



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

CODE: **LENGTH:** **PRICE:**

FNT_FT-FAZ-ANS 8 Hours (1 day) £750.00

Description

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging.

You will also learn how to identify current and potential threats through log analysis.

Finally, you will examine the management of events, incidents, reports, and task automation with playbooks.

These skills will provide you with a solid foundation for becoming a SOC analyst in an environment using Fortinet products.

Product Version

- FortiAnalyzer 7.0.2

Objectives

After completing this course, you will be able to:

- Understand basic concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand FortiSoC features
- Manage events and event handlers
- Configure and analyze incidents
- Perform threat hunting tasks
- Understand outbreak alerts
- Describe how reports function within ADOMs
- Customize and create charts and datasets
- Customize and run reports
- Configure external storage for reports
- Attach reports to incidents
- Troubleshoot reports
- Understand playbook concepts
- Create and monitor playbooks

Audience

Anyone who is responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

Prerequisites

- Familiarity with all topics presented in the NSE 4 FortiGate Security and NSE 4 FortiGate Infrastructure courses.
- Knowledge of SQL SELECT syntax is helpful.

Programme

Programme

1. Introduction and Initial Access
2. Logging
3. FortiSoC—Events and Incidents
4. Reports
5. FortiSoC—Playbooks

Test and Certification

This course is intended to help you prepare for the NSE 5 FortiAnalyzer Analyst certification exam.

https://training.fortinet.com/local/staticpage/view.php?page=nse_5 Exam vouchers are available separately at an additional charge.

Session Dates

On request. Please [Contact Us](#)

Additional Information

[This training is also available as onsite training. Please contact us to find out more.](#)