DESIGNING AND IMPLEMENTING SECURE CLOUD ACCESS FOR USERS AND ENDPOINTS V1.0 (SCAZT)

DESIGNING AND IMPLEMENTING SECURE CLOUD ACCESS FOR USERS AND ENDPOINTS V1.0 (SCAZT)

The Designing and Implementing Secure Cloud Access for Users and Endpoints v1.0 training teaches you the skills for designing and implementing cloud security architecture, user and device security, network and cloud security, cloud application and data security, cloud visibility and assurance, and responding to cloud threats.

This training prepares you for the 300-740 SCAZT v1.0 exam. If passed, you earn the Cisco Certified Specialist – Security Secure Cloud Access certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification.

How you'll benefit

This class will help you:

- Attain skills for designing and implementing cloud security architecture, user and device security, network and cloud security, cloud application and data security, cloud visibility and assurance, and responding to cloud threats
- Gain knowledge for protocols, solutions, and designs to acquire professional-level and expert-level cloud design and implementation roles

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Network Engineers
- Network Security Engineers
- Network Architects
- Sales/Presales Engineers

Course Duration
5 days
Course Price
$4,395.00 or 44 CLCs
Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

OUTLINE

Module 1: Industry Security Frameworks

Module 2: Cisco Security Reference Architecture Fundamentals

Module 3: Cisco Security Reference Architecture Common Use Cases

Module 4: Cisco SAFE Architecture

Module 5: Certificate-Based User and Device Authentication

Module 6: Cisco Duo Multifactor Authentication for Application Protection

Module 7: Cisco Duo with AnyConnect VPN for Remote Access

Module 8: Introducing Cisco ISE Endpoint Compliance Services

Module 9: SSO using SAML or OpenID Connect

Module 10: Deploying On-Premises Threat Prevention

Module 11: Examining Content Filtering

Module 12: Exploring Cisco Umbrella SIG

Module 13: Reverse Proxy

Module 14: Securing Cloud Application with Cisco Umbrella SIG

Module 15: Exploring Cisco SD-WAN ThousandEyes

Module 16: Optimizing SaaS Applications

Module 17: Security Policies for Remote Access VPN

Module 18: Cisco Secure Access

Module 19: Cisco Secure Firewall

Module 20: Web Application Firewall

Module 21: Cisco Secure Workload Deployments, Agents, and Connectors

Module 22: Cisco Secure Workload Structure and Policy

Module 23: Cloud Security Attacks and Mitigations

Module 24: Multicloud Security Policies

Module 25: Cloud Visibility and Assurance

Module 26: Cisco Secure Network Analytics and Cisco Secure Analytics and Logging

Module 27: Cisco XDR

Module 28: Cisco Attack Surface Management

Module 29: Cloud Applications and Data Access Verifications

Module 30: Automation of Cloud Policy

Module 31: Response to Cloud Threats

Module 32: Automation of Cloud Threat Detection and Response

LAB OUTLINE

- **Lab 1: Explore Cisco SecureX**
- **Lab 2: Windows Client BYOD Onboarding Interactive Activity**
- **Lab 3: Use Cisco Duo MFA to Protect the Splunk Application**
- **Lab 4: Integrate the Cisco Duo Authentication Proxy to Implement MFA for Cisco Security Secure Firewall AnyConnect Remote Access VPN**
- **Lab 5: Configure Cisco ISE Compliance Services**
- **Lab 6: Configure Threat Prevention**
- **Lab 7: Implement Web Security**
- **Lab 8: Deploy DIA Security with Unified Security Policy**
- **Lab 9: Configure Cisco Umbrella DNS Policies**
- **Lab 10: Deploy Cisco Umbrella Secure Internet Gateway**
- **Lab 11: Implement CASB Security**
- **Lab 12: Microsoft 365 SaaS Testing by Using Cisco ThousandEyes**
- **Lab 13: Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense**
- **Lab 14: Configure Cisco Secure Firewall Policies**
- **Lab 15: Explore Cisco Secure Workload**
- **Lab 16: Explore the ATT&CK Matrix Cloud-Based Techniques**
- **Lab 17: Explore Cisco Secure Network Analytics**
- **Lab 18: Explore Cisco XDR Incident Response Tasks**