



# Implementing Splunk IT Service Intelligence 4.15

This 18-hour course is designed for administrator users who will implement Splunk IT Service Intelligence for analysts to use. The first day includes the day of content from Using Splunk IT Service Intelligence.

## Course Topics

- IT Service Intelligence analyst user training
- Designing, Implementing Services and Searches
- Defining and Adding Entities
- Defining Service Templates, and User Access
- Using Predictive Analytics
- Creating and Defining Correlation Searches and Event Aggregation

## Prerequisite Knowledge

To be successful, students should have a working understanding of the following courses:

### *Either these completed Certification Paths*

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

### *Or These Courses*

- What is Splunk?
- Intro to Splunk
- Using Fields
- Visualizations
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extraction

## Course Format

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

## Course Objectives

### Using ITSI Modules 1-5

- 1 – Monitoring Services with Service Analyzers
- 2 – Monitoring Entities with Infrastructure Overview
- 3 – Visualizing Services with Glass Tables
- 4 – Investigating Issues with Deep Dives
- 5 – Managing Alerts and Episodes

### Module 1 – Designing Services

- Plan ITSI services
- Design service KPI properties
- Identify entity-oriented KPIs
- Identify dependencies between services

### Module 2 – Data Audit and Base Searches

- Analyze a data environment
- Identify necessary data sources for KPIs
- Plan data intake for IT Service Intelligence configuration
- Implement base searches to support service design

### Module 3 – Access Control

- Identify ITSI roles and capabilities
- Describe service level roles and team ownership
- Control access to ITSI views

### Module 4 – Implementing Services

- Use a service design to implement services in ITSI
- Create KPIs using base searches
- Configure basic KPI settings for calculation and aggregation
- Configure KPI lag and backfill
- Set KPI importance
- Calculate service health score

### Module 5 – Entities

- Define entities and entity types
- Creating and importing entities
- Creating a service using pre-built KPIs
- Associate entities with an existing service
- Delete or retire entities
- Define and use pseudo entities
- Monitoring entities

### Module 6 – Templates and Dependencies

- Define service template use cases
- Create service templates
- Create new services from templates
- Create dependencies between services



#### Module 7 – Thresholds and Time Policies

- Configure KPI thresholds
- Use aggregate and entity-level thresholds
- Use static and adaptive thresholds
- Apply time policies to thresholds
- Create custom threshold templates

#### Module 8 – Anomaly Detection and Predictive Analytics

- Define anomaly detection
- Define predictive analytics
- Configure anomaly detection for KPIs
- Configure predictive analytics for services

#### Module 9 – Correlation Searches and Multi-KPI Alerts

- Define new correlation searches
- Define Multi-KPI alerts
- Manage notable event storage

#### Module 10 – Aggregation Policies

- Define aggregation policy capabilities
- Modify the default aggregation policy
- Understand Smart Mode
- Create new aggregation policies
- Use aggregation policies to automate notable event response

## 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 Splunk Education's course offerings, or to register for a course, go to <http://www.splunk.com/education>

To contact us, email [Education\\_AMER@splunk.com](mailto:Education_AMER@splunk.com)

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

[Contact sales](#)