

Synapse Bootcamp - Module 21

More Fun with Spotlight - Exercises

More Fun with Spotlight - Exercises	1
Objectives	1
Exercises	3
Create Extractors	3
Exercise 1	3
Part 1 - Add an Extractor for Threats	3
Part 2 - Add an extractor for Vulnerabilities	7
Part 3 - Add an extractor for Countries	9
Working with Spotlight Extractors	11
Exercise 2	11
Part 1 - Open the article in Spotlight	11
Part 2 - Use Extractors to capture information	16
Part 3 - View your linked nodes in the Research Tool	20
Spotlight and the Threat Intel Workflow	21
Exercise 3	21
Part 1 - Add information about APT29	22
Part 2 - Link information about APT29	30
Part 3 - View your threat cluster in the Research Tool	35
Appendix - Sample Extractors	38

Objectives

In these exercises you will:

- Create Extractors for use in Spotlight
- Use Spotlight Extractors to create nodes from highlighted text
- Use Spotlight with the Threat Intel Workflow to capture detailed information about threat activity

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

Create Extractors

Exercise 1

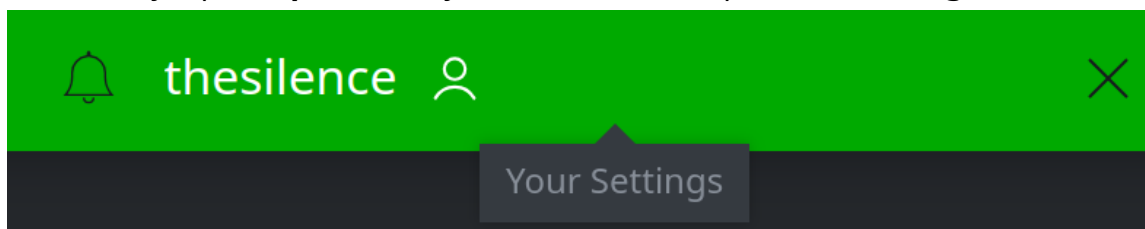
Objective:

- **Add custom Extractors to Spotlight.**

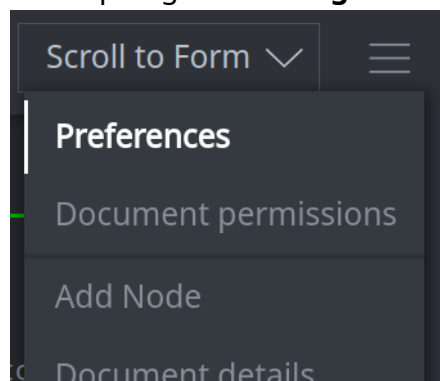
Tip: This exercise creates some (though not all) of the same Extractors used in the Instructor Demo. All of the Extractors are included in the [Appendix - Sample Extractors](#) for reference.

Part 1 - Add an Extractor for Threats

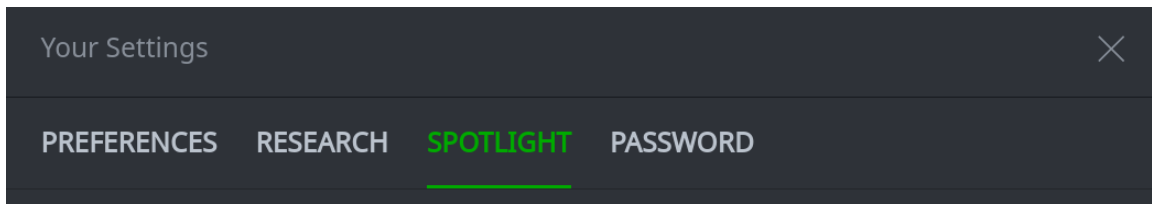
- From the Synapse **Top Bar**, click your **username** to open **Your Settings**:



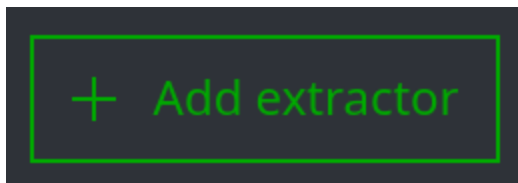
Tip: You can also access **Your Settings** from within the **Spotlight Tool** using the main Spotlight **hamburger menu**:



- In the **Your Settings** dialog, select the **SPOTLIGHT** tab:

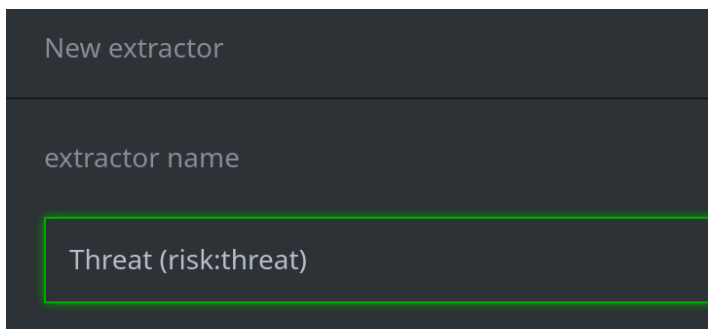


- In the **SPOTLIGHT** tab, click the **+ Add Extractor** button:



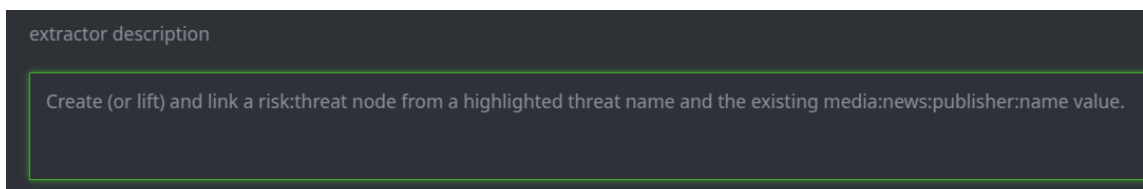
- In the **New extractor** dialog, in the **extractor name** field, enter the following:

Threat (risk:threat)



- In the **New extractor** dialog, in the **extractor description** field, enter the following:

Create (or lift) a risk:threat node from a highlighted threat name and the existing media:news:publisher:name value.

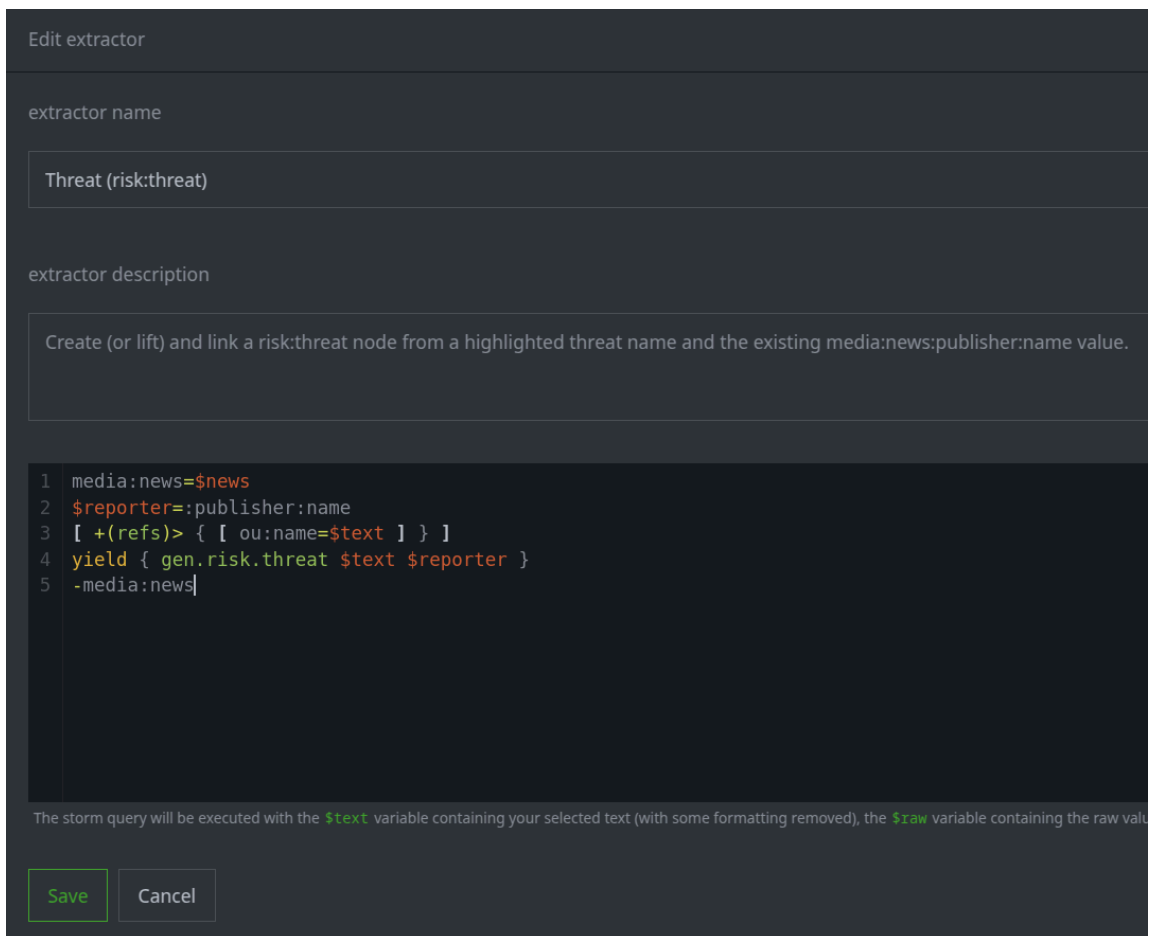


Tip: The text in the **extractor description** field will appear when you hover-over the extractor name in Spotlight's **right click > extractors** menu. If there is no description, the hover-over will display the associated **Storm** code.

- In the **New extractor** dialog, in the **Storm editor window**, enter the following:

```
media:news=$news
$reporter=:publisher:name
[ +(refs)> { [ ou:name=$text ] } ]
yield { gen.risk.threat $text $reporter }
-media:news
```

Click the **Save** button to create the Extractor:



Edit extractor

extractor name

Threat (risk:threat)

extractor description

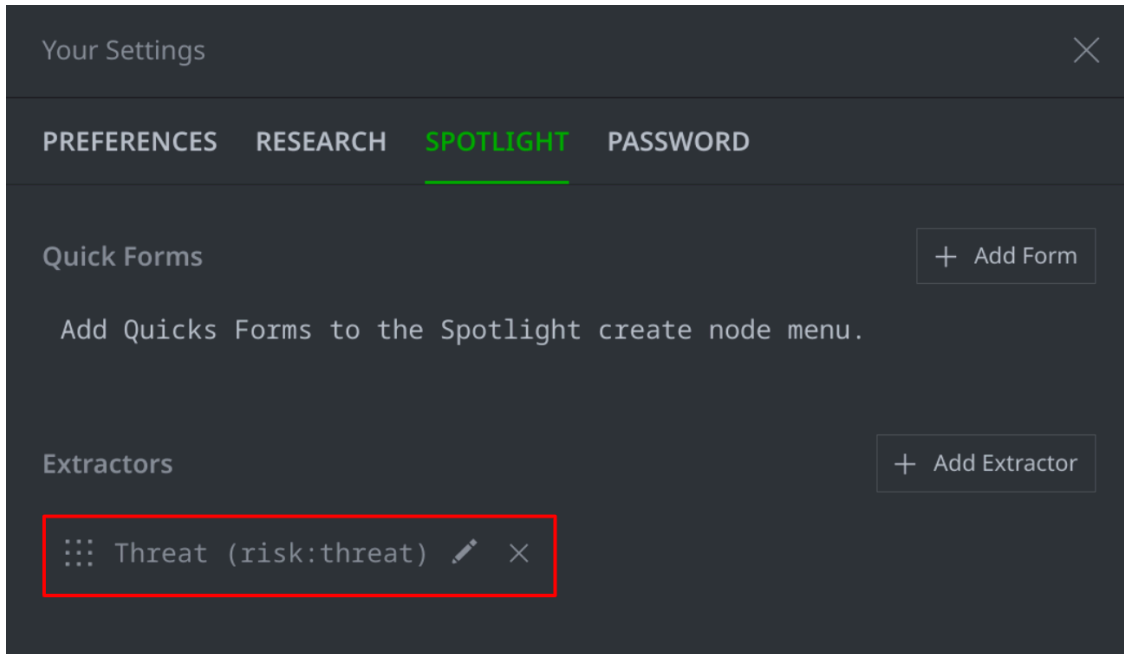
Create (or lift) and link a risk:threat node from a highlighted threat name and the existing media:news:publisher:name value.

```
1 media:news=$news
2 $reporter=:publisher:name
3 [ +(refs)> { [ ou:name=$text ] } ]
4 yield { gen.risk.threat $text $reporter }
5 -media:news|
```

The storm query will be executed with the `$text` variable containing your selected text (with some formatting removed), the `$raw` variable containing the raw value.

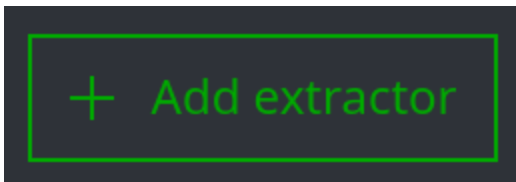
Save Cancel

- You should see the Extractor in your **SPOTLIGHT** tab:



Part 2 - Add an extractor for Vulnerabilities

- Click the **+ Add Extractor** button:



- Use the following **Extractor Name** and **Storm** to create another extractor:

Extractor Name	Vulnerability (risk:vuln)
Extractor Description	Create a risk:vuln node from a highlighted CVE number and the existing media:news:publisher:name value.
Storm	<pre>media:news=\$news \$reporter=:publisher:name [+(refs)> { [it:sec:cve=\$text] }] yield { gen.risk.vuln \$text \$reporter } -media:news</pre>

Click the **Save** button to create the extractor:

New extractor

extractor name

Vulnerability (risk:vuln)

extractor description

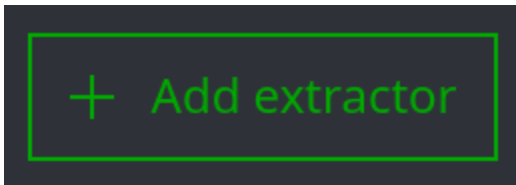
Create a risk:vuln node from a highlighted CVE number and the existing media:news:publisher:name value.

```
1 media:news=$news
2 $reporter=:publisher:name
3 [ +(refs)> { [ it:sec:cve=$text ] } ]
4 yield { gen.risk.vuln $text $reporter }
5 -media:news]
```

The storm query will be executed with the `$text` variable containing your selected text (with some formatting removed), the `$raw` variable

Part 3 - Add an extractor for Countries

- Click the + **Add Extractor** button:



- Use the following **Extractor Name** and **Storm** to create another extractor:

Extractor Name	Country (pol:country)
Extractor Description	Link an existing pol:country node from a highlighted country name.
Storm	<pre>media:news=\$news [+(refs)> { [geo:name=\$text] }] -media:news geo:name=\$text -> pol:country</pre>

Click the **Save** button to create the extractor:

New extractor

extractor name

Country (pol:country)

extractor description

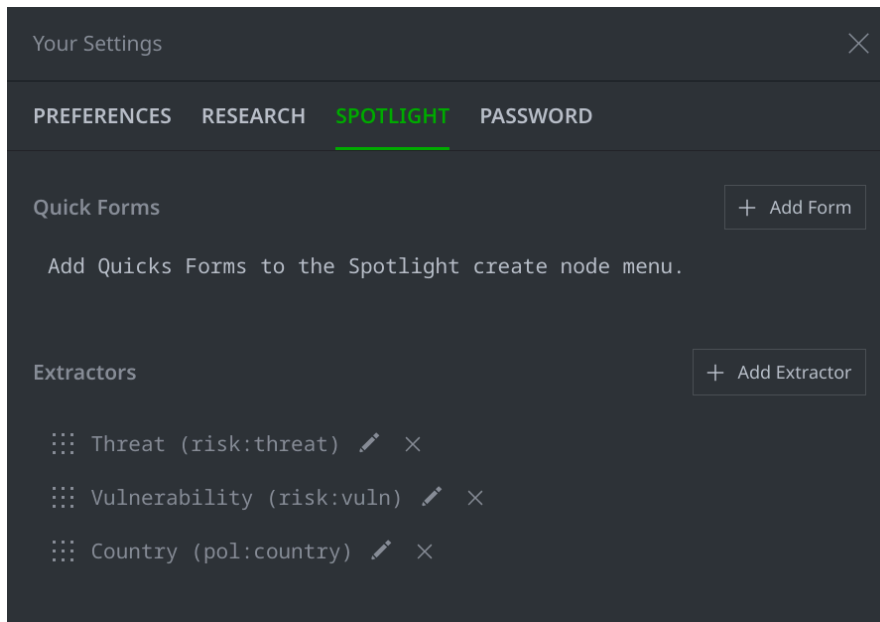
Link an existing pol:country node from a highlighted country name.

```
1 media:news=$news
2 [ +(refs)> { [ geo:name=$text ] } ]
3 -media:news
4 geo:name=$text -> pol:country
```

The storm query will be executed with the `$text` variable containing your selected text (wi

Save Cancel

- When you are finished, the **SPOTLIGHT** tab in the **Your Settings** dialog should look similar to the following:



- Click the **X** in the upper right to **close** the dialog.

Working with Spotlight Extractors

Exercise 2

Objective:

- **Use Extractors to create nodes from highlighted text.**

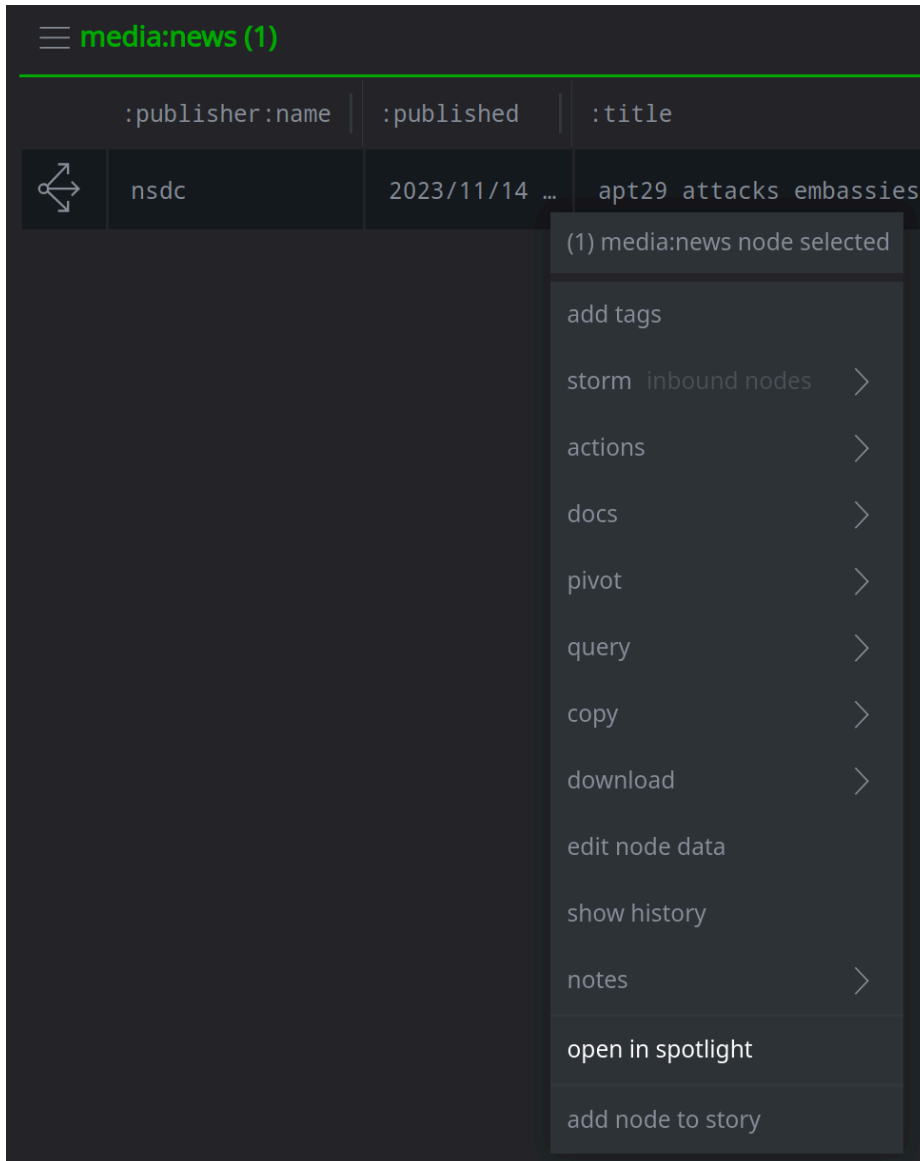
The National Security and Defense Council of Ukraine (NSDC) published a report on APT29. There is a **media:news** node for the report in Synapse. You want to review the report in Spotlight.

Part 1 - Open the article in Spotlight


- In the **Research Tool**, enter the following query into the **Storm Query Bar** and press **Enter** to lift the **media:news** node:

```
media:news=cb5c98f3940bff6e97a99b6ab84f83e3
```

- In your **Results Panel**, right-click the node and select **open in spotlight**:

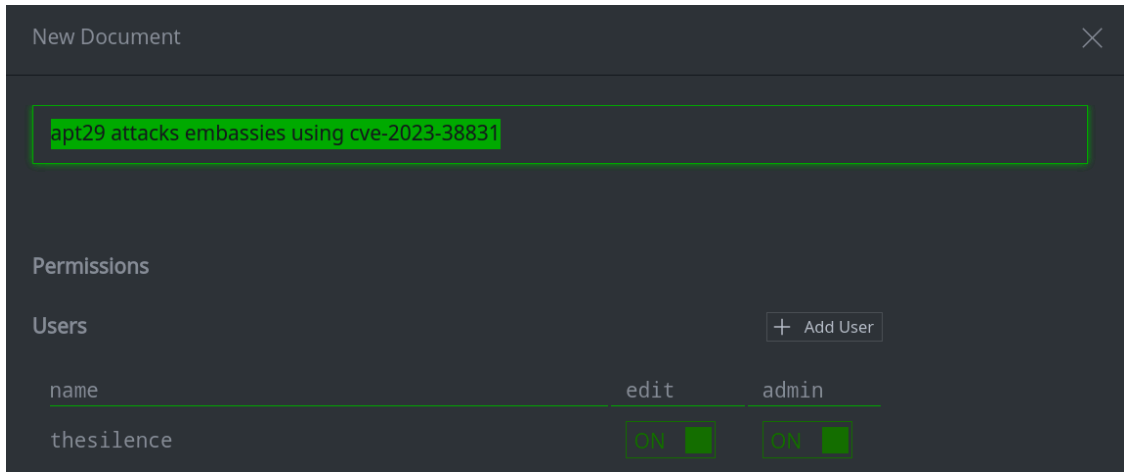


media:news (1)

	:publisher:name	:published	:title
	nsdc	2023/11/14 ...	apt29 attacks embassies

- (1) media:news node selected
- add tags
- storm inbound nodes >
- actions >
- docs >
- pivot >
- query >
- copy >
- download >
- edit node data
- show history
- notes >
- open in spotlight**
- add node to story

