SC-100: Microsoft Cybersecurity Architect

Microsoft - Security

- **Nível:** Avançado
- **Duração:** 28h

Sobre o curso

Este curso prepara os formandos com a especialização necessária para desenhar e avaliar estratégias de cibersegurança nas seguintes áreas: Zero Trust, Governance, Risk and Compliance (GRC), operações de segurança (SecOps) e dados e aplicações.

Os formandos aprendem também a desenhar e arquitetar soluções utilizando princípios de Zero Trust e a definir requisitos de segurança para infraestruturas cloud em diferentes modelos de serviço (SaaS, PaaS, IaaS).

Destinatários

Este curso destina-se a engenheiros de segurança cloud experientes que tenham obtido uma certificação anterior no portefólio de security, compliance e identity.

Pré-requisitos

Este é um curso avançado, de nível especialista. Embora não seja obrigatório para frequentar, recomenda-se fortemente que os formandos tenham frequentado e obtido aprovação noutra certificação de nível associate do portefólio de security, compliance e identity (como AZ-500, SC-200 ou SC-300) antes de frequentarem esta formação.

Em concreto, os formandos devem ter experiência e conhecimentos avançados numa vasta gama de áreas de engenharia de segurança, incluindo identidade e acesso, proteção de plataforma, operações de segurança, proteção de dados e proteção de aplicações.

Devem também ter experiência com implementações híbridas e cloud. Os formandos em início de percurso devem, em alternativa, frequentar o curso SC-900: Microsoft Security, Compliance, and Identity Fundamentals.

Programa

- Desenhar soluções alinhadas com boas práticas e prioridades de segurança
- Desenhar operações de segurança, identidade e capacidades de conformidade
- Desenhar soluções de segurança para aplicações e dados
- Desenhar soluções de segurança para infraestrutura

Desenhar soluções alinhadas com boas práticas e prioridades de segurança

Aprende a utilizar boas práticas críticas de segurança da Microsoft para melhorar a postura de segurança de uma organização, aplicar princípios de Zero Trust e minimizar o risco de ataques emergentes. Os frameworks abordados incluem o Cloud Adoption Framework (CAF), Well-Architected Framework (WAF) e Microsoft Cybersecurity Reference Architecture (MCRA).

- Introdução ao Zero Trust e frameworks de boas práticas
- Desenhar soluções alinhadas com o Cloud Adoption Framework (CAF) e Well-Architected Framework (WAF)
- Desenhar soluções alinhadas com a Microsoft Cybersecurity Reference Architecture (MCRA) e o Microsoft cloud security benchmark (MCSB)
- Desenhar uma estratégia de resiliência contra ransomware e outros ataques com base nas Microsoft Security Best Practices

Desenhar operações de segurança, identidade e capacidades de conformidade

Aprende a desenhar soluções para operações de segurança (SecOps), gestão de identidade e acesso, acesso privilegiado e conformidade regulamentar.

- Desenhar soluções para conformidade regulamentar
- Desenhar soluções para gestão de identidade e acesso
- Desenhar soluções para proteger acessos privilegiados
- Desenhar soluções para operações de segurança

Desenhar soluções de segurança para aplicações e dados

Aprende a desenhar soluções para proteger dados e aplicações, incluindo Microsoft 365, desenvolvimento de aplicações, portefólios de aplicações existentes, descoberta e classificação de dados com Microsoft Purview e segurança de dados para workloads no Azure.

- Avaliar soluções para proteger Microsoft 365
- Desenhar soluções para proteger aplicações
- Desenhar soluções para proteger os dados de uma organização

Desenhar soluções de segurança para infraestrutura

Aprende a desenhar soluções para segurança de infraestrutura. Estas soluções incluem a definição de requisitos para diferentes modelos de cloud, o desenho de soluções para gestão de postura de segurança em ambientes híbridos e multicloud e a proteção de endpoints.

- Definir requisitos para proteger serviços SaaS, PaaS e IaaS

- Desenhar soluções para gestão de postura de segurança em ambientes híbridos e multicloud
- Desenhar soluções para proteger endpoints de servidor e cliente
- Desenhar soluções para segurança de rede