Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå os her

.

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

FCSS - Security Operation Analyst

CODE:	LENGTH:	PRICE:
FNT_FT-SOC-ANS	8 Hours (1 day)	kr 14,640.00

Description

In this course, you will learn how to design, deploy, and manage a Fortinet SOC solution using advanced FortiAnalyzer features and functions to detect, investigate, and respond to cyberthreats. You will learn how to analyze and respond to security incidents according to industry best practices for incident handling. You will also learn how threat actors behave, and how to use widely adopted industry frameworks and models to identify and characterize adversary behavior

Objectives

After completing this course, you will be able to:
Describe the main functions and roles within a SOC
Identify common security challenges that Fortinet SOC solutions address
Analyze simulated attacks and categorize attacker tactics using industry frameworks
Analyze and respond to security incidents according to industry best practices for incident handling
Describe basic FortiAnalyzer SOC concepts, definitions, and features
Manage administrative domains
Describe FortiAnalyzer operation modes
Configure FortiAnalyzer collectors and analyzers
Design and deploy FortiAnalyzer Fabric deployments
Manage Fabric groups
Analyze and manage events, and customize event handlers
Analyze and create incidents
Analyze threat hunting dashboards
Analyze indicators of compromise (IOC) information from compromised hosts
Manage outbreak alerts
Identify playbook components
Describe trigger types and their properties
Create and customize playbooks from a template
Create new playbooks from scratch
Use variables in tasks
Configure connector actions
Monitor playbooks
Export and import playbooks

Audience

Security professionals involved in the design, implementation, and monitoring of Fortinet SOC solutions based on FortiAnalyzer should attend this course

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- FCP - FortiAnalyzer Analyst
- FCP - FortiAnalyzer Administrator

Programme

1. SOC Concepts and Security Frameworks

2. FortiAnalyzer Architecture
3. SOC Operations
4. SOC Automation

Further Information

This course is intended to help you prepare for the FCSS - Security Operations 7.4 Analyst certification exam. This exam is in the Fortinet Certified Solution Specialist - Security Operations certification track.

Session Dates

På anmodning. Kontakt os venligst

Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.