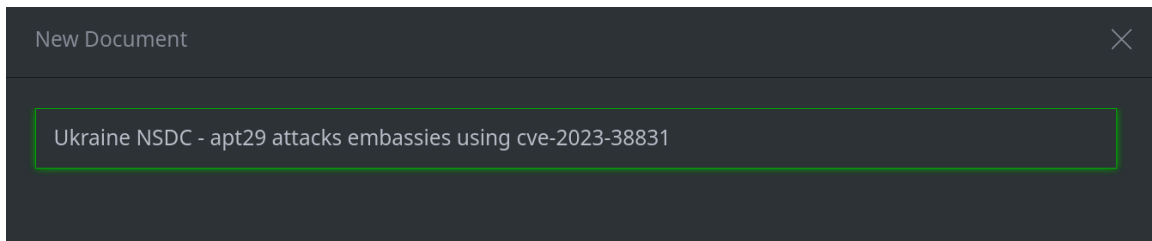
- Synapse will take you to the **Spotlight Tool** and display the **New Document** dialog:



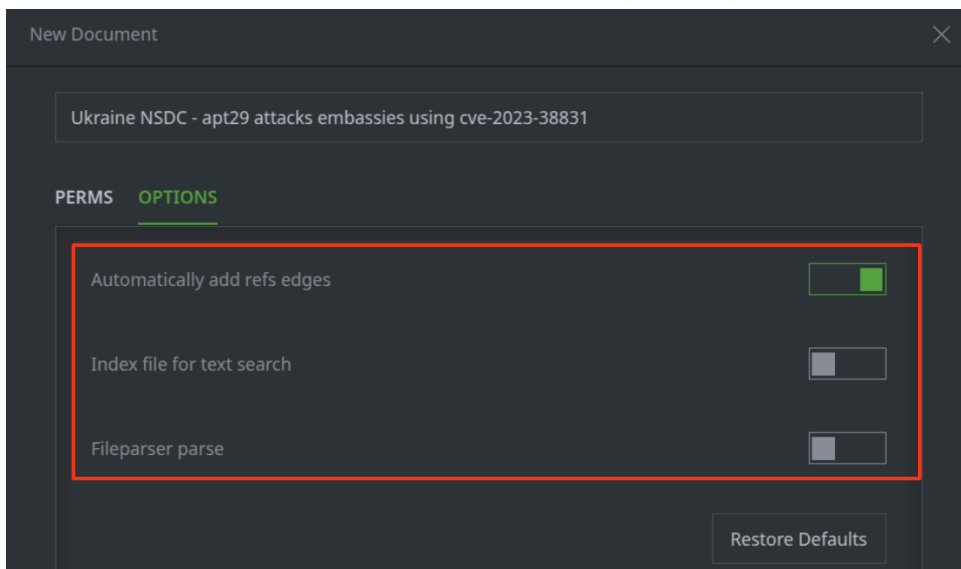
name	edit	admin
thesilence	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- In the **New Document** dialog, in the *Name* field, **edit** the text to include reporting organization in the title:

Ukraine NSDC - apt29 attacks embassies using cve-2023-38831



- On the **OPTIONS** tab, make sure the following settings are selected:

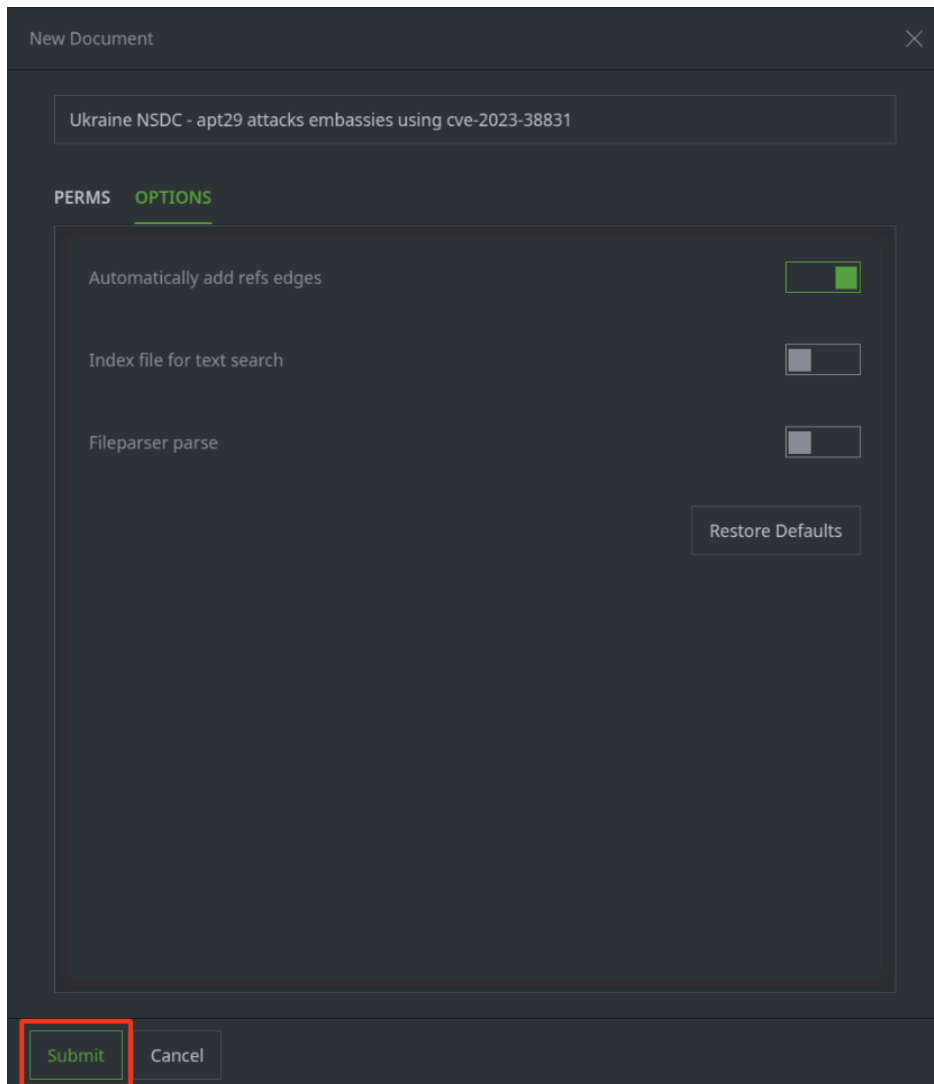


PERMS **OPTIONS**

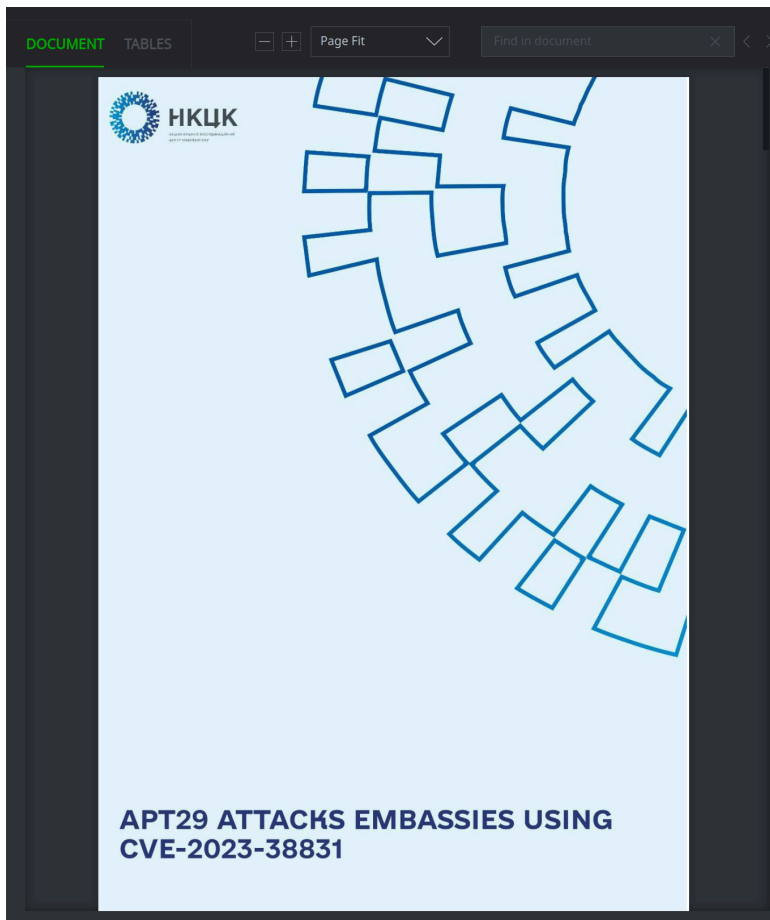
- Automatically add refs edges
- Index file for text search
- Fileparser parse

Restore Defaults

- Click **Submit** to create the document in Spotlight:

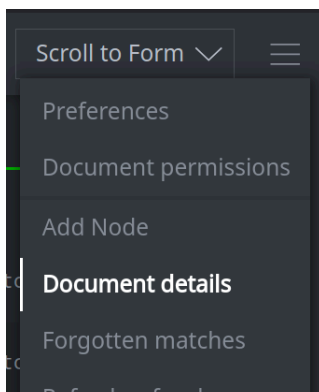


- You should see the document in Spotlight:

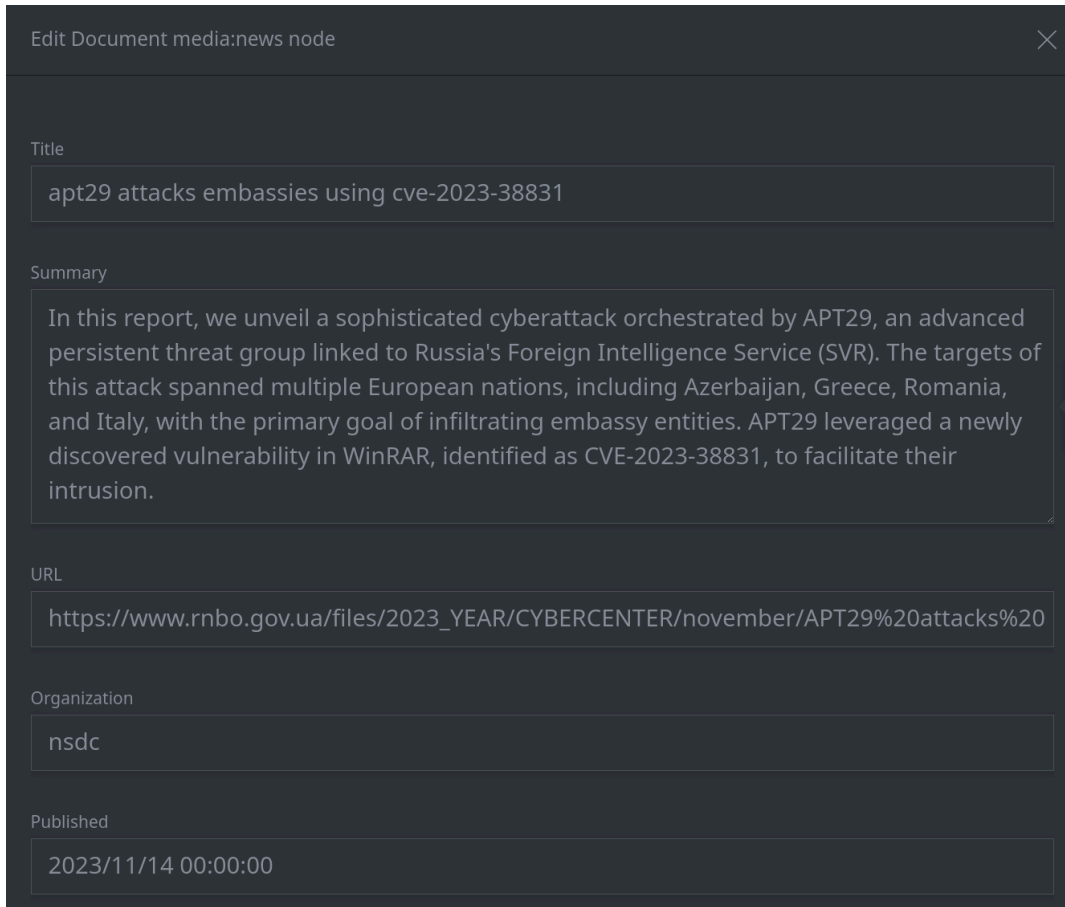


- Because the `media:news` node was already in Synapse, the document properties are **already set**.

