SC-500: Implement end-to-end security controls for cloud and AI workloads

Microsoft - Security

- **Nível:** Intermédio
- **Duração:** 28h

Sobre o curso

Implementa controlos de segurança end-to-end para proteger ambientes Microsoft Azure, Microsoft 365 e workloads de Inteligência Artificial.

Este curso prepara-te para planear, implementar e gerir controlos de segurança end-to-end em ambientes Microsoft Azure e Microsoft 365, incluindo workloads de IA e agentes autónomos. O foco está na aplicação prática de tecnologias de segurança Microsoft para proteger identidades, infraestrutura, dados, aplicações, redes e recursos cloud.

Através de sessões orientadas por formador e laboratórios práticos, desenvolves competências em segurança de identidade, proteção de infraestrutura cloud, deteção de ameaças, conformidade regulatória e gestão da postura de segurança. A formação destina-se a security engineers responsáveis por implementar controlos de segurança em ambientes cloud, híbridos e multicloud.

Destinatários

- Security engineers responsáveis por proteger sistemas e dados organizacionais em ambientes cloud e híbridos.
- Profissionais que implementam controlos de segurança para prevenir acessos não autorizados e mitigar riscos de forma proativa.
- Profissionais que atuam em domínios como identidade, rede, aplicações, dados, compute e segurança de workloads de IA.
- Equipas que trabalham em articulação com arquitetos, administradores, engenheiros, analistas e developers responsáveis por Azure, Microsoft 365, identidade e acesso, proteção de informação, operações de segurança, DevOps, desenvolvimento aplicacional, bases de dados e redes.

Objetivos

- Proteger o acesso a recursos com Microsoft Entra ID e Azure Key Vault.
- Aplicar segurança e conformidade regulatória em ambientes cloud.

- Proteger armazenamento, bases de dados e redes em Azure.
- Implementar controlos de segurança para compute, servidores, máquinas virtuais e serviços aplicacionais.
- Proteger soluções e workloads de Inteligência Artificial.
- Gerir e monitorizar a postura de segurança com tecnologias Microsoft.

Condições

Para particulares

• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.

• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição; restante valor até 7 dias antes do início do curso.

• Possibilidade de pagamento faseado.

• Isenção de IVA para particulares.

Para empresas

• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).

• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

- Experiência prática na administração de ambientes Microsoft Azure e ambientes híbridos, incluindo componentes de compute, rede e armazenamento.
- Forte familiaridade com Microsoft Entra ID, nomeadamente no contexto de gestão de identidade e acesso.
- Familiaridade com a administração de Microsoft 365.

Programa

- Proteger o acesso a recursos com Microsoft Entra
- Proteger o Azure Key Vault com defesa em profundidade para workloads cloud e de IA
- Aplicar governação de segurança e conformidade regulatória
- Implementar segurança para Azure Storage no contexto do Cloud and AI Security Engineer
- Implementar segurança para bases de dados Azure SQL
- Implementar controlos de segurança de rede em Azure
- Implementar segurança para IA
- Implementar segurança para servidores e máquinas virtuais
- Proteger serviços da plataforma aplicacional Azure no contexto do Cloud and AI Security Engineer
- Gerir a postura de segurança com Microsoft Defender for Cloud
- Implementar recolha de atividade e eventos no Microsoft Sentinel
- Implementar e operar o Microsoft Security Copilot

Proteger o acesso a recursos com Microsoft Entra

Este módulo aborda a proteção do acesso a recursos com Microsoft Entra, com foco na autenticação, na gestão

de privilégios e na integração segura de plugins de API para agentes declarativos. Permite compreender como aplicar controlos de identidade e acesso em cenários cloud e de IA.

