Splunk Administration & SIEM

Prerequisites :

1. Basics Of Linux command
2. SIEM concepts

Duration: 6 Days

**Day 1**

**1st Half :**

**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: Installing Splunk**

How should Splunk be configured

Identifying Splunk instance types

Hardware recommendations Indexers

Hardware recommendations Search Heads

Splunk Installation Packages

Supported platforms and browsers

Splunk Installation

Splunk directory structure

The Splunk CLI

\*NIX Run Splunk at boot

Splunk windows services

Splunk Processes: Splunkd

Splunk Processes: Splunkweb

Apps Installed by default

System Settings

Describing General Settings

Restarting the server from Splunk Web

**Use Case :**

* **Splunk Infrastructure Setup**

**2nd Half :**

**Module 3: Universal Forwarders**

* Forwarders and Indexers
* Benefits of using forwarders
* Splunk Universal Forwarder
* Splunk Heavy Forwarder
* Integration of Devices using HF and API based integration
* Configuration Steps
* Configuring the receiving port
* Downloading the universal forwarder installer
* Installing Universal Forwarder manually
* Forwarder configuration files

**Use Case :**

* **Ingest Some data using api**

**Module 4: Basic Data Input**

How can you tell what app you are in

Adding your monitor input

Specify the source

Select Host, Sourcetype and Index

**Use Case :**

1. **Basic and Advanced Onboarding**

**Pre Training Assessment will be conducted**

**Day2**

**1st Half :**

**Module 5 : Manipulating Raw Data**

➢ Explain how data transformations are defined and invoked

➢ Use transformations with props.conf and transforms.conf to:

o Mask or delete raw data as it is being indexed Override sourcetype or host based upon

event values

➢ Route events to specific indexes based on event content

➢ Prevent unwanted events from being indexed

➢ Use SEDCMD to modify raw data

**Use Case :**

1. **Line Breaking**
2. **Masking**
3. **Data Routing Filtering**

**Module 6: Splunk configuration files**

* Configuration directories
* Default vs. local configuration
* Default context vs. user or App context

**2nd Half :**

**Module 7: Deployment Server**

* Role of Deployment Server
* Deployment Clients
* Deploying Apps via DS
* Handling Configuration files via DS

**Use Case :**

1. **Deploy an app to deploy client to onboard data**

**Module 8: License Management**

* Managing Licenses
* Splunk license types
* Adding a license
* License warnings and violations
* What counts as daily license quota
* Viewing alerts
* License Stacking
* Master License Server
* License Pooling

**Day3**

**1st Half :**

**Module 9: Managing Apps**

What is an App?

Apps configured by Default

Viewing all apps

Managing Apps

Installing an App manually

Enabling and Disabling apps

Deleting an App

App permissions

**Use Case:**

1. **Install App**
2. **Delete App**

**Module 10: Splunk Users and Roles**

* About Splunk roles
* Creating new users
* Assigning user roles

**Use Case:**

1. **Create an user**
2. **Create a role**

**2nd Half :**

**Module 11 : 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 12: Using Fields in Searches**

➢ Understand fields

➢ Use fields in searches

➢ Use the fields sidebar

**Module 13 : 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

**Use Case :**

1. **Based on the commands use case will be provided**

* Top
* Rare
* Stats
* Timechart

**Day 4**

**1st Half :**

**Module 14: Creating Reports & Alert and Visualizations**

* Save a search as a report
* Edit reports
* Create reports that include visualizations such as charts and tables
* Add reports to a dashboard
* Create Alert
* Schedule Alerts

**Use Case :**

1. **Create a report**
2. **Create an Alert**
3. **Write Cron Schedule**
4. **Use webhook**

**2nd Half :**

**Module 15: Working with Dashboards**

* Creating a dashboard
* Add a reports to a dashboard
* Edit a dashboard

**Use Case:**

1. **Create a dashboard**
2. **Change the permissions of the dashboard**
3. **Clone a dashboard**

**Module 16 : Lookups**

➢ Lookup Table

➢ Lookup Definition

➢ Automatic Lookup

**Use Case:**

1. **Create lookup**
2. **Work with inputlookup , outputlookup and lookup command**

**Day 5**

**1st Half :**

**Module 18 – ES Introduction**

➢ Overview of ES features and concepts

* CIM model

**Module 19 - 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

**Use Case :**

1. **Make data sources as CIM compliant**

**2nd Half :**

**Module 20 – Tuning Correlation Searches**

➢ Configure correlation search scheduling and sensitivity

➢ Tune ES correlation searches

**Use Case :**

**1} Configure correlation searches**

**2) Configure Scheduling**

**3) Use proper time window**

**Day 6**

**1st Half :**

**Module 21 – Creating Correlation Searches**

➢ Create a custom correlation search

➢ Configuring adaptive responses

➢ Search export/import

**Use Case :**

1. **Create custom correlation search**
2. **Trigger incident using those correlation search**

**2nd Half :**

**Module 22 - 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

**Use Case :**

1. **Triage notable events**
2. **Supress Notable events**

**Post Training Assessment will be conducted**