To view the details, click Spotlight's main **hamburger menu** and select **Document details**:



- The details should look similar to the following:



Edit Document media:news node

Title

apt29 attacks embassies using cve-2023-38831

Summary

In this report, we unveil a sophisticated cyberattack orchestrated by APT29, an advanced persistent threat group linked to Russia's Foreign Intelligence Service (SVR). The targets of this attack spanned multiple European nations, including Azerbaijan, Greece, Romania, and Italy, with the primary goal of infiltrating embassy entities. APT29 leveraged a newly discovered vulnerability in WinRAR, identified as CVE-2023-38831, to facilitate their intrusion.

URL

https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/november/APT29%20attacks%20

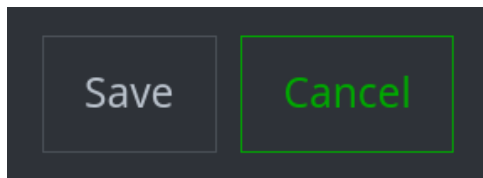
Organization

nsdc

Published

2023/11/14 00:00:00

- Click **Cancel** to close the dialog:



Part 2 - Use Extractors to capture information

Create a risk:threat node for APT29

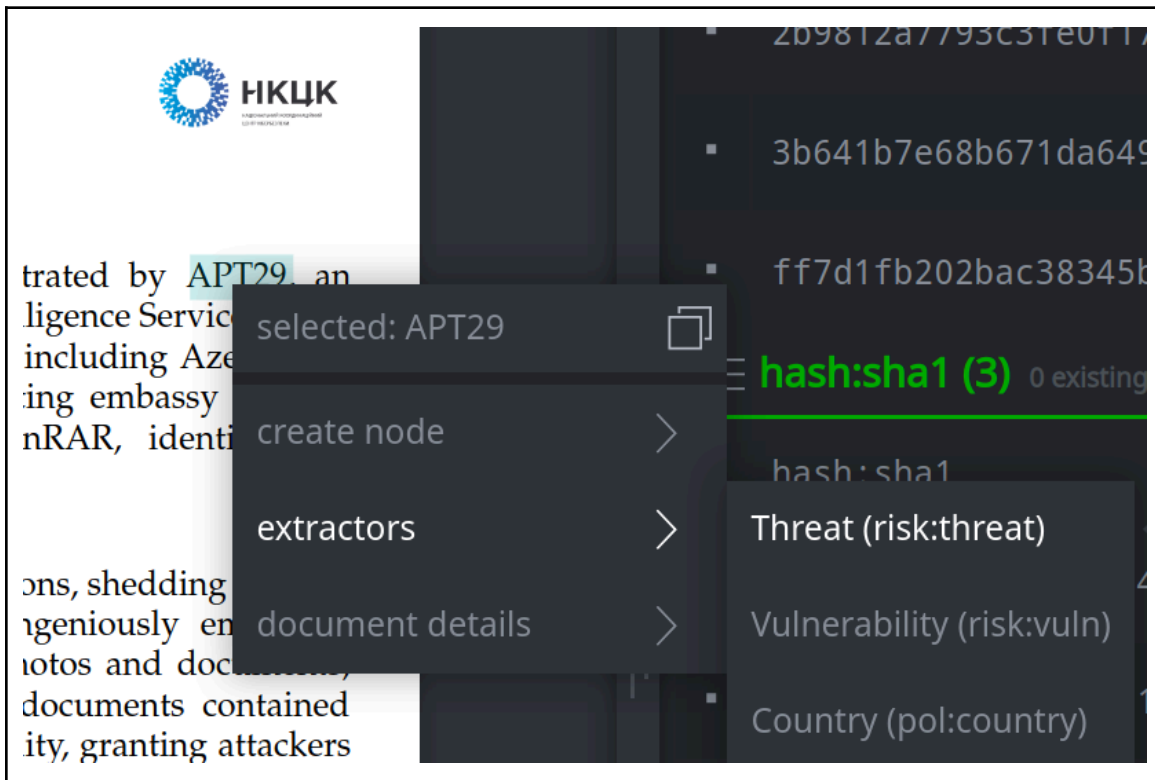
- In the document, locate the **Executive Summary**:



Executive Summary

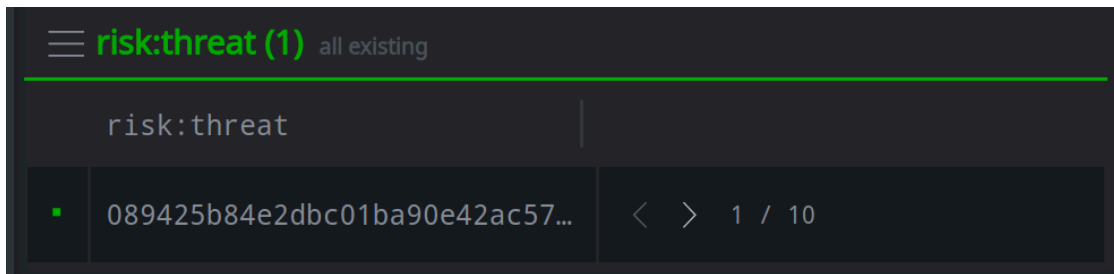
In this report, we unveil a sophisticated cyberattack orchestrated by APT29, an advanced persistent threat group linked to Russia's Foreign Intelligence Service (SVR). The targets of this attack spanned multiple European nations, including Azerbaijan, Greece, Romania, and Italy, with the primary goal of infiltrating embassy entities. APT29 leveraged a newly discovered vulnerability in WinRAR, identified as CVE-2023-38831, to facilitate their intrusion.

- **Highlight** the text **APT29**. **Right-click** the highlighted text and select **extractors** > **Threat (risk:threat)**:



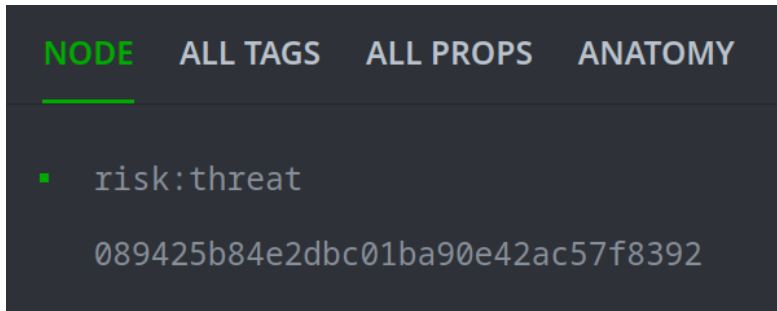
The screenshot shows a document viewer with the HKЦК logo in the top left. The text "trated by APT29, an" is highlighted. A right-click context menu is open over the highlighted text, showing the following options: "selected: APT29", "create node", "extractors", "document details", and "Country (pol:country)". The "extractors" option is selected, and a sub-menu is open showing "Threat (risk:threat)", "Vulnerability (risk:vuln)", and "Country (pol:country)". The "Threat (risk:threat)" option is highlighted in green. In the background, a list of hashes is visible, including "2b9812a7793c31e0117", "3b641b7e68b671da649", and "ff7d1fb202bac38345b".

- Spotlight adds the **risk:threat** node and automatically **selects** it in the **Spotlight Results**:



Tip: If Spotlight does not automatically "jump" to the newly created node, use the **Scroll to Form** button to locate the `risk:threat`.

- Look at the details for the node in the **Spotlight Details Panel**:



Question 1: Did the node already exist, or did Spotlight create a new **risk:threat** node? How can you tell?

Create a `risk:vuln` node for CVE-2023-38831

- In the **Executive Summary**, **highlight** the text **CVE-2023-38831**.

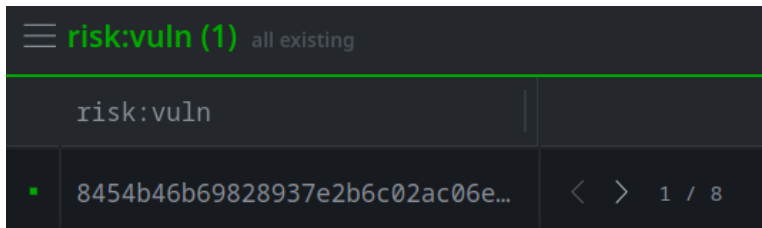
Right-click the highlighted text and select **extractors > Vulnerability (risk:vuln)**:

In this report, we unveil a sophisticated cyberattack orchestrated by **APT29**, an advanced persistent threat group linked to Russia's Foreign Intelligence Service (SVR). The targets of this attack spanned multiple European nations, including Azerbaijan, Greece, Romania, and Italy, with the primary goal of infiltrating embassy entities. **APT29** leveraged a newly discovered vulnerability in WinRAR, identified as **CVE-2023-38831**, to facilitate their intrusion.

This report details the attackers' operations, shedding light on the benign-looking **APT29** ingeniously employed expertly crafted sale photos and document hidden, malicious access to the c... Threat (risk:threat) Vulnerability (risk:vuln) Country (pol:country)

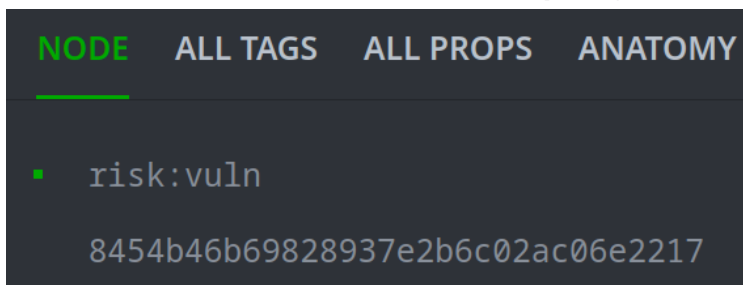
This campaign exemplifies the evolving nature of cyber endeavors of nation-state-sponsored actors to compromise

- Spotlight adds the **risk:vuln** node and automatically **selects** it in the **Spotlight Results**:



The screenshot shows a Spotlight Results panel with a dark background. At the top, it displays "risk:vuln (1) all existing". Below this, a table lists the node details. The first row shows the node name "risk:vuln". The second row shows a list of nodes, with the first one selected and highlighted in green. The selected node's ID is "8454b46b69828937e2b6c02ac06e...". Navigation arrows and "1 / 8" are visible at the bottom right of the table.

