

# Security Operations Architect (SECOP-ARCH)

## ID SECOP-ARCH Prix sur demande Durée 2 jours

Cette formation est fournie par notre partenaire Fortinet.

### A qui s'adresse cette formation

Security professionals involved in the design, implementation, operation, and monitoring of Fortinet SOC solutions using FortiSIEM and FortiSOAR should attend this course.

### Cette formation prépare à la/aux certifications

Fortinet Certified Solution Specialist Security Operations (FCSSSO)

#### Pré-requis

You must have an understanding of the topics covered in the FortiSIEM Analyst course, or have equivalent experience.

### **Objectifs**

After completing this course, you will be able to:

- Describe the main functions and roles within a SOC
- Identify the challenges that can be solved by the Fortinet SOC
- Describe the MITRE ATT&CK Enterprise Matrix and the Cyber Kill Chain
- Describe how to identify and reduce the attack surface
- Describe common attack vectors
- Describe the benefits of using FortiSIEM and FortiSOAR
- Describe different Fortinet SOC deployment architectures
- Describe the FortiSOAR Content Hub and connectors
- Describe FortiAl features
- Describe FortiAl in FortiSIEM and FortiSOAR
- Describe reactive and proactive threat hunting processes
- Generate threat hunting hypotheses
- · Identify and configure data sources
- Configure data ingestion
- Configure FortiSIEM rules
- Execute attack vectors
- Describe the NIST SP 800-61 incident handling process
- Describe the incident handling workflow with FortiSIEM and FortiSOAR

- Analyze, handle, and tune incidents on FortiSIEM
- Ingest FortiSIEM incidents into FortiSOAR for incident handling
- Escalate FortiSOAR alerts into incidents
- Describe automation requirements
- Describe FortiSOAR playbook steps
- · Run playbooks to enrich indicators
- Configure a playbook to retrieve a hash rating from FortiSandbox
- Perform containment on FortiGate, Windows Active Directory, and FortiClient EMS using FortiSOAR connectors
- Eradicate artifacts from a compromised host
- Release a compromised host from quarantine after recovery
- Manage playbook history logs

# Security Operations Architect (SECOP-ARCH)

# Centres de formation dans le monde entier





## Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3 CH-8304 Wallisellen Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch