

## FortiSOAR Design and Development Course

**Course Duration: 16 Hrs.**

**Course Code: FSOAR-DD-7.0**

### Course Overview

The **FortiSOAR Design and Development** course is designed for security professionals and developers responsible for creating, customizing, and optimizing automation workflows within FortiSOAR. This course focuses on advanced playbook design, integration of third-party security tools, and development of custom connectors and scripts to automate security operations. Participants will gain hands-on experience in designing, developing, and deploying FortiSOAR solutions to enhance SOC efficiency and incident response capabilities.

### What You'll Learn?

By completing this course, you will be able to:

- Design and implement FortiSOAR playbooks for automated incident response
- Develop custom integrations with third-party security tools
- Create scripts and connectors to extend FortiSOAR functionality
- Implement advanced workflow automation for SOC operations
- Test, debug, and optimize FortiSOAR playbooks and integrations
- Apply best practices for SOAR development and operational efficiency

### Target Audience

This course is ideal for:

- Security Automation Engineers

- SOC Developers and Analysts
- Incident Response Professionals
- Network and Security Engineers
- Professionals responsible for FortiSOAR deployment and customization

## Pre-Requisites

Participants should have:

- Hands-on experience with FortiSOAR or similar SOAR platforms
- Understanding of SOC processes and incident response workflows
- Familiarity with scripting languages (Python, JavaScript)
- Basic knowledge of APIs and integration concepts

## Course Content

### Module 1: FortiSOAR Architecture and Development Environment

- Overview of FortiSOAR components
- Development and testing environment setup
- System architecture and data flow

### Module 2: Playbook Design and Best Practices

- Playbook concepts and design principles
- Creating automated response workflows
- Modular and reusable playbooks

### Module 3: Custom Connectors and Integrations

- Integration with Fortinet and third-party tools

- Connector creation and configuration
- API-based integration techniques

#### **Module 4: Script Development and Automation**

- Writing scripts for automation tasks
- Debugging and testing scripts
- Scheduling and triggering automated actions

#### **Module 5: Advanced Workflow Optimization**

- Error handling and workflow recovery
- Performance tuning of playbooks
- Incident prioritization and escalation

#### **Module 6: Monitoring, Troubleshooting, and Deployment**

- Playbook monitoring and logging
- Troubleshooting integration and automation issues
- Deployment best practices and operational readiness