INFOSECTRAIN

Splunk>

Practical Approach Training

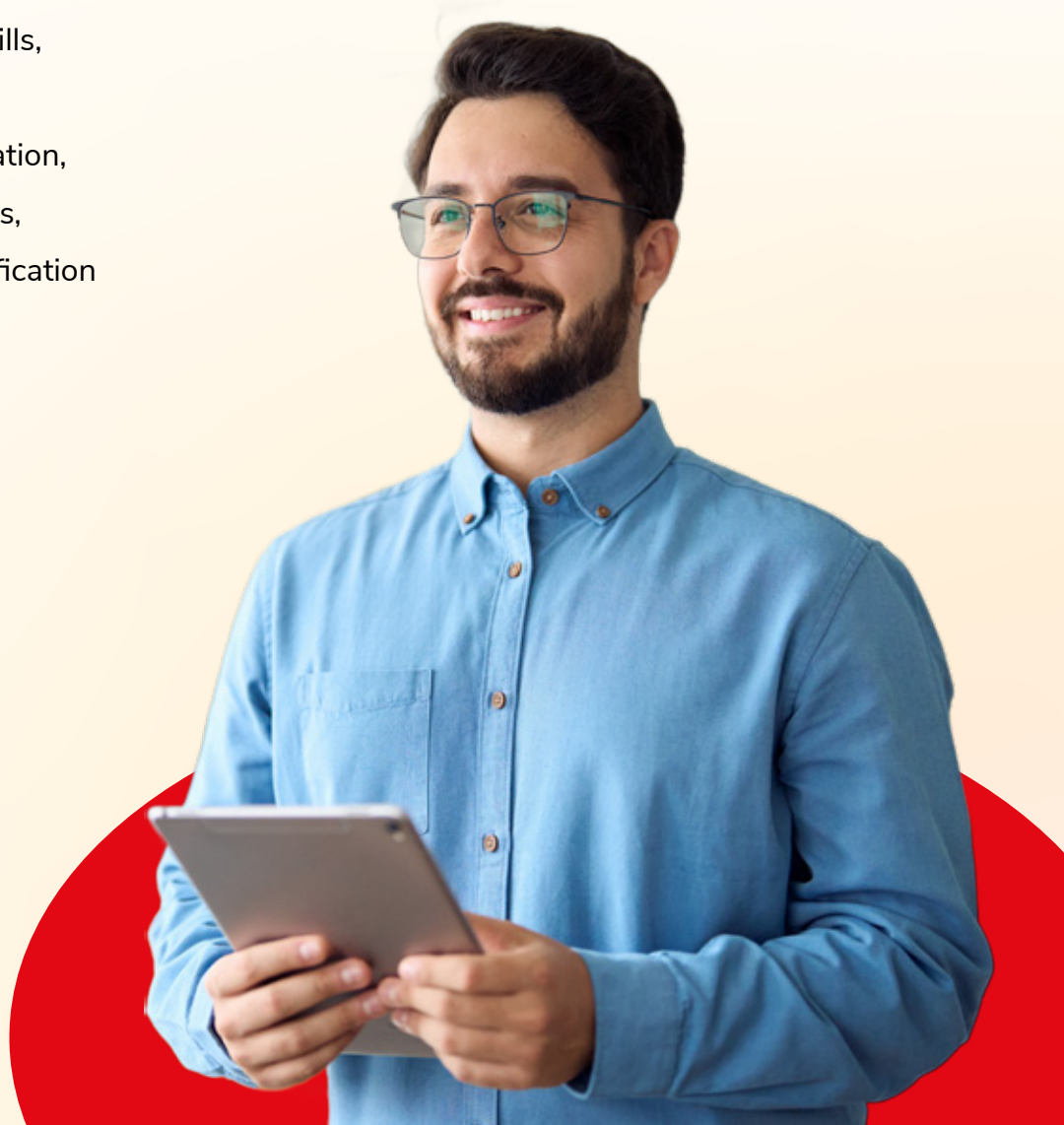
www.infosectrain.com

Course highlights

- **30-Hour LIVE** Instructor-led Training
- Learn from Industry Experts
- Highly Interactive and Dynamic Sessions
- Scenario-based Practical Approach
- Practical Examples from Real-world Case Studies
- Access to Recorded Sessions
- Extended Post-Training Support
- Career Guidance and Mentorship
- Immersive Learning

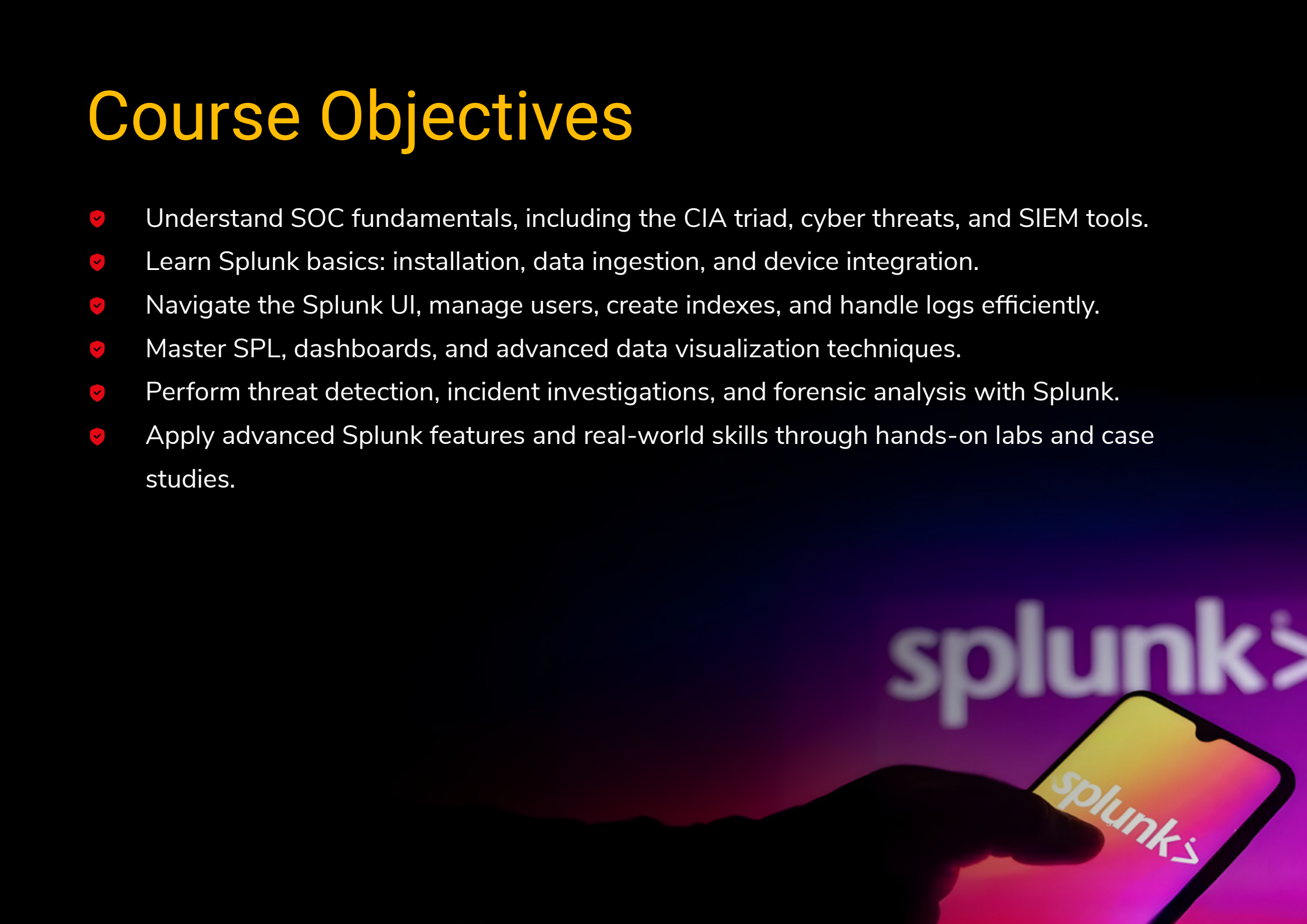
About Course

The Splunk Online Training course by InfosecTrain is tailored for IT and security professionals aiming to master data analytics with Splunk. This comprehensive course covers essential data monitoring and analysis skills, enabling participants to use Splunk for effective cybersecurity and IT operations. Key topics include advanced search functions, data visualization, and threat detection techniques. Through practical labs and case studies, participants gain hands-on experience, preparing them for Splunk certification and for real-world applications in data-driven security environments.



