Splunk Enterprise Security Advance Training (ES)

Curriculum 5 Days

Day - 1

- **Splunk Fundamentals**
  - This course teaches you how to search and navigate in Splunk, use fields, get statistics from your data, create reports, dashboards, lookups, and alerts. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts. It will also introduce you to Splunk's datasets features and Pivot interface.
- **Splunk Fundamentals Course Topics**
  - Introduction to Splunk's interface
  - Basic searching
  - Using fields in searches
  - Search fundamentals
  - Transforming commands
  - Creating reports and dashboards
  - Datasets
  - The Common Information Model (CIM)
  - Creating and using lookups
  - Scheduled Reports
  - Alerts
  - Using Pivot

- **Splunk Fundamentals Course Objectives**
  - **Module 1 – Introduction**
  - **Module 2 – What is Splunk?**
    - Splunk components
    - Installing Splunk
    - Getting data into Splunk
  - **Module 3 – Introduction to Splunk's User Interface**
    - Understand the uses of Splunk
    - Define Splunk Apps
    - Customizing your user settings
    - Learn basic navigation in Splunk
  - **Module 4 – Basic searching**
    - Run basic searches
    - Use autocomplete to help build a search
    - 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 5 – Using Fields in Searches**
  - Understand fields
  - Use fields in searches
  - Use the fields sidebar
- **Module 6 – Search Language Fundamentals**
  - - Review basic search commands and general search practices
  - - Examine the search pipeline
  - - Specify indexes in searches
  - - Use autocomplete and syntax highlighting
  - - Use SPL search commands to perform searches:
- **Module 7 – Using Basic Transforming Commands**
  - - The top command
  - - The rare command
  - - The stats command
- **Module 8 – Creating Reports and Dashboards**
  - - Save a search as a report
  - - Edit reports
  - - Create reports that include visualizations such as charts and tables
  - - Create a dashboard
  - - Add a report to a dashboard
  - - Edit a dashboard
- **Module 9 – Datasets and the Common Information Model**
  - - Naming conventions
  - - What are datasets?
  - - What is the Common Information Model (CIM)?
- **Module 10 – Creating and Using Lookups**
  - - Describe lookups
  - - Create a lookup file and create a lookup definition
  - - Configure an automatic lookup
- **Module 11 – Creating Scheduled Reports and Alerts**
  - - Describe scheduled reports
  - - Configure scheduled reports
  - - Describe alerts
  - - Create alerts
  - - View fired alerts
- **Module 12 - Using Pivot**
  - - Describe Pivot
  - - Understand the relationship between data models and pivot
  - - Select a data model object
  - - Create a pivot report
  - - Create an instant pivot from a search
  - - Add a pivot report to a dashboard

Day - 2

- **Splunk Intermediate**
  - This course focuses on searching and reporting commands as well as on the creation of knowledge objects. Major topics include using transforming commands and visualizations, filtering and formatting results, correlating events, creating knowledge objects, using field aliases and calculated fields, creating tags and event types, using macros, creating workflow actions and data models, and normalizing data with the Common Information Model (CIM).
- **Splunk Intermediate Course Topics**
  - Transforming commands and visualization
  - Filtering and formatting
  - Results
  - Correlating events
  - Knowledge objects
  - Fields (Field aliases, field extractions, calculated fields)
  - Tags and event types
  - Macros
  - Workflow actions
  - Data models
  - Splunk Common In
  - Formation Model (CIM)

- **Splunk Intermediate Course Objectives**
  - **Module 12 - Using Pivot**
    - Overview of Buttercup Games Inc.
    - Lab environment
  - **Module 2 Beyond Search Fundamentals**
    - Search fundamentals review
    - Case sensitivity
    - Using the job inspector to view search performance
  - **Module 2 Using Transforming Commands for Visualizations**
    - Explore data structure requirements
    - Explore visualization types
    - Create and format charts and time charts
  - **Module 3 Using Transforming Commands for Visualizations**
    - Explore data structure requirements
    - Explore visualization types
    - Create and format charts and time charts
  - **Module 4 Using Mapping and Single Value Commands**
    - The iplocation command
    - The geostats command
    - The geom command
    - The addtotals command

