Splunk for Analytics & Data Science

This 13.5-hour course is for users who want to attain operational intelligence level 4, (business insights) and covers implementing analytics and data science projects using Splunk's statistics, machine learning, built-in and custom visualization capabilities.

Course Topics

- Analytics Framework
- Exploratory Data Analysis
- Regression for Prediction
- Cleaning and Preprocessing Data
- Algorithms, Preprocessing and Feature Extraction
- Clustering Data
- Detecting Anomalies
- Forecasting
- Classification

Prerequisite Knowledge

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

- Fundamentals 1, 2, & 3
- Advanced Searching & Reporting

Or the following single-subject courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Working with Time
- Statistical Processing
- Comparing Values
- Result Modification
- Leveraging Lookups and Sub-searches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth
- Search Optimization

Course Format

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

Course Objectives

Topic 1 – Analytics Workflow

- Define terms related to analytics and data science
- Describe the analytics workflow
- Describe common usage scenarios
- Navigate Splunk Machine Learning Toolkit

Topic 2 – Exploratory Data Analysis

- Describe the purpose of data exploration
- Identify SPL commands for data exploration
- Split data for testing and training using the sample command

Topic 3 – Predict Numeric Fields with Regression

- Differentiate predictions from estimates
- Identify prediction algorithms and assumptions
- Describe the fit and apply commands
- Model numeric predictions in the MLTK and Splunk Enterprise
- Use the score command to evaluate models

Topic 4– Clean and Preprocess the Data

- Define preprocessing and describe its purpose
- Describe algorithms that preprocess data for use in models
- Use FieldSelector to choose relevant fields
- Use PCA and ICA to reduce dimensionality
- Normalize data with StandardScaler and RobustScaler
- Preprocess text using Imputer, and NPR, TF-IDF, HashingVectorizer and the cluster command

Topic 5– Cluster Data

- Define Clustering
- Identify clustering methods, algorithms, and use cases
- Use Smart Clustering Assistant to cluster data
- Evaluate clusters using silhouette score
- Validate cluster coherence
- Describe clustering best practices

Topic 6 – Anomaly Detection

- Define anomaly detection and outliers
- Identify anomaly detection use cases
- Use Splunk Machine Learning Toolkit Smart Outlier Assistant
- Detect anomalies using the Density Function algorithm
- Optimize anomaly detection with the Local Outlier Factor
- View results with the Distribution Plot visualization

Topic 7 – Estimation and Prediction

- Differentiate predictions from forecasts
- Use the Smart Forecasting Assistant
- Use the StateSpaceForecast algorithm
- Forecast multivariate data
- Account for periodicity in each time series

Topic 8 – Classification

- Define key classification terms
- Define key classification terms
- Use classification algorithms:
- AutoPrediction,
- LogisticRegression,
- SVM (Support Vector Machines)
- RandomForestClassifier
- Evaluate classifier tradeoffs
- Evaluate results of multiple algorithms

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

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales