

FortiNDR Cloud Analyst

Duration: 2 Days

Course 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.

Target 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.

Course 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

Course Outlines:

- Introduction
- Sensors
- Events
- Internal Query Language
- Detections
- Creating Decetors
- Investigations
- Integrations
- Threat Hunting Supplement

REGISTER NOW!

training@trends.com.ph
(+632) 8863-2123
www.trendssacademy.com.ph