- Look at the details for the node in the **Spotlight Details Panel**:

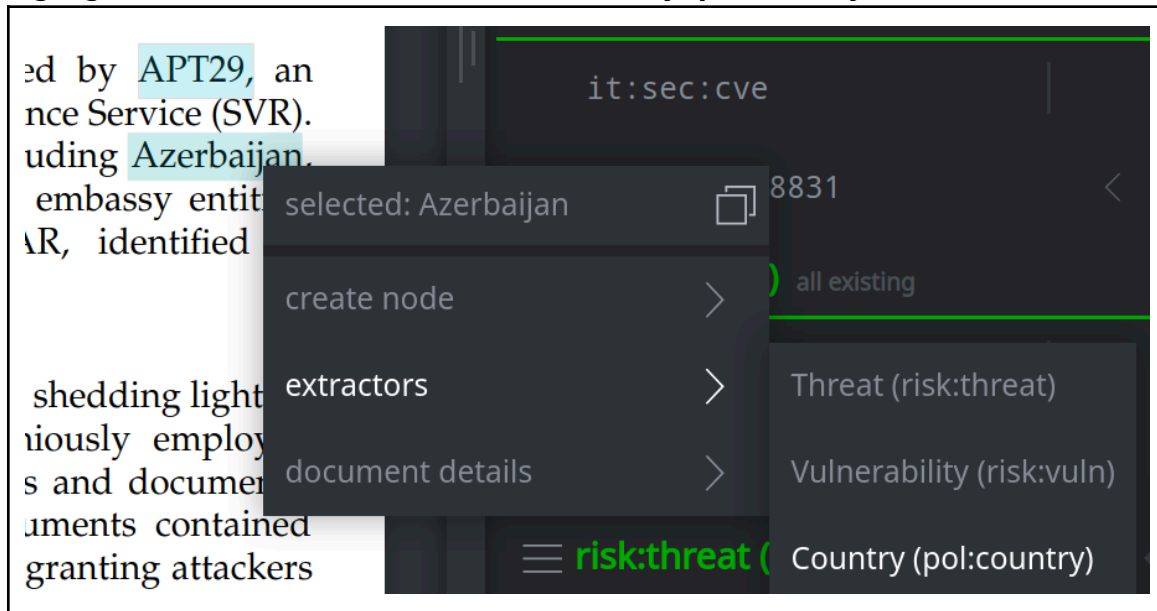


The screenshot shows the Spotlight Details Panel for the selected node. It has a dark background and a tabbed interface. The "NODE" tab is selected and highlighted in green. Below the tabs, the node name "risk:vuln" is displayed. Underneath, the node's ID "8454b46b69828937e2b6c02ac06e2217" is shown.

Question 2: What information is available for the **risk:vuln** node?

Create pol:country nodes

- In the **Executive Summary**, **highlight** the text **Azerbaijan**. **Right-click** the highlighted text and select **extractors > Country (pol:country)**:



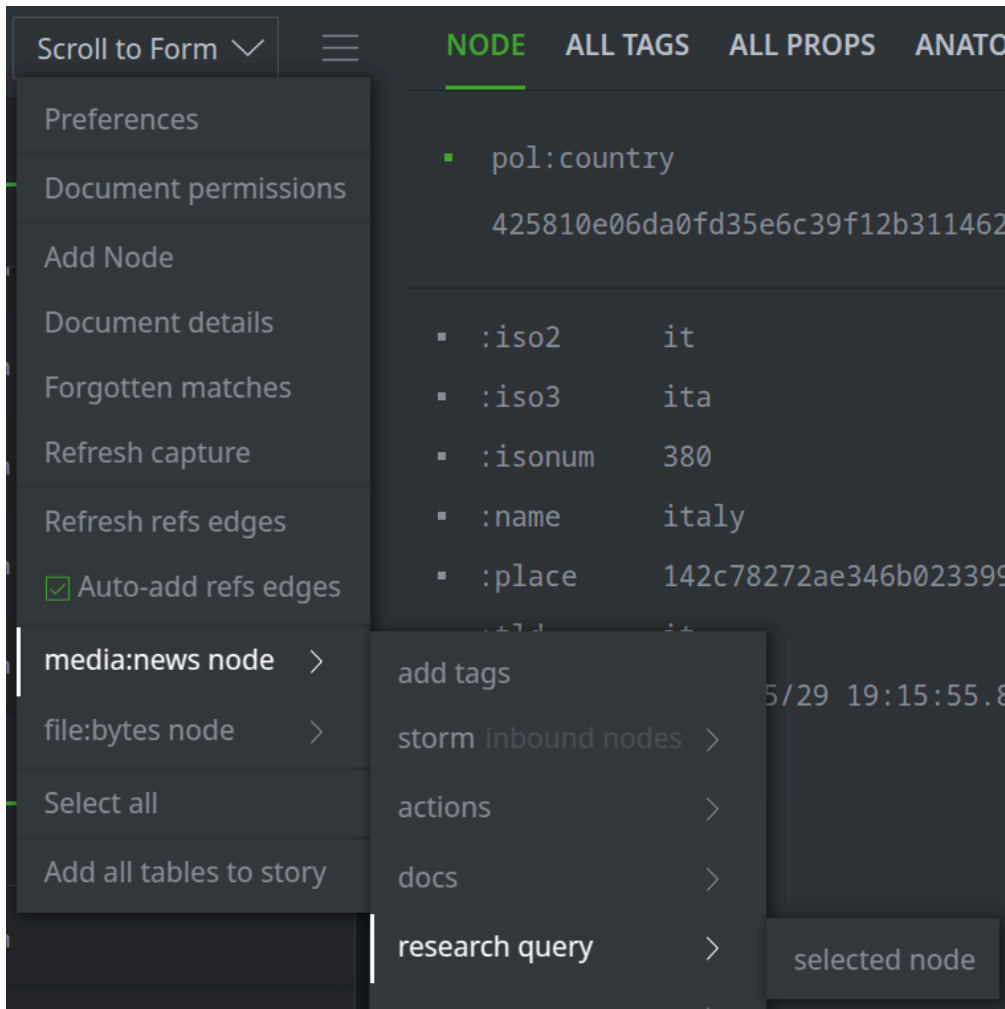
Question 3: Did Spotlight add the **pol:country** node?

- In the **Executive summary**, **repeat** the steps to create additional countries:
 - Greece
 - Romania
 - Italy

Question 4: How many **pol:country** nodes are in your Spotlight results?

Part 3 - View your linked nodes in the Research Tool

- From the Spotlight main **hamburger menu**, select **media:news node** > **research query** > **selected node** to view the node in the **Research Tool**:



- In the **Research Tool**, add the **refs** edge traversal (shown below) to the **Storm query bar** to show the nodes referenced by the **media :news** node:

```
media:news=cb5c98f3940bff6e97a99b6ab84f83e3 -(refs)> *
```

Question 5: Are the nodes that you created in the results?

Spotlight and the Threat Intel Workflow

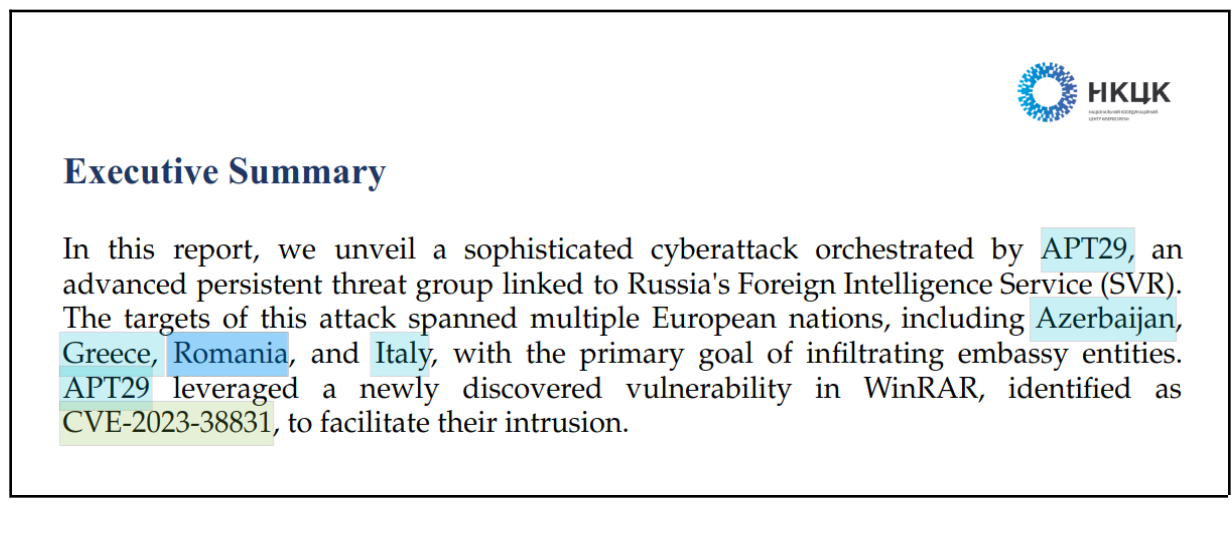
Exercise 3


Objective:

- Use Spotlight, Extractors, and the Threat Intel Workflow to capture detailed information about threat activity.

This is the first time you have added threat data from the Ukraine NSDC to Synapse. You want to record what they say about APT29.

The **Executive Summary** has important details:



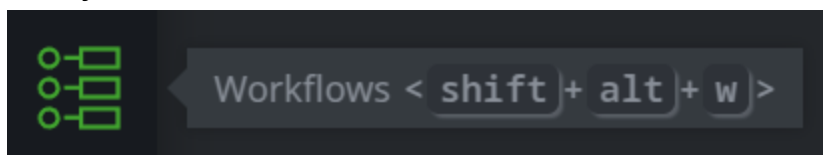
 **HKUJ**

Executive Summary

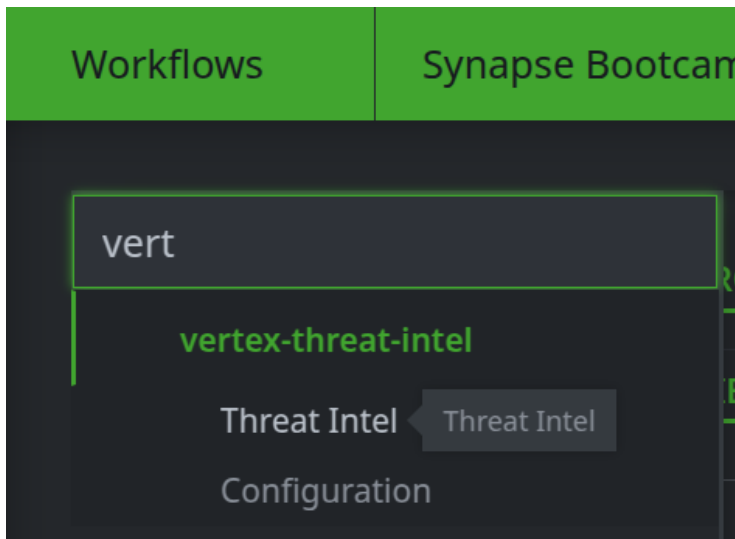
In this report, we unveil a sophisticated cyberattack orchestrated by **APT29**, an advanced persistent threat group linked to Russia's Foreign Intelligence Service (SVR). The targets of this attack spanned multiple European nations, including **Azerbaijan**, **Greece**, **Romania**, and **Italy**, with the primary goal of infiltrating embassy entities. **APT29** leveraged a newly discovered vulnerability in WinRAR, identified as **CVE-2023-38831**, to facilitate their intrusion.

Part 1 - Add information about APT29

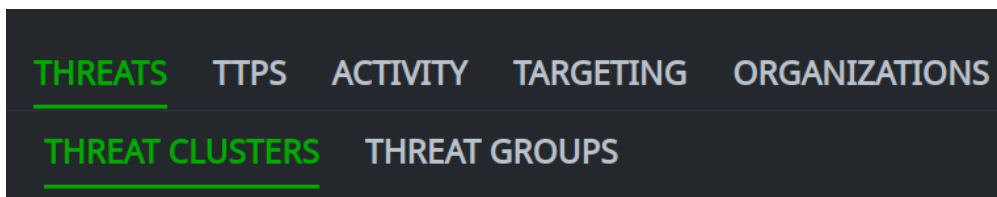
- From your **Toolbar**, select the **Workflows Tool**:



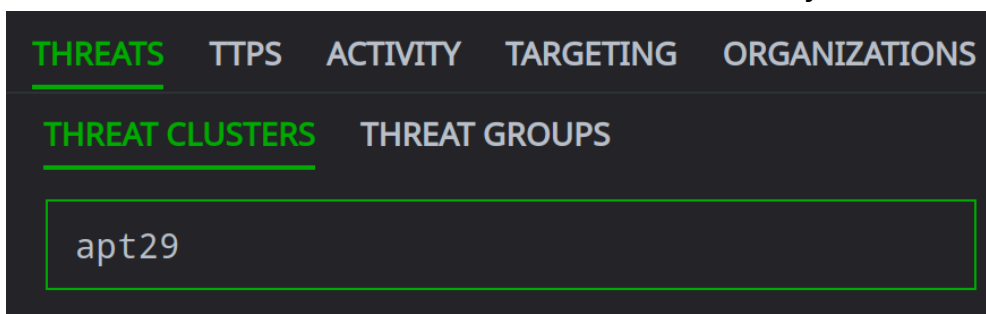
- From the Workflows list, locate the **Vertex Threat Intel** workflow and select **Threat Intel** to open the Workflow:



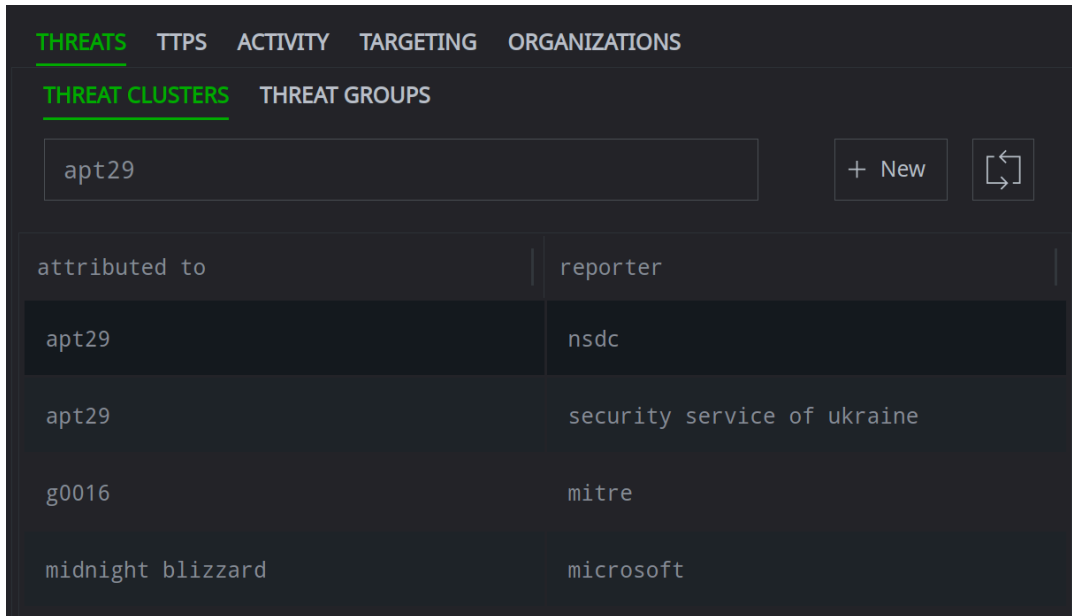
- In the **Selection Panel**, from the **THREATS** tab, select **THREAT CLUSTERS**:



- In the **Search bar**, enter **APT29** to locate the threat cluster you created:



- **Select the apt29 threat cluster associated with the NSDC:**

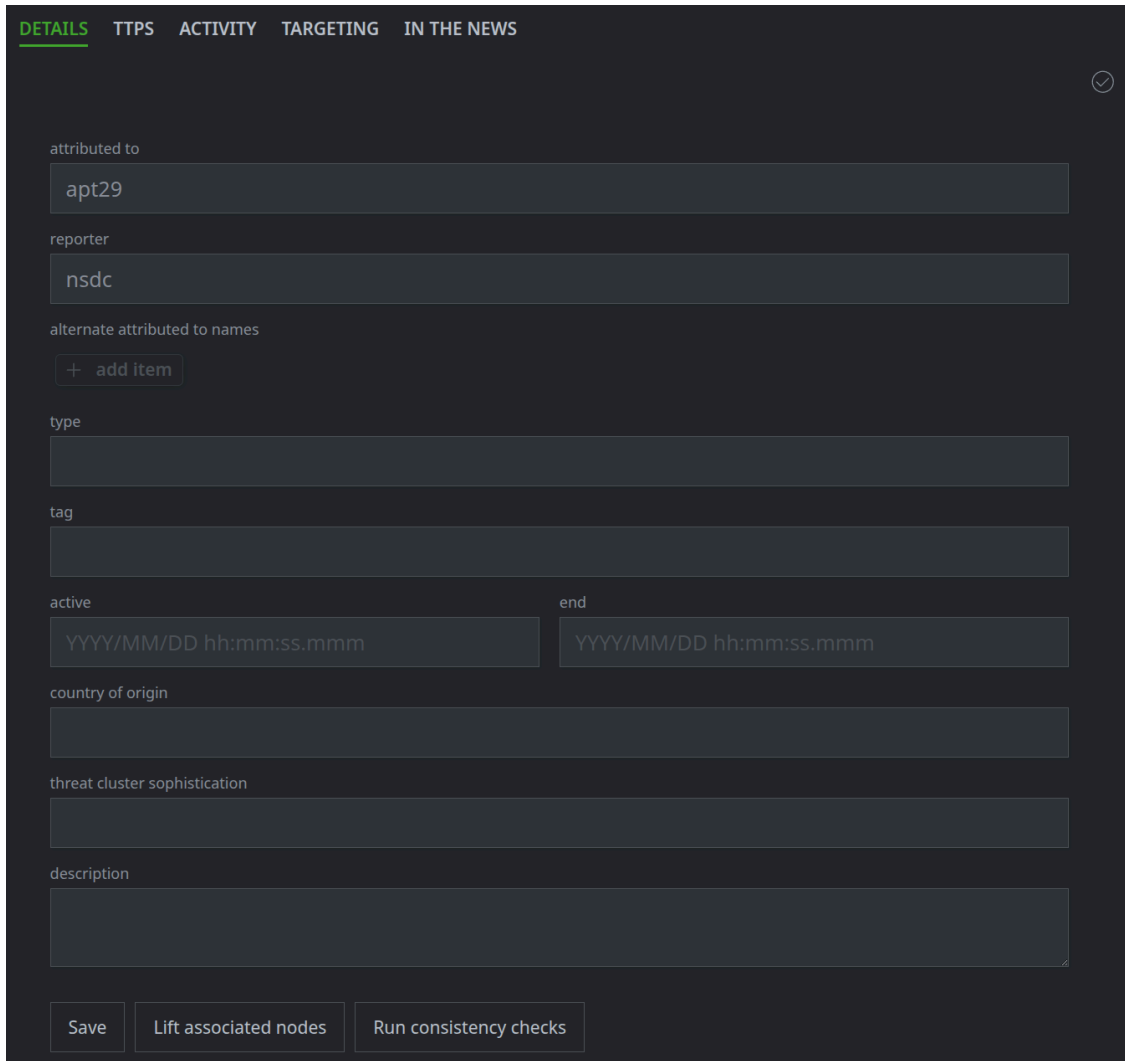


The screenshot shows the Vertex interface with the following elements:

- Navigation tabs: THREATS (selected), TTPS, ACTIVITY, TARGETING, ORGANIZATIONS
- Sub-navigation: THREAT CLUSTERS (selected), THREAT GROUPS
- Search input: apt29
- Buttons: + New, Refresh
- Table of results:

attributed to	reporter
apt29	nsdc
apt29	security service of ukraine
g0016	mitre
midnight blizzard	microsoft

- **View** the threat cluster information in the **Profile Panel (DETAILS tab)**:



The screenshot shows the 'DETAILS' tab of the Profile Panel. The form contains the following fields and controls:

- attributed to:** Text input field containing 'apt29'.
- reporter:** Text input field containing 'nsdc'.
- alternate attributed to names:** Section with a '+ add item' button.
- type:** Text input field.
- tag:** Text input field.
- active:** Text input field with a date-time placeholder 'YYYY/MM/DD hh:mm:ss.mmm'.
- end:** Text input field with a date-time placeholder 'YYYY/MM/DD hh:mm:ss.mmm'.
- country of origin:** Text input field.
- threat cluster sophistication:** Text input field.
- description:** Text area.
- Buttons:** 'Save', 'Lift associated nodes', and 'Run consistency checks'.

Add a **tag** and **description** of the threat.

- In the **DETAILS** tab, in the **tag** field, enter the following:

rep.nsd.c.apt29

type

tag

new tag: rep.nsd.c.apt29

- In the **country of origin** field, enter **russia**:

tag

active

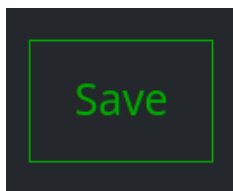
country of origin

- In the **description** field, enter a brief description. For example:

Threat group the Ukraine National Security Defense Council tracks as APT29.

country of origin
ru ssia
threat cluster sophistication
description
Threat group the Ukraine National Security Defense Council tracks as <u>APT29</u> .

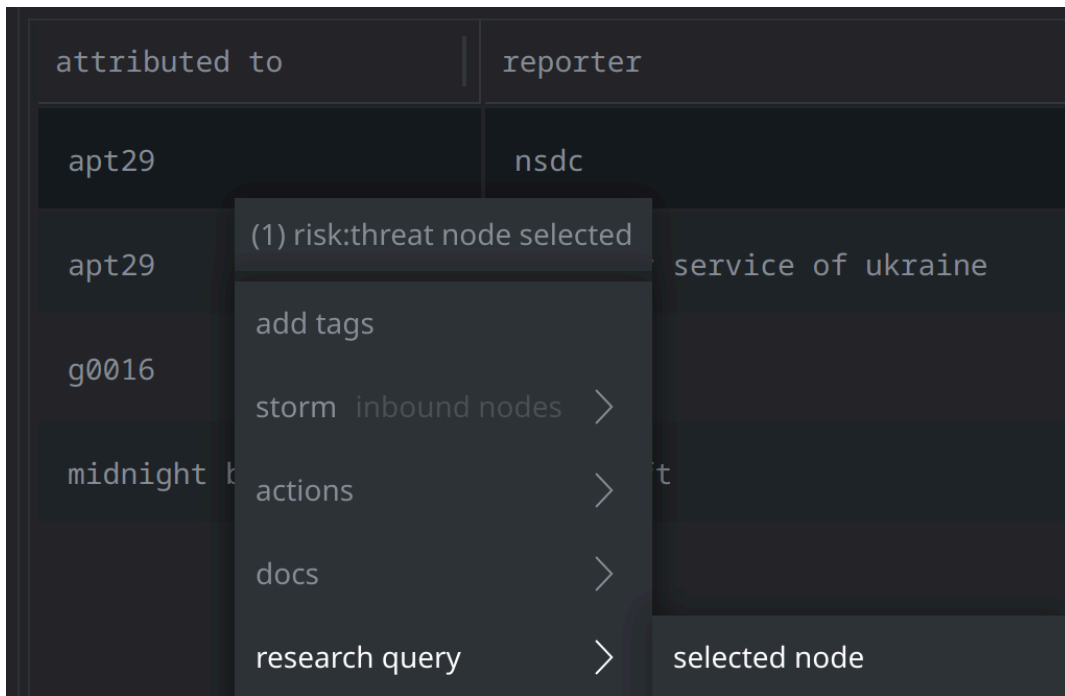
- Click **Save** to save your changes:



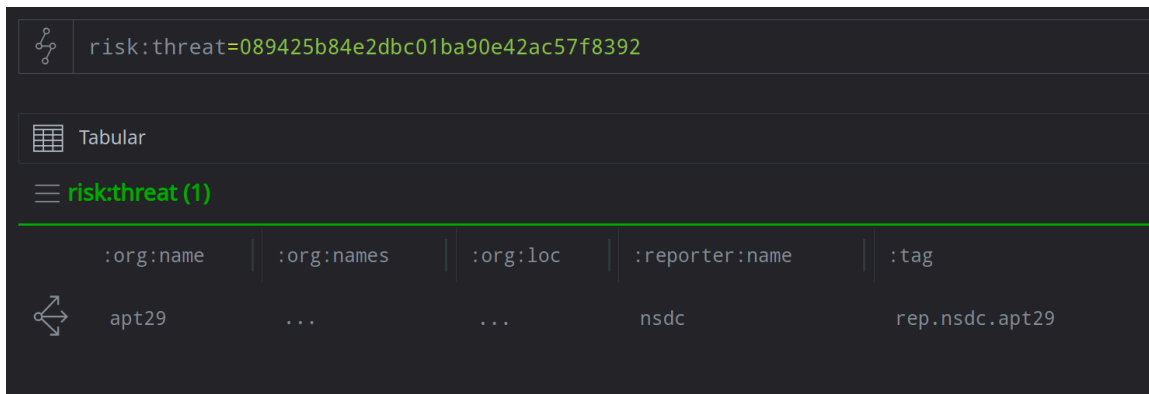
Specifying the **country of origin** in the Threat Intel Workflow adds the `pol:country` node to the threat. We want to add the "human friendly" country abbreviation.

