Developing with Splunk's REST API 8.2

Module 1 – Introduction to the Splunk REST API

- Use the proper case in searches
- Introduce the Splunk development environment and its REST endpoints
- Know to which Splunk server you should be connected to accomplish a desired task
- Authenticate with a Splunk server, with and without a session

Module 2 – Namespaces and Object Management

- Understand general CRUD with the REST API
- Understand how a namespace affects access to objects
- Use the servicesNS node and a namespace to access objects
- Understand how the sharing level and access control lists affect access to objects
- Modify the sharing level and the permissions on an object
- Using the rest command

Module 3 – Parsing Output

- Understand the general structure of Atom-based output

- Format Atom-based JSON output
- Write code that uses the API and parse responses

Module 4 – Oneshot Searches

- Review search language syntax and search best practices
- Execute a oneshot search
- Execute an export search
- Get search results

Module 5–Normal and Export Searching

- Identify types of searches
- Create normal and export searches
- Get:
- Search results
- Search job status and other search job properties

Module 6 – Advanced Searching and Job Management

- Executing a real time search
- Working with large results sets
- Working with saved searches

- Managing search jobs

Module 7 – Working with the KV Store

- Define the function of a KV Store
- Define collections and records
- Perform CRUD operations on collections and records

Module 8 – Using the HTTP Event Collector (HEC)

- Create and use HEC tokens
- Input data using HEC endpoints
- Get indexer event acknowledgements