FORTINET
Premier Authorized Training Center

NSE 6 CERTIFIED SECURITY OPERATIONS FORTINET

fast lane

FortiNDR Cloud Analyst

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.

Course Duration:

2 Days

Prerequisites:

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

Outlines:

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

Objectives:

After completing this course, you will 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

Who should attend

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