

About IntelliPaat

IntelliPaat is a fast-growing professional training provider that is offering training in over 150 most sought-after tools and technologies. We have a learner base of 600,000 in over 32 countries and growing. For job assistance and placement we have direct tie-ups with 80+ MNCs.

Key Features of IntelliPaat Training:

| | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>Instructor Led Training</p> <p>26 Hrs of highly interactive instructor led training</p> |  <p>Self-Paced Training</p> <p>26 Hrs of Self-Paced sessions with Lifetime access</p> |  <p>Exercise and project work</p> <p>40 Hrs of real-time projects after every module</p> |  <p>Lifetime Access</p> <p>Lifetime access and free upgrade to latest version</p> |
|  <p>Support</p> <p>Lifetime 24*7 technical support and query resolution</p> |  <p>Get Certified</p> <p>Get global industry recognized certifications</p> |  <p>Job Assistance</p> <p>Job assistance through 80+ corporate tie-ups</p> |  <p>Flexi Scheduling</p> <p>Attend multiple batches for lifetime & stay updated.</p> |

About the Course

This is IntelliPaat Master Program in Splunk tool includes Splunk Developer and Splunk Administration training. As part of this Splunk course, you will work on searching, sharing, saving Splunk results, creating tags, generating reports and charts, installing and configuring Splunk, monitoring, scaling and indexing large volumes of searches and analyzing it using the Splunk tool.

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|  <p>Instructor Led Duration – 26 Hrs Weekend Batch –3 Hrs/Session</p> |  <p>Self Paced Duration – 26 Hrs</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|

Why take this Course?

Splunk is the most popular tool used for parsing huge volumes of machine-generated data and deriving valuable insights from it. This IntelliPaat instructor-led & self-paced training in Splunk Developer and Splunk Administration is your passport to working in the Splunk domain in order to gain a definitive edge when it comes to deploying Splunk in mission-critical applications in the real world in top MNCs and commanding big salaries in the process.

Course Content

| Module /Topic | Hands-on exercises |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Splunk Development concepts <ul style="list-style-type: none"> ❖ Introduction to Splunk ❖ Splunk developer roles and responsibilities | |
| Basic Searching <ul style="list-style-type: none"> ❖ Writing Splunk query for search ❖ Auto-complete to build a search, time range, refine the search, work with events ❖ Identify the contents of search, control a search job | <ul style="list-style-type: none"> ❖ Write a basic search query |
| Using Fields in Searches <ul style="list-style-type: none"> ❖ Understand Fields ❖ Use Fields in Search ❖ Use Fields Sidebar ❖ Regex field extraction using Field Extractor (FX) ❖ Delimiter field Extraction using FX | <ul style="list-style-type: none"> ❖ Use Fields in Search ❖ Use Fields Sidebar ❖ Use Field Extractor (FX) ❖ Delimit field Extraction using FX |
| Saving and Scheduling Searches <ul style="list-style-type: none"> ❖ Writing Splunk query for search, sharing, saving, scheduling and exporting search results | <ul style="list-style-type: none"> ❖ Schedule a search, Save a search result, Share and export a search result |

