CYBER DEFENTECH

splunk>

Practical Training

Hands-on SIEM & XDR SOC Training

DETECT | MONITOR | RESPOND



www.cyberdefentech.com

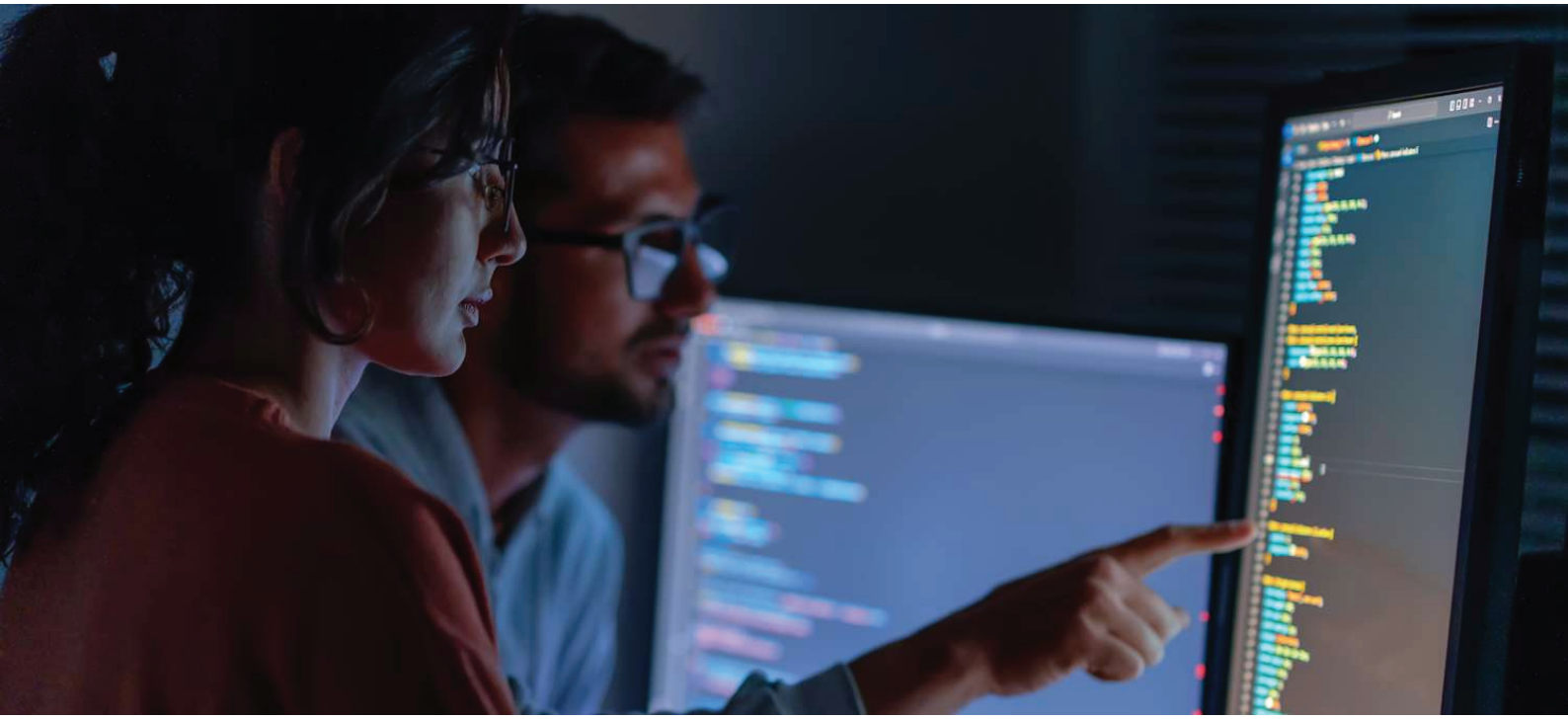
About Course

This course provides a comprehensive introduction to Splunk, a powerful platform used for searching, analyzing, and visualizing machine-generated data in real time. Learners will gain hands-on experience in log management, data ingestion, dashboards creation, alerting, and security monitoring. The course is designed to help you understand how organizations use Splunk for IT operations, cybersecurity, and data-driven decision-making. By the end of this course, you will be able to efficiently analyze data, detect anomalies, and build insightful dashboards for real-world use cases.



