Splunk Training (5 Days)

Day 1: Managing the Splunk Platform

1. **Introduction to Splunk Architecture**
    - Overview of Splunk components: Indexers, Search Heads, Forwarders, Deployment Servers
    - Role of Heavy Forwarders, Aggregators, and DCN Servers in the Splunk ecosystem

2. **Managing Splunk Users & Roles**
    - User management and role-based access control (RBAC)
    - Assigning roles and permissions for L2 tasks

3. **Splunk Configuration Management**
    - Configuration files: inputs.conf, props.conf, outputs.conf
    - Using Deployment Server to manage forwarders

4. **Hands-on Lab: Platform Setup & Configuration**
    - Configure users and roles
    - Manage Splunk settings using configuration files

Day 2: Managing Forwarders and Data Intake 5. **Understanding Forwarders and Data Routing**

- Types of forwarders: Universal and Heavy Forwarders
- Configuring forwarders to route data to indexers
- Monitoring forwarder status using the Deployment Monitor App

6. **Forwarder Management Tasks**
    - Best practices for managing and troubleshooting forwarders
    - Validating forwarder connections and ingestion health

7. **Managing Data Inputs**
    - Setting up data sources: File monitoring, syslog, and network inputs

- Ensuring proper data ingestion with the correct sourcetypes
- Troubleshooting data ingestion issues

8. **Hands-on Lab: Managing Forwarders and Data Intake**
    - Configure forwarders to ingest data from different sources
    - Monitor and troubleshoot forwarder performance

Day 3: Validating Firewall Changes and Log Review 9. **Understanding Firewall Logs in Splunk**

- Common firewall log formats (e.g., Cisco ASA, Palo Alto)
- Parsing and indexing firewall logs for analysis

10. **Validating Firewall Changes**

- How to validate new log ingestion after firewall rule changes
- Searching and filtering logs to verify firewall rule implementations

11. **Troubleshooting Data Ingestion after Firewall Changes**

- Identifying ingestion issues due to firewall misconfigurations
- Using SPL queries to pinpoint errors

12. **Hands-on Lab: Firewall Log Review**

- Simulate firewall log ingestion and validate changes using Splunk

Day 4: Splunk Server Patching & Health Monitoring

13. **Splunk Server Patching: Heavy Forwarder & Aggregator**

- Best practices for patching Heavy Forwarders and Aggregator/DCN Servers
- Pre- and post-patching validation steps

14. **Monitoring Splunk Server Health Post-Patching**

- Checking log ingestion, forwarder status, and search performance after patching
- Using Monitoring Console to track server health

15. **Troubleshooting Issues Post-Patching**

- Common issues related to patching (e.g., service interruptions, log ingestion failure)
- Hands-on troubleshooting methods

16. **Hands-on Lab: Simulated Patching and Validation**

- Simulate patching Heavy Forwarders and validate post-patch log ingestion

Day 5: Advanced Troubleshooting, SPL Commands, and Best Practices

17. **Advanced Troubleshooting Techniques**

- Using internal logs (_internal index) to diagnose issues
- Monitoring and resolving performance bottlenecks (CPU, memory, disk)

18. **Automating Tasks for L2 Support**

- Automating monitoring and alerts for forwarders, ingestion issues, and patch validation
- Setting up alerts to track firewall log ingestion and forwarder status

19. **Best Practices for Splunk Administration**

- Ensuring data consistency and availability across Splunk components
- Planning and preparing for large-scale deployments

20. **Dashboard Studio and Classic Dashboard Base Search Creation**

- Introduction to dashboarding in Splunk
- Using base searches for creating dashboards
- Differences between Dashboard Studio and Classic Dashboards

21. **Data Analysis Using SPL Commands**

- Overview of SPL (Search Processing Language)
- Common SPL commands for data analysis
- Using SPL for troubleshooting and validating data

22. **Props Creation (Magic 8 Elements)**

- Understanding the purpose of props.conf
- Key elements for defining data parsing rules
- Examples of props.conf configurations

23. **Hands-on Capstone Lab: End-to-End Splunk Environment Validation**

- Simulate an L2 scenario with platform management, firewall log validation, and post-patching health checks
- Validate the environment and resolve any issues found

Summary

- Day 1: Splunk platform management, user roles, and configuration
- Day 2: Forwarder management, data intake setup, troubleshooting ingestion
- Day 3: Firewall log review and validation post-firewall changes
- Day 4: Server patching and post-patch health checks for Heavy Forwarders and Aggregators
- Day 5: Advanced troubleshooting, SPL commands, dashboarding, and best practices