SCAZT (Designing and Implementing Secure Cloud Access for Users and Endpoints) Course

Course Duration: 32 Hours **Course Code: SCAZT**

1. Course Overview

The **SCAZT: Designing and Implementing Secure Cloud Access for Users and Endpoints** course equips IT professionals and security practitioners with the skills to design, implement, and manage secure access solutions in modern cloud environments. The training focuses on securing user identities, devices, and applications, ensuring compliance, and mitigating cyber threats. Participants will gain in-depth knowledge of endpoint security, cloud access models, authentication strategies, and policy enforcement to safeguard organizational resources.

2. What You'll Learn?

By the end of this course, you will be able to:

- Understand the principles of secure cloud access for users and endpoints.
- Implement authentication and identity management solutions in cloud environments.
- Design secure access policies for devices, users, and applications.
- Configure endpoint protection to minimize vulnerabilities and attacks.
- Integrate zero-trust security models for enhanced access management.
- Monitor, manage, and troubleshoot secure cloud access solutions.

3. Target Audience

This course is ideal for:

- Cloud Security Engineers
- Identity and Access Management (IAM) Specialists
- Security Administrators and Analysts
- IT Infrastructure and Endpoint Administrators
- Network and Cloud Architects
- Professionals preparing for advanced cloud security roles

4. Pre-Requisites

Before taking this course, participants should have:

- Basic understanding of cloud computing concepts (IaaS, PaaS, SaaS).
- Familiarity with identity and access management fundamentals.
- Knowledge of networking and security principles.
- Prior experience with any major cloud platform (Azure, AWS, or Google Cloud) is recommended.

5. Course Content

Module 1: Introduction to Secure Cloud Access

- Cloud security challenges and trends
- Principles of user and endpoint protection
- Zero Trust security concepts

Module 2: Identity and Access Management (IAM)

- Authentication methods and MFA
- Single Sign-On (SSO) integration

- Role-Based Access Control (RBAC) and Policy-Based Access Control (PBAC)

Module 3: Endpoint Security in Cloud Environments

- Endpoint management strategies
- Device compliance and posture checks
- Securing mobile and remote endpoints

Module 4: Designing Secure Access Policies

- Conditional access design
- Policy enforcement for applications and devices
- Data protection and compliance requirements

Module 5: Implementing Zero Trust Models

- Zero Trust for users and endpoints
- Micro-segmentation and access controls
- Continuous authentication and monitoring

Module 6: Monitoring and Incident Response

- Security monitoring and analytics
- Threat detection and remediation
- Incident response for access-related breaches

Module 7: Hands-On Labs and Case Studies

- Configuring secure access in a cloud environment
- Implementing endpoint protection policies
- Real-world scenarios and troubleshooting