

# Synapse Bootcamp - Module 19

## Introduction to Threat Intelligence in Synapse - Answer Key

<b>Introduction to Threat Intelligence in Synapse - Answer Key</b>	<b>1</b>
<b>Answer Key</b>	<b>2</b>
Exercise 1 Answer	2
Part 1 - View information about a threat	2
Part 2 - View additional threat data	7
Add Threat Intel Data Using the Workflow	8
Exercise 2 Answer	8

---

# Answer Key

## Exercise 1 Answer

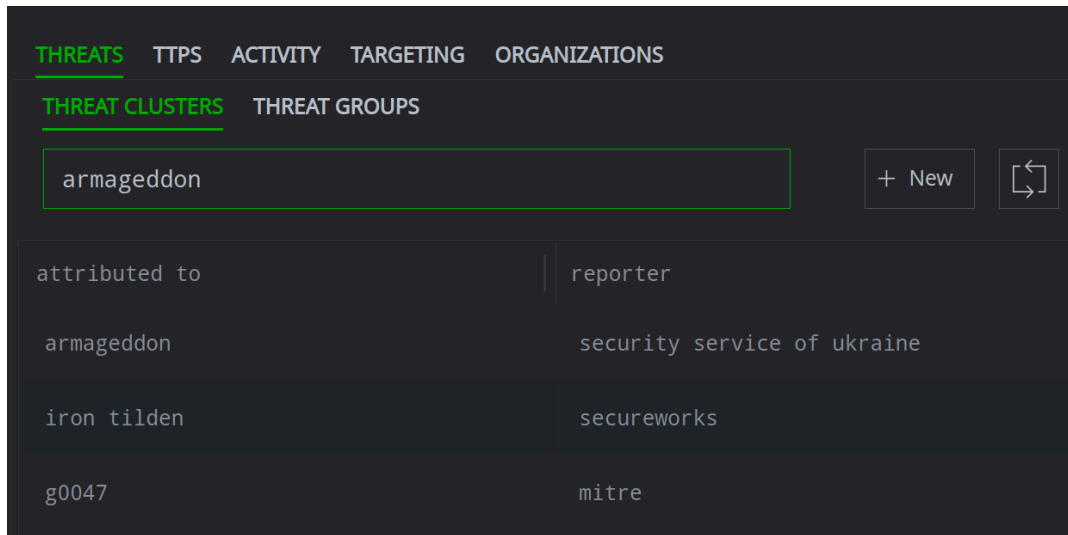
### Objective:

- Use the Threat Intel Workflow to view information related to a threat cluster.

### Part 1 - View information about a threat

#### Question 1: How many **threat clusters** are in your results?

- There are **three** threat clusters that are known as "Armageddon":



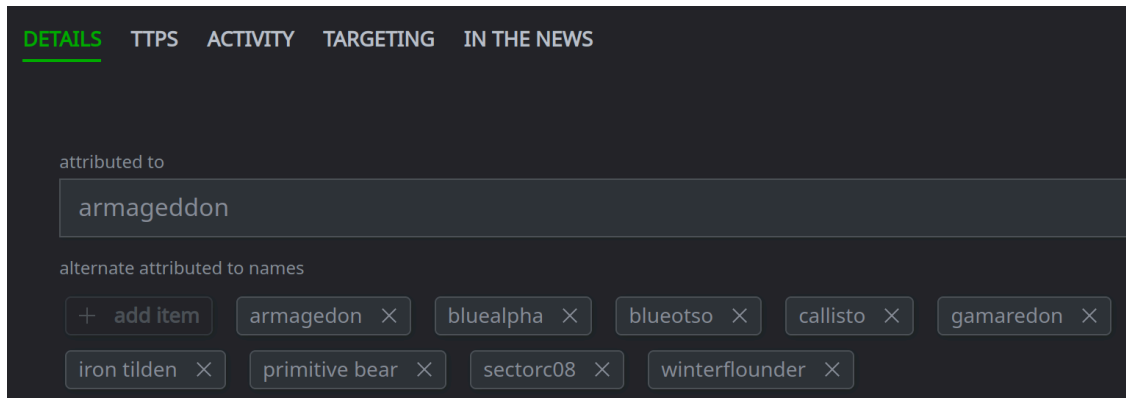
The screenshot shows the 'THREATS' tab in the Threat Intel Workflow. Under 'THREAT CLUSTERS', a search bar contains 'armageddon'. Below the search bar is a table with two columns: 'attributed to' and 'reporter'. The table lists three threat clusters: 'armageddon' (reporter: security service of ukraine), 'iron tilden' (reporter: secureworks), and 'g0047' (reporter: mitre).

THREATS	
THREAT CLUSTERS	
armageddon	
attributed to	reporter
armageddon	security service of ukraine
iron tilden	secureworks
g0047	mitre

**Tip:** The **Search** field searches the threat cluster's **primary** (**risk:threat:name**) and **secondary** (**risk:threat:names**) field. Only the primary (**:name**) property is displayed (in the **attributed to** column).

**Question 2:** How many **alternate names** are used to report on "Armageddon", according to the Security Service of Ukraine (SSU)?

