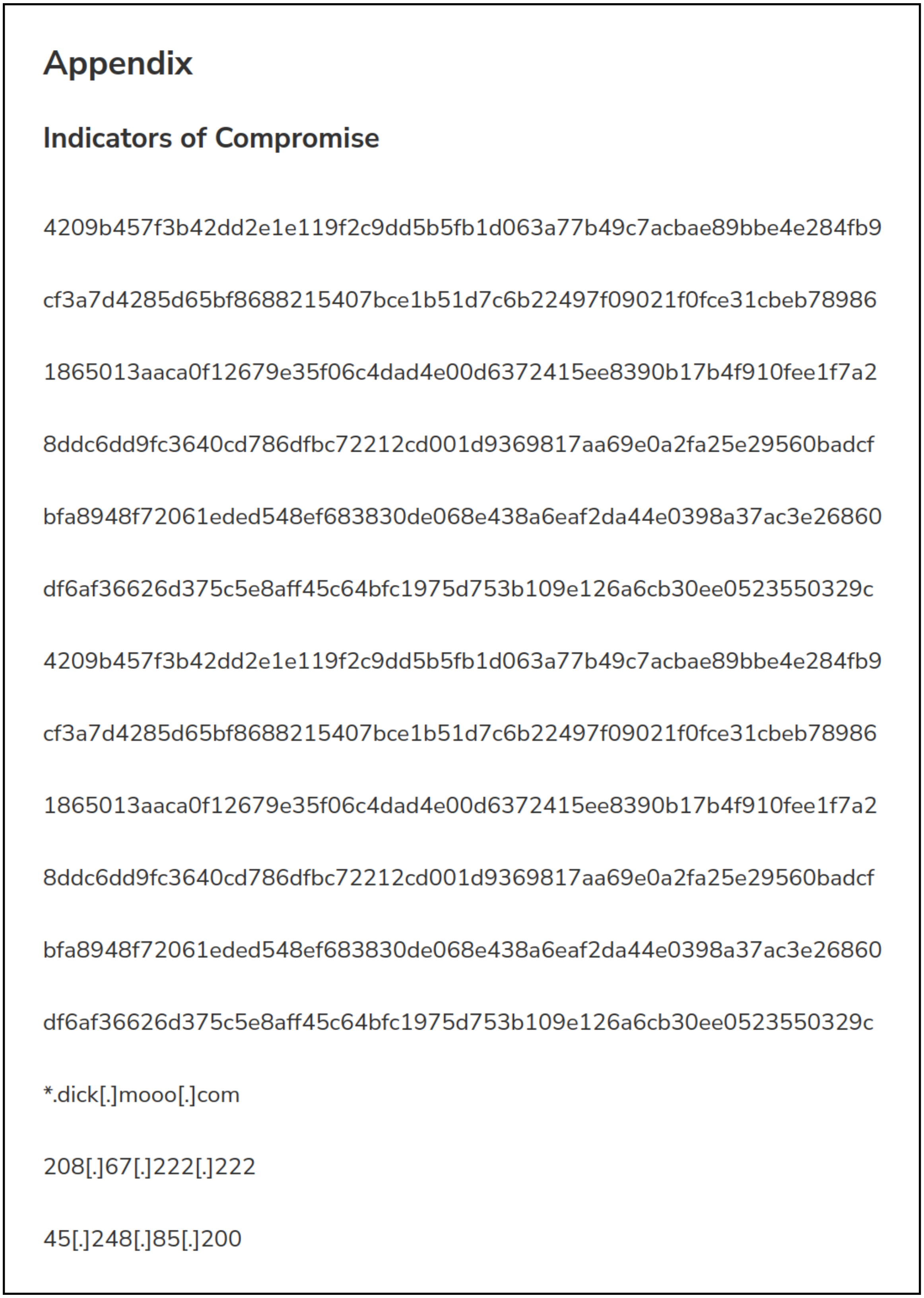
Objective:
- **Use Storm edit operations to add and remove tags.**

Part 1

- In your **web browser,** view the QuoIntelligence blog post:

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

- Scroll to the end of the post to view the indicators included in the article:



Appendix

Indicators of Compromise

4209b457f3b42dd2e1e119f2c9dd5b5fb1d063a77b49c7acbae89bbe4e284fb9

cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986

1865013aaca0f12679e35f06c4dad4e00d6372415ee8390b17b4f910fee1f7a2

8ddc6dd9fc3640cd786dfbc72212cd001d9369817aa69e0a2fa25e29560badcf

bfa8948f72061eded548ef683830de068e438a6eaf2da44e0398a37ac3e26860

df6af36626d375c5e8aff45c64bfc1975d753b109e126a6cb30ee0523550329c

4209b457f3b42dd2e1e119f2c9dd5b5fb1d063a77b49c7acbae89bbe4e284fb9

cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986

1865013aaca0f12679e35f06c4dad4e00d6372415ee8390b17b4f910fee1f7a2

8ddc6dd9fc3640cd786dfbc72212cd001d9369817aa69e0a2fa25e29560badcf

bfa8948f72061eded548ef683830de068e438a6eaf2da44e0398a37ac3e26860

df6af36626d375c5e8aff45c64bfc1975d753b109e126a6cb30ee0523550329c

*.dick[.]mooo[.]com

208[.]67[.]222[.]222

45[.]248[.]85[.]200

Note that the article lists 12 SHA256 hashes, but there are only **six unique** hashes - the values are listed twice.

You have started to review the QuoIntelligence blog on the Winnti threat group. You have already created a `media:news` node to represent the article, and linked the indicators to the article using `refs` light edges.

- Enter the following in the **Storm Query Bar** to lift the `media:news` node and traverse the `refs` edges to the reported indicators:

```
media:news:publisher:name=quointelligence -(refs)> *
```

You want to apply the tag **`rep.quoint.winnti`** to these indicators to show that QuoIntelligence associates them with the Winnti threat group.

Question 1: What Storm **edit operation** can you **add to this query** to apply the tag **`rep.quoint.winnti`** to all of these indicators?

Part 2

The QuoInteligence blog includes information about companies that were reportedly compromised by the Winnti threat group:

"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)."

You want to record this information by applying **tags with timestamps** to the associated `ou:org` nodes.

We'll use the tag **`rep.quoint.tgt.winnti`** to represent "QuoIntelligence reports this company was targeted by the Winnti threat group."

- Enter the following in the **Storm Query Bar** and press **Enter** to run the query to **lift** the `ou:org` node for Henkel:

```
ou:org:name=henkel
```

Question 2: What Storm **edit operation** can you **add to this query** to apply the tag **`rep.quoint.tgt.winnti`** with a **timestamp** of '2014' to indicate the time QuoIntelligence reported for the compromise?

Part 3

Using a **tag** to indicate targeted or compromised entities allows us to easily record victim information. But it does not allow us to record additional details about a compromise that would be useful to track over time.

You decide to model the activity as a **`risk:compromise`** node instead (we'll talk more about these later!), and need to **remove** the "targeted by" tag.

Question 3: What Storm **edit operation** can you use to **fully** remove the tag **`rep.quoint.tgt.winnti`** from the **`ou:org`** node?

Adding Light Edges

Exercise 5

Objective:

- **Use the add edges dialog to add light edges between nodes.**

- In your web browser, view the following ESET blog post:

https://www.welivesecurity.com/en/eset-research/operation-jacana-spying-guyana-entity/

ESET describes a **campaign called Operation Jacana. They provide a list of MITRE ATT&CK techniques (at the end of the blog) that were used in the campaign.**

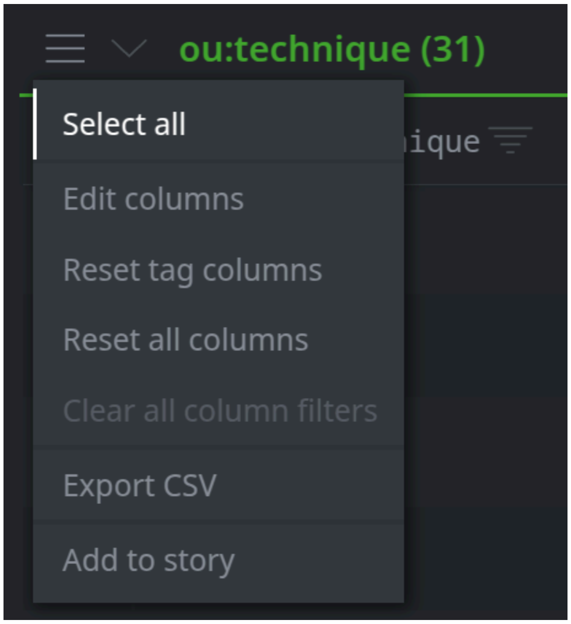
You want to show this relationship in Synapse by linking the campaign (ou:campaign node) to the associated techniques (ou:technique) with “uses” light edges.

