

## FT-FSR-ADM: FortiSOAR Administrator

Course Code: FT-FSR-ADM

Duration: 2 days

Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

### OVERVIEW

In this course, you will learn about FortiSOAR architecture, and how to deploy, configure, manage, operate, and monitor FortiSOAR in a SOC environment. You will learn about various system customization options, HA deployment, security management using role-based access control (RBAC), and various system monitoring tools.

### SKILLS COVERED

After completing this course, you should be able to:

- Identify challenges of security teams, and assist security teams with SOAR best practices
- Identify the role of SOAR in assisting security teams
- Describe the basics of SOAR technology
- Manage licenses
- Deploy and manage a FortiSOAR VM
- Configure teams, roles, and users
- Configure authentication
- Schedule the purging of audit logs and executed playbook logs
- Configure playbook recovery
- Configure environment variables
- Configure company branding
- Configure system fixtures
- Configure the recycle bin
- Monitor and manage audit logs
- Use the configuration manager
- Monitor system resources

- Deploy, configure, manage, and troubleshoot a FortiSOAR high availability cluster
- Identify the types of logs used for troubleshooting
- Collect log files used for troubleshooting
- Troubleshoot key services and processes on FortiSOAR

### WHO SHOULD ATTEND?

This course is intended for cybersecurity professionals responsible for planning, deploying, configuring, and managing FortiSOAR deployments in a SOC environment.

### PREREQUISITES

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

- You must have an understanding of the topics covered in *FCP – FortiGate Security*, or have equivalent experience.
- Familiarity with SOC technologies and processes is recommended.

### MODULES

#### Module 1: Introduction to FortiSOAR

#### Module 2: Device Management

#### Module 3: System Configuration

#### Module 4: High Availability

#### Module 5: Searching, War Rooms, and Upgrading

#### Module 6: System Monitoring and Troubleshooting

END OF PAGE