Course Objectives

- Gain deep understanding of Splunk architecture and components
- Learn end-to-end data pipeline: ingestion, parsing, indexing, and searching
- Master SPL (Search Processing Language) for advanced data analysis
- Build interactive dashboards and meaningful data visualizations
- Implement real-time monitoring and alerting mechanisms
- Perform log analysis for IT operations and cybersecurity use cases
- Correlate data from multiple sources for anomaly and threat detection
- Optimize searches for performance and efficiency



Target Audience

- Cybersecurity Beginners & Students
- SOC Analysts (Security Operations Center)
- IT Support & System Administrators
- Network Security Engineers
- DevOps & Cloud Engineers
- Security Analysts & Incident Response Teams
- Data Analysts interested in log analysis
- Professionals looking to upskill in SIEM tools
- Anyone interested in IT operations and security monitoring

Pre-Requisites

- Basic understanding of IT concepts and systems
- Familiarity with Linux or Windows operating systems
- Basic knowledge of Networking (IP, ports, protocols)
- Understanding of logs and system events (basic level)
- Awareness of Cybersecurity fundamentals
- Basic command-line usage (CLI) knowledge
- Virtual machine setup knowledge (VMware / VirtualBox)
- No prior Splunk experience required (for beginner courses)

Course Content

Module 1: Splunk Architecture & Configuration

- **The Splunk Data Pipeline:** Understanding how data flows from Input → Parsing → Indexing → Search.
- **Key Components:** The specific roles of Search Heads, Indexers, and Universal Forwarders.

Module 2: Data Onboarding & Ingestion

- **Indexing Strategy:** Creating and managing indexes to optimize data retention and search speed.
- **Universal Forwarders (UF):** Best practices for installing and configuring UFs to ship logs securely.
- **Onboarding Security Evidence:**
  - **Endpoints:** Windows Event Logs and Linux OS logs.
  - **Network/Web:** Apache/Nginx Web Server logs and CSV-based data.
- **Custom Data Sources:** Techniques for reliably onboarding proprietary or non-standard log formats.
- **Field Extraction:** Mastering the Extraction of meaningful fields from raw data streams to make them searchable.

Module 3: Finding and Exploring Data (SPL Mastery)

- **Search Fundamentals:** Understanding Fast, Smart, and Verbose search modes.
- **Data Organization:** Using FIELDS, TABLE, and SORT to refine your view.
- **Outlier Detection:** Identifying uncommon values with the TOP and RARE commands.
- **Calculations & Formatting:**

  Endpoints: Windows Event Logs and Linux OS logs.

  Network/Web: Apache/Nginx Web Server logs and CSV-based data.
- **Visualization Commands:** Transforming raw data into visual trends with CHART and TIMECHART.
- **Query Optimization:** Writing efficient SPL to maximize performance and minimize system load.

Course Content

Module 4: Enrichment & Advanced Analytics

- **Data Enrichment:** Using internal and external Lookups to add context (e.g., matching IPs to Threat Intel lists).
- **Subsearches:** Leveraging the results of one search to filter another (searching within searches).
- **Automation:**
  - Saving and sharing search results with other analysts.
  - Creating ad-hoc and scheduled reports for management.
  - Developing real-time and scheduled alerts for incident response.

Module 5: Visualization & Dashboards

- **Dashboard Basics:** Building static dashboards to monitor security KPIs.
- **Dynamic Views:** Creating interactive dashboards with time-range pickers and user inputs.
- **Custom Drilldowns: B**uilding workflows that allow analysts to pivot from a high-level chart directly into raw search results.
- **Dashboard Studio:** Using Splunk's visual editor to create modern, high-fidelity security operations center (SOC) displays.

Module 6: Real-World Security Scenarios (Hands-on Labs)

- **Phishing Investigation:** Identifying look-a-like/typosquatting domains in web traffic**.**
- **Authentication Hunting:** Finding the first time a user logged into a specific system on the network.
- **Brute Force Detection:** Identifying password guessing attempts by correlating failed logons.
- **Evasion Detection:** Finding direct HTTP connections to IP addresses instead of domain names.
- **Exfiltration Analysis:** Detecting high network bandwidth consumption relative to an established baseline.
- **Multi-Source Hunting:** Correlating indicators of compromise (IoCs) across multiple data streams simultaneously.

CYBER DEFENTECH



Follow us on