Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Skontaktuj się z nami

.

Email: szkolenia.ecs.pl@arrow.com
Phone: 12 616 43 00

NSE 5 - FortiAnalyzer Analyst

Kod:	Czas trwania:	Cena netto:
FNT_FT-FAZ-ANS-D02	16 Hours (2 days)	zł6,400.00

Description

In this course, you will gain the practical skills of a SOC analyst using FortiAnalyzer for centralized logging and analytics. You will learn how to examine and manage events, and automate threat response using event handlers and playbooks. You will also learn how to identify current and potential threats through incident analysis and outbreak reports. Finally, you will learn how to incorporate FortiAI in your workflow and generate security reports.

Cel szkolenia

After completing this course, you should be able to:

- Describe SOC objectives, responsibilities, and roles
- Describe the role of FortiAnalyzer in a SOC
- Describe FortiAnalyzer Security Fabric integration
- Describe how logging works in a Security Fabric
- Describe FortiAnalyzer Fabric deployments
- Describe FortiAnalyzer operating modes
- Describe how FortiAnalyzer parses and normalizes logs
- Validate log parsers
- Search logs using normalized fields
- View and search for logs in the log view
- Create saved filters and dashboards
- View summary data in FortiView
- View dashboards and widget features
- Configure event handlers
- Manage events
- Configure indicators
- Create incidents
- Analyze incidents
- Configure incident settings
- Describe FortiAI operations and use cases
- Describe threat hunting
- Use the log count chart
- Use the SIEM log analytics table
- Describe outbreak alerts
- Collect log volume statistics
- Configure an automation stitch
- Configure an event handler with an automation stitch enabled
- Run and fine-tune predefined reports
- Customize reports with macros, custom charts, and datasets
- Configure external storage for reports
- Group reports
- Import and export reports and charts
- Attach reports to incidents
- Manage and troubleshoot reports
- Create new playbooks
- Use variables in tasks
- Monitor playbooks
- Export and import playbooks

Uczestnicy

Security professionals responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

Wymagania wstępne

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

- FCA - *FortiGate Operator*
- FortiAnalyzer Administrator

It is also recommended that you have knowledge of the following topic:

- SQL SELECT statement syntax

Program szkolenia

1. SOC Concepts and Security Fabric
2. Log Data Flow and Navigation
3. Events, Indicators, and Incidents
4. FortiAI, Threat Hunting, and Troubleshooting
5. Reports
6. Playbooks

Test and Certification

This course prepares you for the FCP - FortiAnalyzer 7.6 Analyst exam. By passing this exam, you will be awarded the associated exam badge.
This exam is part of the FCP Security Operations certification track.

Więcej informacji

If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones
- One of the following:
  - HTML 5 support
  - An up-to-date Java Runtime Environment (JRE) with Java Plugin enabled on your web browser

You should use a wired Ethernet connection, *not* a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Terminy

Data	Lokalizacja	Strefa czasowa	Język	Typ szkolenia	Gwarancja	Cena netto
25 Jan 2027	Virtual Classroom	CET	Polish	Instructor Led Online		zł6,400.00
22 Feb 2027	Virtual Classroom	CET	Polish	Instructor Led Online		zł6,400.00

Dodatkowe informacje

Jeśli interesują Cię inne szkolenia tego producenta - skontaktuj się z nami.