- **Nine** other names refer to the same threat cluster, according to the SSU:



These include:

- armagedon (one 'd' vs. two 'dd')
- bluealpha
- blueotso
- callisto
- gamaredon
- iron tilden
- primitive bear
- sectorc08
- winterflounder

---

**Question 3:** Which **vulnerabilities** has Armageddon exploited, according to the SSU?

- Armageddon has exploited **CVE-2017-0199** and **CVE-2018-20250** according to the SSU:

DETAILS	<u>TTPS</u>	ACTIVITY	TARGETING	IN THE NEWS
TOOLS	TECHNIQUES	<u>VULNERABILITIES</u>		
	name	reporter	cve	
≡	winrar absolute path trav...	nist	cve-2018-20250	
≡	microsoft office/wordpad ...	nist	cve-2017-0199	

---

**Question 4:** What **countries** has Armageddon targeted, according to the SSU?

- Armageddon has targeted **Ukraine** according to the SSU:

DETAILS	TTPS	ACTIVITY	<u>TARGETING</u>	IN THE NEWS
<u>COUNTRIES</u>	INDUSTRIES	GOALS		
	iso2	name		
≡	ua	ukraine		

**Question 5:** How many **reports** in Synapse reference the SSU's Armageddon group?

- There are **three** articles that reference or report on "Armageddon":

DETAILS	TTPS	ACTIVITY	TARGETING	<u>IN THE NEWS</u>
	title	published	publisher	
≡	technical report on the...	2021/01/01 ...	security service of ukraine	
≡	ssu identifies fsb hack...	2021/11/04 ...	security service of ukraine	
≡	technical report on the...	2021/01/01 ...	security service of ukraine	

---

**Question 6:** What kinds of indicators are associated with Armageddon? Are there any unusual objects?

- The SSU reported several kinds of indicators:



The list includes technical indicators:

- File names (**file:base**)
- File paths (**file:path**)
- URLs (**inet:url**)
- Windows Registry data (**it:dev:regkey**, **it:dev:regval**)

The SSU also reported on several **people** that they identified as members of the Russian Federal Security Service (FSB). The SSU claims that "Armageddon" is a group within the FSB's 18th Center.<sup>1</sup>

We captured this information in Synapse using contact (**ps:contact**), person (**ps:person**), and position (**ou:position**) nodes, as well as an organization (**ou:org**) for the FSB 18th Center:

---

<sup>1</sup>

<https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-d-erzhavni-orhany-ukrainy>. Details about the FSB members are in the slides embedded at the bottom of the page.

risk:threat=7bcf1dbc6ee9d3b48156ed1746c39ab5 :tag -> syn:tag -> \*

Tabular ps:contact ▾

ps:contact (8)

	:name	:dob	:orgname	:title	:loc
↗	sklianko oleksandr mykolaiovich	1973/08/05 ...	federal security service (fsb) 18th center	deputy chief of the 4th section of service of counterintelligence operations (sco)	ua.sevastopol
↗	mykhailiuk leonid volodymyrovych	1970/01/01 ...	federal security service (fsb) 18th center	head of department of fsb of the russian federation in the republic of crimea and the city of sevastopol	ua.sevastopol
↗	sushchenko oleh oleksandrovych	1989/10/12 ...	federal security	officer of the unit of	ua.sevastopol

## Part 2 - View additional threat data

**Question 7:** Which **threat clusters** have exploited CVE-2021-34523? Who reported on the threats?

- **APT28, Worok, and UNC3762** have all exploited CVE-2021-34523.
- **Mandiant** reported on APT28 and UNC3762.
- **ESET** reported on Worok.

	attributed to	reporter	tag
≡	apt28	mandiant	rep.mandiant.apt28
≡	worok	eset	rep.eset.worok
≡	unc3762	mandiant	rep.mandiant.unc3762

**Question 8:** Which **threat clusters** have targeted Japan? Who reported on the threats?

- **APT1, APT10, APT41, Axiom, Bronze Butler, and Bronze Huntley** have all targeted Japan.
- **Mandiant** reported on APT1 and APT41.
- **Novetta** reported on Axiom.
- **PwC** (PricewaterhouseCoopers) reported on APT10.
- **Secureworks** (Dell Secureworks) reported on Bronze Butler and Bronze Huntley.

	attributed to	reporter	tag
≡	axiom	novetta	rep.novetta.axiom
≡	apt41	mandiant	rep.mandiant.apt41
≡	apt1	mandiant	rep.mandiant.apt1
≡	bronze huntley	secureworks	rep.secureworks.bron...
≡	apt10	pwc	rep.pwc.apt10
≡	bronze butler	secureworks	rep.secureworks.bron...

---

## Add Threat Intel Data Using the Workflow

### Exercise 2 Answer

**Objectives:**

- Use the Threat Intel Workflow to create a threat cluster.
- Use the Workflow to link information to the threat cluster.

**Question 1:** What does the **DETAILS** tab look like?



- The **DETAILS** panel should look similar to the following:

**DETAILS** TTPS ACTIVITY TARGETING IN THE NEWS

attributed to

bronze canal

reporter

secureworks

alternate attributed to names

+ add item

blacktech ×

circuit panda ×

ctg-6177 ×

palmerworm ×

shrouded crossbow ×

type

tag

rep.secureworks.bronze\_canal

active

YYYY/MM/DD hh:mm:ss.mmm

end

YYYY/MM/DD hh:mm:ss.mmm

country of origin

threat cluster sophistication

description

Threat activity Secureworks tracks as Bronze Canal.