- Enter the following in the **Storm Query Bar** and press **Enter** to lift the `ou:technique` nodes:

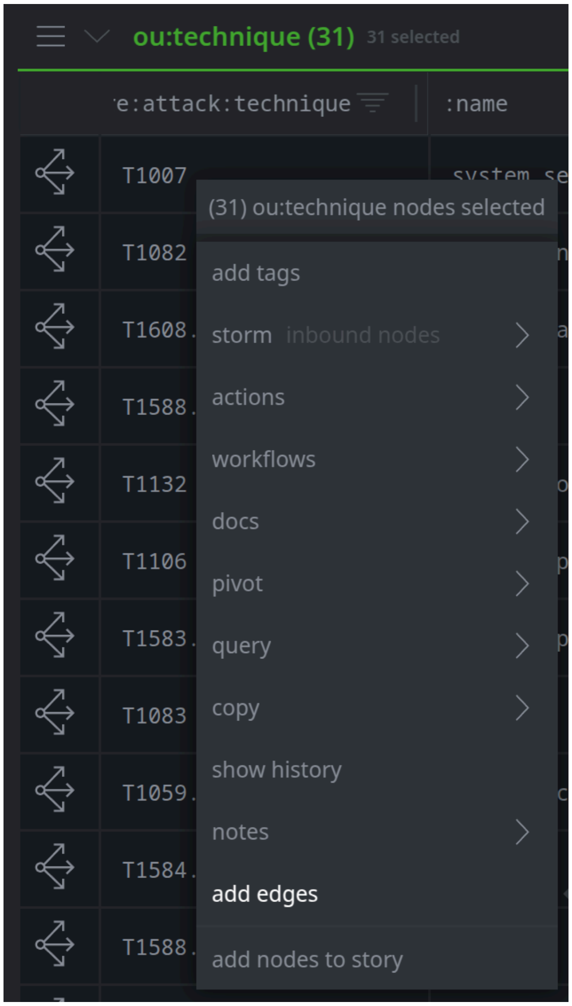
```
media:news:title^='operation jacana' -(refs)>
  it:mitre:attack:technique -> ou:technique
```

Question 1: How many techniques are referenced by the ESET article?

- Click the **hamburger menu** to the left of the **ou:technique** header and choose **Select all:**



- **Right-click** any of the selected nodes and select **add edges:**



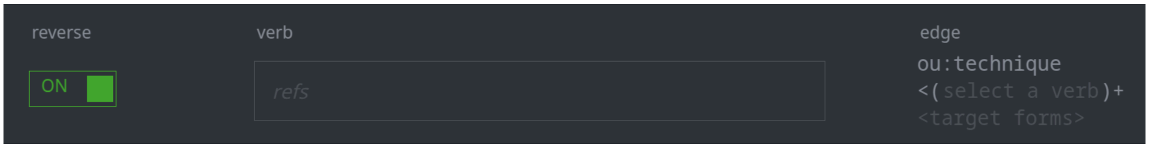
Question 2: In the add edges dialog, in the source nodes section, how many nodes are displayed?

A campaign uses a set of techniques, so we want the edge relationship to look like this:

```
ou:campaign -(uses)> ou:technique
```

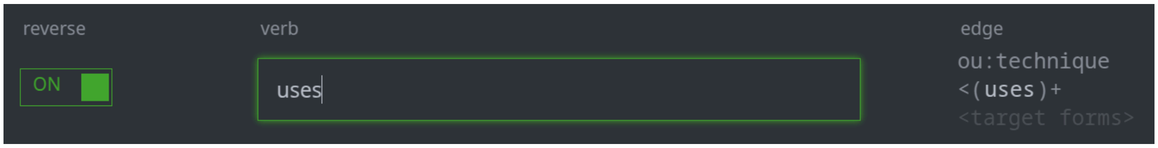
Because the **ou:technique** nodes are our **source,** we need to **reverse** the direction of the edge in the dialog.

- In the add edge dialog, toggle the **reverse** switch to **ON**:



```
ou:technique
<(select a verb)+
<target forms>
```

- In the *verb* field, enter **uses** as the edge name:



```
ou:technique
<(uses)+
<target forms>
```

