Training: Fortinet
FortiSOAR Administrator

Premier Authorized Training Center

TRAINING GOALS:

In this course, you will learn about FortiSOAR architecture, and how to deploy, configure, manage, operate, and monitor FortiSOAR in a SOC environment. You will learn about various system customization options, HA deployment, security management using role-based access control (RBAC), and various system monitoring tools.

Objectives

After completing this course, you should be able to:

- Identify challenges of security teams, and assist security teams with SOAR best practices
- Identify the role of SOAR in assisting security teams
- Describe the basics of SOAR technology
- Manage licenses
- Deploy and manage a FortiSOAR VM
- Configure teams, roles, and users
- Configure authentication
- Schedule the purging of audit logs and executed playbook logs
- Configure playbook recovery
- Configure environment variables
- Configure company branding
- Configure system fixtures
- Configure the recycle bin
- Monitor and manage audit logs
- Use the configuration manager
- Monitor system resources
- Deploy, configure, manage, and troubleshoot a FortiSOAR high availability cluster
- Identify the types of logs used for troubleshooting
- Collect log files used for troubleshooting
- Troubleshoot key services and processes on FortiSOAR

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

Who Should Attend

This course is intended for cybersecurity professionals responsible for planning, deploying, configuring, and managing FortiSOAR deployments in a SOC environment.

CONSPECT:

- Introduction to FortiSOAR
- Device Management
- System Configuration
- High Availability
- Searching, War Rooms, and Upgrading
- System Monitoring and Troubleshooting

REQUIREMENTS:

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

- You must have an understanding of the topics covered in *FCP - FortiGate Administrator*, or have equivalent experience.
- Familiarity with SOC technologies and processes is recommended.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Fortinet (course completion).

This course prepares you also for the *FCP - FortiSOAR Administrator* exam. By passing this exam, you will be awarded the associated exam badge.

TRAINER:

Fortinet Certified Trainer (FCT)

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

ADDITIONAL INFORMATION:

ISC2

- CPE training hours: 7
- CPE lab hours: 6
- CISSP domains: Security Operations

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310