SPLUNK BOOT CAMP

Course Code: 100323

Learn how to use Splunk for monitoring, searching, analyzing, and visualizing your machine generated data in real time.

Splunk is one of the first platforms to help make sense of log data. Splunk is not just a tool for IT Ops, it's a tool for developers. In fact, it's a tool for everyone who's interested in using the power of data. There are a lot of use cases for Splunk, but first, you'll to learn what it's capable of and how to get the most of it.

If you have concerns about security and compliance, don't worry. You can still be compliant while making life easier with Splunk. You'll just need to give everyone visibility on what's happening with your applications in real-time or for analysis purposes. And yes, you can do all of this without giving people access to the servers.

This two-day boot camp is designed to empower you with the knowledge and skills needed to take full advantage of Splunk. This exercise-intensive course is for individuals looking to develop a deeper understanding of the tool. Our hands-on lab classroom format and real-world practice scenarios will cement your new skills with Splunk's various applications and leave you prepared to properly collect, analyze, and utilize your machine data.

What You'll Learn

Join an engaging hands-on learning environment, where you'll learn:

- Splunk essentials
- Indexing in Splunk
- Splunk architecture and components
- Query and search your data
- How to create dashboards and visualizations
- How to apply alerts

This is a hands-on course with engaging instruction, demos, group discussions, labs, and project work.

Who Needs to Attend

Developers, Data Engineers, Architects, and Administrators

Prerequisites

Before attending this course, you should have:

- Basic Linux administration and familiarity with using the command line.
- Basic networking concepts understanding

SPLUNK BOOT CAMP

Course Code: 100323

CLASSROOM LIVE	$2,595 CAD	2 Day

Classroom Live Outline

Introduction to Splunk

- What's Splunk?
- Authentication Methods
- Access Controls and Users
- Products, Licensing, and Costs
- Quick Tour Guide: User Interface

Indexes

- Splunk Data
- What are Indexes?
- What are Indexers?
- Search-Head
- Index Clusters
- Index Pipeline
- Events
- Fields and Field Extraction
- Forwarders
- Metrics
- Removing Data

Splunk Architecture

- Components of Splunk Deployments
- Deployment Scenarios

Search Processing Language

- What is Search Processing Language (SPL)?
- Searching Operators
- Search Commands
- Search Pipeline
- Sub-searches

- Commonly Used Search Commands
- Drilldowns
- Lookups
- Optimize Searches

Dashboard and Visualizations

- Dashboards in Splunk
- Creating Dashboards
- Visualization Types
- Search as Reports
- Dashboards
- Drilldown
- Forms

Alerts

- Creating Alerts
- Scheduling Alerts
- Alerts Notifications

Scheduled Reports

- Creating Scheduled Reports

Putting the Pieces Together

- In your final exercise, you'll configure a typical scenario when using Splunk. You'll install and configure an NGINX, then the Splunk forwarder to collect logs in Splunk. The idea is that you can apply everything you've learned within the Bootcamp: creating searches, visualizations, dashboards, etc.

SPLUNK BOOT CAMP

Course Code: 100323

VIRTUAL CLASSROOM LIVE	$2,595 CAD	2 Day

Virtual Classroom Live Outline

Introduction to Splunk

- What's Splunk?
- Authentication Methods
- Access Controls and Users
- Products, Licensing, and Costs
- Quick Tour Guide: User Interface

Indexes

- Splunk Data
- What are Indexes?
- What are Indexers?
- Search-Head
- Index Clusters
- Index Pipeline
- Events
- Fields and Field Extraction
- Forwarders
- Metrics
- Removing Data

Splunk Architecture

- Components of Splunk Deployments
- Deployment Scenarios

Search Processing Language

- What is Search Processing Language (SPL)?
- Searching Operators
- Search Commands
- Search Pipeline
- Sub-searches

- Commonly Used Search Commands
- Drilldowns
- Lookups
- Optimize Searches

Dashboard and Visualizations

- Dashboards in Splunk
- Creating Dashboards
- Visualization Types
- Search as Reports
- Dashboards
- Drilldown
- Forms

Alerts

- Creating Alerts
- Scheduling Alerts
- Alerts Notifications

Scheduled Reports

- Creating Scheduled Reports

Putting the Pieces Together

- In your final exercise, you'll configure a typical scenario when using Splunk. You'll install and configure an NGINX, then the Splunk forwarder to collect logs in Splunk. The idea is that you can apply everything you've learned within the Bootcamp: creating searches, visualizations, dashboards, etc.

Jan 12 - 13, 2026 | 9:00 AM - 5:00 PM EST

Feb 9 - 10, 2026 | 9:00 AM - 5:00 PM EST

Mar 19 - 20, 2026 | 10:00 AM - 6:00 PM EDT

Apr 20 - 21, 2026 | 9:00 AM - 5:00 PM EDT

May 18 - 19, 2026 | 12:00 - 8:00 PM EDT

Jun 11 - 12, 2026 | 9:00 AM - 5:00 PM EDT

Jul 13 - 14, 2026 | 9:00 AM - 5:00 PM EDT

Aug 19 - 20, 2026 | 10:00 AM - 6:00 PM EDT

Sep 16 - 17, 2026 | 12:00 - 8:00 PM EDT

SPLUNK BOOT CAMP

Course Code: 100323

PRIVATE GROUP TRAINING	2 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.