deerwalk
training center

DTI - SPU- 101

Splunk Proficiency Course: From Core Functions to Cutting-Edge Integration Training

deerwalktrainingcenter.com

Program Information

Nature of the Course
Theory + Practical

Total Hours per Day
8 hours

Course Duration
3 Days

Course Summary

The Splunk course provides an in-depth understanding of how to use Splunk software for searching, monitoring, and analyzing machine-generated big data. This course covers key features of Splunk, such as indexing, searching, data visualization, and creating meaningful reports. Participants will learn how to leverage Splunk to gain insights from logs and data across their IT infrastructure, helping organizations monitor performance, security, and operational health.
By the end of the course, participants will have the ability to set up and configure Splunk environments, interpret and analyze data, build dashboards and alerts, and implement best practices for managing Splunk deployments. This course is ideal for IT professionals, security experts, and data analysts who want to enhance their ability to manage and analyze vast amounts of machine-generated data.

Completion Criteria

After fulfilling all of the following criteria, the student will be deemed tohave finished the Module:

- Has attended 90% of all classes held.

Required Textbooks

- No textbooks are required

Prerequisites

- Basic understanding of IT infrastructure, system administration, and networking is recommended. Familiarity with concepts such as logs, monitoring, and data analysis will be helpful.
- While no formal certifications are required, knowledge of basic scripting or programming concepts and experience with data management tools can enhance the learning experience.

Course Details

Day 1 : Introduction, Installation, and Core Splunk Skills (8 Hours)

Session 1: Introduction to Splunk and Big Data Analytics (2 Hours)

- Understanding Big Data and Its Importance
- Introduction to Splunk: Overview, Use Cases, and Key Features
- Splunk Architecture and Components
- Understanding Splunk Licensing Models

Session 2: Installing and Configuring Splunk (3 Hours)

- Installing Splunk on Different Platforms
- Initial Configuration: Splunk Web, User Roles, Basic Settings
- Data Onboarding: Adding Data Sources and Configuring Inputs
- Hands-On Lab: Installing and Configuring Splunk, Onboarding Data

Session 3: Mastering Splunk Search Processing Language (SPL) - Part 1 (3 Hours)

- Introduction to SPL: Commands, Functions, and Operators
- Transforming Commands: Using stats, eval, table, timechart, and top
- Advanced Searching Techniques: Subsearches, Joins, and Transactions
- SPL Best Practices and Query Optimization
- Hands-On Lab: Performing Searches, Creating Complex Queries

---

Day 2: Advanced Splunk Usage, Monitoring, and Security (8 Hours)

Session 4: Mastering SPL - Part 2 & Building Reports and Dashboards (2 Hours)

- Advanced Searching Techniques (Continued)
- Building Reports: Creating, Saving, and Customizing Reports
- Creating Dashboards: Single Value, Table, Chart, and Event Viewers
- Advanced Dashboards: Dynamic and Interactive Dashboards, Drill-Downs, Tokens
- Hands-On Lab: Creating Reports and Interactive Dashboards

Session 5: Data Models, Pivot, and Real-Time Monitoring (2 Hours)

- Understanding Big Data and Its Importance
- Introduction to Splunk: Overview, Use Cases, and Key Features
- Splunk Architecture and Components
- Understanding Splunk Licensing Models

Session 6: Security, Compliance, and Alerts in Splunk (2 Hours)

- Using Splunk for SIEM: Security Information and Event Management Best Practices
- Compliance Monitoring: Building Compliance Dashboards and Reports
- Creating Alerts: Real-Time and Scheduled Alerts, Configuring Actions
- Incident Response: Investigating and Responding to Security Incidents
- Hands-On Lab: Setting Up a SIEM Dashboard, Configuring Alerts, Simulating Incident Response

---

Day 3: Administration, Integration, and Advanced Topics (8 Hours)

Session 7: Splunk Administration and Maintenance (3 Hours)

- Splunk Deployment Models: Single-Instance, Distributed, and Clustering
- User and Role Management: Implementing Role-Based Access Control (RBAC)
- Managing Splunk Indexes: Creating, Managing, and Optimizing Indexes
- System Maintenance: Monitoring Performance, Backup, and Recovery Procedures
- Hands-On Lab: Performing Administrative Tasks, Managing Roles, Optimizing Splunk

Session 8: Integrating Splunk with Other Systems (3 Hours)

- Integrating with Cloud Services: AWS, Azure, GCP
- APIs and SDKs: Using Splunk REST API and SDKs for Custom Integrations
- Data Forwarding and Receiving: Configuring Splunk Forwarders, Third-Party Data Integration
- Extending Splunk with Apps and Add-Ons: Overview of Splunkbase, Custom App Development
- Hands-On Lab: Integrating Splunk with Cloud Services, Using REST API, Installing Splunk Apps

---

Session 9: Advanced Topics and Final Project (2 Hours)

- Splunk Clustering and Scaling: Indexer and Search Head Clustering, Scaling Best Practices
- Advanced Data Parsing and Indexing: Customizing Data Parsing, Advanced Indexing Techniques
- Machine Learning in Splunk: Using Splunk's Machine Learning Toolkit (MLTK)
- Final Project: Implementing a Real-World Splunk Solution
- Assessment: Project Presentations, Feedback, and Evaluation

Conclusion and Certification Guidance (1 Hour)

- Course Wrap-Up: Review of Key Topics, Final Q&A Session
- Certification Guidance: Information on Splunk Certification Paths, Next Steps for Learning

---

Labs

Lab assignments will focus on the practice and mastery of contents covered in the lectures, and introduce critical and fundamental problem solving techniques to the students.

Learning Outcomes

- Develop client-server communication models for network analysis and security.
- Perform network operations like host discovery, DDoS attacks, port scanning, and HTTP traffic sniffing with Scapy.
- Create automated scripts for brute-force attacks, SQL injections, XSS scans, and web crawling.
- Build custom exploits, reverse shells, and perform privilege escalation with Python and Metasploit.
- Identify and exploit web app vulnerabilities using Burp Suite, Nessus, and John the Ripper.
- Perform privilege escalation, domain attacks, and pivoting through SSH with Metasploit and Impacket.
- Test for vulnerabilities like broken authentication, SQL injection, and remote code execution using OWASP ZAP and W3af.
- Generate penetration test reports and analysis using Python libraries like Pandas, Plotly, and NLTK.

deerwalk
training center

Sifal, Kathmandu, Nepal
Phone: +977 - 01 - 5913021 | 4567153
Mobile: +977 - 9765355167 | 9860422021
Email: training@deerwalkcompware.com
Website: deerwalktrainingcenter.com