

Andreas Wiedner

IT Security Advisor, IT-Projektleiter

junis

Kurzprofil

Andreas Wiedner ist IT Security Advisor und IT-Projektleiter für Microsoft Security Services mit Schwerpunkt auf der Gestaltung und Implementierung sicherer Architekturen in hybriden Cloud-Umgebungen. Seit 2023 begleitet er Unternehmen aus Finanzdienstleistung und Rückversicherung bei der SIEM/SOC-Migration nach Microsoft Sentinel, beim Rollout von Microsoft Defender for Endpoint und bei der Umsetzung von DORA. Zu seinen Schwerpunkten gehören außerdem Microsoft Defender XDR, Microsoft Intune, Policy as Code, DevSecOps und Data Security. Davor verantwortete er IT und Entwicklung eines Web-Plattform-Anbieters im Logistik- und Verkehrssektor, einschließlich agiler Entwicklerteams für cloud-native Webanwendungen und der Absicherung des Microsoft-365-Tenants mit Microsoft Defender.

Schwerpunkte

IT-Strategie · Microsoft Security Services · Microsoft Defender XDR · Microsoft Sentinel SIEM/SOC Architecture · Hybrid Cloud Security · Microsoft Intune · Policy as Code · DevSecOps · Data Security · DORA

Zertifikate

Microsoft Certified

- Azure Security Engineer Associate (AZ-500)
- Security Operations Analyst Associate (SC-200)
- Security, Compliance, and Identity Fundamentals (SC-900)
- Azure Fundamentals (AZ-900)

Weitere

- ITIL v3 Foundation
- Six Sigma Yellow Belt

Ausbildung

- International Business Studies
- International Management
- Mechanical Engineering

Sprachen

- Deutsch (Muttersprache)
- Englisch (C2)
- Schwedisch (A2)
- Spanisch (A2)

Kontakt

junis GmbH · hallo@junis.de · junis.de

Ansprechpartner für Projektvermittler: Lukas Lohrsträter, lukas.lohrstraeter@junis.de

Projekte

Umsetzung des Digital Operational Resilience Act (DORA)

Finanzdienstleistung · Security Advisor, Engineer · seit 06/2024

`Azure` · `PowerShell` · `Microsoft Sentinel` · `Microsoft Defender` · `Confluence`

Beratung und Unterstützung bei der kurzfristigen Erreichung der DORA-Compliance mit Schwerpunkt auf Gestaltung, Implementierung, Automatisierung und Dokumentation der Meldewege. Analyse von Abhängigkeiten sowie Identifikation von Single Points of Failure (SPOF) in der IT-Sicherheitsinfrastruktur und Entwicklung von Empfehlungen dazu.

SIEM/SOC-Migration nach Microsoft Sentinel

Rückversicherung · Security Advisor, Engineer · 02/2024 – 12/2024

`Azure` · `Microsoft Sentinel` · `Microsoft Defender XDR` · `Azure Arc` · `KQL` · `Microsoft Graph` · `Linux Server`

Beratung und Durchführung der kurzfristigen Migration der zentralen SIEM/SOC-Umgebung nach Microsoft Sentinel. Setup der Infrastruktur, unterbrechungsfreie Umleitung aller Logquellen, Optimierung von Datenmengen und Kosten sowie Absicherung des Datentransits. Weiterführende bedarfsgerechte Beratung nach dem Go-live.

Rollout Microsoft Defender for Endpoint

Finanzdienstleistung · Security Advisor, Engineer · 08/2023 – 02/2024

`Azure Arc` · `Microsoft Defender for Endpoint` · `Microsoft Defender XDR` · `Microsoft Intune`

Projektleitung und Security Advisory bei der Migration von McAfee Antivirus zu Microsoft Defender for Endpoint für Linux- und Windows-Server in einer regulatorisch anspruchsvollen Umgebung. Abstimmung und Implementierung der notwendigen Security Policies über Microsoft Defender XDR und Microsoft Intune. Unterstützung beim Aufbau von Microsoft Sentinel und bei der Integration der Logdaten aus Microsoft Defender, Steuerung der Fachbereiche und Beratung zu sicherheitsrelevanten Logdaten.

IT- und Entwicklungsleitung eines Web-Plattform-Anbieters im Logistik- und Verkehrssektor

Logistik · IT- und Entwicklungsleitung · 01/2017 – 07/2023

`Microsoft 365` · `Microsoft Defender for Endpoint` · `Microsoft Defender for Office 365` · `Microsoft Defender for Servers`

Aufbau und Leitung eines neuen Firmenstandorts sowie Leitung mehrerer agiler Entwicklerteams für cloud-native Webanwendungen. Aufbau, Betrieb und Absicherung des standortübergreifenden Microsoft-365-Tenants mit Microsoft-Defender-Produkten für Endpoints, Exchange, SharePoint, Teams und Server. Leitung von Entwicklung und Betrieb mehrerer Produkte zur Erfassung und Steuerung von Lieferverkehren und Flächen auf Messegeländen sowie zur Optimierung intermodaler Seecontainertransporte für Reedereien. Entwicklung von Proofs of Concept für die Stahlindustrie und den Verteidigungssektor.