

Training: Fortinet  
NSE7 - Advanced Threat Protection (ATP)

FORM OF TRAINING	MATERIALS	PRICE	DURATION
Traditional	Digital materials	1650 EUR	2 days
Traditional	CTAB Tablet	1750 EUR	2 days

## LOCATIONS

Krakow - 5 Tatarska Street, II floor, hours: 9:00 am - 4:00 pm

Warsaw - 17 Bielska Street, hours: 9:00 am - 4:00 pm

## TRAINING TERMS

2019-11-12 | 2 days | Warszawa

## TRAINING GOALS:

In this 2-day course, participants will learn the following:

- How to protect their organization and improve its security against advance threats that bypass traditional security controls
- How **FortiSandbox** detects threats that traditional antivirus product miss
- How FortiSandbox dynamically generates local threat intelligence, which can be shared throughout the network
- How other **advanced threat protection (ATP)** components - **FortiGate**, **FortiMail**, **FortiWeb**, and **FortiClient** - leverage this threat intelligence information to protect organizations, from end-to-end, from advanced threats

*Course is based on the FortiSandbox version 2.5*

After completing this course, you should be able to:

- Identify different types of cyber attacks
- Identify threat actors and their motivations
- Understand the anatomy of an attack—the kill chain
- Identify the potentially vulnerable entry points in an Enterprise network
- Identify how the ATP framework works to break the kill chain
- Identify the role of FortiSandbox in the ATP framework
- Identify appropriate applications for sandboxing

- Identify FortiSandbox architecture
- Identify FortiSandbox key components
- Identify the appropriate network topology requirements
- Configure FortiSandbox
- Monitor FortiSandbox operation
- Configure FortiGate integration with FortiSandbox
- Configure FortiMail integration with FortiSandbox
- Configure FortiWeb integration with FortiSandbox
- Configure FortiClient integration with FortiSandbox
- Troubleshoot FortiSandbox-related issues
- Perform analysis of outbreak events
- Remediate outbreak events based on log and report analysis

#### Who Should Attend:

This course is intended for network security engineers responsible for designing, implementing, and maintaining an advanced threat protection solution with FortiSandbox, in an Enterprise network environment.

#### CONSPECT:

- Attack Methodologies and the ATP Framework
- Introduction to FortiSandbox
- Protecting the Edge
- Protecting Email Networks
- Protecting Web Applications
- Protecting End Users
- Protecting Third-Party Appliances
- Results Analysis

#### REQUIREMENTS:

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

- NSE4 - [FortiGate I Security](#)
- NSE4 - [FortiGate II Infrastructure](#)

It is also recommended that participants have an understanding of the topics covered in the following

courses, or have equivalent experience:

- NSE6 - [FortiMail](#)

## Difficulty level



## CERTIFICATE:

The participants will obtain certificates signed by Fortinet.

This course is intended to help participants prepare for the **NSE7 Advanced Threat Protection certification exam**.

## TRAINER:

Fortinet Certified Trainer (FCT).