Vertex

Synapse Bootcamp - Module 6

Putting it All Together - Exercise

Objectives

In these exercises you will:

- Take what you've learned in Modules 1 - 5 and apply them in practice!

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!

Exercise

Summary Exercise: Modules 1 - 5

Objectives:
- **Apply what you've learned in Modules 1 - 5 using real world data.**
- **Continue to explore the features available in the Synapse UI.**

For this exercise, we'll use an article (public threat report) as the starting point to practice what we've learned so far, including:

- Add data to Synapse
- Look up data in Synapse
- Navigate and explore Synapse data
- Use Node Actions to call Power-Ups to enrich data
- Review enriched data
- Modify data
- Add tags

Consider the following EclecticIQ blog from October 2023:

"Chinese State-Sponsored Cyber Espionage Activity Targeting Semiconductor Industry in East Asia"

```
https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia
```

Note: Converting these documents to PDF may insert line breaks where lines wrap within text boxes. If you copy and paste the link above, you may need to manually remove any spaces or line breaks that are inserted. You can also open the blog by clicking here.

The blog contains:

- a description of the activity; and
- a list of indicators of compromise (IOCs) at the end.

- **Review** the article. (You can skim it, or read it in detail - the choice is yours).

- **Add** the IOCs to Synapse. **Then...dive in!**

- **Tag** the data.
    - Tag the **IOCs** based on EclecticIQ's reporting. For example:
        - **rep.eclecticiq.mal** ("EclecticIQ says this is malicious")
        - **rep.eclecticiq.hyperbro** ("EclecticIQ says this is associated with HyperBro")
        - **rep.eclecticiq.chargeweapon** ("EclecticIQ says this is associated with ChargeWeapon")

    Tip: When we use tags to record what other organizations say about threat activity, we are only interested in recording their assessment - **not** whether we agree with what they say. The tag clearly indicates "who" made an assertion - in this case, EclecticIQ. We can use our own tags to record what we believe. This allows us to compare and contrast reporting by different organizations!

- **Enrich** the data using your Power-ups and Node Actions.
    - Use the Node Actions from earlier exercises.
    - Experiment with additional Node Actions and Power-Ups.

- **Explore** the data.
    - Are the IOCs connected to anything we already know about in Synapse?
    - Can we identify additional indicators or connections?
    - Are there additional leads you want to research?

- Use **additional tags** to help keep track of your work as you go.
    - If you decide something is malicious, tag it (e.g., **cno.mal**).
    - Use "scratch" tags to record your initial thoughts or keep track of your progress.

Note: The goal of this exercise is **not** to fully analyze the data, but to practice exploring Synapse and its features using a real-world example.

We'll cover some **specific** analysis workflows (such as how to examine network infrastructure or malware) in upcoming modules. Those modules will focus more closely on examining and navigating particular subsets of data in Synapse. So stay tuned!

General Tips

A few pointers to get you started, if needed:

- **Use tags to help "take notes" while you work.**
  - You can use tags **however you want.**
    - Use "official" tags (like **cno.mal**) for your conclusions.
    - Use "unofficial" tags to help keep track of your work.
      - Use any tags that make sense to you (e.g., **review, legit, maybe.c2,** etc.)
      - Some users like to put their username in their "unofficial" tags (e.g., **mb.review**).

- **Some IOCs may "contain" additional IOCs.**
  - For example, a URL may contain an FQDN or an IPv4. These may not be included in the IOC list in the report, but may still be worth enriching.

Guiding Questions

If you're not sure where to start, you can use any of these sample questions to guide your exploration:

Question 1

EclecticIQ assesses that the activity is most likely the work of groups operating on behalf of the Chinese government, and notes overlaps with prior reporting from other vendors. Use the **synapse-alienvault > files API** Node Action to enrich the **`hash:sha256`** nodes, and then explore to the associated **`file:bytes`** to view the tags applied by the Power-Up.

What are some of the possible group and malware names that appear in AlienVault tags on the `file:bytes` nodes?

(We can optionally try to look up some of these names using **Text-Search** mode to find out more information about these groups/malware families, if needed.)

Question 2

There were several URLs included among the IOCs in the blog. Once you've added these to Synapse, enrich them with the **synapse-alienvault > url API** Node Action.

Which of the URLs does AlienVault associate with Cobalt Strike? How can you tell?

Question 3

The blog also notes that the threat actors used a lure in Mandarin referencing Taiwan Semiconductor Manufacturing (TSMC).

What steps can you take to identify which file makes this reference in its filename?

