FortiAnalyzer

COURSE DETAILS

Course Code: FO-FANALYZER
Current Version: 7.0.2
Delivery Type: Instructor-Led
Duration: 2 days

PREREQUISITES

- Familiarity with all topics presented in the NSE 4 FortiGate Security and NSE 4 FortiGate Infrastructure courses
- Knowledge of SQL SELECT syntax is helpful, but not required

COURSE CONTENT

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging and reporting. You will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, you will examine the management of events, incidents, playbooks, and some helpful troubleshooting techniques.

COURSE OBJECTIVES

After completing this course, you will be able to:

- Describe key features and concepts of FortiAnalyzer
- Deploy an appropriate architecture
- Use administrative access controls
- Monitor administrative events and tasks
- Configure high availability
- Understand HA synchronization and load balancing
- Upgrade the firmware of an HA cluster
- Verify the normal operation of an HA cluster
- Manage ADOMs
- Manage RAID
- Register supported devices
- Troubleshoot communication issues
- Manage disk quota
- Manage registered devices
- Protect log information
- View, search, manage, and troubleshoot logs
- Monitor and manage events
- Manage and customize event handlers
- Create and manage incidents
- Explore tools used for threat hunting
- Create, run, and troubleshoot playbooks
- Import and export playbooks
- Generate and customize reports
- Customize charts and datasets
- Manage and troubleshoot reports

FortiAnalyzer

COURSE OUTLINE

1. Introduction and Initial Configuration
2. Administration and Management
3. Device Registration and Communication
4. Logging
5. FortiSoC—Incidents and Events
6. FortiSoC—Playbooks
7. Reports

WHO SHOULD ATTEND

Anyone who is responsible for the day-to-day management of FortiAnalyzer devices and FortiGate security information.

Tel: (+971 4) 42 89 440 Fax: (+971 4) 42 89 441
training@fastlane-mea.com www.flane.ae