

Azure SOC Basic Workshop



SOC mit Microsoft Sentinel

Ein SOC (Security Operations Center) Service mit Azure Sentinel ist eine leistungsstarke Lösung zur Sicherheitsüberwachung und -reaktion, die von Microsoft Azure angeboten wird. Azure Sentinel ist ein cloudbasierter SIEM (Security Information and Event Management)-Dienst, der entwickelt wurde, um Organisationen bei der Identifizierung, Analyse und Reaktion auf Sicherheitsbedrohungen zu unterstützen

Microsoft Sentinel

- Highly integrated services
- Flexible and scalability
- Easy to customize
- Best organizational support



Best organization structure

- Supports your current organization
- Consideration of cultural aspects
- Impact on your process landscape

Knowing how to go on in your organization

Knowledge of the Tools

- Tools and process overview
- Mapping your organization to Azure Sentinel
- Demo

Best-practice how to use

Related to your requirements

- No fixed agenda
- You define the direction & pace
- Focused on you

Fully fits in your demand

Nach Abschluss dieses Workshops werden die Teilnehmer über das grundlegende Wissen und die Fähigkeiten verfügen, um Azure Sentinel in ihrer Organisation einzuführen und effektiv für die Sicherheitsüberwachung und -reaktion einzusetzen.