+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 24/06/2025

Sign up

Splunk Training

3 days (21 hours)

Introducing

The company was founded in 2003 by co-founders Erik Swan, Rob Das and Michael Baum, three serial entrepreneurs from Silicon Valley. The name "Splunk" refers to the practice of cave exploration known as "spelunking". The name also refers to their plunge into the deep, new realm of Big Data.

Splunk 8 collects and analyzes large volumes of machine-generated data in real time. It uses a standard API enabling direct connection of the service to applications and devices. It can generate graphs, reports, alerts, dashboards and infographics.

Splunk offers products that perform real-time historical searches to extract statistical analyses and dashboards, for decision support. The software can index both structured and unstructured machine data. Searches and analyses are performed using Splunk's own search language.

This language encompasses all search commands and their functions. Its syntax is based on UNIX and SQL, and includes data search, filtering, modification, manipulation, insertion and deletion. Of course, we'll be teaching you the latest version of the tool, Splunk 9.4.

Objectives

- Master the principles of Splunk
- Manage machine data
- Create statistical dashboards

Target audience

- Developers
- Architects
- Administrators

Prerequisites

Knowledge of Big Data and Data Analytics

SPLUNK TRAINING PROGRAM

Introduction to Splunk

- What is Splunk?
- Architecture overview
- Splunk installation
- Setting up

Creating Splunk applications

- Choosing the architecture
- Creating your Splunk app
- Monitoring logs
- Improving application performance
- Packaging the app

Searches and data

- The data
  - Splunk Web
  - Identifying input types
  - Adding and accessing data
- Using the monitor option
- Searching
  - Performing basic searches
  - Automatic entry
  - Search intervals
  - Using the timeline
- Saving search results
- Using fields
- Introduction to SPL
- Pipelines
- Tables, fields and commands

Pivot

- What is a pivot?
- The relationship between data model and pivot
- Selecting a data model object
- Creating a pivot report
- The instant pivot

Reports and dashboard

- Presentation of the interface and elements
- Data Visualization best practices
- What type of view should I use?
- SplunkJS dashboard
- Using tokens
- Event handlers
- Good security practices

Rest API

- Introduction
- Different levels of authorization
- Using indexes
- HTTP Event Collector (**HEC**)
- Advanced search
- Job management

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples and

and group work sessions.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.