FortiDeceptor Administrator

Course Description

In this course, you will learn how to deceive, expose, and eliminate threats early in the attack kill chain using FortiDeceptor. FortiDeceptor lures attackers into revealing themselves by engaging with a range of deception assets distributed throughout the network environment.

Product Version:

- FortiDeceptor 5.3
- The FortiDeceptor 5.3 course is applicable only to hardware devices and VMs.

Course Duration:

1 Day

Certification:

This course does not have a certification exam.

Prerequisites:

You should have an understanding of the topics covered in the FCP - FortiGate Administrator course or have equivalent experience.

Objectives:

After completing this course, you will be able to:

- Describe how FortiDeceptor integrates into Enterprise networks
- Describe FortiDeceptor modules and key features
- Access FortiDeceptor and view the dashboard
- Configure network and system settings
- Configure FortiDeceptor central management
- Configure FortiDeceptor for air-gapped deployments
- Configure deployment networks
- Deploy decoy VMs and configure lure resources
- Use the deployment wizard to create and deploy decoys
- Select the appropriate decoys, services, and lures
- Create and deploy FortiDeceptor token packages
- Analyze the FortiDeceptor deployment map
- Analyze incidents, attacks, and the attack map
- Navigate the MITRE ICS matrix
- Design deception strategies based on network requirements
- Differentiate light-stack and full-stack deception
- Detect and mitigate new outbreaks

- Follow best practices for decoy and token deployment
- Follow best practices for AD integration
- Design deception based on network topology requirements
- Formulate deception strategies against specific attack vectors
- Integrate FortiDeceptor with the Fortinet Security Fabric and other Fortinet products
- Integrate FortiDeceptor with third-party products

Outlines:

1. Introduction
2. Deception and Incidents
3. Deception Strategies
4. FortiDeceptor Integration

Who should attend

Cybersecurity professionals responsible for the day-to-day administration, management, and troubleshooting of FortiDeceptor should attend this course.