Vertex

Synapse Bootcamp - Module 12

Modifying Data with Storm - Answer Key

Answer Key

Creating Nodes in Storm

Exercise 1 Answer

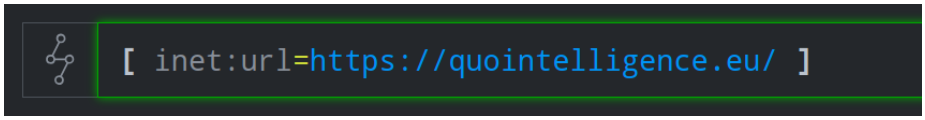
Objective:

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

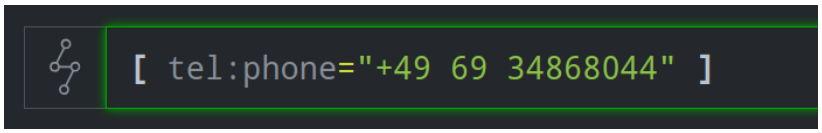
Question 1: What Storm query did you use to create each node?

- You can create each node with the following Storm queries:

```
[ inet:url=https://quointelligence.eu/ ]
```

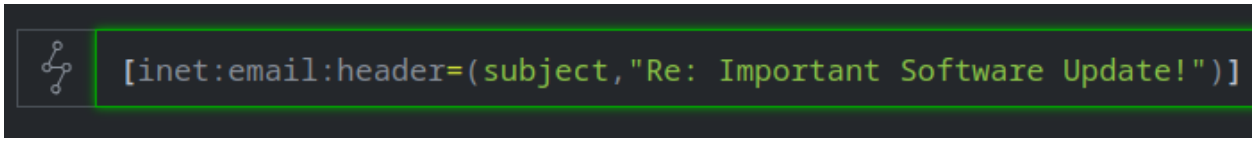



```
[ tel:phone="+49 69 34868044" ]
```



The phone number must be enclosed in **quotes** if the spaces are included.

```
[inet:email:header=(subject,"Re: Important Software Update!")]
```



The email header (**inet:email:header**) is a composite form whose primary property is two elements (the email header's field name and value).

Exercise 2 Answer

Objective:

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

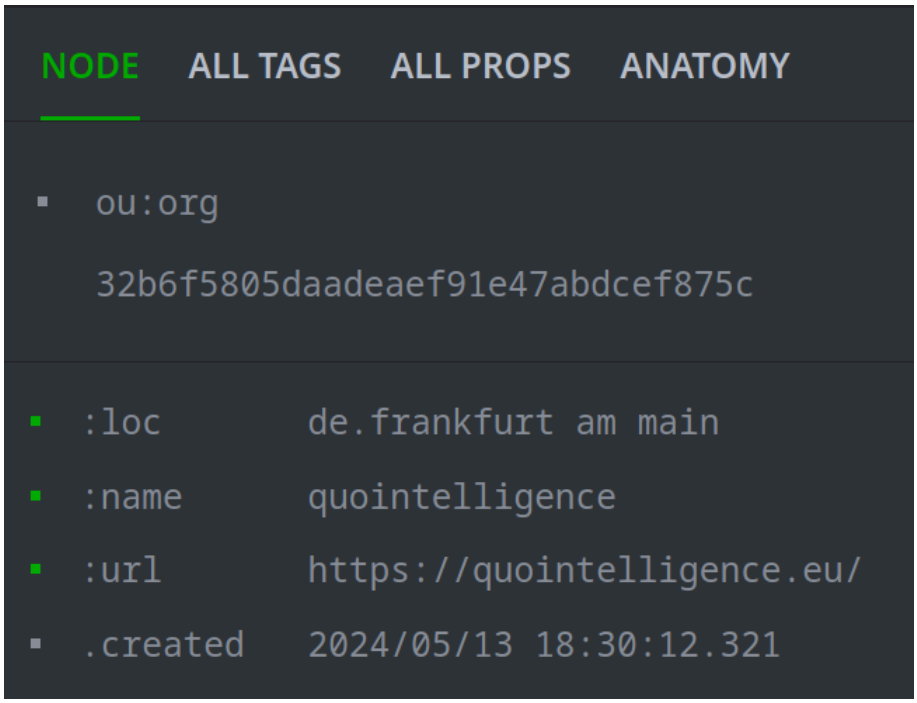
Question 1: What Storm query could you use to create the **ou:org** node and set the listed properties using a single edit operation?

