Vertex

Synapse Bootcamp

Module 2
Getting Started

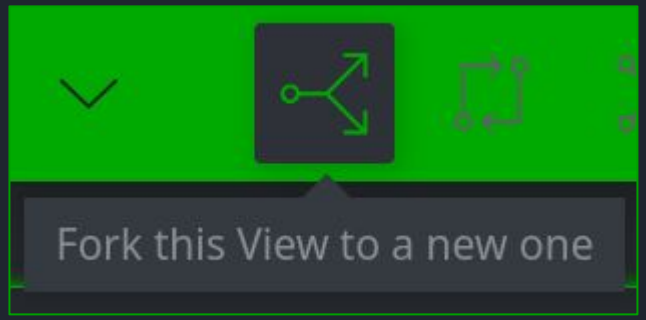
v0.4 - May 2024

Objectives

- Know how (and why) to fork a view
- Learn how to lift (select) and view data in Synapse
- Understand how to view and interpret tags for context
- Know how to lift (select) nodes based on tags

Fork a View

Fork a View



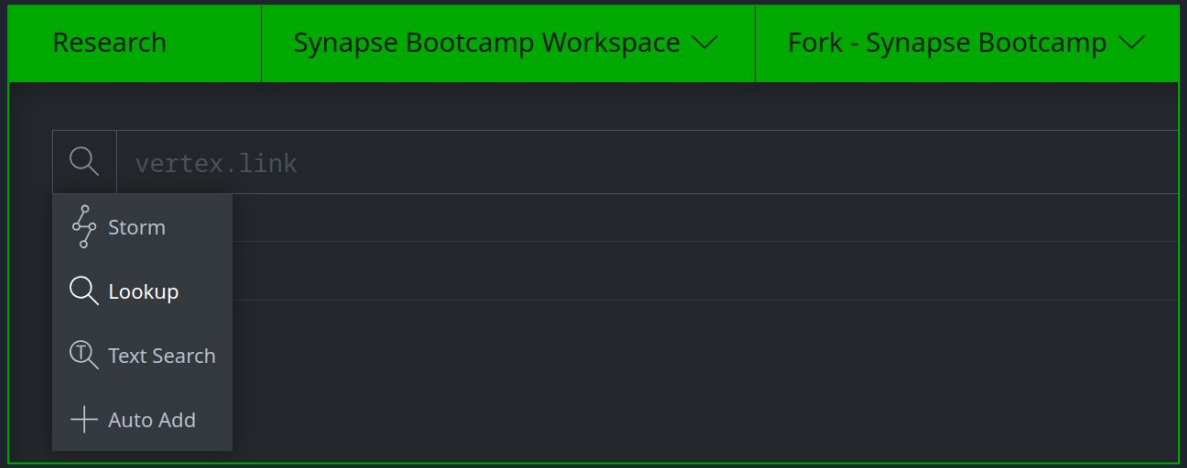
- **First** thing you should **always** do in Synapse!
- Provides a "scratch space" for your work
  - Separate from production data & analysis
  - Preliminary research
  - Initial enrichment
  - Test queries or automation
- Advantages:
  - You can make mistakes and not break things!
  - You are **admin** in your fork!
- Can later **merge** (or discard!) the fork and its data

Fork a View - Demo

Viewing Data in Synapse

Viewing Data in Synapse

- No feature in Synapse to "show me all the data"
- Need to start by telling Synapse what you want to see
- Select or **lift** objects (nodes) from Synapse's data store
- Storm Query Bar
  - **Lookup** mode
  - **Text search** mode



Lift Demo

Context in Synapse

Tags as Context

- Tags give context to nodes
  - "What do we know about this FQDN? This IP address?"
- Tags are a shorthand to:
  - Record observations, assessments, or other important **context**
  - Store that context **directly** on the data itself
- Simply viewing the tags on a node can provide a great deal of information
- Synapse's data store gets richer over time
  - Collected observations / annotations across your team or organization!

Lift by Tag

- Another common way to **lift** (select) data
- Objects that have the same **context**
  - Associated with a threat:
    - `cno.threat.t13`
  - Leverage a vulnerability:
    - `rep.vt.cve_2012_0158`
  - Represent similar infrastructure:
    - `cno.infra.anon.tor`

Tags Demo

Summary

- Analysts should **fork a view** when starting their work
  - "Working space" separate from production data
  - Data from the fork can be **merged** or **deleted**
- **Lift** nodes in Synapse using the **Storm Query Bar**
  - **Lookup** mode
  - **Text Search** mode
- **Tags** on nodes provide context for data
- **Lift by tag** to see nodes with similar context