

Alaa Sakbani

Senior Cybersecurity & IT Risk Consultant

DORA & Regulatory Security | Enterprise Security Architecture | Incident Response | Operational Resilience

Richardplatz 16, 12055 Berlin.

alaa_0005@hotmail.com 017621146432

linkedin.com/in/it-eng-alaasakbani/

B Führerschein * Deutsch - Englisch - Arabisch

ZUSAMMENFASSUNG

Senior Cybersecurity & IT Risk Consultant mit über 10 Jahren Erfahrung in der Absicherung von Unternehmens-, Behörden- und kritischen Infrastrukturen. Spezialisiert auf Enterprise Security Architecture, Vulnerability Management, Incident Response sowie regulatorische Sicherheitsanforderungen. Ich unterstütze Organisationen dabei, Sicherheitsrisiken zu reduzieren, IT-Infrastrukturen resilienter zu gestalten und Sicherheitsmaßnahmen mit geschäftlichen sowie regulatorischen Anforderungen in Einklang zu bringen. Meine Erfahrung umfasst unter anderem Netzwerksegmentierung, Cloud- und Infrastruktursicherheit, Security Governance sowie die Verbesserung von Incident-Response- und Vulnerability-Management-Prozessen in komplexen IT-Umgebungen.

ERFAHRUNG

Freiberuflicher Cybersecurity Consultant – Medical Device & System Image Security

Projekt über FERCHAU GmbH / WaveLight GmbH – Alcon

Februar 2026 - Juni 2026, DE, Teltow

- Durchführung von Vulnerability Assessments und Sicherheitsanalysen von Windows-Systemimages für medizinische Geräte
- Durchführung von Windows Image Hardening und Security Baseline Validation zur Absicherung kritischer Systemkonfigurationen
- Analyse von Systemkonfigurationen, Benutzerrechten und Netzwerkdiensten zur Identifikation potenzieller Angriffsflächen
- Durchführung von Compliance Verification und Security Reviews in regulierten MedTech-Umgebungen
- Unterstützung bei der Verbesserung der Medical Device Security durch gezielte Sicherheitsanalysen und Konfigurationsprüfungen
- Durchführung von System Configuration Reviews zur Stärkung der Systemsicherheit und Reduzierung von Risiken
- Automatisierung von Sicherheitsprüfungen und Analyseprozessen mittels PowerShell
- Zusammenarbeit mit internationalen Engineering- und IT-Security-Teams zur Verbesserung der Sicherheitsarchitektur

Project Manager – Cybersecurity Mini Diploma (Volunteer)

Syrian Youth Assembly

Juli 2025 – heute, DE, Berlin

- Initiierung und Leitung der Bildungsinitiative „Cybersecurity Mini Diploma“ in Zusammenarbeit mit Coursera und der Young Global Citizens Assembly
- Entwicklung und Durchführung von Vorlesungen, Workshops und Trainingsprogrammen im Bereich Cybersecurity
- Aufbau und Weiterentwicklung eines Cybersecurity-Lernbereichs mit über 6.000 registrierten Teilnehmern
- Organisation monatlicher Veranstaltungen und Mentoring für Teilnehmer in Blue, Red und Purple Team Bereichen
- Einführung eines KI-gestützten Broadcast-Formats zur Diskussion aktueller Cybersecurity-Themen
- Entwicklung eines Trainings- und Evaluationsprogramms zur Förderung technischer Fähigkeiten
- Aufbau virtueller Labore für praxisnahe Übungen in Vulnerability Analysis, Patch Management und Incident Response

Externer Cybersecurity Consultant – DORA Projekt

Projekt über FERCHAU GmbH / Investitionsbank des Landes Brandenburg (ILB)

Juli 2024 – August 2025, DE, Potsdam

- Mitarbeit an der Umsetzung von DORA-konformen Sicherheitsmaßnahmen in einer regulierten Banking-Umgebung
- Durchführung von Vulnerability Assessments mit Tenable und CrowdStrike sowie Koordination der Schwachstellenbehebung über Infrastruktur- und Endpoint-Systeme
- Analyse und Bearbeitung von Security Incidents sowie Unterstützung bei der Verbesserung der Incident-Response-Prozesse
- Unterstützung bei der Netzwerksegmentierung zur Reduzierung potenzieller Angriffsflächen
- Dokumentation sicherheitsrelevanter Risiken und Maßnahmen sowie Unterstützung interner und externer Security Audits
- Beitrag zur Verbesserung der Compliance- und Sicherheitsstrategie gemäß regulatorischer Anforderungen (DORA)

