Training: Fortinet
FortiSIEM

TRANING TERMS

2025-06-25 | 3 days | Warszawa / Virtual Classroom
2025-09-10 | 3 days | Kraków / Virtual Classroom
2025-11-26 | 3 days | Warszawa / Virtual Classroom

TRAINING GOALS:

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.

Objectives

After completing this course, you should be able to:

- 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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

Who Should Attend

Anyone who is responsible for the day-to-day management of FortiSIEM should attend this course.

CONSPECT:

- 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

REQUIREMENTS:

You must have an understanding of the topics covered in the *FortiGate Administrator* course, or have equivalent experience.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Fortinet.

This course is intended also to help you prepare for the FCP – FortiSIEM exam. This exam is part of the FCP Network Security certification tracks:

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Fortinet Certified Professional (FCP) - Security Operations

The FCP – FortiSIEM certification exam is one of the options to choose as one of the two elective exams required to pass in order to obtain the Fortinet Certified Professional (FCP) title. Fortinet certification exams are offered at Pearson Vue test centers worldwide. More information about Fortinet Certification Program on the https://www.fortinet.com/training-certification

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

ISC2

- CPE training hours: 11
- CPE lab hours: 9
- CISSP domains: Security Operations

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007