Threat Hunting

In this course, you will explore the practical use of Fortinet solutions as threat intelligence and threat hunting platforms. You will explore fundamental concepts about cyber threat intelligence and how to leverage Fortinet solutions to perform threat intelligence management (collection, enrichment, and so on) and threat hunting.

Product Version

- FortiSIEM 6.2.0
- FortiEDR 4.2.2.23

Course Duration

- Lecture time (estimated): 6 hours
- Lab time (estimated): 14 hours
- Total course duration (estimated): 20 hours/3 days

Who Should Attend

Security professionals involved in the architectural design, implementation, and execution of threat hunting solutions and processes using FortiAnalyzer, FortiSIEM, FortiEDR, and FortiSOAR should attend this course.

Certification

There is no certification associated with this course.

Prerequisites

- Basic end-user experience with command line interfaces (Linux shell and Windows PowerShell)
- Solid knowledge of network protocols (such as IP, TCP, UDP, HTTP, DNS, and so on)
- Basic hands-on experience with Kali Linux
  - Metasploit
  - Burp Suite
- Experience with Browser Exploitation Framework (BeEF)

Recommended NSE training

- *NSE 4 FortiGate Security and FortiGate Infrastructure*
- *NSE 5 FortiAnalyzer*
- *NSE 5 FortiSIEM*
- *NSE 5 FortiEDR*
- *NSE 7 FortiSOAR Design and Development*

Recommended certifications

- NSE 4
- NSE 5 Specialist (FortiSIEM and FortiEDR)
- NSE 7 Security Architect

Agenda

1. Introduction
2. Cyber Threat Intelligence
3. Open-Source Intelligence
4. Threat Intelligence Platforms
5. Threat Hunting Models and Methodologies
6. Basic Malware Analysis

Objectives

After completing this course, you will be able to:

- Understand basic concepts of cyber threat intelligence and threat hunting
- Understand frameworks commonly used to describe, organize, and catalog observed threats and actor behavior (threat intelligence)
- Understand proposed models and methodologies for conducting threat hunting as a process
- Understand basic concepts about malware analysis
- Complete practical hands-on tasks to:
  - Conduct network and endpoint threat hunting using Fortinet solutions and other third-party tools
  - Conduct threat hunting based on TTPs and an established methodology
  - Use FortiSOAR to document threat hunting findings (indicators of compromise) and enrich incident analysis
  - Use Fortinet solutions to analyze malware behavior
  - Emulate adversary behavior

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-FTH

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)^2

- CPE training hours: 6
- CPE lab hours: 14
- CISSP domains: Security Operations

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.