SPLUNK TRAINING

Using Splunk Enterprise Security Course

Master Splunk Enterprise Security to detect, investigate, and respond to advanced threats. Enhance your SIEM capabilities.

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 "Using Splunk Enterprise Security Course" is an essential intermediate-level training designed to equip cybersecurity professionals with the practical skills needed to effectively deploy, configure, and operate Splunk Enterprise Security (ES). This course delves into the core functionalities of Splunk ES as a Security Information and Event Management (SIEM) solution, focusing on advanced threat detection, incident response, and continuous security monitoring. Participants will learn to leverage ES's powerful dashboards, correlation searches, and incident review processes to enhance their organization's security posture against evolving cyber threats. You will gain hands-on experience in navigating the ES interface, understanding notable events, and integrating threat intelligence for a proactive defense strategy. This course specifically emphasizes the practical application of Splunk ES capabilities in a real-world Security Operations Center (SOC) environment.

Duration	2 hours
Level	Intermediate
Vendor	Splunk

COURSE CURRICULUM

01 Module 1: Splunk Enterprise Security Fundamentals

- Overview of Splunk ES capabilities and architecture
- Key security concepts: Data models, correlations, notable events
- Navigating the Splunk ES interface and dashboards
- Understanding the Adaptive Response Framework

02 Module 2: Data Onboarding and ES Configuration

- Ensuring data readiness for ES (CIM compliance)
- Configuring security domains and assets
- Managing identities and correlation searches for security context
- Setting up lookup files for enhanced data enrichment

03 Module 3: Threat Detection and Incident Triage

- Understanding notable events and their lifecycle
- Utilizing the Incident Review dashboard for efficient triage
- Investigating security incidents with ES analytics and visualizations
- Leveraging threat intelligence within Splunk ES

04 Module 4: Security Monitoring and Reporting

- Customizing dashboards and visualizations for security posture analysis
- Creating and managing security reports and alerts
- Utilizing Splunk ES for compliance reporting and auditing
- Best practices for continuous security monitoring

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Security Operations Center (SOC) Analyst L2/L3**

> **Cybersecurity Incident Responder**

> **Splunk ES Administrator/Engineer**

FREQUENTLY ASKED QUESTIONS

Q: What foundational Splunk knowledge is recommended to get the most out of this "Using Splunk Enterprise Security Course"?

This intermediate course assumes familiarity with core Splunk Enterprise concepts, including search language fundamentals (SPL), data ingestion, and basic dashboard creation. While we'll touch upon relevant ES-specific configurations, a solid understanding of general Splunk operations will be highly beneficial for grasping the advanced security functionalities covered.

Q: Will this course cover the customization of Splunk ES content, such as creating new correlation searches or modifying existing ones?

Yes, this course will provide an understanding of how correlation searches function within Splunk ES and guide you through the process of modifying existing ones to suit specific security needs. We'll also explore the integration of custom threat intelligence feeds to enhance your detection capabilities against emerging threats.

Q: How does mastering "Using Splunk Enterprise Security" enhance my value in a Security Operations Center (SOC) environment?

Proficiency in Splunk Enterprise Security significantly boosts your ability to operate effectively in a SOC. You will learn to efficiently monitor security events, accelerate incident investigation using ES's structured workflows, leverage threat intelligence for proactive defense, and contribute to a robust security posture, making you an indispensable asset for threat detection and response teams. This skill set is highly sought after by employers seeking to strengthen their cybersecurity defenses.

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