



Vertex

Synapse Bootcamp

Module 1

Introduction and Overview

v0.4 - May 2024



Administrivia

- Your instructors
- Course overview
- Format
 - Hear it - important concepts and background information
 - See it - instructor demonstrations
 - Do it - hands-on exercises
- Logistics
 - Audio / video, questions, etc.
 - Pre-flight checklist



Your Demo Instance

- Includes multiple data sets ("views")
- Additional activities / challenges
 - APT1 Scavenger Hunt
 - KC7 Cybersecurity Game
- For class, your Top Bar should look like this:



Don't worry, we will set this up during the Exercises!



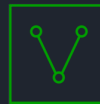
Objectives

- Describe Synapse and its key components
- Provide an overview of essential Synapse UI elements
- Introduce the most commonly used Synapse Tools

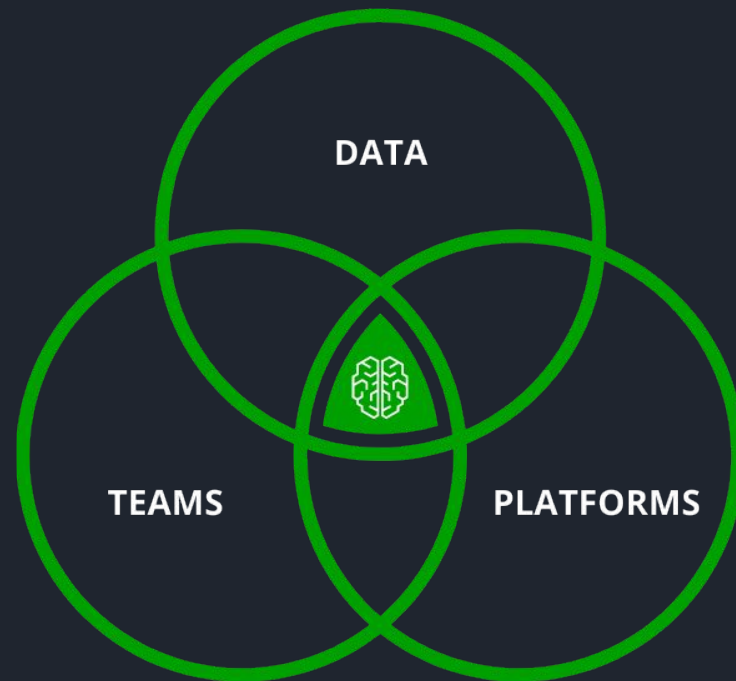


What is Synapse?

Synapse



- A versatile **central intelligence system** created to support analyst teams in every stage of the intelligence life cycle
- Fuses interdisciplinary data, platforms, and teams into a single system to facilitate collaborative analysis





Synapse Terms

Term	Meaning
Synapse	The application and all components - all the things!
Storm	The "data language" used to interact with Synapse
Power-Ups	Provide add-on capabilities to Synapse
Optic	Synapse's UI
Cortex	Synapse's data store / knowledge graph
Axon	Synapse's file storage

We like to be consistent and just use "Synapse" but knowing these additional terms is helpful!



Data Model

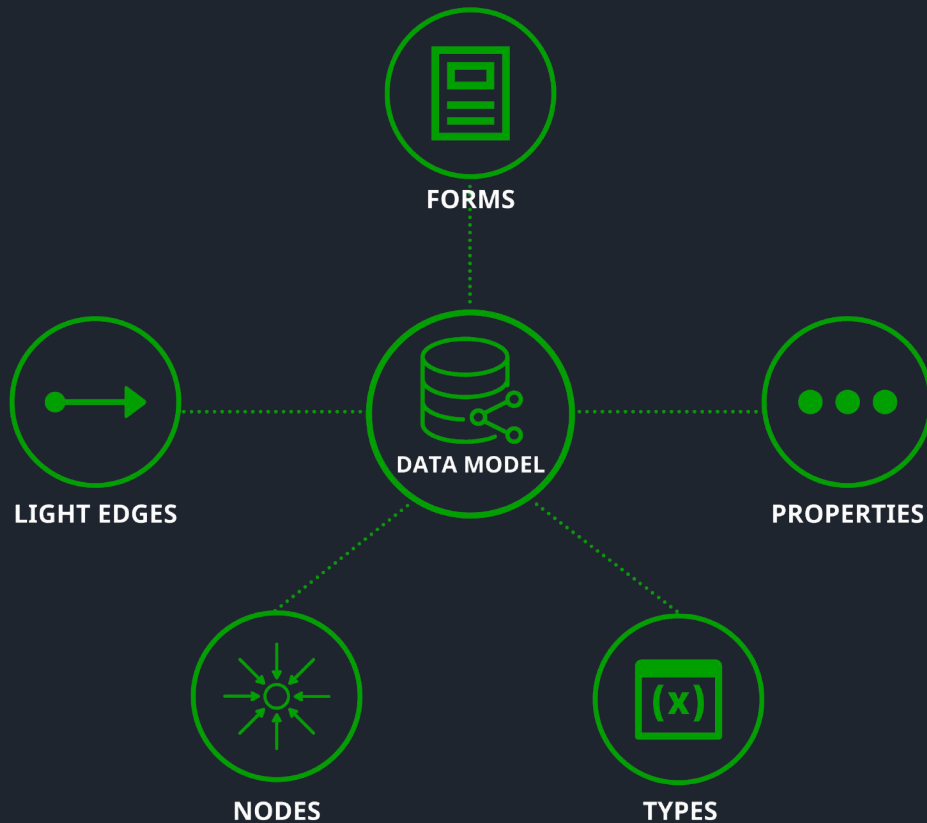
- Structural representation of all analytically relevant data
 - A file wrote another file to disk during execution
 - An FQDN resolved to an IP within a particular time frame
 - An account posted a message to a forum on a particular date
- Automatically capture relationships among data
- Accurately represent "the real world"



Use Synapse's **Data Model Explorer** to examine the data model.



Data Model Elements





Analytical Model

- Allows you to **capture assessments** about data
- Assessments are recorded on nodes using labels called **tags**
 - An FQDN was sinkholed on a particular date
 - An indicator is associated with a specific malware family or threat group
 - A file is a legitimate / trusted binary





Tags

- A specialized node used to **annotate** and **group** objects (nodes)
- Hierarchical to organize / structure your observations
 - `cno.threat.t13.own`
- Optional timestamps
 - Interval when the tag was true or relevant
 - `cno.threat.t13.own=(2017/04/10, 2019/04/10)`

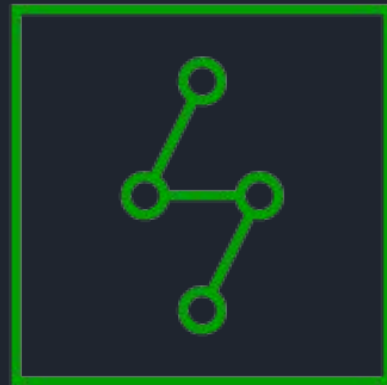


Use Synapse's **Tag Explorer** to examine the tags in your instance of Synapse.



Storm

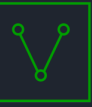
- Synapse's **query language**
- An intuitive "data language"
 - Use Storm the same way you think about data and relationships in the "real world"
- Allows you to ask (and answer) **any** analytical question
- Start simple and build on the basics as needed





Interacting with Data

Operation	Meaning
Lift	Select data (nodes) from Synapse
Pivot	Move from one set of nodes to another set that share the same property
Traverse	Move from one set of nodes to another set that are linked by an edge
Filter	Include / exclude a subset of nodes
Modify / Edit	Add, modify, or delete nodes or properties Add or remove tags
Run	Execute a Storm command



The Synapse UI - Demo



Summary

- **Synapse** is a central analysis and intelligence platform
- Synapse's key components are its **data model**, **analytical model**, and **query language** (Storm)
- Synapse **Power-Ups** add functionality to Synapse
- The Synapse web-based UI includes multiple tools to support analysis tasks, including **Workspaces**, **Console**, **Power-Ups** and **Help**
- **Research** is the main analysis tool, and includes multiple **display modes** for visualizing data