FortiAnalyzer

In this one-day class, students will learn the fundamentals of using FortiAnalyzer 6.2 for centralized logging and reporting. Students will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, students will examine some helpful troubleshooting techniques.

In interactive labs, students will explore administration and management; register devices for log collection with FortiAnalyzer; use FortiAnalyzer to centrally collect logs; perform a forensic analysis of logs based on simulated network attacks; create reports; and explore solutions to common misconfiguration issues.

Product Version

FortiAnalyzer 6.2

Formats

- Instructor-led
- Instructor-led online
- Self-paced online

Agenda

1. Introduction and Initial Configuration
2. Administration and Management
3. Device Registration and Communication
4. Logging
5. Reports

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
- Manage ADOMs
- Configure RAID
- Register supported devices
- Troubleshoot communication issues
- Manage disk quota
- Manage registered devices
- Protect log information
- View and search logs
- Troubleshoot and manage logs
- Monitor events
- Generate and customize reports
- Customize charts and datasets
- Manage reports
- Troubleshoot reports

Who Should Attend

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

Prerequisites

- Familiarity with all topics presented in *FortiGate Security* and *FortiGate Infrastructure*
- Knowledge of SQL SELECT syntax is helpful

System Requirements

If you take an online format of this class, you must have 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 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.

Certification

This course is part of the preparation for the NSE 5 certification exam.