Fortinet Certified Professional Security Operations

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Fortinet Certified Professional Security Operations

Course Modules

Fortinet NSE 5 – FortiAnalyzer 7.2 Analyst

1.Features and concepts

- Describe FortiAnalyzer concepts

2.Logging

- Analyze logs
- Describe log fetching
- Gather log statistics

3.SOC

- Manage events and event handlers
- Manage incidents
- Explain SOC features on FortiAnalyzer

4.Reports

- Manage reports
- Troubleshoot reports

5.Playbooks

- Explain playbook components
- Create and manage playbooks

Zetlan Technologies

Fortinet Certified Professional Security Operations

Fortinet NSE 4 – Forti OS 7.2

6.Deployment and System Configuration

- Perform initial configuration
- Implement the Fortinet Security Fabric
- Configure log settings and diagnose problems using the logs
- Config VDOMs to split a FortiGate into multiple virtual devices
- Configure different operation modes for an FGCP HA cluster
- Diagnose resource and connectivity problems

7.Firewall and authentication

- Configure firewall policies
- Configure firewall policy NAT and central NAT
- Configure different methods of firewall authentication
- Explain how to deploy and configure FSSO

Zetlan Technologies

8.Content inspection

- Inspect encrypted traffic using certificates
- Identify FortiGate inspection modes and configure web filtering
- Configure app control to monitor and control network apps
- Config antivirus scanning modes to neutralize malware threats
- Config IPS to protect network from threats and vulnerabilities

Fortinet Certified Professional Security Operations

9.Routing

- Configure & route packets using static and policy-based routes

10. VPN

- Configure and implement different SSL VPN modes
- Implement a meshed or partially redundant IPsec VPN
- Configure ZTNA to provide role-based application access

FortiGate 7.4 Administrator

11. Deployment and system configuration

- Perform initial configuration
- Implement the Fortinet Security Fabric
- Configure an FGCP HA cluster
- Diagnose resource and connectivity problems

12. Firewall policies and authentication

- Configure firewall policies
- Configure SNAT and DNAT options in firewall policies
- Configure different methods of firewall authentication
- Explain how to deploy and configure FSSO

Fortinet Certified Professional Security Operations

13. Content inspection

- Explain and inspect encrypted traffic using certificates
- Identify FortiGate inspection modes and config web filtering
- Config app control to monitor and control network applications
- Config antivirus scanning modes to neutralize malware threats
- Config IPS to protect networks from threats and vulnerabilities

14. Routing

- Configure and route packets using static routes
- SD-WAN to load blnce traffic betwn multipl WAN links effctivly

15. VPN

- Config & implement difft SSL VPNs to provide secure access
- Implement a meshed or partially redundant IPsec VPN

Zetlan Technologies

NSE 5 – Forti EDR 5.0

16. FortiEDR system

- Explain FortiEDR architecture and technical positioning
- Perform installation process
- Perform FortiEDR inventory and use system tools
- Deploy FortiEDR multi-tenancy
- Use API to carry out FortiEDR management functions

Fortinet Certified Professional Security Operations

17. FortiEDR security settings and policies

- Configure communication control policy
- Configure security policies
- Configure playbooks
- Explain Fortinet Cloud Service (FCS)

18. Events, forensics, and threat hunting

- Analyze security events and alerts
- Configure threat hunting profiles and scheduled queries
- Analyze threat hunting data
- Investigate security events using forensics analysis

19. FortiEDR integration

- Deploy FortiXDR
- Configure security fabric using FortiEDR

20. FortiEDR troubleshooting

- Perform FortiEDR troubleshooting
- Perform alert analysis on FortiEDR security events and logs

Fortinet Certified Professional Security Operations

NSE 5 – Forti SIEM 6.3

21. SIEM Concepts

- Identify FortiSIEM architecture components
- Identify deployment requirements
- Identify event type classification
- Perform system configuration and management tasks
- Tshoot system configuration and deployment related issues

22. FortiSIEM Operations

- Discover devices on FortiSIEM
- Build queries from search results and events
- Tune data collection and notification processes
- Deploy FortiSIEM agents
- Troubleshoot discovery related issues

23. FortiSIEM Analytics

- Apply group by and data aggregation on search results
- Use various reporting functions available on FortiSIEM

Zetlan Technologies

24. Rules and Incidents

- Identify various rule components
- Configure rule sub-patterns, aggregation and group by
- Manage incidents
- Configure clear conditions for incidents
- Configure notification policies

Forti SOAR 7.3 Administrator

25. SOC and SOAR Overview

- Identify deployment requirements
- Manage FortiSOAR licensing
- Configure initial settings
- Manage incidents and alerts

26. System Configuration

- Configure applications, system fixtures, and proxy
- View and manage audit logs
- Export and import FortiSOAR system configuration
- Configure FortiSOAR HA

Zetlan Technologies

Fortinet Certified Professional Security Operations

For Enquiry: +91 8680961847

27. Security Management

- Configure and manage role-based access control (RBAC)
- Configure and manage teams and team hierarchy
- Difft between appliance authentication and user authentication
- Troubleshoot security management issues

28. System Operation

- Externalize and migrate Elasticsearch data
- Configure the recommendation engine
- Configure and operate a war room

29. System Monitoring and Maintenance

- Monitor FortiSOAR using system tools
- Monitor various FortiSOAR processes and services
- View and interpret various FortiSOAR log files
- Upgrade FortiSOAR

Zetlan Technologies

Free Advice: +91 9600579474
www.zetlantech.com

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