FortiInsight

In this interactive course, you will learn the fundamentals of using FortiInsight for threat hunting and reporting, including data analysis through setting up policies, collections and investigations, AI settings, and more. These administration fundamentals will provide you with an understanding of how to manage the FortiInsight device and the event information.

Product Version

FortiInsight 5.2

Formats

Self-paced online

Agenda

1. Introduction to FortiInsight
2. FortiInsight Searching
3. Events and Alerts
4. Policies, AI, and Common Issues

Objectives

After completing this course, you should be able to:

- Understand how to use FortiInsight
- Understand UEBA use cases
- Identify the 5-factor telemetry model
- Identify endpoint agents and the kernel driver
- Identify events and the collector server
- Identify the FortiInsight dashboard and the different widget types
- Identify endpoints, accounts, and a license
- Understand searching criteria and criteria options
- Know why you need concatenators
- Understand search pills
- How to create, group, clear, and delete search pills
- How to find related events
- How to use search queries and sticky searches
- Understand summary tables and threat hunting
- Understand event categories
- Understand collections
- Understand policy and AI alerts
- Know how to find related alerts
- Understand forensic, alert, data flow, applications, and threat reports
- Understand FortiInsight policies, framework, and labels
- Understand augmented intelligence (AI), AI scoring, and feedback
- Understand AI training and settings
- Create, use, and export investigations

- Understand and troubleshoot common FortiInsight issues

Who Should Attend

Anyone who is responsible for the day-to-day management of FortiInsight and event information should attend this course.

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones