

FortiNDR Cloud Analyst (NDR-CA)

ID NDR-CA Preis auf Anfrage Dauer 2 Tage

Zielgruppe

Sicherheitsexperten, die mit der täglichen Verwaltung und Überwachung von FortiNDR Cloud betraut sind, sollten an diesem Kurs teilnehmen.

Empfohlenes Training für die Zertifizierung zum

NSE 6 Certified: Security Operations (NSE6SO)

Voraussetzungen

Sie müssen über Kenntnisse in den Bereichen Netzwerke, Cybersicherheit und SOC-Konzepte verfügen.

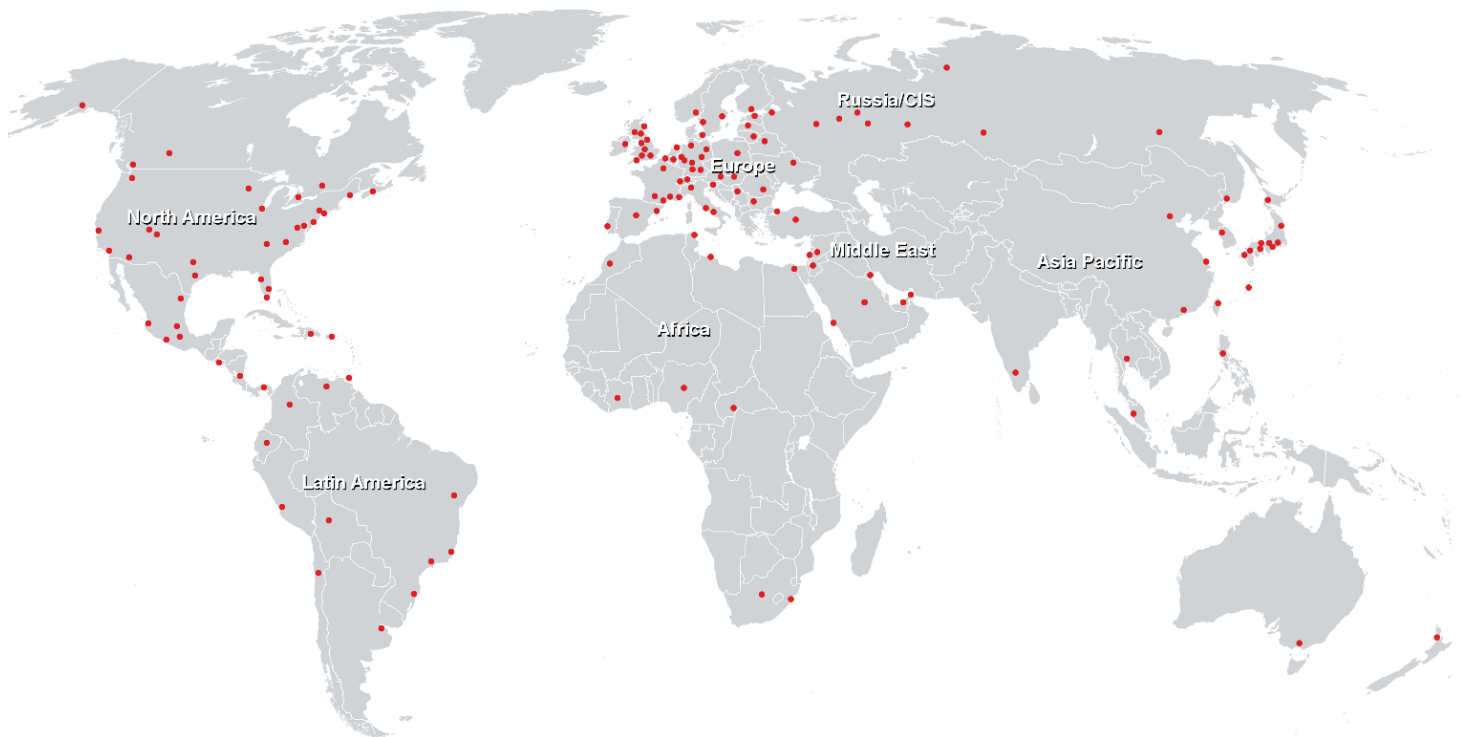
Kursziele

Nach Abschluss dieses Kurses sollten Sie in der Lage sein:

- Beschreiben Sie die Architektur von FortiNDR Cloud
- Navigieren Sie durch das FortiNDR-Cloud-Portal
- Bestimmen Sie die Sensortypen
- Beschreiben Sie die Erstellung von Metadaten
- Beschreiben Sie Ereignistypen und Felder
- Beschreiben Sie die Kernkonzepte von IQL
- Erfassung beschreiben
- Verhaltensbeobachtungen erläutern
- Beschreiben Sie, wie man eine Abfrage schreibt.
- Beschreiben Sie, wie man einen Detektor abstimmt.
- Untersuchungen beschreiben
- Unterstützte Integrationen ermitteln
- Beschreiben Sie das „Essentials“-Lösungspaket
- Erläutern Sie die Vorteile des Fortinet Automation Service
- Erläutern Sie die Konzepte der Bedrohungssuche

FortiNDR Cloud Analyst (NDR-CA)

Weltweite Trainingscenter



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>