SPLUNK TRAINING

Administering Splunk Enterprise Security Course

Master Splunk Enterprise Security administration. Detect, investigate, and respond to advanced cyber threats effectively.

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 "Administering Splunk Enterprise Security Course" is an essential program designed for IT professionals aiming to master the operational aspects of Splunk's premier security solution. This intermediate-level course dives deep into the architecture, configuration, and day-to-day management of Splunk Enterprise Security (ES), equipping you with the knowledge to maintain a robust and effective security monitoring environment. You'll learn to optimize ES for threat detection, incident investigation, and overall security posture enhancement, leveraging its powerful correlation, analytics, and incident review capabilities. This specialized training bridges the gap between general Splunk administration and the specific demands of security operations.

Participants will gain hands-on experience with critical components such as managing ES content, configuring security notable events, understanding data models, and ensuring the health and performance of the ES deployment. The course emphasizes practical skills required to administer ES effectively, enabling you to safeguard organizational assets against evolving cyber threats. By completing this program, you will significantly boost your proficiency in a leading SIEM platform, making you an invaluable asset in any security operations center or IT security team. This certification not only validates your expertise in Splunk ES administration but also opens doors to advanced roles in cybersecurity.

Duration	2 hours
Level	Intermediate
Vendor	Splunk

COURSE CURRICULUM

01 Module 1: Introduction to Splunk ES Administration

- Overview of Splunk Enterprise Security architecture and components
- Understanding data ingestion requirements for ES
- Navigating the ES interface and key dashboards
- Role-Based Access Control (RBAC) in Splunk ES

02 Module 2: Managing ES Content and Configuration

- Administering security content: Correlation searches, lookups, and watchlists
- Configuring notable events and incident review settings
- Managing data models and their impact on ES functionality
- Understanding and customizing ES playbooks and adaptive response actions

03 Module 3: Incident Review and Workflow Management

- Triaging and investigating notable events within the Incident Review dashboard
- Managing incident lifecycles: Assignment, status updates, and annotations
- Utilizing investigation dashboards and forensic tools in ES
- Creating custom views and reports for security monitoring

04 Module 4: Maintaining Splunk ES Health and Performance

- Monitoring ES component health and status
- Troubleshooting common ES deployment issues
- Optimizing ES search performance and resource utilization
- Backup and recovery strategies for Splunk ES configurations and data

Module 5: Advanced ES Deployment and Optimization

05
- Understanding distributed deployment considerations for Splunk ES
- Integrating ES with external systems (e.g., ticketing, threat intelligence feeds)
- Advanced content creation and customization techniques
- Best practices for scaling and securing a Splunk ES environment

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Splunk Security Administrator**

> **Security Operations Center (SOC) Analyst (Tier 2/3)**

> **Cybersecurity Engineer specializing in SIEM platforms**

FREQUENTLY ASKED QUESTIONS

Q: What specific skills will I gain that are critical for managing a Splunk Enterprise Security environment effectively?

This course will equip you with the practical skills to configure and manage security content like correlation searches and notable events, administer data models, optimize ES performance, and troubleshoot common issues. You'll also learn to utilize the Incident Review dashboard for efficient incident triage and investigation, enabling you to maintain a robust and responsive security posture using Splunk ES.

Q: How does this course prepare me for real-world Security Operations Center (SOC) responsibilities related to Splunk Enterprise Security?

This course directly addresses critical SOC responsibilities by focusing on the operational aspects of Splunk ES. You will learn to effectively monitor, detect, and respond to security incidents, manage incident lifecycles, and leverage ES for proactive threat hunting. The hands-on approach ensures you're ready to contribute to a SOC's daily operations from an administrative and analytical perspective.

Q: What are the recommended prerequisites to ensure I get the most out of this intermediate-level Splunk Enterprise Security administration course?

To maximize your learning, we recommend having a foundational understanding of the Splunk platform, including experience with Splunk search processing language (SPL), data onboarding, and basic Splunk administration. Familiarity with general cybersecurity concepts and common security threats will also be highly beneficial.

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