- **Module 5 Filtering and Formatting Results**
    - The eval command
    - Using the search and where commands to filter results
    - The filnull command
- **Module 6 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 7 Introduction to Knowledge Objects**
    - Identify naming conventions
    - Review permissions
    - Manage knowledge objects
- **Module 8 Creating and Managing Fields**
    - Perform regex field extractions using the Field Extractor (FX)
    - Perform delimiter field extractions using the FX
- **Module 9 Creating Field Aliases and Calculated Fields**
    - Describe, create, and use field aliases
    - Describe, create and use calculated fields
- **Module 10 Creating Tags and Event Types**
    - Create and use tags
    - Describe event types and their uses
    - Create an event type
- **Module 11 Creating and Using Macros**
    - Describe macros
    - Create and use a basic macro
    - Define arguments and variables for a macro
    - Add and use arguments with a macro
- **Module 12 Creating and Using Workflow Actions**
    - Describe the function of GET, POST, and Search workflow actions
    - Create a GET workflow action
    - Create a POST workflow action
    - Create a Search workflow action
- **Module 13 Creating Data Models**
    - Describe the relationship between data models and pivot
    - Identify data model attributes
    - Create a data model
    - Use a data model in pivot
- **Module 14 Using the Common Information Model (CIM) Add-On**
    - Describe the Splunk CIM
    - List the knowledge objects included with the Splunk CIM
    - Add-On
    - Use the CIM Add-On to normalize data

Day - 3

- **Splunk Enterprise System Administration**
  - This course is designed for system administrators who are responsible for managing the Splunk Enterprise environment. The course provides the fundamental knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.
- **Splunk Enterprise System Administration Course Topics**
  - Splunk Enterprise System Administration Course Topics
  - Splunk Deployment Overview
  - License Management
  - Splunk Apps
  - Splunk Configuration Files
  - Users, Roles, and Authentication
  - Getting Data In
  - Distributed Search
  - Introduction to Splunk Clusters

- **Splunk Enterprise System Administration Course Objectives**
  - **Module 1 Splunk Developer Overview**
    - Splunk overview
    - Identify Splunk components
    - Identify Splunk system administrator role
  - **Module 2 License Management**
    - Identify license types
    - Describe license violations
    - Add and remove licenses
  - **Module 3 Splunk Apps**
    - Describe Splunk apps and add-ons
    - Install an app on a Splunk instance
    - Manage app accessibility and permissions
  - **Module 4 Splunk Configuration Files**
    - Describe Splunk configuration directory structure
    - Understand configuration layering process
    - Use tool to examine configuration settings
  - **Module 5 Splunk Indexes**
    - Describe index structure
    - List types of index buckets
    - Create new indexes
    - Monitor indexes with Monitoring Console

- **Module 6 Splunk Index Management**
  - Apply a data retention policy
  - Backup data on indexers
  - Delete data from an index
  - Restore frozen data

- **Module 7 Splunk User Management**
  - Describe user roles in Splunk
  - Create a custom role
  - Add Splunk users

- **Module 8 Splunk Authentication Management**
  - Integrate Splunk with LDAP
  - List other user authentication options
  - Describe the steps to enable Multifactor Authentication in Splunk

- **Module 9 Getting Data In**
  - Describe the basic settings for an input
  - List Splunk forwarder types
  - Configure the forwarder
  - Add an input to UF using CLI

- **Describe how distributed search works**
  - Explain the roles of the search head and search peers
  - Configure a distributed search group
  - List search head scaling options

- **Module 10 Distributed Search**
  - Describe how distributed search works
  - Explain the roles of the search head and search peers
  - Configure a distributed search group
  - List search head scaling options

