Curso CSCL300 - Domínio da Cibersegurança na Cloud Microsoft

Duração: 35h

Introdução

Neste curso vai aprender a proteger o seu ambiente com as ferramentas de segurança da Microsoft e uma abordagem em camadas assente nos princípios Zero Trust. Vai adquirir competências práticas na proteção de identidades e acessos, na deteção de ameaças e na proteção de cargas de trabalho, tanto no Microsoft 365 como no Azure.

Vai também aprender a investigar e responder a incidentes com ferramentas como o Microsoft Defender XDR e o Microsoft Sentinel, incluindo threat hunting e automatização.

No fim da formação será capaz de detetar, analisar e responder a incidentes de segurança em todo o seu ambiente e de melhorar a postura de segurança global.

Público-alvo

Este curso destina-se a administradores de sistemas e profissionais de segurança que gerem a segurança e a resposta a incidentes em ambientes cloud e híbridos.

No final do curso

Após a conclusão deste curso, os formandos deverão ser capazes de:
- Proteger identidades na cloud com o Microsoft Entra e o Microsoft Defender for Identity.
- Proteger email, endpoints e aplicações cloud com o Microsoft Defender.
- Detetar e travar ataques com o Microsoft Defender XDR e o Microsoft Security Copilot.
- Aplicar governação e proteção da informação.
- Investigar incidentes e fazer threat hunting com o Microsoft Sentinel e a Kusto Query Language.
- Proteger o acesso a recursos Azure com o Microsoft Defender for Cloud.

Pré-requisitos

Experiência de administração de sistemas em ambientes cloud ou híbridos.

Exames de certificação

(não existem exames)

Conteúdo programático em detalhe

Panorâmica da segurança na cloud
- O panorama das ameaças
- Ameaças e tipos de ataque comuns
- O dilema de quem defende
- O modelo Zero Trust
- O modelo de responsabilidade partilhada
- A attack kill chain

- Identity and access management
- Proteção contra ameaças
- Gestão de segurança
- Proteção da informação
- LAB: panorâmica da segurança na nuvem

Microsoft Entra: proteger as identidades na cloud

- Single sign-on
- Ataques baseados em palavras-passe
- Autenticação multifator
- Autenticação sem palavra-passe
- Roubo de tokens
- Métodos de autenticação do Entra
- Identity Protection
- Conditional access
- Privileged Identity Management
- LAB: proteger as suas identidades

Microsoft Defender for Identity

- Ataques com base em Kerberos
- Funcionalidades do Microsoft Defender for Identity
- Configurar o Defender for Identity
- Proteger as suas contas
- Identificar ameaças: reconhecimento e movimento lateral
- Detetar ataques pass-the-hash e pass-the-ticket
- LAB: Microsoft Defender for Identity

Microsoft Defender for Office 365

- Proteger contra malware, spam, phishing e spoofing
- Autenticação de correio eletrónico: SPF, DKIM e DMARC
- Attack simulator
- Safe attachments e safe links
- Proteção contra ameaças na colaboração: SharePoint, OneDrive e Teams
- LAB: Microsoft Defender for Office 365

Microsoft Defender for Endpoint

- Panorâmica da segurança de endpoints
- Proteger os seus dispositivos
- Integrar dispositivos
- Threat and vulnerability management
- Endpoint detection and response
- Investigação de dispositivos
- Investigação e remediação automatizadas
- LAB: Microsoft Defender for Endpoint

Microsoft Defender for Cloud Apps

- Cloud discovery
- App connectors
- Controlar o acesso às aplicações com políticas

- Conditional access app control
- Proteger informação sensível
- LAB: Microsoft Defender for Cloud Apps

Detetar e travar ataques com o Microsoft Defender XDR

- Microsoft Defender XDR
- Proteger o seu ambiente
- Recomendações de segurança e secure score
- Threat analytics e relatórios de segurança
- Investigação de ataques
- Threat hunting
- LAB: Microsoft Defender XDR

Microsoft Security Copilot

- Investigar incidentes com o Copilot
- Analisar scripts suspeitos
- Fazer threat hunting como um profissional
- Plugins do Copilot
- Fundamentos de prompt engineering para casos de uso de segurança

Governação e proteção da informação

- O portal do Microsoft Purview
- Sensitive information types
- Trainable classifiers
- Sensitivity labels
- Data loss prevention
- Communication compliance
- Insider risk management
- Retention labels e políticas de retenção
- LAB: governação e proteção da informação

Microsoft Sentinel

- Panorâmica do Microsoft Sentinel
- Preçário do Sentinel e retenção dos dados de log
- Ativar o Microsoft Sentinel
- Integrar fontes de segurança: data connectors e Content Hub
- Threat intelligence
- Watchlists
- User and entity behavior analytics (UEBA)
- LAB: Microsoft Sentinel

Kusto Query Language

- Kusto Query Language
- Escrever queries de log básicas
- Filtrar dados
- Agregar dados
- Usar variáveis
- Juntar várias tabelas numa só query
- LAB: Kusto Query Language

Investigação de incidentes e threat hunting com o Microsoft Sentinel

- Análise e investigação no Sentinel
- Automatização e orquestração de segurança: automation rules e playbooks
- Threat hunting
- Gerar relatórios de segurança com os workbooks do Sentinel
- LAB: investigação de incidentes e threat hunting no Microsoft Sentinel

Proteger o acesso a recursos Azure

- Microsoft Identity Platform
- Role-based access control
- Privileged Identity Management (PIM) para papéis do Azure
- Azure Key Vault
- Ciclo de vida de segredos, chaves e certificados
- Workload identities: service principals e managed identities
- App registrations e enterprise apps
- LAB: proteger o acesso a recursos do Azure

Microsoft Defender for Cloud

- Panorâmica do Microsoft Defender for Cloud
- Planos e preçário do Defender for Cloud
- Políticas e iniciativas de segurança
- Recomendações de segurança e secure score
- Conformidade regulamentar
- Funcionalidades de proteção de workloads: just-in-time VM access e file integrity monitoring
- Alertas de segurança, incidentes e investigação
- LAB: Microsoft Defender for Cloud