Vertex

Synapse Bootcamp - Module 10

Filtering in Storm - Exercises

Filtering in Storm - Exercises **1**
Objectives **1**
Exercises **2**
Simple Filters 2
Exercise 1 2
Filters with Mathematical Operators 5
Exercise 2 5
Filters with Extended Operators 7
Exercise 3 7

Objectives

In these exercises you will:

- Use Storm to perform simple filter operations
- Use mathematical operators in Storm filters
- Use extended operators in Storm filters

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

- All exercises use the **Research Tool** with the **Storm Mode Selector** set to **Storm mode.**
- Some example queries may wrap due to length.

The **Storm Quick Reference** on Filtering (included with the supplemental materials provided for this course) may be helpful for this (and future) exercises.

The online **filtering** reference includes detailed documentation and examples for all filter operations. It is part of the Storm Reference included with the Synapse User Guide.

Simple Filters

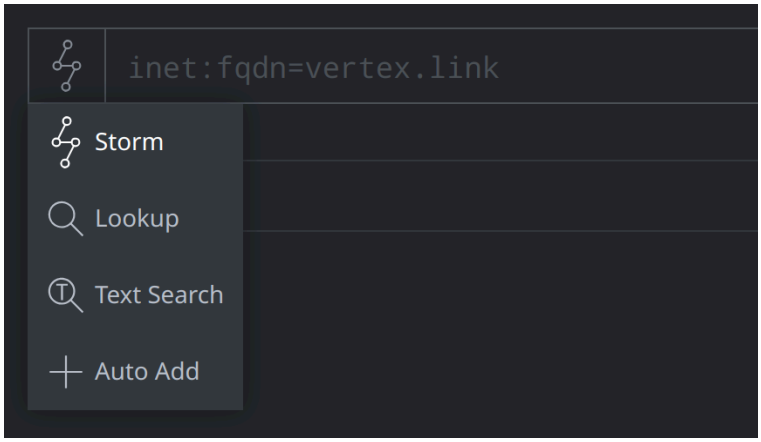
Exercise 1

Objective:
- **Use Storm to perform simple filter operations.**

Part 1

You are reviewing an Accenture blog post on the MUDCARP threat group and want to examine the IOCs listed in the blog.

- In the **Research Tool,** ensure your **Storm Query Bar** is in **Storm mode:**



- Enter the following in the **Storm Query Bar** and press **Enter** to run the query to **lift** the `media:news` node for the blog and **traverse** the `refs` edges:

```
media:news:title="mudcarp's focus on submarine technologies"
  -(refs)> *
```

The blog "references" a wide variety of data.

You are interested in any URLs (`inet:url` nodes) reported by Accenture.

Question 1: How can you **add a filter** to your existing query to **only** display the `inet:url` nodes?

Some of the URLs are malicious indicators, but some are simply references - other articles that support Accenture's reporting.

You want to focus on the **IOCs** that Accenture reported (e.g., things tagged `rep.accenture`).

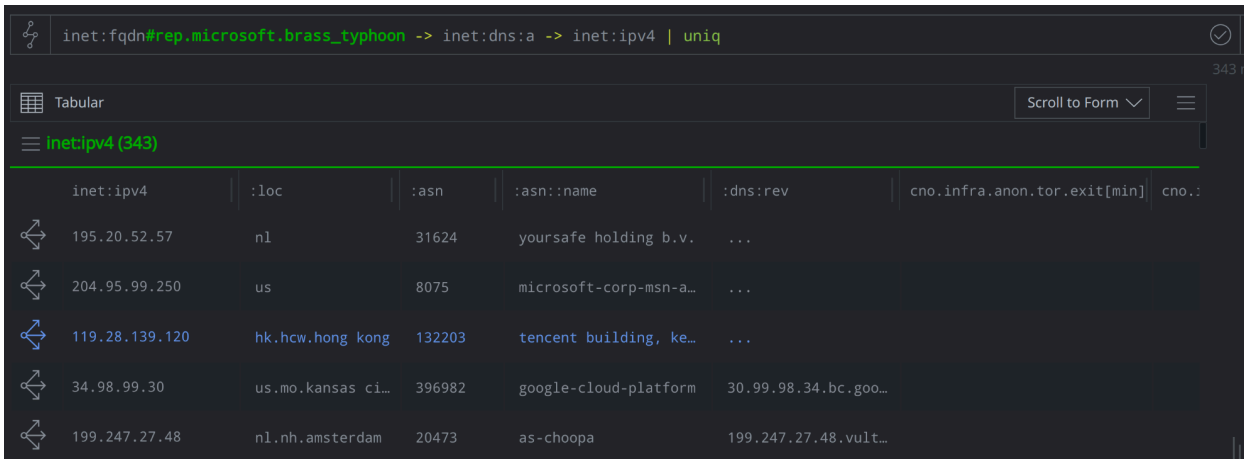
Question 2: How can you **add a filter** to your query to **only** display malicious URLs that Accenture reported?

