Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss her

Postboks 6562 ETTERSTAD, 0606 Oslo, Norge

Email: kurs.ecs.no@arrow.com
Phone: +47 22 02 81 00

NSE 5 - FortiAnalyzer Analyst

CODE:	LENGTH:	PRICE:
FNT_FT-FAZ-ANS	8 Hours (1 day)	kr12,000.00

Description

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging. You will also learn how to identify current and potential threats through log analysis. Finally, you will examine the management of events, incidents, reports, and task automation with playbooks. These skills will provide you with a solid foundation for becoming a SOC analyst in an environment using Fortinet products.
Product version:

- FortiAnalyzer 7.4.1

Objectives

1. Introduction and Initial Access
2. Logging
3. Incidents and Events
4. Reports
5. Playbooks

Audience

Anyone who is responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

Prerequisites

- Familiarity with all topics presented in the FCP - FortiGate Security and FCP - FortiGate Infrastructure courses
- Knowledge of SQL SELECT syntax is helpful

Programme

After completing this course, you should be able to:

- Understand basic FortiAnalyzer concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand SOC features
- Manage events and event handlers
- Configure and analyze incidents
- Perform threat hunting tasks
- Understand outbreak alerts
- Describe how reports function within ADOMs
- Customize and create charts and datasets
- Customize and run reports
- Configure external storage for reports
- Attach reports to incidents

- Troubleshoot reports
- Understand playbook concepts
- Create and monitor playbooks

Test and Certification

Exam:
This course prepares you for the FCP - FortiAnalyzer 7.4 Analyst exam. By passing this exam, you will be awarded the associated exam badge.

Certification:
This exam is part of the FCP Security Operations certification track.

Further Information

If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones

One of the following:

- HTML 5 support
- An up-to-date Java Runtime Environment (JRE) with Java Plugin enabled on your web browser

You should use a wired Ethernet connection, not a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Session Dates

Ved forespørsel. Vennligst kontakt oss

Tilleggsinformasjon

Denne treningen er også tilgjengelig som trening på stedet. Kontakt oss for å finne ut mer.