

# Course Outline

## FortiAnalyzer Analyst 7.2 Course FA: 1 day Instructor Led

*All Fortinet courses are delivered by a Fortinet Authorized Learning Partner*

### **About this course**

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging. You will also learn how to identify current and potential threats through log analysis. Finally, you will examine the management of events, incidents, reports, and task automation with playbooks. These skills will provide you with a solid foundation for becoming a SOC analyst in an environment using Fortinet products.

### **Audience profile**

Anyone who is responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

### **At course completion**

After completing this course, students will be able to:

- Understand basic concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand FortiSoC features
- Manage events and event handlers
- Configure and analyze incidents
- Perform threat hunting tasks
- Understand outbreak alerts
- Describe how reports function within ADOMs
- Customize and create charts and datasets
- Customize and run reports
- Configure external storage for reports
- Attach reports to incidents
- Troubleshoot reports
- Understand playbook concepts
- Create and monitor playbooks Import and export playbooks

### **Course Outline**

1. Introduction and Initial Access
2. Logging
3. FortiSoC—Events and Incidents
4. Reports
5. FortiSoC—Playbooks