# Synapse Bootcamp

Module 4
Modifying and Adding Data

v0.4 - May 2024

# Objectives

- Know the various ways to edit properties in the UI
- Add and remove tags using the UI
- Understand basic tag use cases
- Add data using the Storm Query Bar
- Add data with the Add Node dialog
- Know other ways to add data to Synapse
- Know the use cases for the Synapse Ingest Tool

# Modifying Data in Synapse

# Modifying Data

- Make **changes** to existing data
- Change **properties**
  - Set, modify, delete
  - Ideally Synapse is creating data (and setting properties) **for** you
- Change **tags**
  - Add / apply, remove
  - Partial or full tags
- Most changes / simple edits done in **Research Tool**

# Modifying Data Demo

# Deletes and Forked Views

- "Best practice" is to work in a **forked view**
  - Work in your private, writable layer
  - Merge changes into underlying view / layer when finished
- Deletes must occur in the layer where the data exists
  - In a fork, you cannot remove properties or tags that exist in "production"
  - "Deletes" do not get merged when you merge a view

If you are working in a fork and delete a property (or remove a tag) and it doesn't "go away" - it probably exists in an underlying layer.

# Deleting Nodes

- No means to delete nodes via the UI
- Synapse's data store represents objects and their **connections**
    - Technically, Synapse is an instance of an interconnected hypergraph
- Deleting the wrong data can leave "holes" in the graph
- Synapse incorporates safeguards
    - No simple UI / menu options to delete nodes
    - Working in a forked view
    - Permissions
    - Sanity-checking where possible
    - Requires use of **`delnode`** command

We recommend **limiting** the number of people who can delete data from your production view(s).

# Adding / Removing Tags

# Tag Refresher

– Tags provide **context** for nodes
– Often represent observations or assessments
– Strongly encourage recording "who says what"
– Difference between:
  ○ What **you** assess (based on direct observation)
  ○ What **other people** assess (trust / take their word)
– Benefits:
  ○ Compare / contrast reporting
  ○ Evaluate sources (more / less trusted or reliable)

# Common Tags - Other Organizations

- Uses **rep** top-level tag by default
- Format **rep.**`<reporting_org>.<thing_reported>`
- In rare cases, use **3p** tag element
  - A source reporting info from another source

| Type of Tag | Example |
|---|---|
| Things other people report (#rep)<br>• Applied by Power-Ups (e.g., VirusTotal)<br>• Applied by analysts<br>• `rep.<org>.<thing_reported>` | `#rep.kaspersky.mal`<br>`#rep.trend.pawnstorm`<br>`#rep.clearsky.wilted_tulip`<br>`#rep.shodan.self_signed`<br>`#rep.vt.peexe` |
| Things other people report **about other people**<br>• Applied by Power-Ups (e.g., MalwareBazaar, Mandiant)<br>• `rep.<org>.3p.<org>.<thing_reported>` | `#rep.malwarebazaar.3p.cape.smokeloader`<br>`#rep.orkl.3p.malpedia` |

# Common Tags - Our Assessments

– We use **cno** as the top-level tag
– Consider what you want track / how to structure

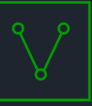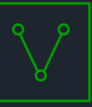| Type of Tag | Example |
|---|---|
| Things we assess are malicious | `#cno.mal` |
| Malware we track | `#cno.mal.redtree` |
| Threats we track | `#cno.threat.t15` |
| Things that are "neutral" but useful to know | `#cno.infra.anon.tor.exit`<br>`#cno.infra.anon.vpn`<br>`#cno.infra.dns.sink.hole` |
| Things that are "not bad" / can be ignored | `#cno.common` |
| Tags for my personal use<br>   • `<my_name>.<tag>` | `#thesilence.review`<br>`#thesilence.merge` |

# Adding / Removing Tags Demo

# Adding Data to Synapse

# Adding Data

| Method | Location in UI | Purpose |
|--------|---------------|---------|
| **Lookup mode** | Storm Query Bar mode | Paste in common indicators |
| **Add Node** dialog | Storm Query Bar menu | Guided way to create individual nodes |
| **Upload file** | Storm Query Bar menu | **Download** single file from URL<br>**Upload** file(s) from disk<br>Optionally use with File Parser |
| **Import nodes file** | Storm Query Bar menu | Load a subset of data (nodes, edges, tags) exported from another instance of Synapse |
| **Workflows** | Workflows Tool | Custom way to work with specific data |

# Adding Data Demo

# More on Adding Data

# Data at Scale

- Analysts should be doing analysis
  - ...not hand-creating nodes
- Where possible, let Synapse do the work!
- How do I get data into Synapse?
  - Power-Ups
  - Automation
  - Spotlight Tool
  - Ingest Tool
- Data may be:
  - Pre-loaded (when you deploy Synapse)
  - Added via feeds
  - Added on demand

# Data Demo

# Summary

- **Edit** most properties inline
  - Widgets / helpers for some data types
- **Delete** properties by removing value or using delete (Details Panel)
- **Add Tags** with the Add Tags dialog
- **Remove tags** via Details Panel
- Multiple methods to **Add Data** to Synapse
  - **Power-Ups** are designed to automated data ingest
  - Users can leverage the **Query Bar** or the **Add Node** dialog
- Additional methods for particular needs
  - Upload file
  - Ingest Tool
  - Other