Splunk Enterprise Architecture (5D TOC)

Day 1: Introduction to Splunk Enterprise Architecture

- Overview of Splunk Architecture
- Introduction to Splunk components (Indexer, Search Head, Forwarder, Deployment Server)
- Data ingestion and processing pipeline
- Licensing model and deployment options (Single-instance, distributed, clustered)
- Splunk Installation and Configuration
- Installation of Splunk on Linux/Windows
- Basic Splunk configuration (inputs.conf, outputs.conf)
- Initial setup and basic commands
- Introduction to Data Onboarding
- Overview of data sources and inputs
- File and directory monitoring
- Network and system data inputs

Day 2: Data Management and Indexing

- Data Parsing and Indexing
- Data input processing: Parsing, Indexing, Searching
- Configure Parsing at HF and Indexer End
- Search time Parsing of Data
- Configuration files (props.conf, transforms.conf)
- Null Queue Concept
- Managing indexes and indexer clustering
- Data Enrichment

• Field extraction, lookups, and event types
• Working with Splunk's Common Information Model (CIM)
• Data normalization and tagging
• Optimizing Data Ingestion
• Forwarder management and data routing
• Load balancing and throttling
• Troubleshooting data ingestion issues
• Troubleshooting using btool

Day 3: Search and Reporting

• Advanced Search Techniques
• Search commands and functions
• Subsearches, joins, and transactions
• Using fields, tags, and event types in searches
• Building Dashboards and Reports
• Creating visualizations and dashboards
• Building advanced reports and alerts
• Performance optimization of searches and dashboards
• Search Head Clustering
• Overview of Search Head clustering
• Deploying and managing a Search Head cluster
• Load balancing and failover configurations

Day 4: Advanced Splunk Administration

• Data Models and Pivot
• Creating and managing data models
• Using Pivot for report generation

- Performance considerations for large data models
- Managing Large-Scale Deployments
- Indexer clustering and high availability
- Deploying and managing multisite clusters
- Backup, restore, and disaster recovery strategies
- Splunk Apps and Add-ons
- Installing and managing Splunkbase apps
- Developing custom apps and add-ons
- App deployment and best practices

Day 5: Security, Scaling, and Performance Tuning

- Security and Access Controls
- User roles, authentication, and authorization
- Securing data and configurations
- Monitoring and auditing Splunk environments
- Performance Tuning and Monitoring
- Indexer and search head performance optimization
- Resource allocation and tuning (CPU, Memory, Disk I/O)
- Using Monitoring Console for environment health checks
- Scaling Splunk Architecture
- Horizontal and vertical scaling strategies
- Managing and scaling data volumes
- Planning for future growth and capacity

Wrap-Up and Q&A

- Review of key concepts and advanced topics
- Q&A session