Part 2

You are researching the Brass Typhoon threat group, examining the FQDNs associated with the group and the IPv4 addresses that the FQDNs resolve to.

- Enter the following in the **Storm Query Bar** and press **Enter** to run the query to pivot to the unique IPv4 addresses associated with Brass Typhoon FQDNs:

```
inet:fqdn#rep.microsoft.brass_typhoon -> inet:dns:a
  -> inet:ipv4 | uniq
```

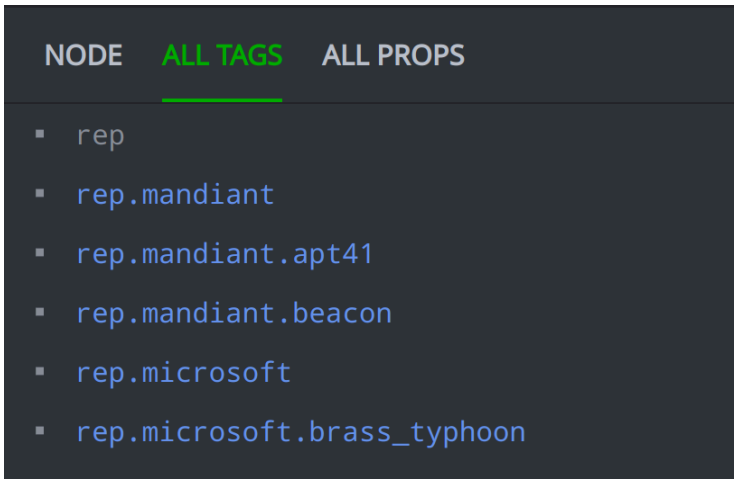


You notice that many of the IPv4s are associated with AS **25820.** You want to limit your results to **only** show IPv4s on that AS.

Question 3: How can you **add a filter** to the above query to **only** show IPv4s on AS 25820?

Hint: Your original query contains a Storm command (`| uniq`). After running a Storm command, you need to use the **pipe character** (`|`) to tell Synapse you are switching from command mode **back** to query mode to add another query operation (in this case, a filter).

Looking at the **All Tags** tab, there are several tags associated with the IPv4s. You want to further limit your results to **only** the IP addresses reported by Microsoft.



Question 4: How can you add a filter to your query to view **only** those IPs reported by Microsoft (**`rep.microsoft`**)?

Based on the **All Tags** tab in the Details Panel, some of the IPv4s were **also** reported by Mandiant. You're interested in the **overlap** between Microsoft's reporting and Mandiant's reporting.

Question 5: How can you add a filter to your query to view **only** those IPs reported by Microsoft (**`rep.microsoft`**) **and** Mandiant (**`rep.mandiant`**)? How many IPs were reported by both organizations?

