Training: Fortinet
FortiSIEM Administrator

Premier Authorized Training Center

TRAINING GOALS:

In this course, you will learn about FortiSIEM initial configurations and architecture, and the discovery of devices on the network. You will also learn how to collect performance information and aggregate it with syslog data to enrich the overall view of the health of your environment, use the configuration database to greatly facilitate compliance audits, and integrate FortiSIEM into your network awareness infrastructure.

Objectives

After completing this course, you should be able to:

- Describe FortiSIEM key features and deployment architectures
- Describe FortiSIEM indicators of compromise (IoC) and reputation check
- Describe how FortiSIEM receives, collects, normalizes, and enriches logs
- Describe event type classifications
- Describe customer scaling with FortiSIEM collectors and collector high availability (HA)
- Describe FortiSIEM agent architecture for managed security services providers (MSSP)
- Describe various Fortinet Security Fabric integrations
- Perform initial configurations, and role-based access management (RBAC)
- Configure and troubleshoot asset discovery
- View performance metrics and perform actions in the configuration management database (CMDB)
- Deploy, assign, register, and upgrade collectors for MSSP customers
- Configure and manage collector HA
- Create and monitor critical business services
- Analyze business services dashboards
- Install and register FortiSIEM agents
- Monitor agent status on the CMDB
- Monitor events per second (EPS) usage
- Configure event dropping rules
- Configure identity and location information in the CMDB

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

- Deploy AI-based user entity behavior analysis (UEBA)
- Configure on-net and off-net detection, and FortiInsight watchlists
- Configure zero-trust network access (ZTNA) integration
- Create custom dashboards
- Load, save, schedule, and import reports
- Create and run CMDB and UEBA reports
- Manage collection jobs
- Define maintenance schedules
- Monitor system status with FortiSIEM health check scripts
- Collect and analyze system logs

Who Should Attend

Security professionals involved in the deployment, administration, maintenance, and troubleshooting of FortiSIEM devices should attend this course.

CONSPECT:

- Architecture
- SIEM and PAM Concepts
- Discovery
- Collectors
- Agents
- Fortinet Fabric Integration
- Reports and Dashboards
- Maintaining and Tuning
- Troubleshooting

REQUIREMENTS:

You should have an understanding of the topics covered in the FCF - FortiGate Operator course, or have equivalent experience.

Difficulty level



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

CERTIFICATE:

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

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

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

ISC2

- CPE training hours: 7
- CPE lab hours: 8
- CISSP domains: Security Operations

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