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

Course Duration: 40 Hours **Course code: SCAZT**

1. Course Overview

The Designing and Implementing Secure Cloud Access for Users and Endpoints course will provide you with the skills to design and implement cloud security architectures, user and device security, network and cloud security, application and data security, visibility and assurance, and threat response. Some of the Cisco solutions covered in this course include Cisco SecureX, Cisco XDR, Cisco Duo, Cisco ISE, Cisco Catalyst SD-WAN, Cisco Umbrella, Cisco Secure Firewall, Cisco Secure Workload, Cisco Secure Analytics, and more.

2. What you'll learn?

After completing this course, participants will be able to:

- Describe identity and access management in cloud environments
- Implement secure access using Zero Trust Architecture
- Configure and enforce Conditional Access policies
- Integrate endpoint protection with cloud identity solutions
- Securely onboard and monitor devices
- Manage authentication methods including MFA and passwordless
- Protect cloud-based apps using Cloud App Security and Defender
- Implement compliance policies and risk-based access
- Monitor and investigate access-related incidents
- Apply real-time remediation and automation workflows

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

3. Target Audience

Anyone involved in the Design and Implementation of a Cisco Secure Cloud Access Solution.

4. Pre-Requisites

Attendees should meet the following prerequisites:

- Basic understanding of Enterprise Routing
- Basic understanding of WAN Networking
- Basic understanding of Cisco SD-WAN
- Basic understanding of Public Cloud services

Recommended prerequisites:

- CCNA - Implementing and Administering Cisco Solutions
- SDWFND - Cisco SD-WAN Operation and Deployment
- SCOR - Implementing and Operating Cisco Security Core Technologies

5. Course content

1- Certificate-Based User and Device Authentication

- PKI Overview
- PKI Operations
- User versus Machine or Device-Based Certificates
- 802.1X and EAP Methods
- Cisco ISE Certificate Services
- Cisco ISE BYOD Client Certificate Configuration

2- Cisco Duo Multifactor Authentication for Application Protection

- Zero Trust Security Using MFA
- About Duo MFA and Splunk
- Cisco Duo with AnyConnect VPN for Remote Access

- Use Cisco Duo Authentication
- About Cisco Duo MFA and Remote Access VPN

3- Introducing Cisco ISE Endpoint Compliance Services

- Endpoint Compliance Services Overview

4- SSO using SAML or OpenID Connect

- SSO using Security Assertion Markup Language
- Using SAML or OpenID Connect
- Single Sign-On with Cisco Duo

5- Reverse Proxy

- Reverse Proxy
- Reverse Proxy Implementation to Protect Applications

6- Cisco SD-WAN Security Content Filtering

- Cisco SD-WAN Content Filtering
- Secure Direct Internet Access
- Impelmenting Unified Security Polices

7- Cisco SD-WAN to Cisco Umbrella SIG Integration

- SIG Overview
- Integrating SIG and Cisco SD-WAN
- Cisco Umbrella DNS Deep Dive
- Cisco Umbrella CDFW and IPS
- Cisco Umbrella Secure Web Gateway

8- Cisco Umbrella Cloud Access Security Broker

- Cloud Application Security Overview

- Implementing Cisco Umbrella CASB

9- Security Policies for Remote Access VPN

- Cisco Secure Firewall Remote Access VPN Security
- Cisco IOS XE SD-WAN Remote Access VPN Security

10- Cisco Secure Access

- Cisco Secure Access: SSE Reimagined
- Cisco Secure Client New Capabilities
- QUIC and MASQUE Protocol Benefits
- Cisco Secure Access Use Cases

11- Cisco Secure Firewall

- Cisco Secure Firewall Platforms
- Cisco Secure Firewall Use Cases
- Cisco Secure Firewall Policies Configuration

12- Web Application Firewall

- Introduction to WAFs
- Cisco Secure WAF Best Practices

13- Cisco Secure Workload Deployments, Agents, and Connectors

- Cisco Secure Workload Capabilities and Deployments
- Cisco Secure Workload Deployments, Agents and Connectors

14- Cisco Secure Workload Structure and Policy

- Cisco Secure Workload Inventory and Scopes
- Cisco Secure Workload Workspaces
- Cisco Secure Workload Policy Discovery

15- Multicloud Security Policies

- Multicloud Security Policies Benefits and Requirements
- Multicloud Security Architecture
- Cisco Multicloud Defense

16- Cloud Security Attacks and Mitigations

- Cloud Security Models
- MITRE ATT&CK® Framework
- MITRE ATT&CK® Matrix for Enterprise Cloud-Based Techniques
- Practical Application of MITRE ATT&CK®
- MITRE ATT&CK® Navigator

17- Cloud Visibility and Assurance

- Cloud Visibility and Assurance Requirements
- Cloud Visibility and Assurance Tools
- Cloud Visibility and Assurance Automation

18- Cisco Secure Network Analytics and Cisco Secure Analytics and Logging

- Cisco Secure Network Analytics
- Cisco Secure Network Analytics Components
- Secure Network Analytics Use Cases
- Cisco Security Analytics and Logging (SAL)

19- Cisco XDR

- Cisco XDR Overview
- Cisco XDR Components
- Cisco Secure Cloud Analytics

20- Cisco Attack Surface Management

- Cisco Attack Surface Management Introduction
- Cisco XDR Integration
- Cisco Attack Suface Management Use Cases

21- Cloud Applications and Data Access Verifications

- User Cloud Access Verification
- User Cloud Access Verification Using Cisco Duo
- User Cloud Access Verification Using Cisco Cloud Analytics
- User Cloud Access Verification Usng Cisco Secure Workload
- User Cloud Access Verification Usng Cisco Umbrella
- User Cloud Access Verification Usng Cisco Secure Firewall

22- Industry Security Frameworks

- Introduction to Security Frameworks
- National Institute of Standards and Technologies Cybersecurity Framework
- Cybersecurity and Infrastructure Security Agency Framework
- Defense Information System Agency Framework
- Comparison of Security Frameworks

23- Cisco Security Reference Architecture Fundamentals

- Talos Threat Intelligence
- XDR Security Operations Toolset
- User/Device Security
- Network Security: Cloud Edge and On-Premises
- Workload, Application and Data Security

24- Cisco Security Reference Architecture Common Use Cases

- Common Identity

- Converged Multicloud Policy
- SASE Integration
- ZeroTrust Network Access
- XDR Telemetry and Orchestration

25- Cisco SAFE Architecture

- Cisco SAFE Framework
- Key Components of Cisco SAFE
- Cisco SAFE Phases

26- Exploring Cisco SD-WAN ThousandEyes

- Cisco ThousandEyes Overview
- Deploying Cisco ThousandEyes with Cisco SD-WAN

27- Automation of Cloud Policy

- Automation of Cloud Policy
- Tools for Automation of Cloud Policy and Troubleshooting

28- Response to Cloud Threats

- Threat Response Fundamentals
- Response to Data Breaches and User or Application Compromises
- Regulatory Changes and Security Audit Responses

29- Automation of Cloud Threat Detection and Response

- Cloud Threat Detection and Respnse Automation
- Automation of Cloud Threat Detection and Response Tools
- Cisco XDR Response Tasks and MITRE ATT&CK® Mappings