Course Objectives

- Understand SOC fundamentals, including the CIA triad, cyber threats, and SIEM tools.
- Learn Splunk basics: installation, data ingestion, and device integration.
- Navigate the Splunk UI, manage users, create indexes, and handle logs efficiently.
- Master SPL, dashboards, and advanced data visualization techniques.
- Perform threat detection, incident investigations, and forensic analysis with Splunk.
- Apply advanced Splunk features and real-world skills through hands-on labs and case studies.



Target Audience

- Security Analysts
- IT Operation Staff
- Data Analysts
- Managers and Consultants
- Beginners and IT students

Pre-Requisites

- Basic understanding of network essentials, including OSI layer concepts.
- Knowledge of fundamental logical operations and digital communication concepts.

Course Content

Module 01

Security Operations Center Concepts

- CIA Triad: Confidentiality, Integrity, Availability in SOC operations
- Concepts of Encryption, Hashing with practical demonstration via tool
- SOC Overview: Definition, purpose, objectives (monitoring, detection, response)
- Common Attacks: DDoS, Ransomware, Malware, Phishing, Brute-force attacks
- Definition of SIEM Solution, working mechanism of SIEM tools
- Introduction to SPLUNK and its features as a SIEM Solution, AI integrated features of SPLUNK for user entity and behavior analysis

Module 02

Fundamentals of Networking and Cyber Security Devices

- Detailed understanding of networking concepts (protocols/ports) in collaboration with OSI model
- Basic Concepts of Security Devices: Anti-Virus (EPP), Next generation anti-virus (EDR), Firewall, WAF, IDS, IPS, Anti-defacement solution
- Understanding the concepts of cyber hygiene integrated with SPLUNK

Module 03

Introduction to SPLUNK and Device Integration/Log Ingestion

- Introduction to Splunk Enterprise
- Introduction to Splunk Enterprise Security
- Splunk Enterprise Practical Lab Environment Setup
- Introduction of SPLUNK Components
- Creation of Indexes
- Integration Of Various devices with Splunk such as Windows, Unix, Firewall Syslog, Application and Database logs

Module 04

Introduction to SPLUNK User Interface and Admin Stuffs

- Customizing the user settings
- Learn basic navigation in Splunk
- Understanding various components of Splunk
- Various deployment Architecture of Splunk
- User Creation, assigning responsibilities, changing the roles of existing users and deletion of existing users, changing passwords of the existing users if users forget the existing passwords