Cybersecurity Consultant

FERCHAU GmbH

Juni 2024 - Juni 2026, DE, Potsdam

- Beratung von Kunden im Bereich Cybersecurity, Informationssicherheit und IT-Risikomanagement
- Durchführung von Vulnerability Assessments und Sicherheitsanalysen
- Analyse und Bearbeitung von Security Incidents sowie Unterstützung bei der Verbesserung von Incident-Response-Prozessen
- Planung und Umsetzung von Netzwerksegmentierung und Sicherheitsmaßnahmen zur Reduzierung von Angriffsflächen
- Unterstützung bei Security Audits und regulatorischen Anforderungen, einschließlich Compliance- und Governance-Themen
- Dokumentation sicherheitsrelevanter Risiken, Maßnahmen und Sicherheitsprozesse

Founder & CEO – IT & Technology Services

Fastdealexpress

Mai 2023 – März 2024, DE, Berlin – NL, 's-Hertogenbosch

- Gründung und Aufbau eines IT- und Technologieunternehmens für kleine und mittelständische Unternehmen
- Planung und Implementierung von **IT-Infrastrukturen, Sicherheitslösungen und Backup-Systemen**
- Beratung von Kunden zu **Netzwerksicherheit, Serverlösungen und IT-Systemarchitektur**
- Projektmanagement für IT- und Security-Implementierungen in verschiedenen Branchen
- Aufbau und Betreuung internationaler Technologie- und Lieferkettenpartnerschaften
- Akquise und Betreuung von Kunden sowie Entwicklung individueller IT- und Sicherheitslösungen

IT & Cybersecurity Consultant

BlueTeam GmbH

Februar 2023 – April 2023, DE, Hannover

- Beratung von Unternehmen zur Verbesserung ihrer Cybersecurity- und IT-Sicherheitsstrategie
- Durchführung von Vulnerability Assessments und Penetrationstests zur Identifikation von Sicherheitsrisiken
- Implementierung und Konfiguration von Security-Lösungen (Palo Alto Firewalls, Check Point, Cortex SOC)
- Mitarbeit in einem Managed Security Operations Center (SOC) zur Analyse und Bearbeitung von Security Incidents
- Unterstützung bei Hardware- und Infrastruktur-Upgrades zur Verbesserung der Systemsicherheit
- Analyse von Sicherheitsvorfällen und Durchführung erster forensischer Untersuchungen unter Berücksichtigung der DSGVO

IT Consultant (Infrastructure & Security)

Chambionic GmbH

April 2022 - Dezember 2022, DE, Berlin

- Planung und Implementierung moderner **IT-Infrastrukturen, Cloud- und Netzwerklösungen** für Unternehmensumgebungen
- Beratung von Kunden zu **IT-Sicherheit, Serverarchitekturen und Digitalisierungslösungen**
- Implementierung und Konfiguration von **Firewall- und Netzwerksicherheitslösungen** (u.a. Securepoint)
- Leitung technischer Supportteams und Koordination von IT-Projekten
- Beschaffung und Integration von **Server- und Netzwerkinfrastruktur** für Kundenprojekte
- Einführung neuer **IT-Sicherheitsprotokolle**, wodurch die Systemsicherheit um **35 % verbessert** und rund **85 % der Sicherheitslücken reduziert** werden konnten

Niederspannungsingenieur

Al-Etqan Engineering Consultant Office

Mai 2011 - Mai 2015, Saudi-Arabien, Mekka

- Planung und Umsetzung technischer Infrastruktur- und Niederspannungsprojekte gemäß internationalen Standards
- Erstellung technischer Studien, Spezifikationen und Projektanalysen für öffentliche und private Bauprojekte
- Überwachung der Installation und Implementierung technischer Systeme vor Ort
- Sicherstellung der Einhaltung von Sicherheits- und Qualitätsstandards während der Projektumsetzung

PROJEKTE

Medical Device Security & System Image Hardening

Alcon Laboratories — 2026

- Durchführung von Sicherheitsanalysen und Vulnerability Assessments von Windows-Systemimages für medizinische Geräte
- Umsetzung von Windows Image Hardening und Security Baseline Validation
- Durchführung von System Configuration Reviews und Compliance Verification
- Automatisierung von Sicherheitsprüfungen und Analyseprozessen mittels PowerShell

