Splunk Architect Master's Certification Training

IntelliPaat

Table of Contents

About the Program

Intellipaat offers Splunk online classes that include Splunk Developer, Administration, and SIEM components. This Splunk Architect master's program helps you learn Splunk search and search commands, report creation, analyzing data with Splunk visualization, data management, deploying Splunk SIEM for investigating and monitoring security solutions, and more.

About Intellipaat

Intellipaat is one of the leading e-learning training providers with more than 600,000 learners across 55+ countries. We are on a mission to democratize education as we believe that everyone has the right to quality education.

Our courses are delivered by subject matter experts from top MNCs, and our world-class pedagogy enables learners to quickly learn difficult topics in no time. Our 24/7 technical support and career services will help them jump-start their careers in their dream companies.

Key Features

46 HRS INSTRUCTOR-LED TRAINING

46 HRS SELF-PACED TRAINING

80 HRS REAL-TIME PROJECT WORK

LIFETIME ACCESS

24/7 TECHNICAL SUPPORT

INDUSTRY-RECOGNIZED CERTIFICATION

JOB ASSISTANCE THROUGH 80+ CORPORATE TIE-UPS

FLEXIBLE SCHEDULING

Career Support

SESSIONS WITH INDUSTRY MENTORS

Attend sessions from top industry experts and get guidance on how to boost your career growth

MOCK INTERVIEWS

Mock interviews to make you prepare for cracking interviews by top employers

GUARANTEED INTERVIEWS & JOB SUPPORT

Get interviewed by our 400+ hiring partners

RESUME PREPARATION

Get assistance in creating a world-class resume from our career services team

Why take up this course?

Splunk is the most popular tool for working with machine data. It is also extensively used for security monitoring, analysis, and threat mitigation. Intellipaat's Splunk master's program is created to help you be a complete Splunk professional. Once you learn Splunk Developer and Administration domains, you will be qualified to learn the Splunk SIEM domain. Upon the completion of the training, your skills will be highly demanded by the industry, which will help you fast-track your career.

Who should take up this course?

Software Developers, System Administrators, Search Analysts, Security Professionals, Database Administrators, and others.

Program Curriculum

Splunk Architect Master's Training Course Content

- **SPLUNK DEVELOPMENT CONCEPTS**

  1.1 Introduction to Splunk and Splunk Developer roles and responsibilities

- **BASIC SEARCHING**

  2.1 Writing Splunk query for a search
  2.2 Auto-complete to build a search
  2.3 Time range
  2.4 Refining the search
  2.5 Working with events
  2.6 Identifying the contents of the search
  2.7 Controlling a search job

  ***Hands-on Exercise**: Write a basic search query*

- **USING FIELDS IN SEARCHES**

  3.1 What is a Field?
  3.2 How to use Fields in a search?
  3.3 Deploying Fields Sidebar and Field Extractor for REGEX field extraction
  3.4 Delimiting Field Extraction using FX

  ***Hands-on Exercise**: Use Fields in a search, use Fields Sidebar, use Field Extractor (FX), and delimit field Extraction using FX*

- **SAVING & SCHEDULING SEARCHES**

  4.1 Writing Splunk query for a search and sharing, saving, scheduling, and exporting search results

  ***Hands-on Exercise**: Schedule a search, save the search result, and share and export the search result*

- **CREATING ALERTS**

  5.1 How to create alerts

  5.2 Understanding alerts

  5.3 Viewing fired alerts

  Hands-on Exercise*: Create an alert in Splunk and view the fired alerts*

- **SCHEDULED REPORTS**

  6.1 Understanding and configuring scheduled reports

- **TAGS & EVENT TYPES**

  7.1 Introduction to tags in Splunk

  7.2 Deploying tags for a Splunk search

  7.3 Understanding event types and utility

  7.4 Generating and implementing event types in the search

  Hands-on Exercise*: Deploy tags for a Splunk search and generate and implement event types in the search*

- **CREATING & USING MACROS**

  8.1 What is a Macro?

  8.2 What are variables and arguments in Macros?

  Hands-on Exercise*: Define a Macro with arguments and use variables within it*

- **WORKFLOW**

  9.1 Creating get, post, and search workflow actions

  Hands-on Exercise*: Create get, post, and search workflow actions*

- **SPLUNK SEARCH COMMANDS**

  10.1 Understanding a search command

  10.2 General search practices

  10.3 What is a search pipeline?

  10.4 How to specify indexes in a search?

  10.5 Highlighting the syntax

10.6 Deploying various search commands such as fields, tables, sort, rename, rex, and erex

***Hands-on Exercise**: Steps to create a search pipeline, search index specification, highlight the syntax, use the auto-complete feature, and deploy various search commands such as sort, fields, tables, rename, rex, and erex*

- **TRANSFORMING COMMANDS**

  11.1 Using top, rare, and stats commands

  ***Hands-on Exercise**: Use top, rare, and stats commands*

- **REPORTING COMMANDS**

  12.1 Using the following commands and their functions: addcoltotals, addtotals, top, rare, and stats

  ***Hands-on Exercise**: Create reports using the following commands and their functions: addcoltotals and addtotals*

- **MAPPING & SINGLE-VALUE COMMANDS**

  13.1 Using iplocation, geostats, geom, and addtotals commands

  ***Hands-on Exercise**: Track the IP using iplocation and the get geo data using geostats*

- **SPLUNK REPORTS & VISUALIZATIONS**

  14.1 Exploring the available visualizations
  14.2 Creating charts and time charts
  14.3 Omitting null values and formatting results

  ***Hands-on Exercise**: Create time charts, omit null values, and format results*

- **ANALYZING, CALCULATING, & FORMATTING RESULTS**

  15.1 Calculating and analyzing results
  15.2 Value conversion
  15.3 Rounding off and formatting values
  15.4 Using the eval command

15.5 Using conditional statements

15.6 Filtering calculated search results

***Hands-on Exercise**: Calculate and analyze results, perform the conversion of a data value, round off numbers, use the eval command, write conditional statements, and apply filters on calculated search results*

- **CORRELATING EVENTS**

16.1 How to search for transactions?

16.2 Creating a report on transactions

16.3 Grouping events using time and fields

16.4 Comparing transactions with stats

***Hands-on Exercise**: Generate a report on transactions, and group events using fields and time*

- **ENRICHING DATA WITH LOOKUPS**

17.1 Learning data lookups

17.2 Examples and lookup tables

17.3 Defining and configuring automatic lookups

17.4 Deploying lookups in reports and searches

***Hands-on Exercise**: Define and configure automatic lookups and deploy lookups in reports and searches*

- **CREATING REPORTS & DASHBOARDS**

18.1 Creating search charts, reports, and dashboards

18.2 Editing reports and dashboards

18.3 Adding reports to dashboards

***Hands-on Exercise**: Create search charts, reports, and dashboards, edit reports and dashboards, and add reports to dashboards*

- **GETTING STARTED WITH PARSING**

19.1 Working with raw data for data extraction, transformation, parsing, and preview

***Hands-on Exercise**: Extract useful data from raw data, perform transformation, parse different values, and preview them*

- **USING PIVOT**

  20.1 Understanding a pivot
  20.2 Relationship between a data model and a pivot
  20.3 Selecting a data model object
  20.4 Creating a pivot report
  20.5 Creating an instant pivot from a search
  20.6 Adding a pivot report to the dashboard

  ***Hands-on Exercise**: Select a data model object, create a pivot report, create an instant pivot from a search, and add a pivot report to the dashboard*

