Course Code: HYSPL01G

Course Title: Splunk Services Implementation

Description:

This expert-level course is an immersive five-day assessment-based bootcamp used to give attendees the opportunity to cement their knowledge in working with the Splunk core platform effectively and at-scale using Professional Services (PS) best-practice techniques

Objectives:

This training will cover how to make Splunk Enterprise run efficiently in large, clustered environments and will give a more in-depth understanding of the inner workings of Splunk.

Prerequisites:

Attendees must be comfortable and competent in core Linux skills such as:

- File & permission management
- Service configuration
- Installation best-practices
- ssh & scp

Duration:

40 Hrs

Topics:

Module 1 – Deploying Splunk

- Introduce the Splunk Validated Architectures

Module 2 — Monitoring Console

- Discuss the best instance to configure as the Monitoring Console
- Configure the MC for a single or distributed environment
- Examine how the MC uses the server roles and groups assigned to instances
- Discuss health checks and how they are run

Module 4 — Access and Roles

- Discuss how to manage Deployment Server at scale
- Identify authentication methods
- Describe LDAP concepts and configuration
- Discuss SAML and SSO options
- Define roles and how they are used to protect data

Module 5 — Data Collection

- Examine Splunk to Splunk (S2S) communication and the different ways data is sent from forwarder to indexer
- Describe the types and configuration of data inputs
- Discuss ways to troubleshoot data inputs

Module 6 — Indexing

- Review indexing artifacts and locations
- Discuss event processing and data pipelines
- Understand the underlying text parsing and indexing process
- Examine data retention controls

Module 7 — Search

- Examine the inner workings of a search
- Discuss how to use search job inspection
- Look at the different search types and how to maximize search efficiency
- Review sub searches and how they work
- Examine some sample searches and how to make them more efficient

Module 8 — Index Clustering

- Provide an architecture overview
- Describe deployment and component configuration
- Review upgrade strategy
- Discuss Data buckets and lifecycle
- Examine failure modes and recovery processes
- Introduce multi-site clustering
- Explain migration procedures

Audience:

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

Certification:

None