splunk>

Administering Phantom

This 9 hour course prepares IT and security practitioners to install, configure and use a Phantom server in their environment and will prepare developers to attend the playbook development course.

Course Topics

- Phantom topics and concepts
- Installation
- Initial configuration
- Apps and assets
- User management
- Ingesting data
- Events and containers
- Mission control
- Running actions and playbooks
- Case management
- Case workflows
- Multi tenancy
- Clustering

Course Prerequisites

None

Class Format

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

Course Objectives

Module 1 – Introduction & Concepts

- Describe Phantom operating concepts
- Identify documentation and community resources
- Identify installation options
- Perform initial configuration
- Configure multi tenancy to enable use of Phantom by multiple teams

Module 2 –Installation

- Deployment planning
- Pre-installation steps
- Identify installation options
- Upgrading Phantom

Module 3 – Initial Configuration

- Product settings
- Access control
- Authentication settings
- Response settings

Module 4 – Apps and Assets

- Describe how apps and assets work in Phantom
- Add and configure new apps
- Configure assets

Module 5 – Data Ingestion

- Assets as data sources
- Configuring data polling
- Labels and tags
- Data ingestion management
- Event settings

Module 6 – Analyst Queue

- Work with the analyst queue
- Filtering and sorting
- Using search
- Container export and import
- Aggregation settings

Module 7 – Mission Control

- Use Mission Control to work on events
- Use indicators to find matching artifacts in multiple events
- Using the heads-up display
- Using notes

Module 8 – Actions, Playbooks and Files

- Manually run actions and examine action results
- Manually run playbooks
- Use the vault to store related files

Module 9 – Case Management and Workbooks

- Use case management for complex investigations
- Use case workflows
- Define new workbooks
- Customize case management

Module 10 –Reporting and System Health

- Run reports
- Use Phantom audit tools
- Monitor system health

Module 11 – Customization

- Create custom severity levels
- Create custom status levels
- Add custom fields and CEF settings
- Create custom workbooks

Module 12 – Multi tenancy and Clustering

- Define clustering best practices
- Configure multi-server Phantom clusters
- Configure multi-tenancy

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

splunk>

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