Module 05

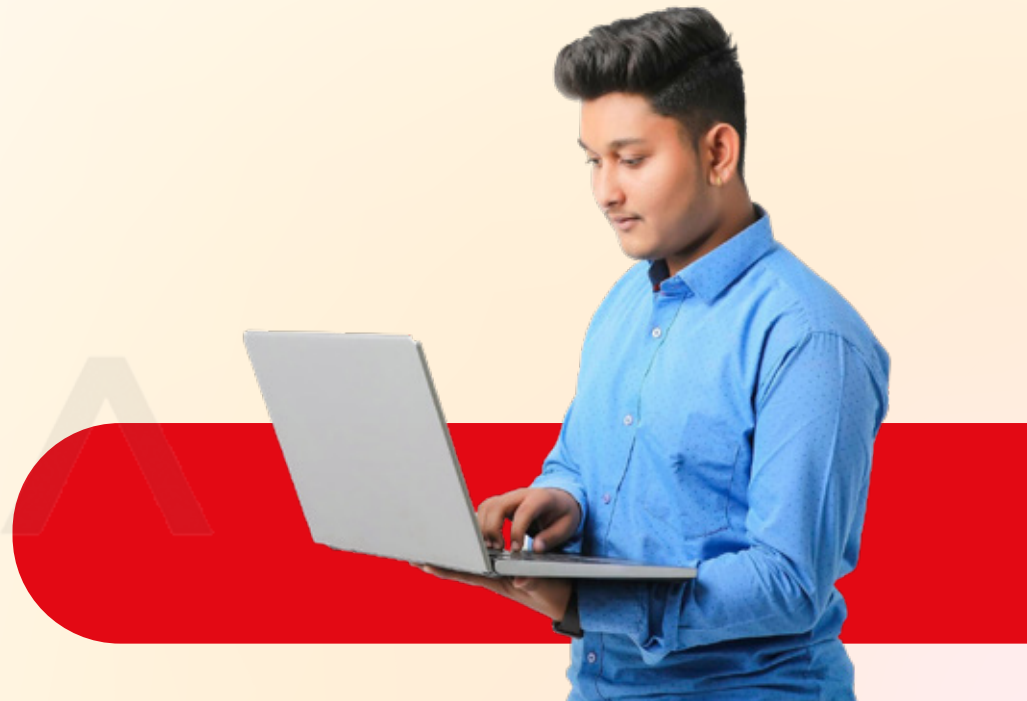
Introduction to SPLUNK Basic Configuration and Splunk AI

- Integrated Architecture
- Introduction to Splunk Configuration files
- Introduction to Splunk Universal Forwarder
- Introduction to Splunk Forwarder management
- Introduction to Splunk Data management
- Introduction to Splunk Troubleshooting and monitoring
- Concepts of Clustering: Search head clustering, index clustering, forward clustering for single-site deployment and multi-site deployment in on-prem and hybrid cloud environment

Module 06

Introduction to Fields and Table Commands

- What is a Field
- Use Fields in search
- Deploying Fields Sidebar
- Understanding the default fields and interesting fields
- Field Extractor for REGEX field extraction Delimiting Field Extraction using FX



Module 07

Introduction to SPLUNK Searching Processing Language (SPL)

- Introduction to Splunk Search Commands
- Writing Splunk query for search
- Learn Write basic search queries
- Use autocompletes to help build a search
- Identify the contents of search results
- Set time range of a search, refine search, working with events
- Identifying the contents of search and controlling a search job

Module 08

Introduction to Transforming Commands

- Introduction to Splunk Transforming Commands and resolving use cases for real-time incident scenarios:

✓ Stats	✓ List
✓ Countchart	✓ Search
✓ Timechart	✓ Where
✓ Dedup	✓ Sort
✓ DC	✓ Max
✓ Top	✓ Min
✓ Rare	✓ Avg
✓ Limit	✓ Eval

- Investigation of brute force attack using SPLUNK commands in collaboration with Virus Total and AbuseIPDB tools

Module 09

Case Analysis with SPLUNK

- Analysis of data to understand the gravity of the incident
- Data interpretation to understand the false positive and true positive alerts
- Usage of Splunk to understand the DOS attack
- Queries in SPLUNK to understand the load average of the server

