BLUEMARK ACADEMY

Splunk Operations

Duration: 3 Days · **Training format:** Virtual Classroom / Online

Description

Splunk provides the leading software platform for real-time Operational Intelligence. Splunk software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. Enterprises, government agencies, universities and service providers in over 90 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce cost.

This instructor-led onsite course provides information on how to use Splunk and its components in order to turn raw data into valuable business insights.

Delegates will learn how to:

- collect and normalize data
- install, configure, and manage Splunk components
- search and visualization details and examples

In addition to the lectures, the content will be enforced with hands-on labs.

Audience

Data Architects, Data Administrators, System Administrators, DevOps

Setup Requirements

• Mac, Linux or Windows

• Latest version of Chrome or Firefox

• SSH Client software (e.g. PuTTY)

• Stable internet connection

• Access to lab servers over tcp/22 and tcp/8000

Outline

1. Splunk Introduction & Components
2. Splunk Walk-through
3. How Indexing Works
4. Getting Data In
5. Knowledge Objects
6. Searching and Visualizations
7. Splunk Enterprise Administration
8. Distributed Deployment
9. Monitoring Splunk Enterprise

Prerequisites

There are no prerequisites