Question 4

EclecticIQ included two IPv4 addresses in their IOC list. (Additional IPv4 addresses were reported within URLs / servers; we just want to focus on the two plain IPv4s.)

Enrich these IPv4 addresses with the **synapse-virustotal > communicating files** Node Action.

How many files (total) communicate with the two IPv4 addresses?

How many files (SHA256 hashes) were **not** included in the EclecticIQ report?

Question 5

According to the blog, the threat activity includes the use of a file named **bin.config** which contains XOR encrypted Cobalt Strike shellcode. Use the **synapse-virustotal > file behavior** Node Action to enrich the hashes included in the IOC list.

Which hash is associated with the file that attempts to download **`bin.config`** from **`hxxp://154.93.7[.]99:8090/CDGServer3/images/zh/bin.config`**?

Guide - Enriching Data with Power-Ups

Below is a brief guide to how the Power-Ups in your demo instance of Synapse may be used to enrich indicators associated with the EclecticIQ article used in this exercise.

This is not a complete list, but includes several that may be useful or interesting to test out.

Refer to the Help for specific Power-Ups / Node Actions for additional detail.

URLs (`inet:url` nodes)

Node Action	Purpose
`synapse-alienvault > url API`	Obtain additional detail about the URL from AlienVault OTX.
`synapse-virustotal > enrich`	Obtain VirusTotal report data for the URL (e.g., scan/reputation data, any HTTP results from querying the URL, etc.)

IPv4 Addresses (`inet:ipv4` nodes)

Tip: EclecticIQ listed **two** IPv4 addresses in their IOCs (23.224.61.12 and 45.32.33.17). There are three **additional** IPv4s present (as part of the URLs). You may want to tag and / or enrich all of them.

Network Data

Node Action	Purpose
synapse-maxmind > maxmind	Obtain geolocation and AS number data from Maxmind.
synapse-nettools > dns	Obtain DNS PTR (reverse lookup) data using a **live** query.
synapse-nettools > whois	Obtain IP netblock registration (whois) data using a **live** query.
synapse-virustotal > whois history	Obtain historical IP netblock registration (whois) data from VirusTotal.

Passive DNS Data

Node Action	Purpose
synapse-alienvault > pDNS API	Obtain passive DNS data from AlienVault.
synapse-virustotal > pdns	Obtain passive DNS data from VirusTotal.

IP or Host Data

Node Action	Purpose
synapse-alienvault > ip API	Obtain additional IP data from Alienvault (e.g. AS / geolocation data, tags, etc) from AlienVault.
synapse-virustotal > enrich	Obtain VirusTotal report data for the IPv4 (e.g., scan/reputation data, servers/ports identified on the IPv4, the most recent SSL certificate observed on the IPv4 (if any), netblock registration (whois) data for the IPv4, etc.)

Node Action	Purpose
synapse-virustotal > ssl history	Obtain information on historical SSL certificates (if any) observed on the IPv4 from VirusTotal.

Malware or C2 Data

Node Action	Purpose
synapse-virustotal > communicating files	Obtain information about any files VirusTotal says "communicate with" the IPv4.

SHA256 Hashes (hash:sha256 nodes)

> **Note:** Remember that public reporting includes **hashes** as IOCs, but a hash represents a **file.** Data returned by Power-Ups is modeled as a **file:bytes** node connected to the **hash:*** node (vs being "added to" the **hash:*** node itself).

Download the Files

Node Action	Purpose
synapse-malwarebazaar > malwarebazaar.download	Download the file from MalwareBazaar.
synapse-malshare > malshare.download	Download the file from MalShare.

Get information about the file

> **Tip:** Different Power-Ups will return different data. This may be very basic (a file's size and hash values) or very detailed (file metadata, detection / AV scan data, etc.)

Node Action	Purpose
synapse-alienvault > files API	Obtain file metadata and / or execution data from AlienVault OTX.
synapse-malshare > malshare.details	Obtain file information (e.g., additional hash values) from MalShare.
synapse-malwarebazaar > malwarebazaar.enrich	Obtain file information from MalwareBazaar.
synapse-virustotal > enrich	Obtain VirusTotal report data for the associated file (e.g., scan/reputation data, file metadata, associated tags, etc.)
synapse-virustotal > file report	Obtain VirusTotal report data (same as the **enrich** command) **plus** additional relationship data (specifically: contacted_domains, contacted_urls, contacted_ips, embedded_domains, embedded_ips, and 'embedded_urls).

Get information about file behavior

Node Action	Purpose
synapse-alienvault > files API	Obtain file metadata and / or execution data from AlienVault OTX.
synapse-virustotal > file behavior	Obtain file execution data for the associated file from VirusTotal.