Module 10

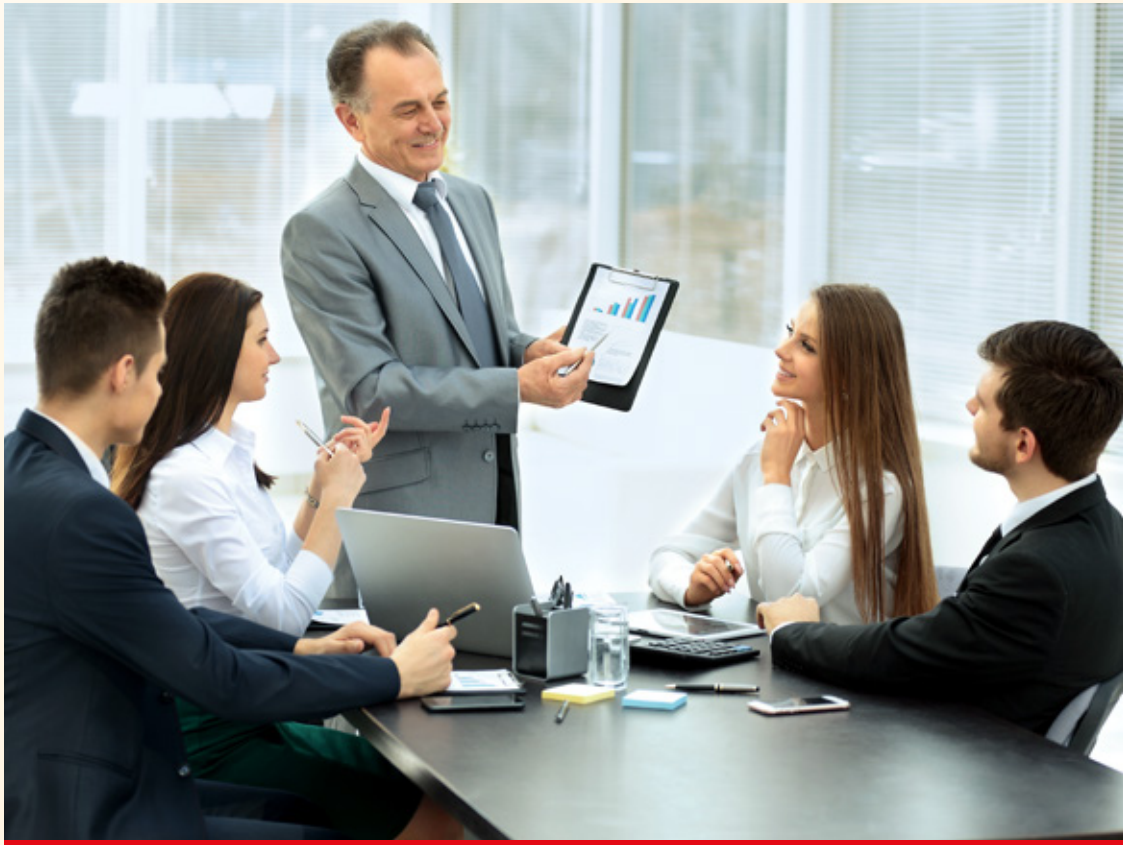
Creating and Using Macros

- What is a Macro
- How to define and invoke a macro
- Arguments in Macros
- Creation of use cases using macros

Module 11

Creating and Using Lookups

- Describe lookups
- Create a lookup file and create a lookup definition
- Configure an automatic lookup
- Case study analysis using Lookups



Module 12

Creation of Pivots and Data model

- Describe Pivot and Data model
- 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

Module 13

Creation of Reports and Dashboards

- Save a search as a report and 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 14

Investigation and Monitoring

- How to monitor the dashboard and brief on each panel
- Investigating notable events with incident review dashboards
- Workflow investigation and relative action on identified flow

Module 15

Splunk Advanced Searches and Mechanisms

- Common Information Model
- Analysis of Cyber Incidents like: Vulnerability scanner detected, unhandled malware detected in the end-point devices, sink-hold DNS queries detected, IPDS threat detected, network scanning detected, country-wise statistics of unauthorized connections over the server or network level.
- Concepts of Unscheduled downtime: Full unscheduled downtime, partial unscheduled downtime and intermittent downtime, business performance/loss incurred due to unscheduled downtime

Module 16

Next Generation Threat Hunting Framework Integrated with Splunk

- Concepts of Cyber 360 framework
- Next generation Threat Hunting Framework
- Splunk Integration with Threat Hunting Mechanism

Module 17

Email Forensic Integrated with Splunk

- Concepts of Email Forensic
- Introduction of DMARC, DKIM and SPF
- Diagrammatic representation of email communication through SMTP and POP3 protocol
- Understanding the vulnerability of Email communication
- Splunk Integration with MXTOOLBOX for IP checking and email domain analysis

Module 18

Interview Questions and QA Session

- Distribution of latest interview questions with unique solutions for Splunk and SOC profiles
- End Term quiz consisting of 50 latest questions
- Interview Questions for Infosec Profiles and Security Delivery Manager roles

INFOSECTRAIN

Educate. Excel. Empower.

www.infosectrain.com

sales@infosectrain.com