NSE 7 Public Cloud Security Course

Course Duration: 16 Hrs. **Course Code: NSE7-PCS-101**

Course Overview

The **NSE 7 Public Cloud Security** course is designed for security and cloud professionals responsible for protecting public cloud environments such as AWS, Microsoft Azure, and Google Cloud Platform (GCP). This advanced course focuses on cloud-native security controls, policy enforcement, identity management, threat detection, and compliance in public cloud infrastructures. Participants will gain hands-on experience in securing cloud workloads, implementing best practices, and integrating Fortinet cloud security solutions for enterprise-grade protection.

What You'll Learn?

By completing this course, you will be able to:

- Understand the security challenges in public cloud environments
- Implement cloud-native security controls and policies
- Secure cloud workloads and data across AWS, Azure, and GCP
- Configure identity and access management in cloud environments
- Monitor and respond to cloud-based security threats
- Apply compliance and governance best practices
- Integrate Fortinet cloud security solutions with public cloud services

Target Audience

This course is ideal for:

- Cloud Security Engineers and Architects

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Network and Security Administrators managing public cloud environments
- SOC Analysts focusing on cloud security
- IT and DevOps professionals responsible for cloud operations
- Professionals preparing for the NSE 7 Public Cloud Security certification

Pre-Requisites

Participants should have:

- Solid understanding of cloud computing concepts
- Familiarity with networking and cybersecurity fundamentals
- Experience with AWS, Azure, or GCP is recommended
- Knowledge of identity management, security policies, and compliance frameworks

Course Content

Module 1: Introduction to Public Cloud Security

- Overview of public cloud platforms
- Cloud security challenges and threat landscape
- Shared responsibility model

Module 2: Identity and Access Management

- Cloud IAM best practices
- Role-Based Access Control (RBAC) and policies
- Multi-Factor Authentication (MFA) and conditional access

Module 3: Cloud Workload and Data Security

- Securing virtual machines and containers
- Data encryption and key management
- Cloud storage and database security

Module 4: Network Security in the Cloud

- Virtual networks, subnets, and firewalls
- Cloud-native DDoS protection and traffic inspection
- Secure connectivity (VPN, Direct Connect, ExpressRoute)

Module 5: Threat Detection and Monitoring

- Cloud security monitoring tools and dashboards
- Event logging, alerting, and SIEM integration
- Automated incident response

Module 6: Compliance, Governance, and Best Practices

- Regulatory compliance in public clouds
- Policy management and security frameworks
- Operational best practices for cloud security

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com