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

Duration: 180 days

The Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) Learning Path 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 Learning Path 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.

Skills You'll Learn

- Design and implement cloud security architecture, including user, device, network, and cloud security
- Configure and manage certificate-based authentication and Cisco Duo multi-factor authentication for applications and VPNs
- Understand and apply Cisco Secure Firewall, web application firewall, and Cisco Umbrella Secure Internet Gateway features
- Utilize Cisco Secure Workload, Secure Network Analytics, and automation for cloud threat detection and response

Learning Path Objectives

1. Cloud Security Architectures: Learn some of the main industry security frameworks and the components of the Cisco Security Reference Architecture (SRA).
2. User and Device Authentication and Posturing: Discover the methods for authenticating the users and devices, determining the device security posture, and understanding Single Sign On operations with SAML and OpenID.
3. Control and Secure Access to Cloud Applications: Implement various on-prem and cloud-based security solutions to control and secure access to the cloud applications, and to implement secured remote access VPN.
4. Cloud Application and Data Security: Explore how to secure cloud workloads and cloud data and learn about cloud attacks and mitigations.
5. Cloud Visibility and Assurance: Learn how to provide cloud visibility and assurance for all cloud assets.
6. Responding to Threats in the Cloud: Discover how to response to regulatory compliance issues, cloud mis-configuration issues, cloud threats, and cloud data breaches.