Filters with Mathematical Operators

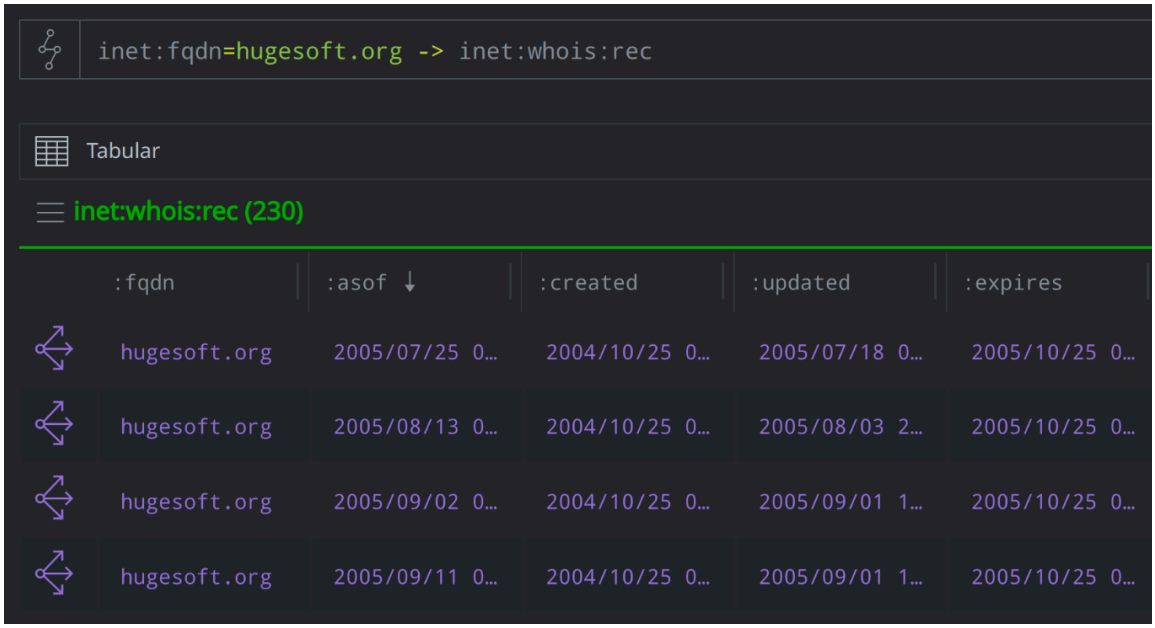
Exercise 2

Objective:
- **Use mathematical operators to perform filter operations with Storm.**

You are examining historical domain Whois records for APT1 FQDN **`hugesoft.org`**.

- Enter the following in the **Storm Query Bar** and press **Enter** to run the query to show the Whois records for this FQDN:

```
inet:fqdn=hugesoft.org -> inet:whois:rec
```



Hint: If you sort by the `:asof` column (the date the individual Whois record was captured), you can view the records in timeline order.

The domain was used by APT1, but was later sinkholed by Kleissner & Associates on January 11, 2014, based on the registration (`:created`) date for Kleissner's records.

You want to view the Whois records from **before** the date the domain was sinkholed.

Question 1: How can you **add a filter** to your query to **only** display WhoIs records created **before** January 11, 2014 (the date Kleissner & Associates registered / sinkholed the domain)?

Hint: Synapse stores dates as **integers** (specifically, as epoch milliseconds / millis). You can use operators such as "less than" or "greater than or equal to" to filter date/time properties.

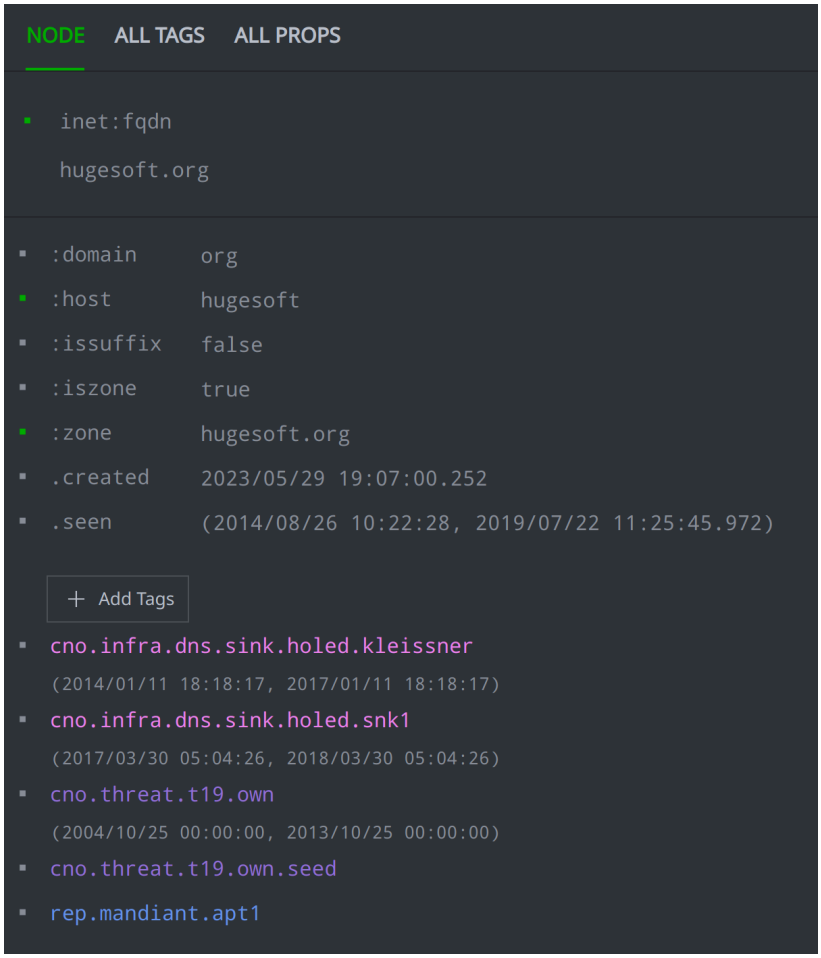
Filters with Extended Operators

Exercise 3

Objective:

- **Use extended operators to perform filter operations in Storm.**

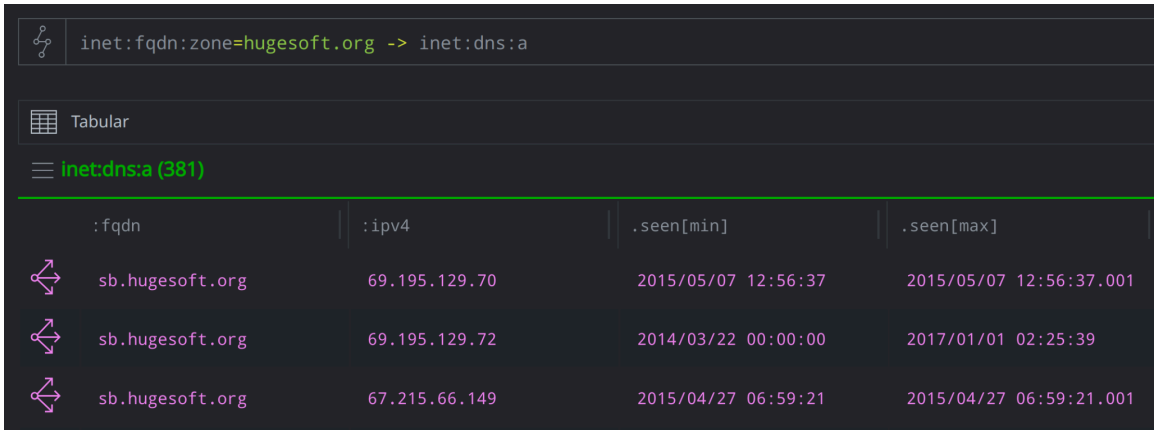
You are still researching the **hugesoft.org** FQDN. This APT1 domain is part of an internally tracked threat cluster **T19.** Based on tags on the FQDN, Vertex believes T19 controlled this FQDN between **October 2004** and **October 2013:**



You want to see DNS A records for **hugesoft.org** and its subdomains.

- Enter the following in the **Storm Query Bar** and press **Enter** to run the query to show the DNS A records:

```
inet:fqdn:zone=hugesoft.org -> inet:dns:a
```



You want to limit your results to **only** DNS A resolutions observed during the time T19 controlled the domain (between **2004/10/25** and **2013/10/25**).

Question 1: How can you **add a filter** to the query above to **only** display DNS A records whose observation window (**.seen** times) overlap with those dates?

Question 2: How many DNS A records are in your results after adding the filter operation?
