SPLUNK TRAINING

Splunk Fundamentals 3 Training Certification Course

Advance your Splunk skills. Master advanced searching, reporting, and dashboard creation in Splunk Fundamentals 3 to analyze complex data.

DURATION
2 hours

LEVEL
Intermediate

FORMAT
Instructor-Led

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

The Splunk Fundamentals 3 Training Certification Course is designed for professionals looking to master advanced data analysis and operational intelligence within the Splunk platform. Building upon the foundational knowledge of Splunk Fundamentals 1 and 2, this intermediate-level course dives deep into sophisticated search commands, data model creation, pivot table utilization, and advanced dashboarding techniques. Participants will learn to extract deeper insights from their data, optimize search performance, and implement robust alerting mechanisms to proactively monitor complex IT environments.

This certification equips you with the expertise to tackle challenging data analysis scenarios, enhance security postures, and improve operational efficiency across an organization. By mastering the core technologies of Splunk Enterprise's Search Processing Language (SPL) at an advanced level, you will gain the ability to create impactful reports, design interactive dashboards, and leverage data models for expedited incident response and forensic analysis. This course is crucial for anyone aspiring to become a power user or a key contributor in a Splunk-driven environment, enabling you to transform raw data into actionable intelligence and drive informed decision-making.

Duration	2 hours
Level	Intermediate
Vendor	Splunk

COURSE CURRICULUM

01 Module 1: Advanced Search Commands and Functions

- Review of basic search commands
- Understanding eval commands for field manipulation
- Using join and append for combining data
- Implementing transaction and subsearch commands
- Advanced statistical and reporting commands (top, rare, stats, chart)

02 Module 2: Data Models and Pivot Tables

- Introduction to Splunk Data Models
- Creating and managing data model objects (datasets, fields)
- Utilizing Splunk Pivot for interactive data exploration
- Building reports and visualizations from data models via Pivot
- Accelerating data models for performance

03 Module 3: Advanced Dashboards and Visualizations

- Designing interactive dashboards
- Incorporating advanced visualizations (treemaps, choropleth maps, gauges)
- Using forms and inputs for dynamic dashboards
- Working with drilldowns and external links
- Optimizing dashboard performance and user experience

04 Module 4: Alerts, Workflow Actions, and Macros

- Configuring scheduled alerts and real-time alerts
- Setting up trigger conditions and alert actions (email, script, webhook)
- Understanding workflow actions for quick investigations
- Creating and utilizing search macros for efficiency

- Managing alert suppression and throttling

05 Module 5: Search Optimization and Best Practices

- Strategies for optimizing search performance
- Understanding search processing order
- Leveraging indexes and time ranges effectively
- Best practices for writing efficient SPL
- Troubleshooting common search performance issues

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Splunk Power User / Advanced Analyst**

> **Security Operations Center (SOC) Tier 2 Analyst**

> **IT Operations Analytics Specialist**

FREQUENTLY ASKED QUESTIONS

Q: What are the prerequisites for enrolling in the Splunk Fundamentals 3 Training Certification Course?

To get the most out of this course, participants are strongly recommended to have successfully completed Splunk Fundamentals 1 and Splunk Fundamentals 2, or possess equivalent hands-on experience with Splunk Enterprise search, basic reporting, and dashboard creation. A foundational understanding of Splunk Search Processing Language (SPL) is essential, as this course builds upon those core concepts to introduce more advanced techniques.

Q: How does mastering Splunk Fundamentals 3 directly impact my ability to conduct advanced security investigations?

Mastering Splunk Fundamentals 3 significantly enhances your capacity for advanced security investigations by equipping you with the skills to use sophisticated SPL commands for anomaly detection, correlate disparate security events, and build detailed data models for forensic analysis. You'll learn to create targeted alerts for security incidents and design interactive dashboards that provide a comprehensive overview of your security posture, enabling faster threat identification and response.

Q: Will this course provide practical experience in building custom reports and dashboards for specific business needs?

Absolutely. This course is heavily focused on practical application. You will engage in hands-on labs and exercises designed to teach you how to create advanced custom reports using complex search queries, develop dynamic and interactive dashboards with various visualization types, and leverage data models for streamlined data access. These skills are directly transferable to addressing specific business requirements for operational intelligence and performance monitoring.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+	10,000+	50+
Years of Excellence	Professionals Trained	Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email
info@computer-pride.co.ke

Phone
+254 705 900 900

www.computer-pride.co.ke