Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Woluwedal 30, 1932 Sint-Stevens-Woluwe

Email: education.ecs.benelux@arrow.com
Phone: +32 2 332 19 57

FortiNDR Cloud Analyst

CODE:	LENGTH:	PRICE:
FNT_FT-NDR_ANALYST	16 Hours (2 days)	Request Price

Description

In this course, you will learn the fundamentals of using FortiNDR Cloud. You will learn how to identify and investigate detections and indicators of compromise using the tools available on FortiNDR Cloud.
Product Versions

- FortiNDR Cloud 26

Objectives

After completing this course, you should be able to:

- Describe FortiNDR Cloud architecture
- Navigate the FortiNDR Cloud portal
- Identify the sensor types
- Describe metadata production
- Describe event types and fields
- Describe core IQL concepts
- Describe detections
- Explain behavioral observations
- Describe how to write a query
- Describe how to tune a detector
- Describe investigations
- Identify supported integrations
- Describe the essentials solution pack
- Explain the Fortinet Automation Service benefits
- Explain threat hunting concepts

Audience

Security professionals involved in the day-to-day management and monitoring of FortiNDR Cloud should attend this course.

Prerequisites

You must have knowledge of networking, cybersecurity, and SOC concepts.

Programme

Programme

1. Introduction
2. Sensors
3. Events
4. Internal Query Language
5. Detections
6. Creating Decetors
7. Investigations
8. Integrations
9. Threat Hunting Supplement

Test and Certification

Preparation of NSE 6 Security Operations

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.