Curso CSDF200 - Segurança na Cloud com o Microsoft Defender XDR

Duração: 21h

Introdução

Este curso ensina profissionais de segurança e de TI a detetar, investigar e responder a ameaças de segurança em ambientes cloud e híbridos modernos. Os participantes aprendem a proteger identidades, dispositivos, aplicações e dados contra técnicas de ataque comuns e avançadas. O curso foca-se em compreender o comportamento dos ataques, analisar sinais de segurança, investigar incidentes e tomar as ações de resposta adequadas para limitar o impacto e evitar a repetição. Através de laboratórios práticos e cenários realistas, os participantes desenvolvem competências concretas em deteção de ameaças, investigação de incidentes e threat hunting proativo, aprendendo também a aplicar boas práticas que melhoram a postura de segurança global da organização.

Se também lhe interessa a segurança do Microsoft Azure, recomenda-se o curso CSCL300 «Domínio da Cibersegurança na Cloud Microsoft».

Público-alvo

Este curso destina-se a profissionais de TI e especialistas de segurança responsáveis por proteger, monitorizar e governar ambientes Microsoft 365.

No final do curso

Após a conclusão deste curso, os formandos deverão ser capazes de:
• Proteger identidades com o Microsoft Entra e o Microsoft Defender for Identity.
• Proteger email, endpoints e aplicações cloud com o Microsoft Defender.
• Detetar, investigar e travar ataques com o Microsoft Defender XDR.
• Utilizar o Microsoft Security Copilot.
• Aplicar governação e proteção da informação.

Pré-requisitos

Experiência de administração de ambientes Microsoft 365.

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

www.actualtraining.pt
Tel: +351 217 158 018

- 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