



85% remote - Principal Infrastructure & Security Architect / Technical Delivery Lead (m/w/d)

Für unseren Kunden suchen wir einen Principal Infrastructure & Security Architect / Technical Delivery Lead (m/w/d).

Rahmendaten:

Start: asap

Laufzeit: 02/11/2026 bis 30/04/2027 (plus Verlängerungsoption)

Auslastung: Vollzeit

Einsatzort: 15% vor Ort, sonst remote

Aufgaben1. Technische Gesamtarchitektur und Zielbild

- + Bestehende Architekturen, Systemlandschaften, Abhängigkeiten und Schutzbedarfe analysieren und validieren.
- + Zielarchitekturen für Server, Hosting, Netzwerk und Security entwickeln und dokumentieren.
- + Architekturprinzipien und technische Entscheidungsgrundlagen projektübergreifend sicherstellen.
- + Optionen wie Weiterbetrieb, Härtung, Upgrade, Migration, Konsolidierung oder Rückbau bewerten.
- + Architekturbrüche, fehlende Voraussetzungen und Betriebsrisiken frühzeitig identifizieren.

2. Server-, Plattform- und Legacy-Modernisierung

- + Windows- und Legacy-Serverlandschaften bewerten, Linux-Grundlagen berücksichtigen.
- + Lifecycle- und End-of-Support-Risiken analysieren und priorisieren.
- + Upgrade-, Migrations-, Replatforming- und Stilllegungsstrategien erstellen.
- + Abhängigkeiten zu AD, DNS, Zertifikaten, Anwendungen, Datenbanken, Storage und Netzwerk berücksichtigen.
- + Assessments, Pilotierungen, Migrationen und Fehleranalysen aktiv unterstützen.

3. Server Security, Defender und Härtung

- + Microsoft Defender for Servers, Endpoint und Cloud bewerten.
- + Onboarding, Abdeckung, Ausnahmen und technische Voraussetzungen dokumentieren.
- + CIS Benchmarks und Microsoft Security Baselines auf bestehende Umgebungen anwenden.
- + Konflikte zwischen Security-Anforderungen und Legacy-Systemen analysieren.
- + Vulnerability-, Patch-, Logging- und Monitoring-Themen technisch unterstützen.

4. Netzwerk-, Infrastruktur- und Applikationsabhängigkeiten

- + Netzwerkpfade, Firewalls, Routing, DNS und Zertifikate analysieren.
- + Abhängigkeiten zwischen Servern, Proxies, Load Balancern, Gateways und Anwendungen bewerten.
- + Komplexe Störungen und Sicherheitskonflikte technologieübergreifend eingrenzen.
- + Netzwerk- und Firewall-Änderungen spezifizieren, testen und begleiten.
- + Cutover-, Rollback- und Abnahmeszenarien ausarbeiten.

5. Technische Orchestrierung und Qualitätssicherung

- + Arbeitspakete und Ergebnisse mehrerer Teams koordinieren.
- + Konzepte, Schätzungen, Migrationsstrategien und Umsetzungsstände kritisch prüfen.
- + Abstimmungen mit Infrastruktur-, Security-, Netzwerk- und Applikationsteams führen.
- + Risiken bewerten, Widersprüche auflösen und Handlungsoptionen entwickeln.
- + Akzeptanzkriterien und technische Vorgaben aus Architekturentscheidungen ableiten.

6. Eigenständige technische Umsetzung

- + Discovery-, Analyse- und Konfigurationsaufgaben selbstständig durchführen.
- + Konfigurationen, Skripte, Abfragen, Testfälle und Automatisierungen erstellen und prüfen.
- + PoCs, Pilotmigrationen, Härtings-, EDR- und Patchmaßnahmen umsetzen.
- + Fehleranalysen anhand von Logs, Monitoring, Konfigurationen und Netzwerktraces durchführen.
- + Ergebnisse inklusive Dokumentation, Tests und Betriebsübergaben verantworten.

7. Risiko-, Maßnahmen- und Eskalationsmanagement

- + Technische Risiken hinsichtlich Ursache, Auswirkung und Eintrittswahrscheinlichkeit bewerten.
- + Sicherheits- und Lifecycle-Risiken priorisieren.
- + Entscheidungsvorlagen mit Optionen, Aufwand, Voraussetzungen und Restrisiken erstellen.
- + Kritische Themen konsequent verfolgen und adressieren.
- + Eskalationen bis Management- und C-Level-Ebene fundiert begleiten.

8. Modernisierung, Rückbau und Betriebsübergabe

- + Kriterien für Weiterbetrieb, Migration, Ablösung oder Rückbau definieren.
 - + Abschaltvoraussetzungen und Abhängigkeiten prüfen.
 - + Migrations- und Decommissioning-Runbooks erstellen und begleiten.
 - + Abnahmekriterien, Testnachweise und Betriebshandover sicherstellen.
 - + Restrisiken, Ausnahmen und technische Schulden transparent dokumentieren.
-