- The following query will create the **ou:org** node and set the properties:

```
[ ou:org=* :name=QuoIntelligence :loc='de.frankfurt am main'
  :url=https://quointelligence.eu/ ]
```

```
[ ou:org=* :name=QuoIntelligence :loc='de.frankfurt am main' :url=https://quointelligence.eu/ ]
```

The node should look similar to the following:



Modifying Nodes in Storm

Exercise 3 Answer

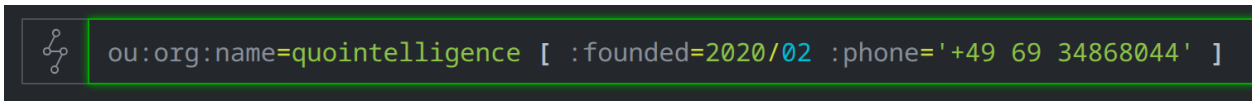
Objective:

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

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

- The following query will apply all the changes:

```
ou:org:name=quointelligence [ :founded=2020/02
  :phone='+49 69 34868044' ]
```



Adding and Removing Tags

Exercise 4 Answer

Objective:

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

Part 1

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

- The following query applies the tags (the highlighted portion was added to the original query; line wraps):

```
media:news:publisher:name=quointelligence -(refs)> *
  [ +#rep.quoint.winnti ]
```

```
media:news:publisher:name=quointelligence -(refs)> * [ +#rep.quoint.winnti ]
```

The "hashtag" symbol (**#**) indicates this is a tag, and the plus (**+**) indicates we are adding the tag.

Part 2

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?

- The following query applies the tag:

```
ou:org:name=henkel [ +#rep.quoint.tgt.winnti=2014 ]
```

Note: Quoint only provided "2014" as the date of the compromise. If we use this single date to set the timestamp, Synapse sets the "minimum" time to January 1, 2014 and the "maximum" time to one millisecond later:

```
▪ #rep.quoint.tgt.winnti
  (2014/01/01 00:00:00, 2014/01/01 00:00:00.001)
```

If we have a **date range** (or we want to represent more clearly "some time during 2014"), we need to specify the range in parentheses. For example:

```
ou:org:name=henkel [ +#rep.quoint.tgt.winnti=(2014, 2015) ]
```

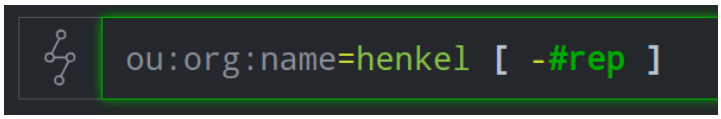
```
▪ #rep.quoint.tgt.winnti
  (2014/01/01 00:00:00, 2015/01/01 00:00:00)
```

Part 3

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

- The following query removes the tag:

```
ou:org:name=henkel [ -#rep ]
```



Note: Removing the **`#rep`** tag removes that tag and all tags below it in the tag tree (i.e., the full tag).

If you used the edit operation **`[ -#rep.quoint.tgt.winnti ]`** it would remove **only** the final **`winnti`** element, leaving the tag **`#rep.quoint.tgt`** on the node.

Adding Light Edges

Exercise 5

Objective:

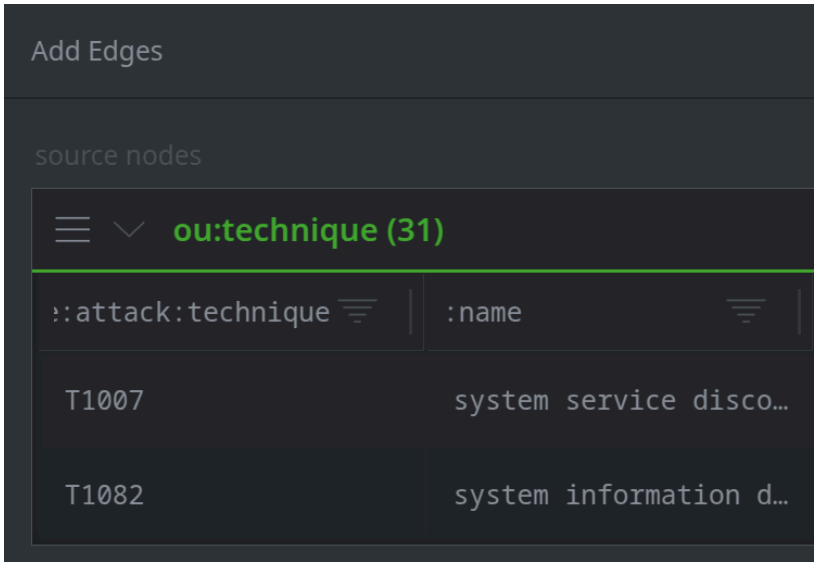
- **Use the add edges dialog to add light edges between nodes.**

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

- There are **31** techniques listed in the article:

