**SPLUNK ENTERPRISE SECURITY & DEVELOPMENT**

**Prerequisites: - SIEM knowledge will be preferrable**

**Module 1 – Basic Understanding of Architecture**

* What are the components
* Discussion on Forwarders- UF/HF
* Common ports for the set up
* License Master/Slave relationship
* Understanding of Deployment Server and Indexer

**Module 2 – Introduction to Splunk's User Interface**

* Understand the uses of Splunk
* Define Splunk Apps
* Learn basic navigations in Splunk

**Module 3 – Searching**

* Run basic searches
* Set the time range of a search
* Identify the contents of search results
* Refine searches
* Use the timeline
* Work with events
* Control a search job
* Save search results

**Module 4 – Using Fields in Searches**

* Understand fields
* Use fields in searches
* Use the fields sidebar

**Module 5 – Search Fundamentals**

* Review basic search commands and general search practices
* Examine the anatomy of a search
* Use the following commands to perform searches:
  + Search
  + Fields
  + Table
  + Where
  + Rename
  + Replace

**Module 6 – Reporting Commands, Part 1**

* Use the following commands and their functions:
  + Top, Rare, Stats, Timechart
  + Addcoltotals, Addtotals, Append, Appendcols etc.

**Module 7 – Analyzing, Calculating and formatting Results**

* Using the eval command:
  + Perform calculations
  + Convert values
  + Round values
  + Format values
  + Use conditional statements
* Further filter calculated results

**Module 8 – Creating Field Aliases and Calculated Fields**

* Define naming conventions
* Create and use field aliases
* Create and use calculated fields

**Module 9 – Creating Field Extractions**

* Perform field extractions using Field Extractor

**Module 10 – Creating Tags and Event Types**

* Create and use tags
* Describe event types and their uses
* Create an event type

**Module 11 – Lookups**

* Lookup Table
* Lookup Definition
* Automatic Lookup

**Module 12 – Creating and Using Macros**

* Describe macros
* Manage macros
* Create and use a basic macro
* Define arguments and variables for a macro
* Add and use arguments with a macro

**ENTERPRISE SECURITY**

**Module 1 – ES Introduction**

* Overview of ES features and concepts

**Module 2 - Getting Started with ES**

* Provide an overview of Splunk for Enterprise Security (ES)
* Identify the differences between traditional security threats and new adaptive threats
* Describe correlation searches, data models and notable events, tstats
* Describe user roles in ES
* Log on to ES

**Module 3 – Tuning Correlation Searches**

* Configure correlation search scheduling and sensitivity
* Tune ES correlation searches

**Module 4 – Creating Correlation Searches**

* Create a custom correlation search
* Configuring adaptive responses
* Search export/import

**Module 5 - Security Monitoring and Incident Investigation**

* Use the Security Posture dashboard to monitor enterprise security status
* Use the Incident Review dashboard to investigate notable events
* Take ownership of an incident and move it through the investigation workflow
* Use adaptive response actions during incident investigation
* Create notable events
* Suppress notable events

**Module 6 – Investigations**

* Use ES investigation timelines to manage, visualize and coordinate incident investigations
* Use timelines and journals to document breach analysis and mitigation efforts

**Module 7 – Forensic Investigation with ES**

* Investigate access domain events
* Investigate endpoint domain events
* Investigate network domain events
* Investigate identity domain events

**Module 8 – Risk and Network Analysis**

* Understand and use Risk Analysis
* Use the Risk Analysis dashboard
* Manage risk scores for objects or users

**Module 9 – Web Intelligence**

* Use HTTP Category Analysis, HTTP User Agent Analysis, New Domain Analysis, and Traffic Size Analysis to spot new threats
* Filter and highlight events

**Module 10 – User Intelligence**

* Evaluate the level of insider threat with the user activity and access anomaly dashboards
* Understand asset and identity concepts
* Use the Asset Investigator to analyze events
* Use the Identity Investigator to analyze events

**Module 11 – Threat Intelligence**

* Use the Threat Activity dashboard to analyze traffic to or from known malicious sites
* Inspect the status of your threat intelligence content with the threat artifact dashboard

**Module 12 – Glass Tables and Navigation Control**

* Examine glass tables
* Build glass tables to display security status information
* Add glass table drilldown options
* Create new key indicators for metrics on glass tables
* Configure navigation and dashboard permissions

**Module 13 – Lookups and Identity Management Overview**

* Identify ES-specific lookups
* Overview lookup lists