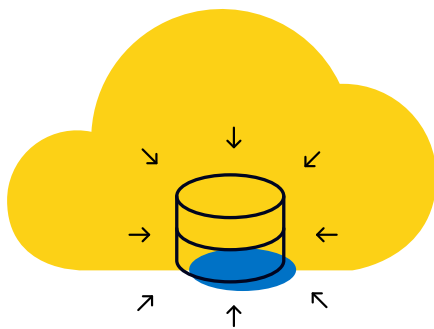


Microsoft Sentinel POC



Remote 3-Day Workshop | 4.500 €



Aggregate Your Data with Microsoft Sentinel

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel aggregates data from all sources, including users, applications, servers, and devices in any cloud or on-premises. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Have an overview about the functions of Azure Sentinel

- Security Overview
- E5 Security Framework
- Zero Trust

Understand how to use Azure Sentinel and the infrastructure

- On-board Sentinel
- Connect Data sources
- Discover rule templates

Setup your Workspaces and connect your data sources

- Define Playbooks
- Detecting Threats
- Demonstrate remediation



Contact Details

Jan Geisbauer
Lead Security Architect
jan.geisbauer@glueckkanja-gab.com

About glueckkanja-gab

glueckkanja-gab.com/csoc
info@glueckkanja-gab.com
+49 69 4005520