- Gerir e implementar métodos de autenticação no Microsoft Entra ID
- Implementar e configurar o Privileged Identity Management (PIM)
- Autenticar o plugin de API para agentes declarativos com APIs protegidas

Proteger o Azure Key Vault com defesa em profundidade para workloads cloud e de IA

Com foco na proteção de segredos, chaves e certificados, este módulo explora a configuração segura do Azure Key Vault em workloads cloud e de IA. A formação trabalha uma abordagem de defesa em profundidade, incluindo monitorização, gestão de ciclo de vida e proteção com Microsoft Defender for Cloud.

- Configurar e proteger o Azure Key Vault
- Gerir chaves e segredos no Azure Key Vault
- Gerir certificados e monitorizar o Azure Key Vault
- Proteger o Azure Key Vault com Microsoft Defender for Cloud

Aplicar governação de segurança e conformidade regulatória

Este módulo centra-se na governação de segurança e conformidade regulatória em ambientes Azure. São abordadas políticas, bloqueios de recursos, recomendações de segurança, RBAC, proteção de backups e controlos de segurança em infraestrutura como código, com foco na aplicação de requisitos organizacionais.

- Aplicar governação com Azure Policy e bloqueios de recursos
- Configurar controlos de segurança e corrigir recomendações no Defender for Cloud
- Avaliar a conformidade regulatória no Defender for Cloud
- Gerir e dimensionar corretamente atribuições de funções RBAC para aplicar o princípio do menor privilégio
- Proteger dados de backup com funcionalidades de segurança do Azure Backup
- Implementar controlos de segurança em infraestrutura como código

Implementar segurança para Azure Storage no contexto do Cloud and AI Security Engineer

Este módulo aborda a implementação de segurança em Azure Storage no contexto do perfil Cloud and AI Security Engineer. Explora serviços de armazenamento, gestão de acessos, segurança de rede e proteção com Microsoft Defender for Storage, aplicando controlos para reduzir riscos sobre dados e workloads.

- Descrever os serviços de Azure Storage
- Implementar segurança e gerir acessos para Azure Storage
- Configurar a segurança de rede para Azure Storage
- Implementar o Microsoft Defender for Storage

Implementar segurança para bases de dados Azure SQL

Este módulo foca-se na proteção de Azure SQL Database e Azure SQL Managed Instance. A formação aborda configurações de segurança ao nível da plataforma, auditoria e Microsoft Defender for Databases, permitindo implementar controlos para proteger dados e monitorizar riscos em bases de dados Azure.

- Configurar a segurança ao nível da plataforma para Azure SQL
- Configurar auditoria para Azure SQL Database e Azure SQL Managed Instance
- Implementar o Microsoft Defender for Databases

Implementar controlos de segurança de rede em Azure

Explora a implementação de controlos de segurança de rede em Azure, incluindo segmentação, isolamento de workloads, inspeção de tráfego, conectividade remota e híbrida, e redução da exposição pública de serviços PaaS. O módulo reforça práticas de proteção em arquiteturas cloud.

- Segmentar e isolar workloads Azure através de controlos de segurança de rede
- Centralizar e aplicar a inspeção de tráfego com Azure Firewall
- Proteger a conectividade remota e híbrida com VPN Gateways e Microsoft Entra Private Access
- Eliminar a exposição pública de rede de serviços Azure PaaS

Implementar segurança para IA

Este módulo aborda a segurança de soluções e workloads de Inteligência Artificial, incluindo identidades de agentes, riscos associados a IA, proteção de agentes Copilot Studio, AI Gateway, guardrails, Microsoft Defender for Cloud, Microsoft Agent 365 e Microsoft Purview Data Security Posture Management.

- Proteger o acesso para identidades de agentes Microsoft Entra
- Analisar riscos de identidade de IA com Microsoft Defender XDR
- Ativar proteção em tempo real para agentes Copilot Studio
- Configurar a segurança do AI Gateway no Microsoft Foundry
- Configurar e gerir guardrails no Microsoft Foundry
- Proteger workloads de IA com Microsoft Defender for Cloud
- Ativar a proteção de workloads do Defender for AI Services no Microsoft Defender for Cloud
- Gerir agentes com Microsoft Agent 365
- Identificar riscos de dados de IA com Microsoft Purview Data Security Posture Management

Implementar segurança para servidores e máquinas virtuais

Este módulo trabalha a proteção de servidores e máquinas virtuais em Azure e ambientes híbridos. São abordados temas como encriptação de discos, trusted launch, Azure Bastion, Azure Arc, Microsoft Defender for Servers, acesso just-in-time e configuração segura com Azure Machine Configuration.

