FORTINET
Premier Authorized Training Center

NSE 6 CERTIFIED SECURITY OPERATIONS FORTINET

fast lane

FortiRecon Analyst

Course Description

In this course, you will learn how to use FortiRecon to onboard customers and add customer seed data. You will also learn how to identify and analyze an organization's internal and external attack surface. Additionally, you will learn how to analyze security incidents that Attack Surface Management (ASM), Brand Protection (BP), and Adversary Centric Intelligence (ACI) generated. You will explore FortiRecon assets and intelligence reports, learn how to analyze them using various filters, and understand how to automate workflows using Security Orchestration and APIs.

Course Duration:

1 Day

Prerequisites:

You must have a basic understanding of network security and security operation center (SOC) concepts.

Outlines:

1. Introduction to FortiRecon
2. Product Overview and Initial Access
3. Modules
4. Intelligence Reports
5. Security Orchestration and APIs

Objectives:

After completing this course, you will be able to:

- Describe how to identify the attack surface
- Differentiate between the surface web, deep web, and dark web
- Describe the MITRE ATT&CK Matrix and Cyber Kill Chain for Enterprise
- Describe FortiRecon use cases
- Describe the FortiRecon license and initial access
- Describe the FortiRecon provisioning form and seed data
- Identify FortiRecon managed security service provider (MSSP) onboarding and prerequisites
- Describe the FortiRecon overview page, digital risk posture, and ASM
- Identify FortiRecon exposed services and technologies
- Describe FortiRecon BP and ACI components
- Describe FortiRecon reports, objectives, and data
- Describe automation and FortiRecon Security Orchestration
- Create and run playbooks
- Explore APIs and examples

Who should attend

Security professionals involved in threat analysis and ASM using FortiRecon should attend this course.