TRIVID TECHNOLOGY SERVICES

Module 1 – Introduction to Data Administration

- Splunk overview
- Identify Splunk data administrator role

Module 2 – Configuring Forwarders

- Understand the role of production Indexers and Forwarders
- Understand the functionality of Universal Forwarders and Heavy Forwarders
- Configure Forwarders
- Identify additional Forwarder options

Module 3 – Forwarder Management

- Explain the use of Forwarder Management
- Describe Splunk Deployment Server
- Manage forwarders using deployment apps
- Configure deployment clients
- Configure client groups
- Monitor forwarder management activities

Module 4 – Monitor Inputs

- Create file and directory monitor inputs
- Use optional settings for monitor inputs
- Deploy a remote monitor input

Module 5 – Network and Scripted Inputs

- Create network (TCP and UDP) inputs
- Describe optional settings for network inputs
- Create a basic scripted input

+91 8007377665
+1(404)491-8800
abhay@trividtech.com
www.ttstechloot.com
Block AE-23 , Salt Lake City , Sector - I, Tank No:- 4. Land Mark : Lake Town Foot Bridge, Kolkata : 700064
737 Saint George's Ave Woodbridge, NJ, 07065

Module 6 – Agentless Inputs

- Identify Windows input types and uses
- Understand additional options to get data into Splunk
- HTTP Event Collector Splunk App for Stream

Module 7 – Fine Tuning Inputs

- Understand the default processing that occurs during input phase
- Configure input phase options, such as sourcetype finetuning and character set encoding

Module 8 – Parsing Phase and Data

- Understand the default processing that occurs during parsing
- Optimize and configure event line breaking
- Explain how timestamps and time zones are extracted or assigned to events
- Use Data Preview to validate event creation during the
- parsing phase

+91 8007377665
+1(404)491-8800
abhay@trividtech.com
www.ttstechloot.com
Block AE-23 , Salt Lake City , Sector - I, Tank No:- 4. Land Mark : Lake Town Foot Bridge, Kolkata : 700064
737 Saint George's Ave Woodbridge, NJ, 07065

Module 9 – Manipulating Raw Data

- Explain how data transformations are defined and invoked
- Use transformations with props.conf and transforms.conf to:
  Mask or delete raw data as it is being indexed
  Override sourcetype or host based upon event values
  Route events to specific indexes based on event content
  Prevent unwanted events from being indexed
- Use SEDCMD to modify raw data

Module 10 – Supporting Knowledge Objects

- Create field extractions
- Configure collections for KV Store
- Manage Knowledge Object permissions
- Control automatic field extraction

Module 11 – Creating a Diag

- Identify Splunk diag
- Using Splunk diag

+91 8007377665
+1(404)491-8800
abhay@trividtech.com
www.ttstechloot.com
Block AE-23 , Salt Lake City , Sector - I, Tank No:- 4. Land Mark : Lake Town Foot Bridge, Kolkata : 700064
737 Saint George's Ave Woodbridge, NJ, 07065