

F8: Fortinet NSE 5 - FortiSiem

In this course, you will learn about FortiSIEM initial configurations, 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, how to use the configuration database to greatly facilitate compliance audits, and how to integrate FortiSIEM into your network awareness infrastructure.
Die Teilnehmer erhalten Informationen zu Erstkonfigurationen, zur Architektur und zur Erkennung von Geräten im Netzwerk. Die Teilnehmer lernen auch, wie sie Leistungsinformationen sammeln und mit Syslog-Daten zusammenfassen, um die Gesamtansicht der Gesundheit der Umgebung zu verbessern. Darüber hinaus lernen die Kandidaten, wie Sie die Konfigurationsdatenbank verwenden können, um Compliance-Audits erheblich zu vereinfachen.

Listenpreis

1.990,00 € exkl. MwSt

2.368,10 € inkl. MwSt

Dauer

3 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
- SIEM and PAM Concepts
- Discovery and FortiSIEM Agents
- FortiSIEM Analytics
- CMDB Lookups and Filters
- Group By and Data Aggregation
- Rules and MITRE ATT&CK
- Incidents and Notification Policies
- Reports and Dashboards
- Maintaining and Tuning
- Troubleshooting



Ziele

- Identify business drivers for using SIEM tools
- Describe SIEM and PAM concepts
- Describe key features of FortiSIEM
- Understand how collectors, workers, and supervisors work together
- Configure notifications
- Create new users and custom roles
- Describe and enable devices for discovery
- Understand when to use agents
- Perform real-time, historic structured searches
- Group and aggregate search results
- Examine performance metrics
- Create custom incident rules
- Edit existing, or create new, reports
- Configure and customize the dashboards
- Export CMDB information
- Identify Windows agent components
- Describe the purpose of Windows agents
- Understand how the Windows agent manager works in various deployment models
- Identify reports that relate to Windows agents
- Understand the FortiSIEM Linux file monitoring agent
- Understand agent registration
- Monitor agent communications after deployment
- Troubleshoot FortiSIEM issues

Zielgruppe

Dieser Kurs richtet sich an alle Personen, die für das tägliche Management von FortiSIEM verantwortlich sind.

Voraussetzungen

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

NSE 4 FortiGate Security
NSE 4 FortiGate Infrastructure

Prüfung/Zertifizierung

Dieser Kurs bereitet Sie auf die FortiSIEM-Specialist Prüfung vor.
Prüfung: Fortinet NSE 5 - FortiSIEM