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Creating Alerts</p> <ul style="list-style-type: none"> ❖ Creation of alert ❖ Explaining alerts and viewing fired alerts | <ul style="list-style-type: none"> ❖ Create an alert ❖ View fired alerts |
| <p>Scheduled Reports</p> <ul style="list-style-type: none"> ❖ Describe and Configure Scheduled Reports | |
| <p>Tags and Event Types</p> <ul style="list-style-type: none"> ❖ Introduction to Tags in Splunk ❖ Deploying Tags for Splunk search ❖ Understanding event types and utility ❖ Generating and implementing event types in Search | <ul style="list-style-type: none"> ❖ Deploy tags for Splunk search, generate and implement event types in Search |
| <p>Creating and Using Macros</p> <ul style="list-style-type: none"> ❖ Define Macros ❖ Arguments and Variables in a Macro | <ul style="list-style-type: none"> ❖ Define a Macro with arguments and use variables in it |
| <p>Workflow</p> <ul style="list-style-type: none"> ❖ GET, POST, and Search workflow actions | <ul style="list-style-type: none"> ❖ Create GET, POST, and Search workflow |
| <p>Splunk Search Commands</p> <ul style="list-style-type: none"> ❖ Search Command study ❖ Search practices in general, search pipeline ❖ Specify indexes in search ❖ Syntax highlighting, autocomplete ❖ Search commands like tables, fields, sort, multikv, rename, rex & erex | <ul style="list-style-type: none"> ❖ Create search pipeline, specify indexes in search, highlight syntax, use autocomplete feature, use search commands like tables, fields, sort, multikv, rename, rex & erex |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Transforming Commands</p> <ul style="list-style-type: none"> ❖ Using Top ❖ Rare ❖ Stats Commands | <ul style="list-style-type: none"> ❖ Using Top ❖ Rare ❖ Stats Commands |
| <p>Reporting Commands</p> <ul style="list-style-type: none"> ❖ Using following commands and their functions: addcoltotals, add totals, top, rare, stats | <ul style="list-style-type: none"> ❖ Create reports using following commands and their functions: addcoltotals, add totals |
| <p>Mapping and Single Value Commands</p> <ul style="list-style-type: none"> ❖ iplocation, geostats, geom, addtotals commands | <ul style="list-style-type: none"> ❖ Track ip using IP location, get geo data using geo stats |
| <p>Splunk Reports & visualizations</p> <ul style="list-style-type: none"> ❖ Explore the available visualizations ❖ Create charts and time charts ❖ omit null values and format results | <ul style="list-style-type: none"> ❖ Create time charts, omit null values and format results |
| <p>Analyzing, Calculating and Formatting Results</p> <ul style="list-style-type: none"> ❖ Calculating and analyzing results ❖ Value conversion, roundoff and format values, using eval command, ❖ Conditional statements, filtering calculated search results | <ul style="list-style-type: none"> ❖ Calculate and analyze results ❖ Perform conversion on a data value, round off numbers, use eval command, write conditional statements, apply filters on calculated search results |
| <p>Correlating Events</p> <ul style="list-style-type: none"> ❖ Search with Transactions ❖ Report on Transactions ❖ Group events using fields and time ❖ Transaction vs Stats | <ul style="list-style-type: none"> ❖ Generate Report on Transactions, Group events using fields and time |
| <p>Enriching Data with Lookups</p> <ul style="list-style-type: none"> ❖ Learn about data lookups, example, a lookup table ❖ Defining and configuring automatic lookup ❖ Deploying lookup in reports and searches | <ul style="list-style-type: none"> ❖ Define and configure the automatic lookup ❖ Deploy lookup in reports and searches |

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Creating Reports and Dashboards</p> <ul style="list-style-type: none"> ❖ Creating search charts ❖ Reports and dashboards ❖ Editing reports and Dashboard ❖ Adding reports to dashboard | <ul style="list-style-type: none"> ❖ Create search charts, reports and dashboards ❖ Edit reports and Dashboard, Add reports to dashboard |
| <p>Getting started with Parsing</p> <ul style="list-style-type: none"> ❖ Working with raw data for data extraction ❖ Transformation, parsing, and preview | <ul style="list-style-type: none"> ❖ Extract useful data from raw data ❖ Perform transformation ❖ Parse different values and preview |
| <p>Using Pivot</p> <ul style="list-style-type: none"> ❖ Describe Pivot ❖ The relationship between the data model and pivot ❖ Select a data model object, create a pivot report, instant pivot from a search ❖ Add a pivot report to a dashboard | <ul style="list-style-type: none"> ❖ Select a data model object ❖ Create a pivot report ❖ Create instant pivot from a search ❖ Add a pivot report to a dashboard |
| <p>Common Information Model (CIM) Add-On</p> <ul style="list-style-type: none"> ❖ What is Splunk CIM? ❖ Using the CIM Add-On to normalize data | <ul style="list-style-type: none"> ❖ Use the CIM Add-On to normalize data |

Splunk Administration Topics

| Module /Topic |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Overview of Splunk <ul style="list-style-type: none">❖ Introduction to the Splunk 3 tier architecture❖ Understanding the Server settings, control, preferences and licensing, managing & pooling license, setting up alerts, the types & usage of the license❖ The most important components of Splunk too❖ The hardware requirements, conditions for installation of Splunk |
| Splunk Installation <ul style="list-style-type: none">❖ Understanding how to install and configure Splunk❖ Index creation, input configuration in the standalone server❖ The search preferences❖ Installing Splunk in the Linux environment❖ Practical administration and architect class |
| Splunk Installation in Linux <ul style="list-style-type: none">❖ Installing Splunk in the Linux environment❖ The various prerequisites❖ The configuration of Splunk in Linux |
| Distributed Management Console <ul style="list-style-type: none">❖ Introduction to the Splunk Distributed Management Console❖ Index clustering, forwarder management and distributed search in Splunk environment❖ Providing the right authentication to users, access control |
| Introduction to Splunk App <ul style="list-style-type: none">❖ Introducing the Splunk app❖ Developing Splunk apps, managing the Splunk app❖ The various add-ons in Splunk app❖ Deleting and installing apps from Splunk Base❖ Deploying the various app permissions, deploying the Splunk app, apps on the forwarder |

Splunk indexes and users

- ❖ Understanding the index time configuration file and search time configuration file

Splunk configuration files

- ❖ Learning about the index time and search time configuration files in Splunk
- ❖ Installing the forwarders
- ❖ Configuring the output and inputs.conf
- ❖ Managing the Universal Forwarders
- ❖ Additional features of Splunk Universal Forwarder

Splunk Deployment Management

- ❖ Deploying the Splunk tool
- ❖ The Splunk deployment Server
- ❖ Setting up the Splunk deployment environment
- ❖ Deploying the clients grouping in Splunk

Splunk Indexes

- ❖ Understanding the Splunk Indexes
- ❖ The default Splunk Indexes
- ❖ Segregating the Splunk Indexes
- ❖ Learning about Splunk Buckets and Bucket Classification
- ❖ Estimating index storage, creating a new index

User roles and authentication

- ❖ Understanding the concept of role inheritance
- ❖ Splunk authentications
- ❖ Native authentications
- ❖ LDAP authentications

Splunk Administration Environment

- ❖ Splunk installation
- ❖ Configuration, data inputs, app management
- ❖ Splunk important concepts
- ❖ Parsing machine-generated data
- ❖ Search indexer and forwarder

Basic Production Environment

- ❖ Introduction to Splunk Configuration Files

| |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">❖ Universal Forwarder, Forwarder Management❖ Data management❖ Troubleshooting and monitoring |
| Splunk Search Engine <ul style="list-style-type: none">❖ Converting machine-generated data into operational intelligence❖ Setting up Dashboard❖ Reports and Charts, integrating Search Head Clustering & Indexer Clustering |
| Various Splunk Input Methods <ul style="list-style-type: none">❖ Understanding the input methods❖ Deploying scripted, Window❖ Network and agentless input types, fine-tuning it all |
| Splunk User & Index Management <ul style="list-style-type: none">❖ Splunk User authentication and Job Role assignment❖ Learning to manage❖ Monitor and optimize Splunk Indexes |
| Machine Data Parsing <ul style="list-style-type: none">❖ Understanding parsing of machine-generated data❖ Manipulation of raw data❖ Previewing and parsing, data field extraction❖ Comparing single line and multi-line events |
| Search Scaling and Monitoring <ul style="list-style-type: none">❖ Distributed search concepts❖ Improving search performance❖ Large-scale deployment and overcoming execution hurdles❖ Working with Splunk Distributed Management Console for monitoring the entire operation |
| Splunk Cluster implementation <ul style="list-style-type: none">❖ Cluster indexing, configuring individual nodes❖ Configuring the cluster behavior, index and search behavior❖ Setting node type to handle different aspects of cluster-like master node❖ Peer node and search head |

Project Work

Splunk Developer Project

Topics: This project gives you hands-on experience in working with the Splunk tool. You will have the data set of employee details in a text file based on which you will create a dashboard and report. Then you will deploy the various Splunk commands to perform row operations, extract certain data fields, edit the event, add tags, and search with tag name for the event and then save the tag search. Upon completion of this project, you will learn to create a searchable repository using data that is captured, correlated and indexed in real time and ultimately visualize it using dashboard, report, and alert.

