Security Operations

In this two-day course, you will explore the practical use of Fortinet security operations solutions to detect, investigate, and respond to Advanced Persistent Threats (APTs). Comprised of theory lessons and hands-on labs, this course will guide you to understand how to execute advanced threats, how threat actors behave, and how security operations handle such threats.

You will leverage widely adopted industry frameworks and models to comprehend advanced complex attacks (APTs) and adversary behavior. Then, you will use these foundations to build detection capabilities and emulate adversary activity.

Finally, you will go through industry guidelines for incident handling and practical utilization of Fortinet solutions to detect, analyze, and respond to the previously emulated incident.

Product Version
- FortiSIEM 5.3.0
- FortiSOAR 6.0.0

Formats
- Instructor-led

Agenda
1. Security Operations Overview
2. Attack Frameworks
3. Adversary Behavior
4. Building Detection Capabilities
5. Adversary Emulation and Detection
6. Incident Handling

Objectives
After completing this course, you should be able to:
- Understand the basic concepts of security operations and Fortinet SOC Automation Framework
- Understand frameworks commonly used to describe, organize, and catalog observed threats and actor behavior (threat intelligence)
- Understand how to use a framework for proper incident handling
- Use MITRE ATT&CK® to map adversary behavior based on a mock threat report
- Use MITRE ATT&CK® to elect potential data sources for building detection capabilities
- Build FortiSIEM rules to detect specific adversary behavior
- Emulate adversary behavior
• Handle an incident throughout the main stages of the incident handling life cycle (detection, analysis, containment, eradication, and recovery) based on the NIST 800-61—Computer Security Incident Handling Guide.

MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

Who Should Attend

Security professionals involved in the architectural design, implementation, and monitoring of Fortinet SOC solutions based on FortiSOAR and FortiSIEM devices.

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

• Basic knowledge of security operations
• NSE 4 FortiGate Security
• NSE 5 FortiSIEM
• NSE 7 FortiSOAR Design and Development

It is also recommended that you have an understanding of the topics covered in the following course, or have equivalent experience:

• NSE 7 Advanced Threat Protection

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
• HTML5 support

You should use a wired Ethernet connection, not a Wi-Fi connection. Firewalls, including Windows Firewall and FortiClient, must allow connections to the online labs.

Certification

There is no certification for this course at this time.