- Implementar encriptação de discos para máquinas virtuais Azure
- Configurar funcionalidades de segurança trusted launch para máquinas virtuais Azure
- Planear e implementar o Azure Bastion
- Gerir a segurança de servidores híbridos compatíveis com Azure Arc
- Implementar o Microsoft Defender for Servers
- Ativar e aplicar acesso just-in-time a máquinas virtuais
- Aplicar configuração de segurança em máquinas virtuais com Azure Machine Configuration

Proteger serviços da plataforma aplicacional Azure no contexto do Cloud and AI Security Engineer

Focado na segurança de serviços aplicacionais Azure, este módulo aborda riscos em containers, AKS, Azure Container Registry, Container Instances, Container Apps, Function Apps, Logic Apps, App Services, Web Application Firewall e API Management, com aplicação a ambientes cloud e IA.

- Detetar riscos em containers com Microsoft Defender for Containers
- Implementar controlos de segurança para Azure Kubernetes Service
- Implementar controlos de segurança para Azure Container Registry, Container Instances e Container Apps
- Implementar controlos de segurança para Azure Function Apps e Logic Apps
- Implementar controlos de segurança para Azure App Services e Web Application Firewall
- Implementar segurança de backend de API com Azure API Management

Gerir a postura de segurança com Microsoft Defender for Cloud

Este módulo aborda a gestão da postura de segurança com Microsoft Defender for Cloud. A formação inclui ligação de ambientes híbridos e multicloud, identificação de riscos, CSPM, exposição externa, conformidade regulatória, proteção de workloads e gestão de vulnerabilidades em Azure VMs.

- Ligar ambientes híbridos e multicloud ao Microsoft Defender for Cloud
- Identificar riscos de segurança através de Cloud Security Posture Management
- Descobrir ativos desprotegidos e vulnerabilidades com Microsoft Defender External Attack Surface Management
- Avaliar a conformidade regulatória no Defender for Cloud
- Ativar e configurar planos de proteção de workloads no Microsoft Defender for Cloud
- Configurar definições de Microsoft Defender Vulnerability Management para máquinas virtuais Azure

Implementar recolha de atividade e eventos no Microsoft Sentinel

Este módulo explora a recolha de atividade e eventos no Microsoft Sentinel. O foco está na criação e gestão de workspaces, conteúdos, conectores Microsoft, syslog, Common Event Format, hosts Windows, regras de automação, playbooks, armazenamento de dados e auditoria de logs.

- Criar e gerir workspaces do Microsoft Sentinel
- Gerir conteúdos no Microsoft Sentinel
- Ligar serviços Microsoft ao Microsoft Sentinel
- Ligar fontes de dados syslog ao Microsoft Sentinel
- Ligar logs Common Event Format ao Microsoft Sentinel
- Ligar hosts Windows ao Microsoft Sentinel
- Implementar regras de automação e playbooks no Microsoft Sentinel
- Gerir armazenamento de dados e consultar logs de auditoria no Microsoft Sentinel

Implementar e operar o Microsoft Security Copilot

Este módulo aborda a implementação e operação do Microsoft Security Copilot em contextos de segurança modernos. O foco está no acesso seguro para identidades de agentes, análise de riscos de identidade de IA,

proteção de agentes, AI Gateway, guardrails, Defender for Cloud, Microsoft Agent 365 e riscos de dados com Microsoft Purview.

- Descrever o Microsoft Security Copilot
- Configurar workspaces para Microsoft Security Copilot
- Gerir plugins e agentes no Microsoft Security Copilot