

Synapse Bootcamp - Module 21

More Fun with Spotlight - Answer Key

More Fun with Spotlight - Answer Key	1
Answer Key	2
Create Extractors	2
Exercise 1 Answer	2
Working with Spotlight Extractors	2
Exercise 2 Answer	2
Spotlight and the Threat Intel Workflow	6
Exercise 3 Answer	6
Part 1 - Add information about APT29	6
Part 2 - Link information about APT29	7
Part 3 - View your threat cluster in the Research Tool	8

Answer Key

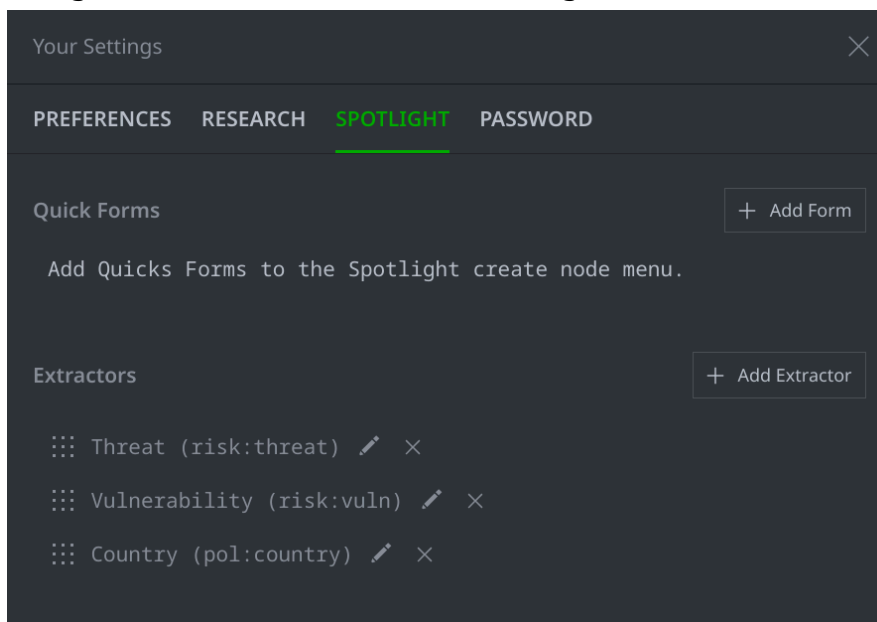
Create Extractors

Exercise 1 Answer

Objective:

- Add custom Extractors to Spotlight.

- When you have added the Extractors, the **SPOTLIGHT** tab in the **Your Settings** dialog should look similar to the following:



Working with Spotlight Extractors

Exercise 2 Answer

Objective:

- Use Extractors to create nodes from highlighted text.

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

- Spotlight created a **new risk:threat** node:

NODE	ALL TAGS	ALL PROPS	ANATOMY
▪ risk:threat			
089425b84e2dbc01ba90e42ac57f8392			
▪ :org:name apt29			
▪ :reporter 1a38cf1eeea13ea2017b80bd...			
▪ :reporter:name nsdc			
▪ .created 2025/02/27 17:31:57.127			

You can see that this is a new node because:

- The only properties that are set are the threat name (APT29), the reporter name (NSDC), and the reporter organization (the guid for NSDC's **ou:org** node, which was already in Synapse).
- The **.created** time is the current date / time.

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

- Spotlight created a **new risk:vuln** node and set properties using data from the **media:news** node:

NODE	ALL TAGS	ALL PROPS	ANATOMY
▪ risk:vuln			
8454b46b69828937e2b6c02ac06e2217			
▪ :cve		cve-2023-38831	
▪ :reporter		1a38cf1eeea13ea2017b80bdb004d7b0	
▪ :reporter:name		nsdc	

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

- **Yes.** Spotlight added the **pol:country** node:

▪ pol:country	
8cb9f747d5c576f53e9bbe493d94398a	
▪ :iso2	az
▪ :iso3	aze
▪ :isonum	31
▪ :name	azerbaijan
▪ :place	a0abcbd1479ef2285b02e88af8e5023a
▪ :tld	az
▪ .created	2023/05/29 19:15:56.167