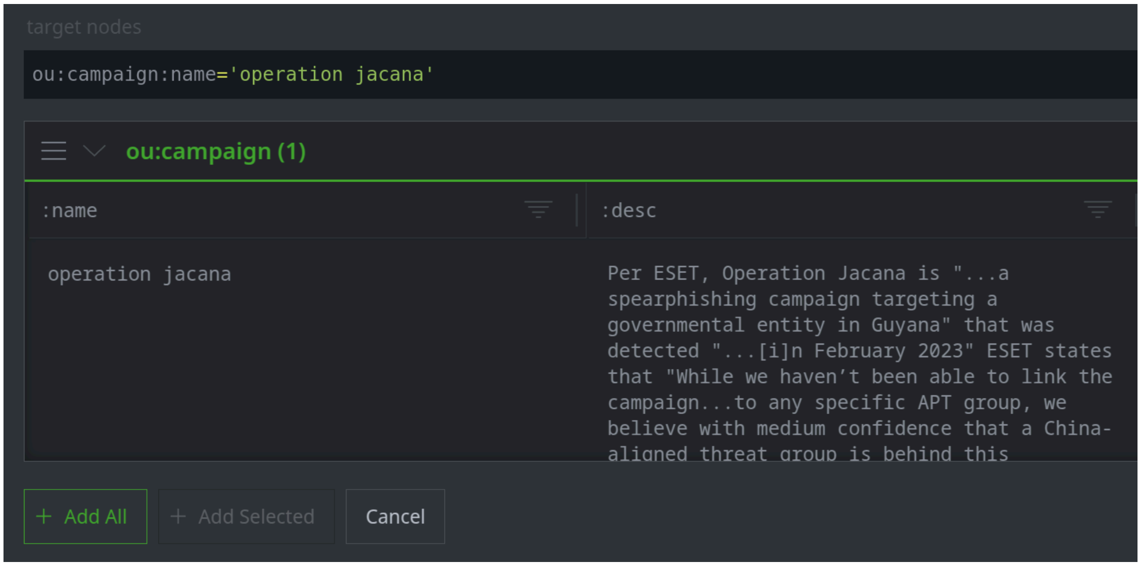
Note that the dialog displays the Storm "hinting" syntax on the right.

- In the **target nodes section**, enter the following Storm query and press **Enter** to lift the campaign node for Operation Jacana:

```
ou:campaign:name='operation jacana'
```

Question 3: How many nodes are displayed?

- Click the **+ Add All** button to link the `ou:campaign` node to the `ou:technique` nodes:



```
ou:campaign:name='operation jacana'
```

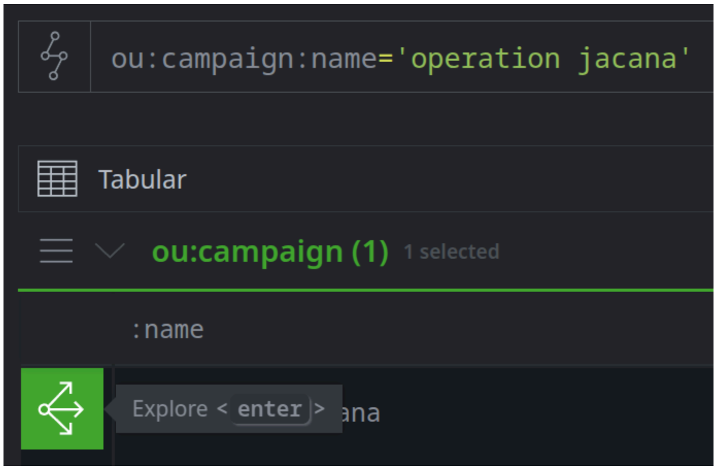
:name	:desc
operation jacana	Per ESET, Operation Jacana is "...a spearphishing campaign targeting a governmental entity in Guyana" that was detected "...[i]n February 2023" ESET states that "While we haven't been able to link the campaign...to any specific APT group, we believe with medium confidence that a China-aligned threat group is behind this

Now we'll confirm that the edges were created.

- Enter the following in the **Storm Query Bar** and press **Enter** to lift the campaign node:

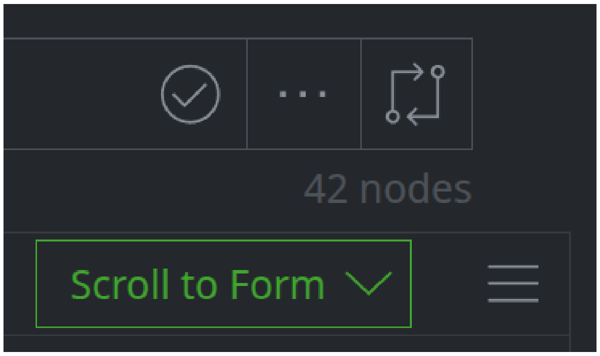
```
ou:campaign:name='operation jacana'
```

- **Select** the node in the results and click the **Explore** button to navigate to adjacent nodes:



```
ou:campaign:name='operation jacana'
```

- Browse the results (or use **Scroll to Form**):



Question 4: Are the **`ou:technique`** nodes present? How are they linked to the **`ou:campaign`**?