Designing Cisco Security Infrastructure (CPLL-SDSI)

Duration: 180 Days

The Designing Cisco Security Infrastructure (SDSI) Learning Path teaches you about security architecture design, including secure infrastructure, applications, risk, events, requirements, artificial intelligence (AI), automation, and DevSecOps.

This Learning Path prepares you for the 300-745 SDSI v1.0 exam. If passed, you earn the Cisco Certified Specialist – Designing Cisco Security Infrastructure certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification.

Skills You'll Learn:

- Identify and explain fundamental security architecture concepts and how they guide the secure design, building, and maintenance of infrastructure
- Analyze and apply security layers, core technologies, and infrastructure concepts to build robust defenses
- Implement and enforce security design principles, frameworks, and regulatory compliance to align with business and legal requirements
- Deploy and manage detection, response, and access control tools to secure networks, endpoints, and cloud environments
- Adapt and optimize security strategies and architectures to address evolving threats, modern enterprise needs, and technology advancements

Learning Path Objectives:

1. Security Architecture Design Fundamentals: Gain the expertise to design, implement, and sustain comprehensive, compliant, and resilient network security architectures that protect modern enterprise environments and ensure regulatory adherence.
2. Security Architecture for Infrastructure Protection: Develop your abilities to design, implement, and manage comprehensive cybersecurity strategies that enable you to anticipate, mitigate, and respond to threats while ensuring resilient and high-performance digital infrastructure.
3. Firewall Technologies and Advanced Security Solutions: Strengthen your skills to deploy and manage Next-Generation Firewalls, Intrusion Detection and Prevention Systems, and web application security measures to proactively detect, prevent, and respond to advanced cyber threats while ensuring comprehensive protection for your network, endpoints, and web applications.

4. Application Security and Secure Data Flow: Empower yourself to defend your digital assets by mastering strategies for securing web and mobile applications, APIs, and cloud-native environments while gaining insights into how emerging technologies like AI and quantum computing are transforming the application security landscape.
5. Risk Management and Incident Response Strategies: Learn to use SIEM and SOAR tools for real-time incident detection and response, proactively manage risks, and apply industry-standard post-incident recovery strategies to strengthen your organization's security and resilience.
6. DevSecOps Integration and Automated Security Pipelines: Enhance your skills in DevSecOps to ensure security is integral to your CI/CD pipeline, automate secure development workflows, and improve your organization's threat detection and response capabilities.