



FORTINET TRAINING

FortiSIEM Analyst

In this course, you will learn how to use FortiSIEM to search, enrich, and analyze events from customers in a managed security service provider (MSSP) organization.

DURATION

18 Hours

LEVEL

Advanced

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

In this course, you will learn how to use FortiSIEM to search, enrich, and analyze events from customers in a managed security service provider (MSSP) organization. You will learn how to perform real-time and historical searches, and build advanced queries. You will also learn how to perform analysis and remediation of security incidents using traditional and machine learning (ML)assisted methods.

Duration	18 Hours
Level	Advanced
Vendor	Fortinet

WHO IS THIS FOR?

- Security professionals responsible for the detection, analysis, and remediation of security incidents using FortiSIEM should attend this course.

PREREQUISITES

- FortiGate Operator
- FortiSIEM Administrator

COURSE CURRICULUM

- Module 1: Introduction to FortiSIEM**
 - Introduction to FortiSIEM
- Module 2: Analytics**
 - Analytics
- Module 3: Nested Queries and Lookup Tables**
 - Nested Queries and Lookup Tables
- Module 4: Rules and Subpatterns**
 - Rules and Subpatterns
- Module 5: Incidents**
 - Incidents
- Module 6: Clear Conditions and Remediation**
 - Clear Conditions and Remediation
- Module 7: Threat Hunting**
 - Threat Hunting
- Module 8: Performance Metrics and Baselines**
 - Performance Metrics and Baselines
- Module 9: Machine Learning**
 - Machine Learning
- Module 10: User and Entity Behavior Analytics**

- User and Entity Behavior Analytics

11 Module 11: FortiSIEM ZTNA

- FortiSIEM ZTNA

12 Module 12: Reports and Dashboards

- Reports and Dashboards

FREQUENTLY ASKED QUESTIONS

Q: What is the total duration and format of the FortiSIEM Analyst course?

The course estimated duration is 18 Hours (18 hours of lecture and hands-on lab time), available in instructor-led and self-paced online formats.

Q: Which Fortinet certification track does FortiSIEM Analyst belong to?

This course is part of the Fortinet NSE 6 certification path under the Advanced track.

Q: What product version is covered in this class?

The training and interactive lab environment cover FortiSIEM 7.4.

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+

Years of Excellence

10,000+

Professionals Trained

50+

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