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

FortiSIEM Basic Training

CODE:	LENGTH:	PRICE:
FTN_FT-FSM	24 Hours (3 days)	€3,228.00

Description

In this three-day course, you will learn how to use FortiSIEM, and how to integrate FortiSIEM into your network awareness infrastructure.
You will learn about 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 the environment. Additionally, you will learn how you can use the configuration database to greatly facilitate compliance audits.

Who Should Attend

Anyone who is responsible for day-to-day management of FortiSIEM.

Agenda

1. Introduction
2. SIEM and PAM Concepts
3. Discovery
4. FortiSIEM Analytics
5. CMDB Lookups and Filters
6. Group By and Aggregations
7. Rules
8. Incidents and Notification Policies
9. Reports and Dashboards
10. Maintaining and Tuning
11. FortiSIEM Agents

Objectives

After completing these courses, you will 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 the discovery process
- 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 what Windows Agents are used for
- Understand how the Windows Agent Manager works in various deployment models
- Identify reports that relate to Windows Agents
- Understand FortiSIEM Linux File Monitoring Agent
- Understand agent registration
- Monitor agent communications after deployment

System Requirements

If you take an online format of this class, you must have a computer with:

- High-speed Internet connection
- Up-to-date web browser
- PDF viewer
- Speakers / headphones
- Either:
  - HTML 5 support or
  - Up-to-date Java runtime environment (JRE) with Java plugin enabled in your web browser

Wired Ethernet connection (not Wi-Fi) recommended. Firewalls including Windows Firewall or FortiClient must allow connections with 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.