- **COMMON INFORMATION MODEL (CIM) ADD-ON**

  21.1 What is a Splunk CIM?
  21.2 Using the CIM add-on to normalize data

  ***Hands-on Exercise**: Use the CIM add-on to normalize data*

Splunk Administration Topics

- **OVERVIEW OF SPLUNK**

  22.1 Introduction to the architecture of Splunk
  22.2 Various server settings
  22.3 How to set up alerts
  22.4 Various types of licenses
  22.5 Important features of the Splunk tool
  22.6 The requirements of hardware and conditions needed for the installation of Splunk

- **SPLUNK INSTALLATION**

  23.1 How to install and configure Splunk
  23.2 The creation of an index
  23.3 Standalone server's input configuration

23.4 The preferences for a search

23.5 Linux environment Splunk installation

23.6 Administering and architecting Splunk

- **SPLUNK INSTALLATION IN LINUX**

24.1 How to install Splunk in the Linux environment

24.2 The conditions needed for Splunk

24.3 Configuring Splunk in the Linux environment

- **DISTRIBUTED MANAGEMENT CONSOLE**

25.1 Introducing Splunk distributed management console

25.2 Indexing of clusters

25.3 How to deploy a distributed search in the Splunk environment

25.4 Forwarder management

25.5 User authentication and access control

- **INTRODUCTION TO THE SPLUNK APP**

26.1 Introduction to the Splunk app

26.2 How to develop Splunk apps

26.3 Splunk app management

26.4 Splunk app add-ons

26.5 Using Splunk-base for the installation and deletion of apps

26.6 Different app permissions and implementation

26.7 How to use the Splunk app

26.8 Apps on forwarder

- **SPLUNK INDEXES & USERS**

27.1 Index time configuration file

27.2 Search time configuration file

- **SPLUNK CONFIGURATION FILES**

28.1 Understanding the Index time and search time configuration files in Splunk

28.2 Forwarder installation

28.3 Input and output configuration

28.4 Universal Forwarder management

28.5 Splunk Universal Forwarder highlights

- **SPLUNK DEPLOYMENT MANAGEMENT**

29.1 Implementing the Splunk tool

29.2 Deploying it on the server

29.3 Splunk environment setup

29.4 Splunk client group deployment

- **SPLUNK INDEXES**

30.1 Understanding Splunk Indexes

30.2 Default Splunk Indexes

30.3 Segregating Splunk Indexes

30.4 Learning Splunk buckets and bucket classification

30.5 Estimating index storage

30.6 Creating a new index

- **USER ROLES & AUTHENTICATION**

31.1 Understanding the concept of role inheritance

31.2 Splunk authentications

31.3 Native authentications

31.4 LDAP authentications

- **SPLUNK ADMINISTRATION ENVIRONMENT**

32.1 Splunk installation and configuration

32.2 Data inputs

32.3 App management

32.4 Splunk important concepts

32.5 Parsing machine-generated data

32.6 Search indexer and forwarder

- **BASIC PRODUCTION ENVIRONMENT**

33.1 Introduction to Splunk configuration files

33.2 Universal Forwarder

33.3 Forwarder management

33.4 Data management, troubleshooting, and monitoring

- **SPLUNK SEARCH ENGINE**

34.1 Converting machine-generated data into operational intelligence

34.2 Setting up the dashboard, reports, and charts

34.3 Integrating search head clustering and indexer clustering

- **VARIOUS SPLUNK INPUT METHODS**

35.1 Understanding input methods

35.2 Deploying scripted Windows and network

35.3 Agentless input types and fine-tuning them all

- **SPLUNK USER & INDEX MANAGEMENT**

36.1 Splunk user authentication and job role assignment

36.2 Learning to manage, monitor, and optimize Splunk Indexes

- **MACHINE DATA PARSING**

37.1 Parsing machine-generated data

37.2 Manipulation of raw data

37.3 Previewing and parsing

37.4 Data field extraction

37.5 Comparing single-line and multi-line events

- **SEARCH SCALING & MONITORING**

38.1 Distributed search concepts

38.2 Improving search performance

38.3 Large-scale deployment and overcoming execution hurdles

38.4 Working with Splunk Distributed Management Console for monitoring the entire operation

- **SPLUNK CLUSTER IMPLEMENTATION**

39.1 Cluster indexing

39.2 Configuring individual nodes

39.3 Configuring cluster behavior, index behavior, and search behavior

39.4 Setting up a node type to handle different aspects of a cluster such as the master node, the peer node, and the search head

