Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Advanced Threat Protection

CODE:	LENGTH:	PRICE:
FTN_FT-ATP	16 Hours (2 days)	€1,850.00

Description

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

- How to protect your organization and improve its security against advanced threats that bypass traditional security controls
- How FortiSandbox detects threats that traditional antivirus products 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

Who Should Attend

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

Agenda

1. Attack Methodologies and the ATP Framework
2. FortiSandbox Key Components
3. High Availability, Maintenance and Troubleshooting
4. Protecting the Edge
5. Protecting Email Networks
6. Protecting Web Applications
7. Protecting End Users
8. Protecting Third-Party Appliances
9. Results Analysis

Objectives

After completing this course, candidates will 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
- Identify the role of machine learning in preventing zero day attacks and advanced threats
- Configure machine learning on FortiWeb
- Analyze attack logs from machine learning system
- Configure FortiClient integration with FortiSandbox
- Troubleshoot FortiSandbox-related issues
- Perform analysis of outbreak events
- Remediate outbreak events based on log and report analysis

System Requirements

If you take an 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 / headphones

One of the following:

- HTML 5 support
- An up-to-date Java runtime environment (JRE) with Java plugin enabled in the web browser

Participants should use a wired Ethernet connection *not* a Wi-Fi connection. The firewall or FortiClient must allow connections to the online labs.

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.