Splunk  
Program Code: BD-SPLNK  
Program Overview: Splunk training focuses on large enterprise deployments. Participants will be able to understand the various best practices and steps for preparing, data collecting, and sizing. Workshop style labs provide participants with an opportunity to devise a deployment based on a common distributed use case. Splunk is a software that enables, and manages search data from any application, server, and network device in no time. Splunk makes machine data reachable, utilizable and helpful to everyone. It’s the secure way to examine the enormous streams of machine data produced by technology infrastructure and IT systems —virtual, physical, and in the cloud.  
Program Duration: 4 Days.  
Prerequisite Skills:  
§ Must have good knowledge of system administration  
§ Basics of Linux and Windows helps  
§ Anyone from the analytics and IT Operations domain will have a short learning curve while attempting the Administration with Splunk course  
Who should attend?  
Splunk Training is best suited for Splunk users, customers and partners who wish to manage and administer Splunk enterprise environments.  
In addition, the following roles can benefit after clearing their administration with Splunk certification exam:  
§ System Analysts  
§ System Developers  
§ Support Engineers  
§ Support Analysts  
§ IT Managers  
§ Any other IT professional who is a part of data center, IT monitoring or IT Support teams  
Contents:

**Day.1**  
§ Introduction to SPLUNK  
• Introduce Splunk  
• Run basic searches  
• Identify the contents of search results  
• Control a search job  
• Set the time range of a search  
• Use the output of a search to refine your search  
§ SPLUNK Installation  
• Requirement before installation  
• Splunk Installation on window & linux

**Day.2**  
2019 Capgemini. All rights reserved. 41  
§ SPLUNK Authentication  
• Describe Authentication  
• Set Authentication  
• Maintain user & groups under splunk  
§ SPLUNK - Log Architecture  
• Importance of logs  
• Centralized Log Architecture  
• Maintain and monitor Logs  
§ SPLUNK - Using Search  
• Export search results  
• Save and share search results  
• Save searches

**Day.3**  
• Schedule searches  
§ SPLUNK - Fields  
• Understand fields  
• Use fields in searches  
• Use the fields sidebar  
§ SPLUNK - Tags and Event Types  
• Introduce tags  
• Set tags and use tags in a search  
• Configure event types and their uses  
• Set and use event types in a search  
§ SPLUNK – Alerts  
• Describe alerts  
• Set Alert Monitoring alerts  
§ SPLUNK - Indexing  
• Describe Indexing  
• Set Index  
• Set IIS logs under index

**Day.4**  
§ SPLUNK - Dashboard  
• Describe Dashboard  
• Configure Dashboard  
• Importance of Dashboard  
2019 Capgemini. All rights reserved. 42  
§ SPLUNK - Reports  
• Develop reports and carts  
• Maintain Dashboards  
• Utilization with reports  
On Completion of this program:  
§ Get an in-depth understanding of Splunk admin concepts  
§ Learn to install Splunk, configure reports for monitoring and set up alerts as well  
§ Know how to set up Spunk for data visualization through dashboards and graphs  
§ Use Search Processing Language or SPL to troubleshoot application issues  
§ Learn how to use the search functionality, tags, event types, and different fields of Splunk