Splunk SIEM Course Content

- **INTRODUCTION TO SPLUNK SECURITY**

  Understanding the fundamentals of Splunk security, details of traditional security threats, and describing correlation searches and the security data model

- **INVESTIGATION & MONITORING**

  How to monitor the dashboard and brief on each panel, investigating notable events with incident review dashboards, workflow investigation, and the relative action on the identified flow

- **INVESTIGATIONS**

  Deploying ES investigation timelines for managing, visualizing and coordinating incident investigations, using journals and timelines for documenting breach analysis, and efforts needed to mitigate issues

- **RISK & NETWORK ANALYSIS**

  Deploying risk analysis and identification, risk dashboard utilization, and how to manage risk scores for objects and users

- **WEB INTELLIGENCE**

  Using HTTP category analysis, HTTP user agent analysis, analyzing a new domain, analyzing the traffic size for spotting new threats, and highlighting investigable events

- **USER INTELLIGENCE**

  Accessing the anomaly dashboards for user role and access logs and understanding identity and asset concepts

- **THREAT INTELLIGENCE**

  Monitoring malicious sites with the threat activity dashboard and inspecting the threat intelligence content with the threat artifact dashboard

Project Work

Splunk Architect Master's Projects

Project 1: Creating an Employee Database of a Company

Industry: General

Problem Statement: How to build a Splunk dashboard where employee details are readily available

Topics: In this project, you will create a text file of employee data with details such as full name, salary, designation, ID, and so on. You will index the data based on various parameters and use various Splunk commands for evaluating and extracting the information. Finally, you will create a dashboard and add various reports to it.

Highlights:

- Splunk search and index commands
- Extracting a field in search and saving results
- Editing event types and adding tags

Project 2: Building an Organizational Dashboard with Splunk

Industry: E-commerce

Problem Statement: Analyzing website traffic and gather insights

Topics: In this project, you will build an analytics dashboard for a website and create alerts for various conditions. You will capture access logs of the web server and the sample logs and then will upload them. You will analyze the top 10 users, the average time spent, the peak response time of the website, the top 10 errors, and the error code description. You will also create a Splunk dashboard for reporting and analyzing.

Highlights:

- Creating bar and line charts
- Sending alerts for various conditions

- Providing admin rights for dashboard

Project 3: Field Extraction in Splunk

Industry: General

Problem Statement: How to extract the fields from event data in Splunk

Topics: In this project, you will learn to extract fields from events using the Splunk field extraction technique. You will gain knowledge in the basics of field extractions and understand the use of the field extractor, the field extraction page in Splunk web, and field extract configuration in files. You will learn the regular expression and delimiters method of field extraction. Upon the completion of the project, you will gain expertise in building the Splunk dashboard and using the extracted field data in it to create rich visualizations in an enterprise setup.

Highlights:

- Field extraction using the delimiter method
- Delimit field extracts using FX
- Extracting fields with the search command

Project 4: A BPO Firm Wants to Secure Its Confidential Data

Industry: Outsourcing

Problem Statement: How to ensure that an outsourcing firm does not fall prey to IT security threats

