Andreas Wiedner

IT SECURITY ADVISOR, IT-PROJEKTLEITER

Andreas ist ein erfahrener IT-Projektleiter und Security-Architekt mit über einem Jahrzehnt Branchenerfahrung. Sein fundiertes Fachwissen erstreckt sich über verschiedene Bereiche, wobei sein Schwerpunkt auf der Gestaltung und Implementierung sicherer Architekturen liegt.

KONTAKT

andreas.wiedner@junis.de

+49 171 2114389

www.junis.de

33100 Paderborn

SPRACHEN

Deutsch	(m)
Englisch	C2
Schwedisch	A2
Spanisch	A2

ZERTFIKATE UND SCHULUNGEN

Microsoft Azure Security Technologies (AZ-500)

Microsoft Security Operations Analyst (SC-200)

Azure Services for Security Engineers Microsoft Security, Compliance, and Identity Fund. (SC-900)

Azure Fundamentals (AZ-900)

ITIL v3

Six Sigma Yellow Belt

AUSBILDUNG

International Business Studies
Paderborn, Deutschland

International Management
Jönköping, Schweden

Mechanical Engineering
Paderborn, Deutschland

SCHWERPUNKTE

IT Strategy · Microsoft Security Services · Defender XDR · Sentinel SIEM/SOC Architecture · Hybrid Cloud Security · Microsoft Intune Azure Enterprise Policy as Code · DevSecOps · Data Security

PROJEKTERFAHRUNG

Umsetzung Digital Operational Resilience Act (DORA) für eine deutsche Privatbank

Branche:	privat Bank
Rolle:	Security Advisor, Engineer
Zeitraum:	06/2024 – ongoing

Genutzte Technologien:

- Azure
- Powershell
- Sentinel
- Defender
- Confluence

Projektbeschreibung:

Beratung und Unterstützung bei der kurzfristigen Erreichung der DORA-Compliance mit Schwerpunkt auf die Gestaltung und Implementierung von Meldewegs-Prozessen, deren Automatisierung und Dokumentation. Darüber hinaus die Analyse von Abhängigkeiten, sowie der Identifikation und Empfehlungsentwicklung für SPOFs in Bezug auf IT-Sicherheits-Infrastruktur.

SIEM/SOC-Migration nach Microsoft Sentinel für einen internationalen Rückversicherer

Security Advisor, Engineer

02/2024 - 12/2024

Genutzte Technologien:

- Azure
- Microsoft Sentinel
- Defender XDR
- Azure Arc
- KQL, Graph-API
- Linux Servers

Beratung und Durchführung der kurzfristigen Migration der zentralen SIEM/SOC Umgebung eines globalen Rückversicherers nach Microsoft Sentinel. Das Projekt umfasste u.a. das Setup der Infrastruktur, die unterbrechungsfreie Umleitung aller weltweiten Logquellen, Datenmengen- und Kostenoptimierung, sowie die Absicherung des Datentransits. Weiterführende bedarfsgerechte Beratung nach Go-Live.

Rollout Defender for Endpoint für eine deutsche Privatbank

Security Advisor, Engineer

08/2023 - 02/2024

Genutzte Technologien:

- Azure Arc
- Defender for Endpoint
- Defender XDR
- Intune

Projektleitung und Security Advisory bei der Migration von McAfee Antivirus zu Defender for Endpoint für ca. 1000 Linux und Windows Server in einer regulatorisch anspruchsvollen Umgebung. Abstimmung und Implementierung notwendiger Security-Policies über Defender XDR und Intune. Unterstützung beim Aufbau von Microsoft Sentinel und der Integration von Logdaten aus Defender. Steuerung der Fachbereiche und Beratung bzgl. Security-relevanter Logdaten.

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

2017 - 2023

Aufbau und Leitung eines neuen Firmenstandorts sowie der Leitung mehrerer agilen Entwicklerteams aus 15 Entwicklern für cloud-native Web- Applikationen. Inklusive Aufbau, Betrieb und der Absicherung des standortübergreifenden Microsoft-Tenants mit Microsoft Defender Produkten (Endpoint, Exchange, SharePoint, Teams, Server). Vollständige Leitung über die Entwicklung und den Betrieb mehrerer Produkte zur Erfassung und Steuerung aller Lieferverkehre und Flächen für die größten Messegelände der EU, der Optimierung von internationalen Seecontainer Intermodaltransporten für die führenden Reedereien, sowie der Entwicklung von Proof of Concepts für die Stahlindustrie und das Cyber-Innovation-Hub der Bundeswehr.