

Wird noch definiert

### Ihr Nutzen

Wird noch definiert

### Voraussetzungen

Keine

### Preis pro Teilnehmer

EUR 850,- exklusive der gesetzlichen MwSt.

### Hinweise

SC-5001,

### Seminardauer

1 Tag(e)/Day(s)

Version: N/A

### Seminarinhalte

- \* Create and manage Microsoft Sentinel workspaces
  - Introduction
  - Plan for the Microsoft Sentinel workspace
  - Create a Microsoft Sentinel workspace
  - Manage workspaces across tenants using Azure Lighthouse
  - Understand Microsoft Sentinel permissions and roles
  - Manage Microsoft Sentinel settings
  - Configure logs
  - Knowledge check
  - Summary and resources
- \* Connect Microsoft services to Microsoft Sentinel
  - Introduction
  - Plan for Microsoft services connectors
  - Connect the Microsoft Office 365 connector
  - Connect the Microsoft Entra connector
  - Connect the Microsoft Entra ID Protection connector
  - Connect the Azure Activity connector
  - Knowledge check
  - Summary and resources
- \* Connect Windows hosts to Microsoft Sentinel
  - Introduction
  - Plan for Windows hosts security events connector
  - Connect using the Windows Security Events via AMA Connector
  - Connect using the Security Events via Legacy Agent Connector
  - Collect Sysmon event logs
  - Knowledge check
  - Summary and resources
- \* Threat detection with Microsoft Sentinel analytics
  - Introduction
  - Exercise - Detect threats with Microsoft Sentinel analytics
  - What is Microsoft Sentinel Analytics?
  - Types of analytics rules
  - Create an analytics rule from templates
  - Create an analytics rule from wizard
  - Manage analytics rules
  - Exercise - Detect threats with Microsoft Sentinel analytics
  - Summary
- \* Automation in Microsoft Sentinel
  - Introduction
  - Understand automation options
  - Create automation rules
  - Knowledge check
  - Summary and resources

- \* Configure SIEM security operations using Microsoft Sentinel
  - Introduction
  - Exercise - Configure SIEM operations using Microsoft Sentinel
  - Exercise - Install Microsoft Sentinel Content Hub solutions and data connectors
  - Exercise - Configure a data connector Data Collection Rule
  - Exercise - Perform a simulated attack to validate the Analytic and Automation rules
  - Summary

