Module 1 – Start Searching

- Introduce Splunk and the Search app
- 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

Module 2 – Saving Results and Searches

- Export search results
- Save and share search results
- Save searches
- Schedule searches

Module 3 – Using Fields

- Understand fields
- Use fields in searches
- Use the fields sidebar

Module 4 – Tags and Event Types

- Understand tags
- Create tags and use tags in a search
- Describe event types and their uses
- Create and use event types in a search

Module 5 – Creating Alerts

- Describe alerts
- Create an alert
- View fired alerts

Module 6 – Creating Reports

- Create reports and charts
- Create dashboards and add reports

Module 7 – Search Fundamentals

- Review basic search commands and general search practices
- Examine the anatomy of a search
- Use the following commands to perform searches:

1. fields
2. table
3. rename
4. rex & erex
5. multikv

Module 8 – Reporting Commands, Part 1

- Use the following commands and their functions:

1. top
2. rare
3. stats
4. addcoltotals
5. addtotals

Module 9 – Reporting Commands, Part 2

- Explore the available visualizations
- Create a basic chart
- Split values into multiple series
- Omit null and other values from charts
- Create a timechart
- Chart multiple values on the same timeline
- Format charts
- Explain when to use each type of reporting command

Module 10 – Analyzing, Calculating, and Formatting Results

- Using the eval command:

1. Perform calculations
2. Convert values
3. Round values
4. Format values
5. Use conditional statements

Module 11 – Correlating Events

- Identify transactions
- Group events using fields
- Group events using fields and time
- Search with transactions
- Report on transactions
- Determine when to use transactions vs. stats

Module 12 – Enriching Data with Lookups

- Describe lookups
- Examine a lookup file example
- Create a lookup table
- Define a lookup
- Configure an automatic lookup
- Use the lookup in searches and reports