Fortinet Certified Solution Specialist Security Operations

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Fortinet Certified Solution Specialist Security Operations

Course Modules

NSE 7 – Advanced Analytics 6.3

1.Multi-Tenancy SOC Solution for MSSP

- Describe multi-tenancy solutions for SOC environment
- Define and deploy collectors and agents
- Install and manage FortiSIEM Windows and Linux agents

2.FortiSIEM Rules

- Explain FortiSIEM rule processing
- Construct FortiSIEM rules
- Explain the MITRE ATT&CK® framework

3.FortiSIEM Baseline and UEBA

- Explain FortiSIEM baseline and profile reports
- Construct FortiSIEM baseline rules
- Configure UEBA on FortiSIEM

Fortinet Certified Solution Specialist Security Operations

4.Clear Conditions and Remediation

- Remediate incidents on FortiSIEM manually and automatically
- Remediate incidents using FortiSOAR

Advanced Analytics 6.7 Architect

5.Multi-Tenancy SOC Solution for MSSP

- Describe multi-tenancy solutions for SOC environments
- Define and deploy collectors and agents
- Install and manage FortiSIEM Windows and Linux agents

6.FortiSIEM Rules and Analytics

- Explain FortiSIEM rule processing
- Construct FortiSIEM rules
- Configure advanced nested queries and lookup tables

7.FortiSIEM Baseline and UEBA

- Explain FortiSIEM baseline and profile reports
- Construct FortiSIEM baseline rules
- Explain UEBA on FortiSIEM

Fortinet Certified Solution Specialist Security Operations

8.Conditions and Remediation

- Incidents on FortiSIEM both manually & automatically
- Remediate incidents through FortiSOAR

Security Operations 7.4 Analyst

9.SOC concepts and adversary behavior

- Analyze security incidents and identify adversary behaviors
- Map adversary behaviors to MITRE ATT&CK tactics & techniqes
- Identify components of the Fortinet SOC solution

10. Architecture and detection capabilities

- Configure and manage collectors and analyzers
- Design stable and efficient FortiAnalyzer deployments
- Design, configure, & manage FortiAnalyzer Fabric deploymnts

11. SOC operation

- Configure and manage event handlers
- Analyze and manage events and incidents
- Analyze threat hunting information feeds
- Manage outbreak alert handlers and reports

12. SOC automation

- Configure playbook triggers and tasks
- Configure and manage connectors
- Manage playbook templates
- Monitor playbooks

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474