Splunk Core Certified User

This Splunk Core Certified User training covers everything you need to pass Splunk's entry-level certification exam and start working confidently in Splunk Enterprise and Splunk Cloud. You'll learn how to run searches, use the Search Processing Language pipeline, work with fields and lookups, and build reports and dashboards. The course also covers scheduled reports and alerts, the operational basics an analyst needs in an SOC or any environment where Splunk is the SIEM. No prior Splunk experience is required.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Welcome to Splunk

What all can Splunk do?

Lab Setup

Applications for Splunk

Challenge

Managing Splunk

Managing Splunk

Application location

Splunk Settings

General Settings

User Management

Challenge

Searching Basics

Searching in Splunk

Basic searching

Looking at a result

Refining the ability to search (with repeats)

Challenge

Expanding the search

Getting comfortable

Installing Universal Forwards

Checking the Forwarders

Search Heads

Snap-To

Challenge

Using Fields

Fields

Default Fields

Using the Fields

All the Fields

Challenge

Search Language Fundamentals

Introduction

Basic Search Commands

General Search Practices

Searching Best Practices

Search Pipelines

More Search Commands

Validation

Practicing SPL Searches

Introduction

Firewall Denied Connections

Suspicious HTTP Traffic

Failed Windows Login Attempts

Windows Suspicious Process Execution

AWS VCP Flow Log Analysis

Validation

Top, Rare and Stats Commands

Introduction

The "top" Command

The "top" Command In Action

The "rare" Command

The "rare" Command In Action

The "stats" Command

The "stats" Command In Action

Validation

Reports and Dashboards

Introduction

Save A Search As A Report and Editing It.

Displaying Statistics & Visualizations

Creating and Editing A Dashboard

Validation

Using Lookups

Lookups

Manual lookup

Using the manual lookup

Automatic lookup

Challenge

Scheduled Reports and Alerts

Introduction

Scheduled Reports

Configuring Scheduled Reports

Describe Alerts

Creating Alerts

Validation

Last updated 7.8.2026