Day - 4

- **Using Splunk Enterprise Security**
  - This course prepares security practitioners to use Splunk Enterprise Security (ES). Students will use ES to identify and track security incidents, analyze security risks, use predictive analytics, and threat discovery.
- **Splunk Enterprise Security Course Topics**
  - ES concepts
  - Security monitoring and Incident investigation
  - Assets and identities
  - Detecting known types of threats
  - Monitoring for new types of threats
  - Using analytical tools
  - Analyze user behavior for insider threats
  - Use risk analysis and threat intelligence tools
  - Use protocol intelligence and live stream data
  - Use investigation timelines and journal tools
  - Build glass tables to display security status

- **Splunk Enterprise Security Course Objectives**
  - **Module 1 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
    - Describe user roles in ES
    - Log on to ES
  - **Module 2 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 3 – Investigations**
    - Use ES investigation timelines to manage, visualize and coordinate incident investigations
    - Use timelines and journals to document breach analysis and mitigation efforts
  - **Module 4 – Forensic Investigation with ES**
    - Nvestigate access domain events
    - Investigate endpoint domain events
    - Investigate network domain events
    - Investigate identity domain events

- **Module 5 – Risk and Network Analysis**
  - Understand and use Risk Analysis
  - Use the Risk Analysis dashboard
  - Manage risk scores for objects or users
- **Module 6 – 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 7 – 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
  - Use the session center for identity resolution (UBA integration)
- **Module 8 – 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 9 Protocol Intelligence**
  - Describe Stream events data is input into Splunk events
  - Use ES predictive analytics to make forecasts and view trends
- **Module 10 – Glass Tables**
  - Build glass tables to display security status information
  - Add glass table drilldown options
  - Create new key indicators for metrics on glass tables

Day - 5

- **Administering Splunk Enterprise Security**
  - This course prepares architects and systems administrators to install, configure and manage Splunk Enterprise Security. It covers ES event processing and normalization, deployment requirements, technology add-ons, settings, risk analysis settings, threat intelligence and protocol intelligence configuration, and customizations.
- **Administering Splunk Enterprise Security Course Topics**
  - Monitoring and Investigation
  - Security Intelligence
  - Forensics, Glass Tables and Navigation Control
  - ES Deployment
  - Installation and Configuration
  - Validating ES Data
  - Custom Add-ons
  - Tuning Correlation Searches
  - Creating Correlation Searches
  - Lookups and Identity Management
  - Threat Intelligence Framework

- **Administering Splunk Enterprise Security Course Objectives**
  - **Module 1 – ES Introduction**
    - Overview of ES features and concepts
  - **Module 2 Security Monitoring and Incident Investigation**
    - Security Posture
    - Incident Review
    - Notable events management
  - **Module 3 – Security Intelligence**
    - Overview of security Intel tools
  - **Module 4 – Forensics, Glass Tables and Navigation Control**
    - Explore forensics dashboards
    - Examine glass tables
    - Configure navigation and dashboard permissions
  - **Module 4 – Forensics, Glass Tables and Navigation Control**
    - Explore forensics dashboards
    - Examine glass tables
    - Configure navigation and dashboard permissions
  - **Module 5 – ES Deployment**
    - Identify deployment topologies
    - Examine the deployment checklist
    - Understand indexing strategy for ES
    - Understand ES Data Models

- **Module 6 – Installation and Configuration**
  - Prepare a Splunk environment for installation
  - Download and install ES on a search head
  - Test a new install
  - Understand ES Splunk user accounts and roles
  - Post-install configuration tasks
- **Module 7 – Validating ES Data**
  - Plan ES inputs
  - Configure technology add-ons
- **Module 8 – Custom Add-ons**
  - Design a new add-on for custom data
  - Use the Add-on Builder to build a new add-on
- **Module 9 – Tuning Correlation Searches**
  - Configure correlation search scheduling and sensitivity
  - Tune ES correlation searches
- **Module 10 – Creating Correlation Searches**
  - Create a custom correlation search
  - Configuring adaptive responses
  - Search export/import
- **Module 11 – Lookups and Identity Management**
  - Identify ES-specific lookups
  - Understand and configure lookup lists
- **Module 12 – Threat Intelligence Framework**
  - Understand and configure threat intelligence
  - Configure user activity analysis