We can add this property from the **Research Tool**.

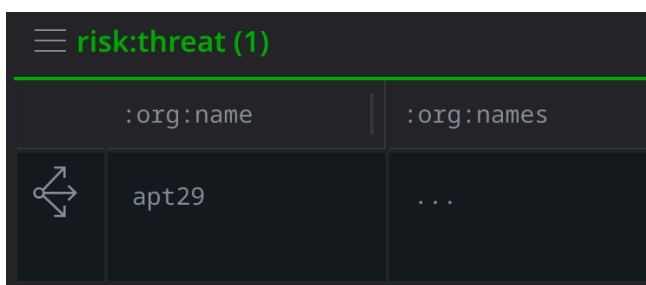
- In the **Workflow**, in the **Selection Panel**, **right-click** the APT29 threat cluster and select **research query > selected node**:



- Synapse takes you to the **Research Tool**:



- In the **Results Panel**, **select** the node:



- In the **Details Panel**, view the node's properties. Note that the **:country** property has been set with the guid of the **pol:country** node for russia:

```

NODE ALL TAGS ALL PROPS ANATOMY
├─ risk:threat
│   └─ 089425b84e2dbc01ba90e42ac57f8392
├─ :country      ba74642d02dbf3ee224f27...
│   └─ :desc      Threat group the Ukrai...
│   └─ :org:name   apt29
├─ :reporter     1a38cf1eeea13ea2017b80...
│   └─ :reporter:name nsdc
│   └─ :tag        rep.nsd.c.apt29
└─ .created      2024/07/01 22:24:28.154

```

- In the **Results Panel**, **double-click** the three dots (...) in the **:org:loc** property to edit the property:

:org:names	:org:loc	:reporter:name
...	<input type="text"/>	nsdc


- Enter **ru** for the property value and press **Enter** to save your change:

:org:names	:org:loc	:reporter:name
...	ru	nsdc

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

Part 2 - Link information about APT29

The **Executive Summary** includes information on **vulnerabilities** used by APT29 and **countries** they target:

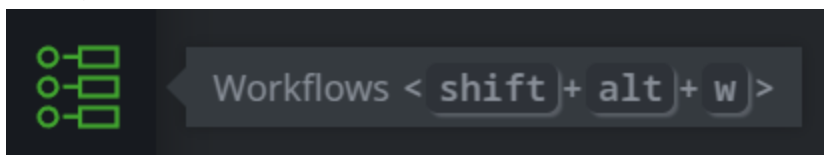
 HKU
HAKKON KUNIK

Executive Summary

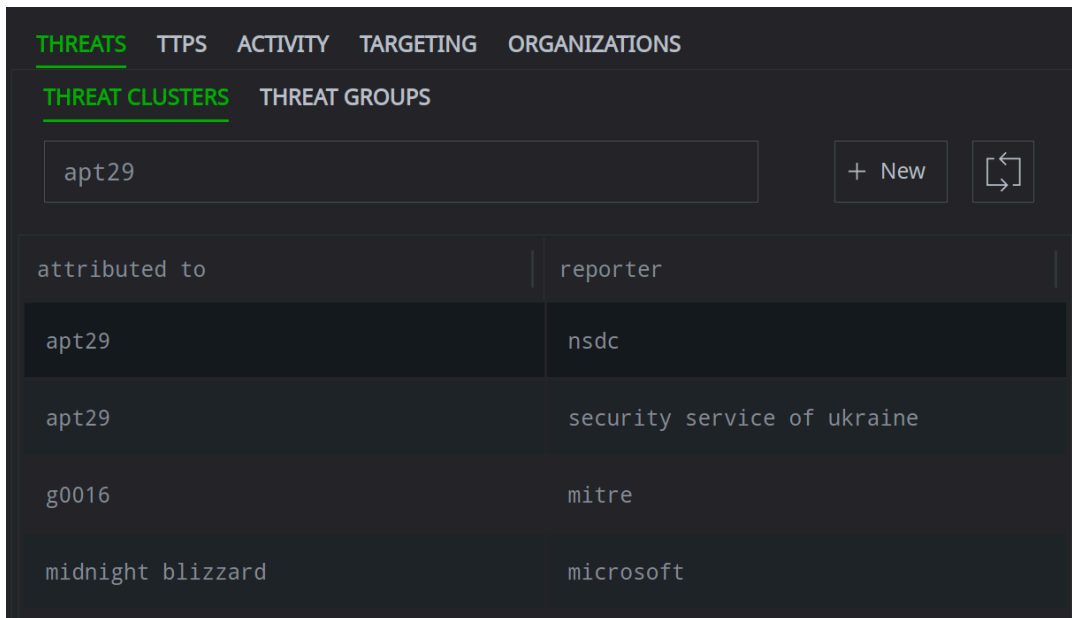
In this report, we unveil a sophisticated cyberattack orchestrated by **APT29**, an advanced persistent threat group linked to Russia's Foreign Intelligence Service (SVR). The targets of this attack spanned multiple European nations, including **Azerbaijan**, **Greece**, **Romania**, and **Italy**, with the primary goal of infiltrating embassy entities. **APT29** leveraged a newly discovered vulnerability in WinRAR, identified as **CVE-2023-38831**, to facilitate their intrusion.

Add Vulnerabilities

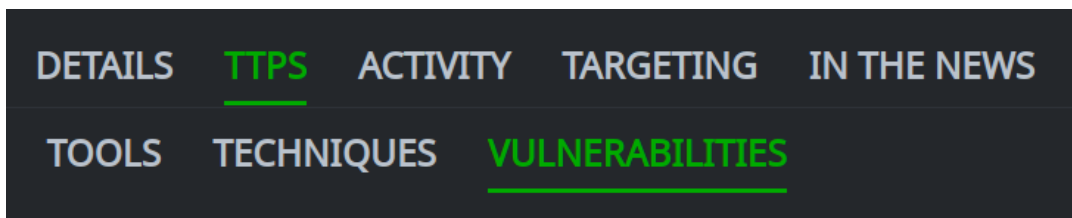
- From your **Toolbar**, select the **Workflows Tool**:



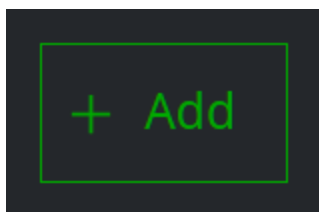
- In the **Selection Panel**, **THREATS** tab, **THREAT CLUSTERS** subtab, **select** the APT29 threat cluster from **NSDC**:



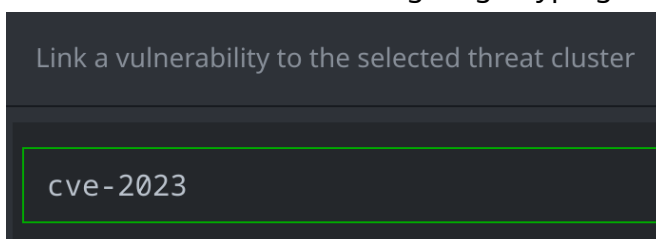
- In the **Profile Panel**, select the **TTPS** tab and the **VULNERABILITIES** subtab:



- Click the **+ Add** button to add a vulnerability:



- In the **Search bar** in the dialog, begin typing the CVE number (CVE-2023-38831):



- From the results, click the **hamburger menu** next to the **cve-2023-38831** entry for the **nsdc** and select **Link selected node(s)**:

Link a vulnerability to the selected threat cluster

cve-2023

cve	name	reporter
☰ cve-2023-25690	...	nist
☰ cve-2023-27522	...	nist
☰ cve-2023-38831	...	nsdc

Link selected node(s)

- The CVE should appear on the **VULNERABILITIES** tab:

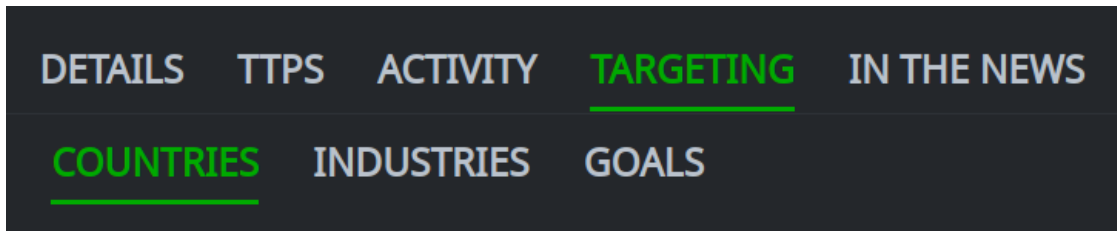
DETAILS TTPS ACTIVITY TARGETING IN THE NEWS

TOOLS TECHNIQUES VULNERABILITIES

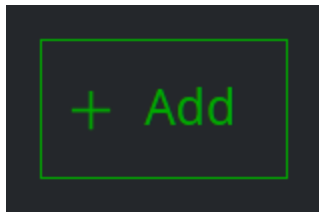
name	reporter	cve	description
☰ ...	nsdc	cve-2023-38831	...

Add Targeted Countries

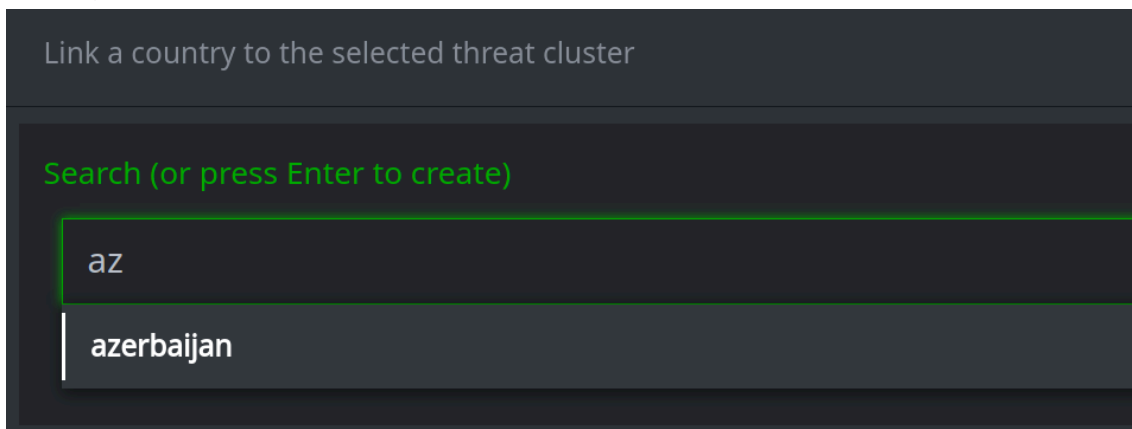
- In the **Profile Panel**, select the **TARGETING** tab and the **COUNTRIES** subtab:



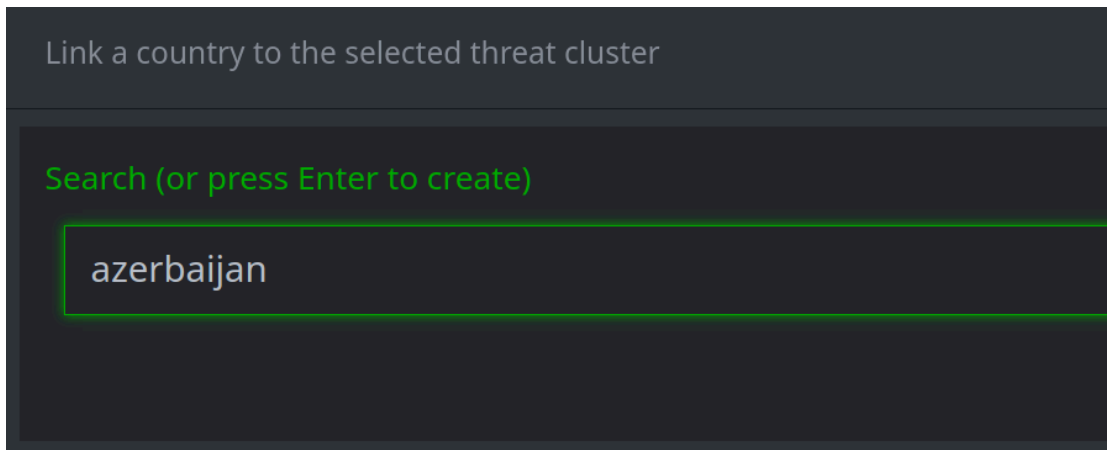
- Click the **+ Add** button to add a country:



- In the **Search bar**, begin typing to locate the country **Azerbaijan**. **Select** the country from the list:



- Press **Enter** to add the country:



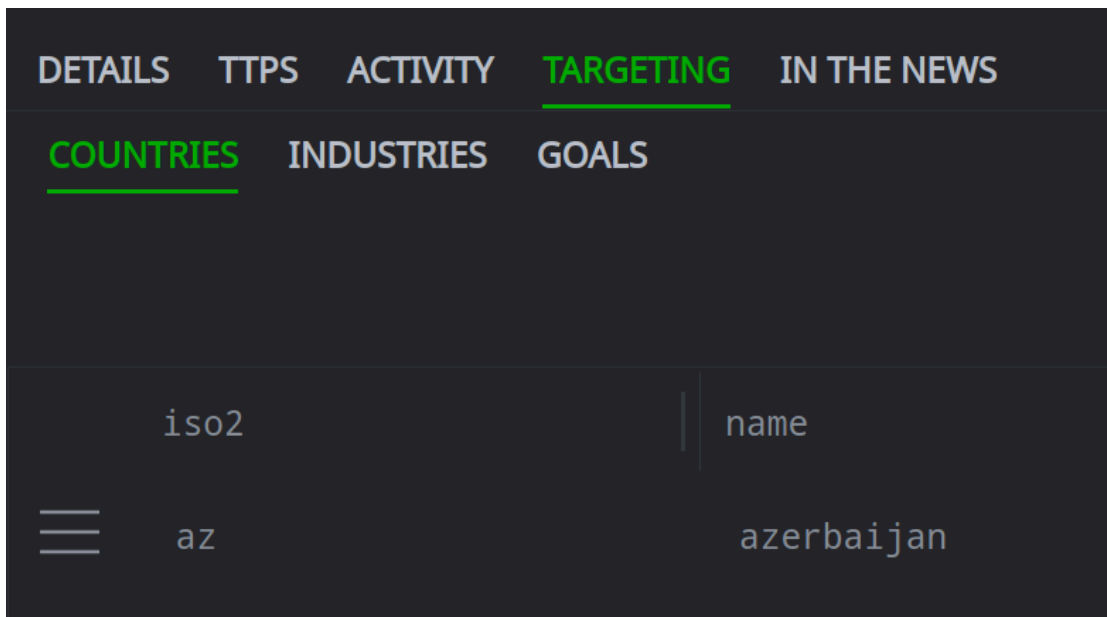
Link a country to the selected threat cluster

Search (or press Enter to create)

azerbaijan

Tip: your cursor must be in the Search bar when you press Enter.

- The country should appear on the **COUNTRIES** tab:



DETAILS TTPS ACTIVITY **TARGETING** IN THE NEWS

COUNTRIES INDUSTRIES GOALS

iso2	name
az	azerbaijan

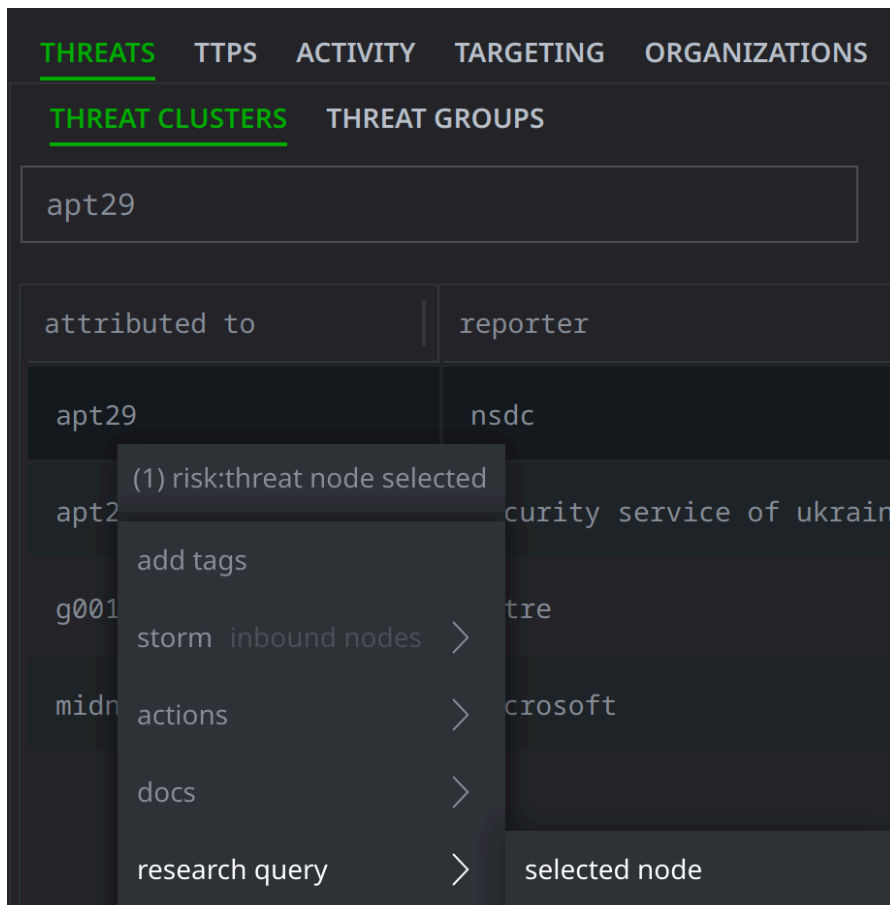
- **Repeat** the steps above to add the following countries:
 - Greece
 - Romania
 - Italy

Question 2: What does the **COUNTRIES** tab look like?

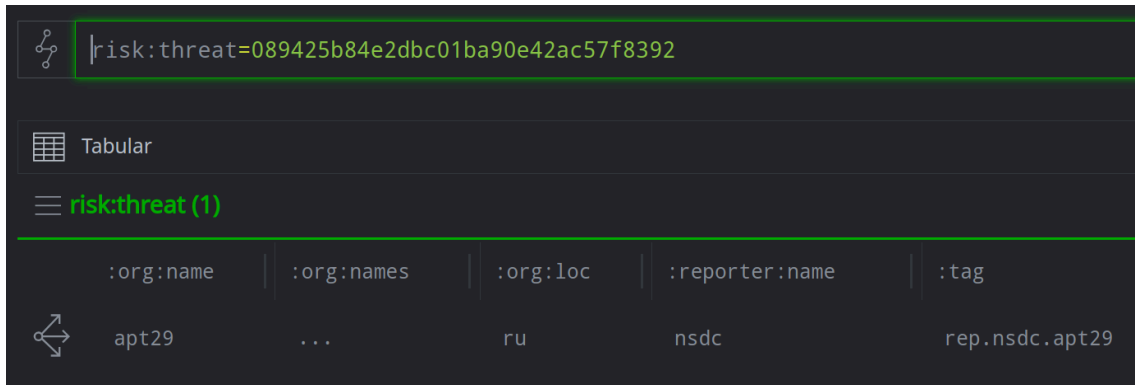
Part 3 - View your threat cluster in the Research Tool

Now that you have added information about NSDC's APT29, you want to see what it looks like in the Research Tool.

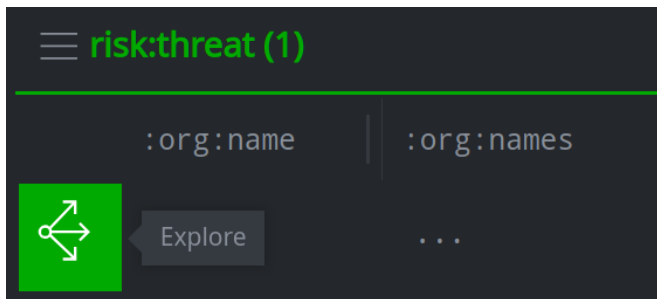
- In the **Selection Panel**, **right-click** the APT29 threat cluster for NSDC and select **research query > selected node**:



- Synapse takes you to the **Research Tool**:



- In the **Results Panel**, click the **Explore** button next to the `risk:threat` to view adjacent nodes:



Question 3: What kinds of nodes is the `risk:threat` connected to?

You want to check the light edges that were used to create these links.

- In the **Research Tool**, run each of the following in the **Storm query bar**:

```
risk:threat=089425b84e2dbc01ba90e42ac57f8392 <(refs)- *
```

```
risk:threat=089425b84e2dbc01ba90e42ac57f8392 -(targets)> *
```

```
risk:threat=089425b84e2dbc01ba90e42ac57f8392 -(uses)> *
```

Question 4: What kinds of nodes are connected by each edge?

- refs
- targets
- uses

Appendix - Sample Extractors

Additional examples of both [table extractors](#) and [extractors](#) can be found in our blogs.

Extractor Name	Storm
Threat (risk:threat)	<pre>media:news=\$news \$reporter=:publisher:name [+(refs)> { [ou:name=\$text] }] yield { gen.risk.threat \$text \$reporter } -media:news</pre>
Tool (risk:tool:software)	<pre>media:news=\$news \$reporter=:publisher:name [+(refs)> { [it:prod:softname=\$text] }] yield { gen.risk.tool.software \$text \$reporter } -media:news</pre>
Vulnerability (risk:vuln) creates a reporter-specific vulnerability	<pre>media:news=\$news \$reporter=:publisher:name [+(refs)> { [it:sec:cve=\$text] }] yield { gen.risk.vuln \$text \$reporter } -media:news</pre>
Vulnerability (risk:vuln) creates a NIST-specific vulnerability and populates the risk:vuln node using the synapse-nist-nvd Power-Up	<pre>[+(refs)> { [it:sec:cve=\$text] }] yield { gen.risk.vuln \$text nist }</pre>
Country (pol:country)	<pre>media:news=\$news [+(refs)> { [geo:name=\$text] }] -media:news geo:name=\$text -> pol:country</pre>
hash:sha256	<pre>[hash:sha256=\$text]</pre>
inet:url	<pre>\$text=\$text.replace('hxxp','http') \$text=\$text.replace(':',':') \$text=\$text.replace('[.]','.') \$text=\$text.replace(' ','') [inet:url=\$text]</pre>

