FortiNDR Cloud Analyst (NDR-CA)

ID NDR-CA **Price** on request **Duration** 2 days

Who should attend

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

This course is part of the following Certifications

NSE 6 Certified: Security Operations (NSE6SO)

Prerequisites

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

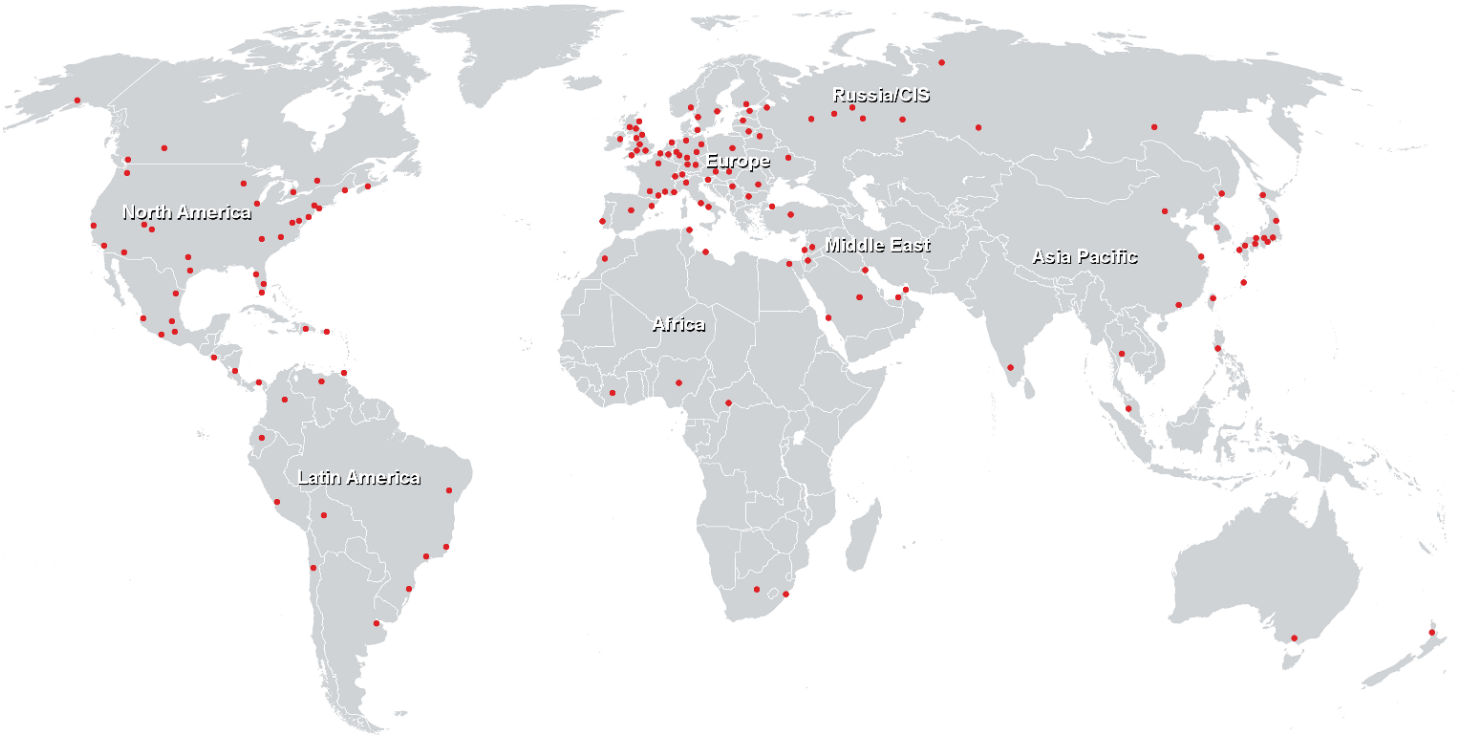
Course Objectives

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

FortiNDR Cloud Analyst (NDR-CA)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch