

Fortinet FortiAnalyzer 7.4 Analyst (FCP)

This Fortinet training teaches you how to use FortiAnalyzer 7.4 to strengthen your security operations, and pass the FortiAnalyzer 7.4 Analyst exam. You'll practice configuring ADOMs, collecting and searching logs, and building custom reports. You'll also tune event handlers, manage incidents and create playbooks that automate your response workflows. Whether you're a SOC analyst or network engineer, this course aligns with one of two exams you need to pass in order to earn the Fortinet Certified Professional (FCP) in Security Operations certification, or the Fortinet Certified Professional (FCP) in Network Security certification, so you can run a smarter Security Fabric.

[CBT Nuggets course material](#) →



WEEK 1

Understand FortiAnalyzer Key Concepts

- FortiAnalyzer Key Concepts Overview
- Initial Access to FortiAnalyzer
- Centralized Logging with FortiAnalyzer
- Fortinet Security Fabric and FortiAnalyzer
- Working with Logs and FortiView
- FortiAnalyzer Scenario

Using ADOMs, Logs, and FortiView

- Intro to ADOMs and FortiAnalyzer Logs
- FortiAnalyzer Administrative Domains (ADOMS) Overview
- Creating ADOMs
- Log Overview
- Viewing and Searching Logs
- Using FortiView Dashboards
- Using FortiView Monitors
- Log Rate and Device Usage Stats
- FortiAnalyzer Customer Scenario

Using FAZ Event Management

- Intro to FortiAnalyzer Event Management
- Event Management Overview
- Working FortiAnalyzer Events
- Event Handlers

WEEK 2

- Create a Custom Event Handler
- Event Management Validation Section

Using FAZ Incident Management

Intro to Incident Management on the FortiAnalyzer

Incident Management Overview

Creating an Incident

Analyzing an Incident

Working on an Incident

MITRE ATT@CK Framework

Incident Example

Customer Scenario

Using FortiAnalyzer Reports

Intro to FortiAnalyzer Reports

FortiAnalyzer Reports Overview

Default Reports

Templates

Datasets and Macros

Charts

Create Custom Reports and Templates

Managing Reports

Reports Validation Section

Using FortiAnalyzer Playbooks

Intro to FortiAnalyzer Automation and Playbooks

Playbooks Overview

Playbook Connectors

Playbook Triggers

Webhooks

Playbook Examples

WEEK 3

Playbook Monitor

Validation of Playbooks