



F5: Fortinet NSE5 FortiAnalyzer

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging and reporting. You will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, you will examine the management of events, incidents, playbooks, and some helpful troubleshooting techniques.

Listenpreis

1.790,00 € exkl. MwSt

2.130,10 € inkl. MwSt

Dauer

2 Tage

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin



Gabriela Bücherl
Geschäftsführung
Vertrieb

Kontakt/Fragen:

g.buecherl@cbt-training.de

Telefon: +49 (0)89-4576918-16

Inhalte

- Introduction and Initial Configuration
- Administration and Management
- Device Registration and Communication
- Logging
- FortiSoC-Incidents and Events
- FortiSoC-Playbooks
- 7. Reports



Ziele

After completing this course, you will be able to:

- Describe key features and concepts of FortiAnalyzer
- Deploy an appropriate architecture
- Use administrative access controls
- Monitor administrative events and tasks
- Configure high availability
- Understand HA synchronization and load balancing
- Upgrade the firmware of an HA cluster
- Verify the normal operation of an HA cluster
- Manage ADOMs
- Manage RAID
- Register supported devices
- Troubleshoot communication issues
- Manage disk quota
- Manage registered devices
- Protect log information
- View, search, manage, and troubleshoot logs
- Monitor and manage events
- Manage and customize event handlers
- Create and manage incidents
- Explore tools used for threat hunting
- Create, run, and troubleshoot playbooks
- Import and export playbooks
- Generate and customize reports
- Customize charts and datasets
- Manage and troubleshoot reports

Zielgruppe

Anyone who is responsible for the day-to-day management of FortiAnalyzer devices and FortiGate security information.

Voraussetzungen

- Familiarity with all topics presented in the FortiGate Security (FORT-SECI) and FortiGate Infrastructure (FORT-SECII) courses
- Knowledge of SQL SELECT syntax is helpful, but not required

Prüfung/Zertifizierung

Prüfung: Fortinet NSE 5 - FortiAnalyzer 7.2 Analyst

To obtain certification, you must pass a minimum of any two Fortinet NSE 5 exams. NSE 5 certification is valid for two years from the date of completion