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

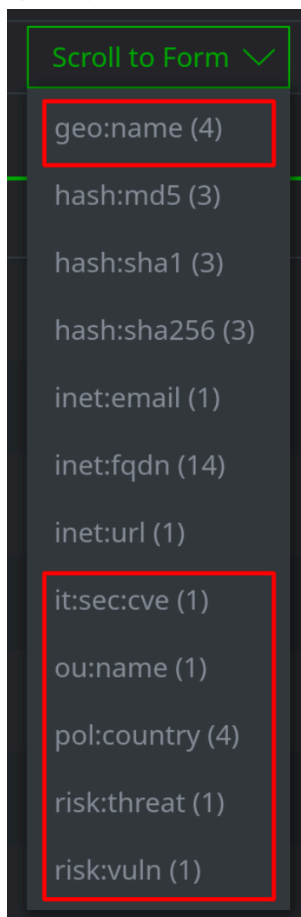
- There are **four** **pol:country** nodes:

pol:country (4) all existing		
pol:country		
▪	0833a0aa6e897a33a53c0191...	< > 5 matches
▪	425810e06da0fd35e6c39f12...	< > 6 matches
▪	6aaf3ebc665b7465bd675e02...	< > 4 matches
▪	8cb9f747d5c576f53e9bbe49...	< > 9 matches

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

- **Yes.** Your results should include:
 - For **APT29**: one **risk:threat** and one **ou:name**.
 - For **CVE-2023-38831**: one **risk:vuln** and one **it:sec:cve**.
 - For the **countries**: four **pol:country** nodes and four **geo:name** nodes.

Other nodes (such as **inet:fqdn** nodes) are also linked, based on indicators that Spotlight extracted automatically from the report:



Spotlight and the Threat Intel Workflow

Exercise 3 Answer

Objective:

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

Part 1 - Add information about APT29

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

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

NODE	ALL TAGS	ALL PROPS	ANATOMY
▪ risk:threat			089425b84e2dbc01ba90e42ac57f8392
▪ :country			ba74642d02dbf3ee224f276...
▪ :desc			Threat group the Ukrain...
▪ :org:loc			ru
▪ :org:name			apt29
▪ :reporter			1a38cf1eeea13ea2017b80b...
▪ :reporter:name			nsdc
▪ :tag			rep.nsd.c.apt29
▪ .created			2024/07/01 22:24:28.154

Part 2 - Link information about APT29

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

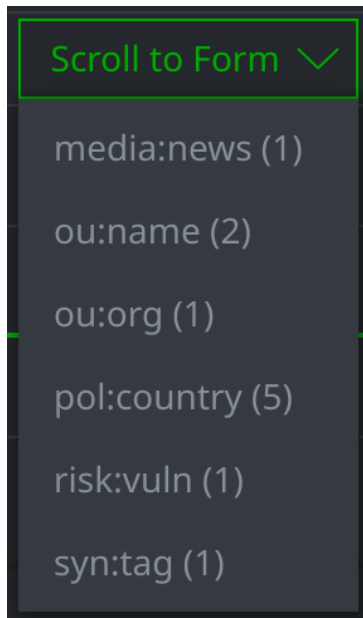
- There should be four countries listed:

DETAILS		TTPS	ACTIVITY	TARGETING	IN THE NEWS
COUNTRIES		INDUSTRIES		GOALS	
iso2				name	
☰	gr			greece	
☰	az			azerbaijan	
☰	ro			romania	
☰	it			italy	

Part 3 - View your threat cluster in the Research Tool

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

- The **risk:threat** is connected to several kinds of nodes:



Some of the connections are based on **properties** of the **risk:threat** node:

- The **ou:name** nodes (from the threat's **:org:name** / **:org:names** and **:reporter:name** properties).
- The **ou:org** node (from the threat's **:reporter** property).
- One of the five **pol:country** nodes (russia, from the threat's **:country** property).
- The **syn:tag** node (from the threat's **:tag** property).

The remaining nodes are connected based on **light edges** that we created in Spotlight and the Threat Intel Workflow. These include:

- **media:news**
- **pol:country**
- **risk:vuln**

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

- **refs**
- **targets**
- **uses**
- The **refs** edge links the threat to the **NSDC report** (**media:news**).
- The **targets** edge links the threat to the **countries** (**pol:country**) reported by NSDC.
- The **uses** edge links the threat to the **vulnerability** (**risk:vuln**) reported by NSDC.