DORA Cybersecurity Compliance – Banking Sector

Investitionsbank des Landes Brandenburg (ILB) — 2024–2025

- Unterstützung bei der Umsetzung von DORA-konformen Sicherheitsmaßnahmen
- Durchführung von Vulnerability Assessments mit Tenable und CrowdStrike
- Verbesserung von Incident-Response-Prozessen und Netzwerksegmentierung
- Unterstützung bei Security Audits und regulatorischer Compliance

High Availability Infrastructure & Virtualization

ImmoMa GmbH — 2022

- Aufbau eines Hyper-V Hochverfügbarkeitsclusters
- Entwicklung einer Backup- und Disaster-Recovery-Strategie
- Zentralisierung der Virtualisierungsinfrastruktur

Selected Engineering & Security Infrastructure Projects

Critical Infrastructure Security Systems

Government Facilities & Smart City Projects — Saudi Arabia

- Planung und Implementierung von Zutrittskontroll- und Videoüberwachungssystemen für Hochsicherheitsinfrastrukturen
- Integration von Sicherheitslösungen für Regierungsanlagen und kritische Einrichtungen
- Unterstützung beim Aufbau von technischer Infrastruktur und Rechenzentrumskomponenten

Enterprise Hotel Security Systems

Four Seasons, Mövenpick, Le Méridien, Ibis Hotels

- Implementierung von CCTV- und Zutrittskontrollsystemen für internationale Hotelketten
- Planung und Installation von Sicherheits- und Überwachungssystemen
- Integration von Sicherheitslösungen in bestehende Gebäudetechnik

BILDUNG

Informatik (laufend)

Kiron Open Higher Education — Berlin

IT-Fachinformatiker / Systemintegration

COMCAVE College — Berlin | 2023

Bachelor in Informationstechnologie – Schwerpunkt Netzwerktechnik

Universität für Informationstechnologie und Ingenieurwesen — Damaskus | 2010

ZERTIFIZIERUNGEN

Cybersecurity

- CompTIA Security+ — 2025
- ISC² Certified in Cybersecurity (CC) — 2023
- Palo Alto Networks Certified System Engineer — 2023

Cloud & Infrastructure

- Microsoft Certified: Azure Administrator Associate — 2022
- CompTIA Cloud+ — 2025

Networking

- Cisco Certified Network Associate (CCNA) — 2021
- Cisco Cybersecurity Analyst — in progress

Professional Programs

- ISC² Security Certification Track (SSCP, CCSP, CISSP) — in progress
- IBM Cybersecurity Analyst Professional Certificate — in progress

Training & Specializations

- ISO 27001 Lead Auditor (Training)
- SOC Operations & Security Monitoring
- Network Operations Center (NOC) Operations
- SIEM Monitoring & Analysis (Splunk)

FÄHIGKEITEN

Cybersecurity

- Schwachstellenmanagement
- Incident Response / Sicherheitsvorfallanalyse
- Sicherheitsarchitektur
- Netzwerksegmentierung
- Windows-System-Härtung
- Sicherheitsaudits & Compliance
- DORA & regulatorische Sicherheitsanforderungen

Sicherheitswerkzeuge & Plattformen

- Tenable
- CrowdStrike
- Splunk (SIEM)
- Palo Alto Networks
- Check Point

Infrastruktur & Netzwerke

- Netzwerksicherheit (Firewalls, IDS/IPS)
- VPN-Technologien
- TCP/IP, DNS, DHCP
- Windows Server Administration
- Hyper-V Virtualisierung

Cloud & Automatisierung

- Microsoft Azure
- PowerShell Automatisierung
- Security Baseline Validation
- Systemkonfigurationsanalyse

Governance & Compliance

- ISO 27001 Sicherheitsprinzipien
- IT-Risikomanagement
- SOC / SIEM Monitoring
- NOC Operations

SOFT SKILLS

- Strategisches und analytisches Denken
- Kommunikation mit Stakeholdern (Management & Technik)
- Sicherheitsrisikobewertung
- Projekt- und Teamkoordination
- Strukturierte Problemlösung und Entscheidungsfähigkeit