SC-5001: Configure SIEM security operations using Microsoft Sentinel

Microsoft - Security

Live Training (também disponível em presencial)

- **Localidade:**
- **Data:** 14 Feb 2025
- **Preço:** 590 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das 9h00 às 17h00
- **Nível:** Intermédio
- **Duração:** 7h

Sobre o curso

Descubra as operações de segurança do Microsoft Sentinel através da configuração do workspace do mesmo.

Entre no mundo do Microsoft Sentinel e das suas operações de segurança, dando os primeiros passos no mesmo através da configuração do workspace do Microsoft Sentinel, da conexão de serviços da Microsoft e de eventos de segurança do Windows ao Microsoft Sentinel, da configuração de regras de analítica do Microsoft Sentinel e da resposta a ameaças com recurso a respostas automatizadas.

Destinatários

Profissionais que pretendam configurar as operações de segurança do sistema SIEM recorrendo ao Microsoft Sentinel.

Pré-requisitos

- Compreensão fundamental do Microsoft Azure
- Compreensão básica do Microsoft Sentinel
- Experiência com a linguagem Kusto Query Language (KQL) no Microsoft Sentinel

Programa

- Criação e gestão de workspaces do Microsoft Sentinel
- Conexão de serviços da Microsoft ao Microsoft Sentinel
- Conexão de hosts do Windows ao Microsoft Sentinel
- Deteção de ameaças através da processo de analítica realizado pelo Microsoft Sentinel
- Automação no Microsoft Sentinel
- Configuração das operações de segurança do sistema SIEM recorrendo ao Microsoft Sentinel

Criação e gestão de workspaces do Microsoft Sentinel

- Neste módulo, os participantes ficarão a saber mais sobre a arquitetura dos workspaces do Microsoft Sentinel, de modo a garantirem a configuração do seu sistema de acordo com os requisitos relativos às operações de segurança delineados pela organização para a qual laboram.

Conexão de serviços da Microsoft ao Microsoft Sentinel

- Os participantes aprenderão a conectar os logs de serviço do Microsoft 365 e do Azure ao Microsoft Sentinel.

Conexão de hosts do Windows ao Microsoft Sentinel

- Os eventos de segurança do Windows são um dos logs mais comummente recolhidos. Os participantes ficarão a par de como o Microsoft Sentinel facilita este processo graças ao conector de Eventos de Segurança.

Deteção de ameaças através da processo de analítica realizado pelo Microsoft Sentinel

- Neste módulo, os participantes aprenderão como o processo de analítica executado pelo Microsoft Sentinel pode ajudar a equipa de SecOps a identificar e parar ciberataques.

Automação no Microsoft Sentinel

- No final deste módulo, os participantes estarão aptos a usar regras de automação no Microsoft Sentinel, de forma a proceder à gestão automatizada de incidentes.

Configuração das operações de segurança do sistema SIEM recorrendo ao Microsoft Sentinel

- Neste último módulo, os participantes aprenderão a configurar as operações de segurança do sistema SIEM recorrendo ao Microsoft Sentinel.