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

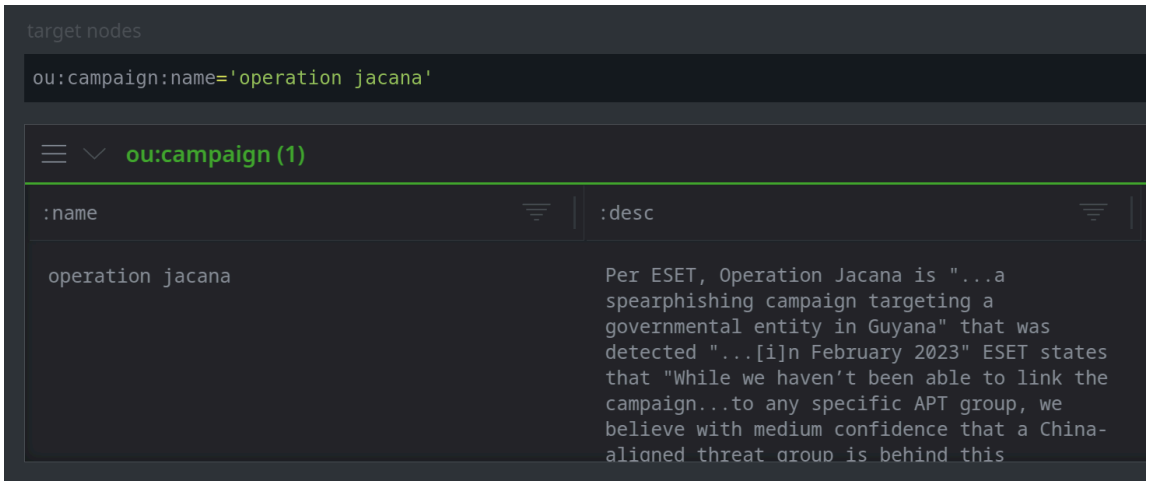
- There are **31** source nodes:



> **Tip:** You can use the vertical scroll bar (on the right) to scroll through the results. Keep in mind that **all source nodes** will be linked to the selected target node(s) by the edge you specify.

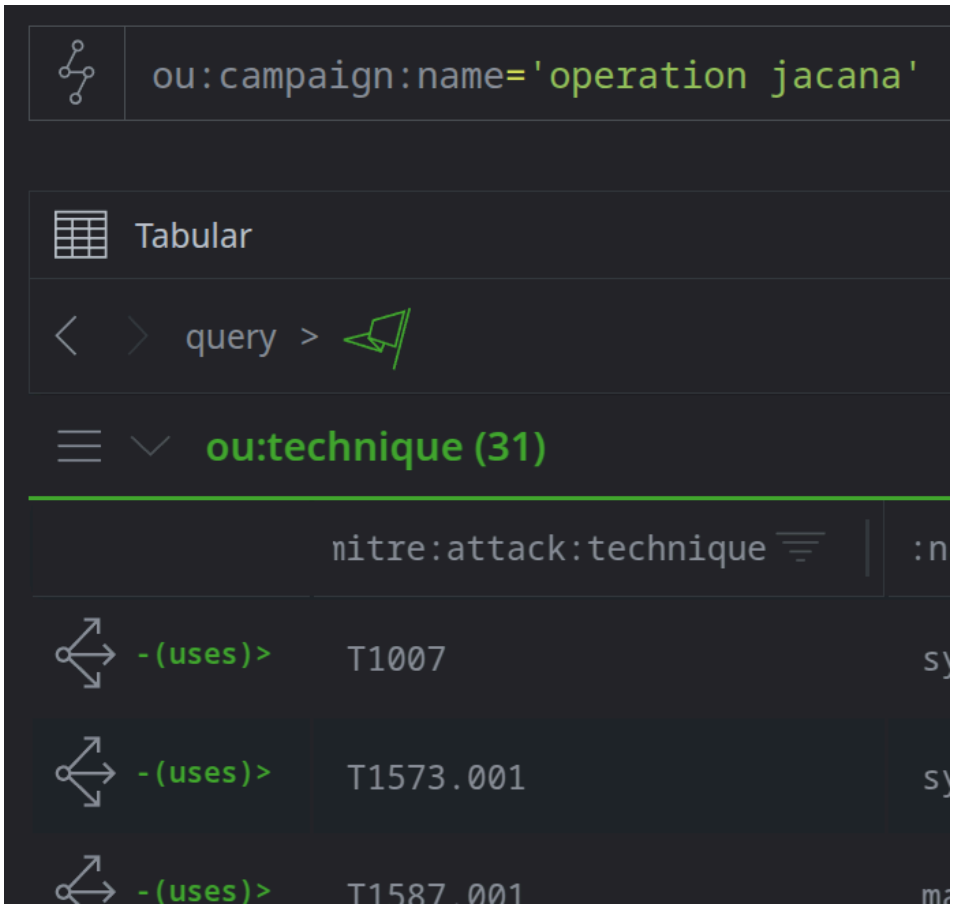
Question 3: How many nodes are displayed?

- Only **one** campaign node is displayed:



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

- **Yes** - the 31 **`ou:technique`** nodes are present, and linked via a **`-(uses)>`** light edge:



Tip: The **Explore** button makes it easy to quickly check that the edge is present (and pointing in the correct direction). You can also verify that the edges were created using your new Storm skills! If the edges were created correctly, the query below will return the 31 **`ou:technique`** nodes:

```
ou:campaign:name='operation jacana' -(uses)> ou:technique
```