

**SPLK-AP4.10: Administering Phantom 4.10**

Course Code: SPLK-AP4.10

Duration: 2 days

Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

**OVERVIEW**

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

**SKILLS COVERED**

- Please refer to course overview.

**WHO SHOULD ATTEND?**

Everyone can attend.

**PREREQUISITES**

There is no prerequisites required to attend this course.

**MODULES****Module 1: Introduction, Deployment and Installation**

- Describe Phantom operating concepts
- Identify documentation and community resources
- Identify installation and upgrade options
- Phantom & Splunk Architecture
- Splunk/Phantom relationships

**Module 2: Initial Configuration**

- Product settings

- Access control
- Authentication settings
- Response settings
- Understanding roles
- Creating users
- Managing user access

**Module 3: Apps, Assets and Playbooks**

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

**Module 4: Ingesting Data**

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

**Module 5: Analyst Queue**

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

**Module 6: Investigation**

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

**Module 7: Actions, Playbooks and Files**

- Manually run actions and examine action results

- Manually run playbooks
- Use the vault to store related files

### **Module 8: Case Management and Workbooks**

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

### **Module 9: Customization**

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

### **Module 10: Advance Topics**

- Run reports
- Use Phantom audit tools
- Monitor system health
- Define clustering best practices
- Configure multi-server Phantom clusters
- Configure multi-tenancy
- Backup/restore

**END OF PAGE**