Splunk Administration Project

Project: 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, understand the use of field extractor, the field extraction page in Splunk web and field extract configuration in files. Learn about the regular expression and delimiters method of field extraction. Upon completion of the project, you will gain expertise in building Splunk dashboard and use the extracted field's data in it to create rich visualizations in an enterprise setup.

Highlight:

- ❖ Field extraction using delimiter method
- ❖ Delimit field extract using FX
- ❖ Extracting fields with the search command.

Intellipaate Job Assistance Program

Intellipaate is offering comprehensive job assistance to all the learners who have successfully completed the training. A learner will be considered to have successfully completed the training if he/she finishes all the exercises, case studies, projects and gets a minimum of 60% marks in the Intellipaate qualifying exam.

Intellipaap has exclusive tie-ups with over 80 MNCs for placement. All the resumes of eligible candidates will be forwarded to the Intellipaap job assistance partners. Once there is a relevant opening in any of the companies, you will get a call directly for the job interview from that particular company.

Frequently Asked Questions:

Q 1. What is the criterion for availing the Intellipaap job assistance program?

Ans. All Intellipaap learners who have successfully completed the training post April 2017 are directly eligible for the Intellipaap job assistance program.

Q 2. Which are the companies that I can get placed in?

Ans. We have exclusive tie-ups with MNCs like **Ericsson, Cisco, Cognizant, Sony, Mu Sigma, Saint-Gobain, Standard Chartered, TCS, Genpact, Hexaware**, and more. So you have the opportunity to get placed in these top global companies.

Q 3. Does Intellipaap help learners to crack the job interviews?

Ans. Intellipaap has an exclusive section which includes the top interview questions asked in top MNCs for most of the technologies and tools for which we provide training. Other than that our support and technical team can also help you in this regard.

Q 4. Do I need to have prior industry experience for getting an interview call?

Ans. There is no need to have any prior industry experience for getting an interview call. In fact, the successful completion of the Intellipaap certification training is equivalent to six months of industry experience. This is definitely an added advantage when you are attending an interview.

Q 5. What is the job location that I will get?

Ans. Intellipaap will try to get you a job in your same location provided such a vacancy exists in that location.

Q 6. Which is the domain that I will get placed in?

Ans. Depending on the Intellipaap certification training you have successfully completed, you will be placed in the same domain.

Q 7. Is there any fee for the IntelliPaat placement assistance?

Ans. IntelliPaat does not charge any fees as part of the placement assistance program.

Q 8. If I don't get a job in the first attempt, can I get another chance?

Ans. Definitely, yes. Your resume will be in our database and we will circulate it to our MNC partners until you get a job. So there is no upper limit to the number of job interviews you can attend.

Q 9. Does IntelliPaat guarantee a job through its job assistance program?

Ans. IntelliPaat does not guarantee any job through the job assistance program. However, we will definitely offer you full assistance by circulating your resume among our affiliate partners.

Q 10. What is the salary that I will be getting once I get the job?

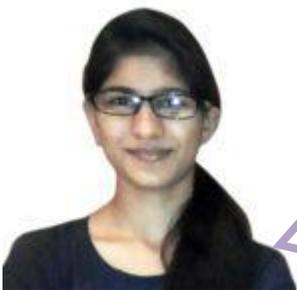
Ans. Your salary will be directly commensurate with your abilities and the prevailing industry standards.

What makes us who we are?



"I am completely satisfied with the IntelliPaat training. The trainer came with over a decade of industry experience. The entire online course was segmented into modules that were created with care so that the learning is complete and as per the industry needs."

-Bhuvana



"Full marks for the IntelliPaat support team for providing excellent support services. The entire course was completely oriented towards the practical aspects."

- Bharati Jha