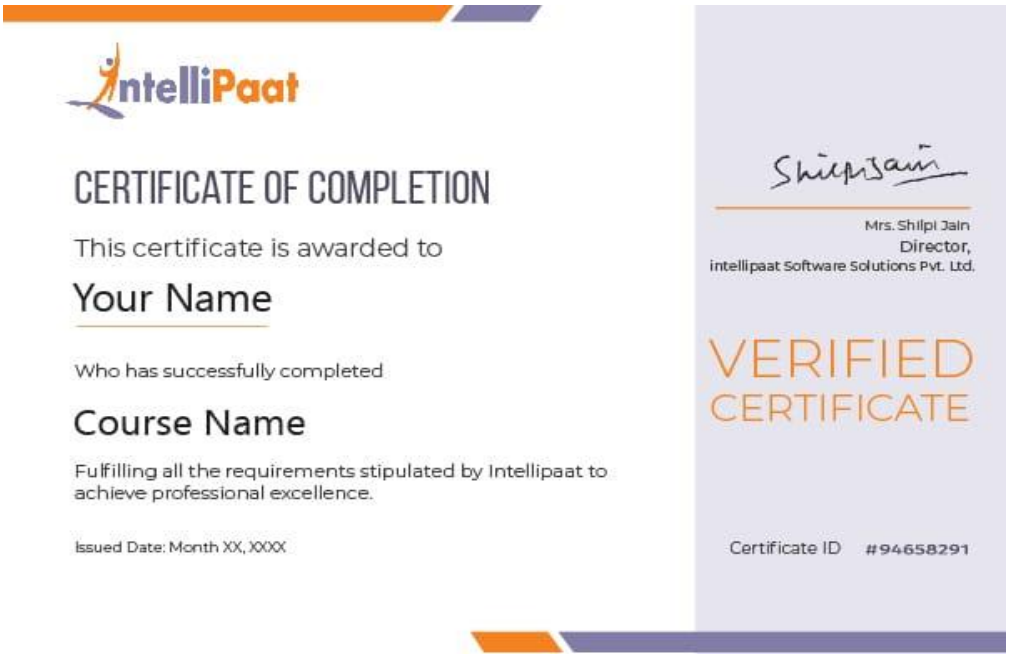
Topics: In this project, you will work with the business process outsourcing firms' machine-generated data to look for suspicious activities, anomalies, and suspected threats. You will deploy the Splunk SIEM tool for combing huge volumes of data and will deploy Splunk analytics to come up with enterprise security reports and recommendations for securing the activities of the enterprise.

Highlights:

- Deploy Splunk Enterprise Security
- Investigate and monitor events
- Enterprise security model validation

Certification

After the completion of the course, you will get a certificate from Intellipaat.



Success Stories

Kevin K Wada

Thank you very much for your top-class service. A special mention should be made for your patience in listening to my queries and giving me a solution, which was exactly what I was looking for. I am giving you a 10 on 10!

Sampson Basoah

The Intellipaat team helped me in selecting the perfect course that suits my profile. The whole course was practically oriented, and the trainers were always ready to answer any question. I found this course to be impactful. Thank you.

Nii Akai

My overall training journey was good. The trainers were cooperative. All my questions were quickly answered with a detailed explanation. I always received more than what I had asked for. Thanks a lot.

Sugandha Sinha

Intellipaat's course instructors were excellent and well-versed with their concepts. The support team solved all my queries within the promised 24 hours. They explained all topics and concepts well, and the course material was updated and included videos, exercises, etc. I would highly recommend Intellipaat to those who wish to excel in the IT field.

.

Vishal Pentakota

The best part of this course was the series of hands-on demonstrations that the trainer performed. Not only did he explain each concept theoretically, but he also implemented all those concepts practically. Great job! A must go for beginners.

CONTACT US

INTELLIPAAT SOFTWARE SOLUTIONS PVT. LTD.

Bangalore

AMR Tech Park 3, Ground Floor, Tower B,
Hongasandra Village, Bommanahalli,
Hosur Road, Bangalore – 560068

USA

1219 E. Hillsdale Blvd. Suite 205,
Foster City, CA 94404

If you have any further queries or just want to have a conversation with us, then do call us.

IND: +91-7022374614 | US: 1-800-216-8930