

Synapse Bootcamp

Objective

Provide new users with a basic understanding of Synapse's key design features and enable them to use Synapse, the Synapse UI, the Storm query language, and Synapse tools and Power-Ups with confidence.

Skill Level

Beginner

Description

Synapse Bootcamp provides a hands-on introduction to Synapse. The course combines background material on Synapse's architecture, data model, and analytical model with practical in-class exercises.

Students will learn the features and components of Synapse, how to navigate and work with data using the Synapse UI (Optic), and the fundamentals of the Storm query language. They will examine key parts of the data model used for cyber threat intelligence (CTI) and threat tracking / threat hunting, and gain practice with important tools such as Spotlight and Stories.

Upon successful completion of this course, students will be able to:

- Navigate and work with the Synapse UI.
- Customize their Synapse user environment.
- Use the most relevant analyst-focused tools, such as Research and Workspaces.
- Describe the components of the Synapse data and analytical models.
- Use Data Model Explorer and Tag Explorer to examine model elements.
- Locate and use help features, including Power-Up help, Storm command help, and Synapse / Storm reference documents.
- Create, modify, enrich, explore, and analyze data in Synapse.
- Use tags to annotate data and capture analytical assessments and assertions.
- Leverage Synapse Power-Ups to support analysis tasks.
- Write and execute common queries using the Storm query language.

- Use Synapse's Spotlight Tool to load, view, and process reports.
- Understand the types of automation available in Synapse, and how each can be used to streamline repetitive tasks and analytical workflows.
- Understand how Synapse's threat intelligence data model represents objects such as threat groups, malware families, attacks, and campaigns.
- Use the Vertex Threat Intel Workflow to view and work with threat intel objects.
- Fork, review, and merge (or discard) a View, and vote on merging data using Quorum.
- Create reports using the Synapse Stories Tool.

Delivery Format

- Instructor-led via Google Meet.
- Live instruction, demonstration, and hands-on exercises performed in class.

Duration

Approximately 32 hours total class time (including instructor time, labs/exercises, and breaks), equivalent to four full days of training.

The course material is modular and can be presented on a flexible schedule to meet attendee needs. (We recommend scheduling half-day (four-hour) sessions held over eight days for the best balance of pacing and student retention.)

Resources and Materials

Attendees will receive:

- A Vertex-hosted demo instance of Synapse valid for 30 days (a link to your personal demo instance will be emailed to you before the start of class).
- A digital copy of the course material (presentation materials/slides).
- A digital copy of the exercises (lab materials).
- Various Synapse quick reference / jump start materials summarizing common operations and queries in the Storm query language.

The Vertex Project will also provide copies of or links to additional supplemental materials such as blogs, documentation, or video recordings. These supplemental materials are not

mandatory but may be helpful to gain an increased understanding of Synapse, Synapse features, and the Storm query language.

Additional Training Materials

The Synapse demo instances include additional data sets that can be used for self-guided or group training exercises:

- **The APT1 Scavenger Hunt.** Use the Scavenger Hunt documentation (included with the course materials) to answer questions and solve challenges using the Synapse UI and / or Storm query language.
- The **KC7 EngolveLabs** training scenario. Create an account with [KC7](#) to solve their EngolveLabs scenario using Synapse.
- The **Default** data set. While not associated with specific training materials, the **default** view contains a baseline of pre-loaded (and continually updated) data that students can use to further explore Synapse and its use cases.

Prerequisites

- Some Synapse Power-Ups require vendor API keys. **For the best experience, attendees will need to register for and obtain free API keys for a handful of vendors prior to the start of class. The process should take approximately 30 - 60 minutes.**

API keys will be installed and configured in class during hands-on exercises. Upon confirmed registration, The Vertex Project will provide a list of vendors / websites and detailed API key registration instructions.

Technical Requirements

- A stable Internet connection
- A desktop or laptop computer
- Chrome web browser (up-to-date version)
- Audio / video capabilities (microphone, speakers / headset, and optional camera) to allow interaction with instructors and fellow students
- Free API keys for specified Power-Ups (list of vendors to be provided)

Attendance and Punctuality

For live online courses, attendance is equated to the demonstration of an active and regular presence in the virtual course environment.

Accommodations

For questions about accessibility or to request a special accommodation, please contact us at support@vertex.link.

Course Modules

The following Modules are included in Synapse Bootcamp as of May 2024.

Module	Summary
Module 1: Introduction and Overview	The first six modules introduce Synapse's Optic UI and focus on using the UI to perform common analysis tasks. Module 6 is a freeform exercise that allows students to apply what they've learned so far.
Module 2: Getting Started	
Module 3: Exploring and Filtering Data	
Module 4: Modifying and Adding Data	
Module 5: Power-Ups	
Module 6: Putting it All Together	
Module 7: Pre-Storm Background	The next six modules provide additional detail on Synapse's data model as important background for the Storm query language. We then introduce Storm's basic operations so students learn to compose Storm queries.
Module 8: Intro to Storm	
Module 9: Pivoting and Traversal in Storm	
Module 10: Filtering in Storm	
Module 11: Building Queries in Storm	
Module 12: Modifying Data in Storm	

Module	Summary
Module 13: More Fun with Power-Ups	The next five modules provide more information on some key Synapse skills, building on what students have learned to date.
Module 14: Modeling Data Manually	
Module 15: Static Malware Analysis	
Module 16: Dynamic Malware Analysis	We also focus on specific portions of the data model that are relevant to certain types of data and analysis. This allows students to recognize and work with particular types of data. We also discuss using Power-Ups and navigation to enrich and examine this data.
Module 17: Network Infrastructure Analysis	
Module 18: Reports, Articles, and the Spotlight Tool	<p>The final six modules provide an overview of important tools in Synapse (Spotlight and Stories) along with intermediate topics such as:</p> <ul style="list-style-type: none"> • Synapse's Threat Intelligence data model and associated Workflow. • How automation in Synapse can be used to streamline analysis, ensure consistency, and offload tedious tasks. • How Synapse's views and layers architecture provides both security and flexibility, and how Quorum supports collaborative review of analysis. <p>By the end of the course, students will have a solid foundation for working with Synapse and understand how Synapse's components work together to create a powerful intelligence system.</p>
Module 19: Introduction to Threat Intelligence in Synapse	
Module 20: Automation in Synapse	
Module 21: More Fun with Spotlight	
Module 22: Views, Layers, and Quorum	
Module 23: Reporting with the Stories Tool	