Advanced Phantom Implementation

This three virtual-day course is intended for experienced Phantom consultants who will be responsible for complex Phantom solution development, and will prepare the attendee to integrate Phantom with Splunk as well as develop playbooks requiring custom coding and REST API usage.

Potential attendees should carefully consider the pre-requisites and should ensure they can devote all of their attention to the class, as the course work is very challenging. Students will develop a custom solution with Phantom, Splunk and custom Python code. The labs provide requirements for the solution; the student must plan and execute the development. This will require thoughtful focus, experimentation and problem-solving skills.

Course Topics

- Using external Splunk search in Phantom
- Sending events from Splunk to Phantom
- Updating Splunk events from Phantom
- Running Phantom reports on Splunk
- Executing Phantom playbooks from Splunk
- Searching Splunk from Phantom playbooks
- Writing custom code in Phantom Playbooks
- Using the Phantom REST API in Phantom Playbooks

Course Prerequisites

Attendees for this class must ensure that they meet all course pre-requisites. This is a challenging, advanced class that draws on technical knowledge from many areas in Splunk and Phantom, and the demanding labs and course schedule leave little time to learn the basics.

- Experience with Python programming
- Administering Splunk Phantom
- Developing Splunk Phantom Playbooks
- Splunk Enterprise Data Administration
- Splunk Enterprise System Administration
- Either Using or Administering Splunk Enterprise Security

Class Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

Module 1 – Implementing Splunk and Phantom

- Review of Phantom UI and concepts
- Describe interactions between Splunk and Phantom
- Identify key concepts and data flows
- Pre-requisites for integration

Module 2 – Configuring External Splunk Search

- Describe the benefits of externalizing search to Splunk
- Configure the Phantom instance for externalization
- Configure the Splunk instance for externalization
- Use the Splunk app for Phantom Reporting

Module 3 – Sending Splunk Events to Phantom

- Configure the Phantom Add-on for Splunk
- Map CIM fields to CEF
- Send Enterprise Security notables to Phantom
- Automatically trigger Phantom playbooks for Splunk notables

Module 4 – Accessing Splunk from Phantom

- Install and configure the Phantom App for Splunk
- Ingest Splunk events into Phantom
- Use Splunk search from playbooks
- Update Splunk notable events

Module 5 – Custom Coding in Playbooks

- Phantom coding best practices
- Use custom function blocks
- Using the Phantom API in custom code
- Store and retrieve persistent data

Module 6 – Using Phantom REST

- Use Django queries to search for data in Phantom
- Use REST from other systems to access Phantom data
- Use the HTTP app to execute REST from playbooks

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education

To contact us, email education@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
250 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com