SECUINFRA
Cyber Defense. Made in Germany.

Wir suchen Dich als **CYBER DEFENSE CONSULTANT** (m/w/d)

Als Cyber Defense Consultant begleitest Du unsere Kunden in führender Position bei der Konzeptionierung, dem Design, der Implementierung und dem Betrieb von Lösungen zur Erkennung, Analyse und Abwehr von Cyberangriffen im SOC-Umfeld.

Konkret erwartet Dich folgendes:

- Aufnahme und Analyse der Ziele und Rahmenbedingungen beim Aufbau eines SOC/CDC bzw. den technischen Lösungen in diesem Umfeld
- Entwicklung von Betriebs-, Rollen-/Rechte-Konzepten sowie SOC- und CDC-Prozessen
- Konzeption, Design und Implementierung von Softwarelösungen zur Erkennung, Reaktion & Abwehr von Cyberangriffen
- Entwicklung, Implementierung und Optimierung von Detektionsmechanismen
- Mentoring von Kollegen mit weniger Berufserfahrung
- Projekt- & Teamleitung bei größeren Kundenprojekten

Anforderungsprofil

- Mindestens 2 Jahre Berufserfahrung im Aufbau und/oder dem Betrieb von Security Operations Centern (SOC) bzw. in angrenzenden Themenbereichen
- Eine solide Grundlage in allen Makrobereichen der IT (Networking, Betriebssysteme & grundlegendes Scripting)
- Sehr gute Deutsch- und Englischkenntnisse in Wort und Schrift.
- Reisebereitschaft (90% unserer Projekte sind aktuell remote)
- Eine analytische, strukturierte und eigenständige Denk- und Arbeitsweise
- Eine hohe Kunden- und Serviceorientierung und Übernahme von Verantwortung im Team
- Unternehmerisches Denken & Handeln
- Kenntnisse und Hands-on-Erfahrungen in einem oder mehreren der folgenden Produktsegmente:
    - SIEM (z.B. Elastic SIEM, Microsoft Sentinel, Splunk Enterprise Security, QRadar)
    - EDR (z.B. Microsoft Defender for Endpoint, Elastic Defend, CrowdStrike Falcon)
    - NDR (z.B. Corelight, Vectra AI, Darktrace)
    - SOAR (z.B. Swimlane, Palo Alto XSOAR, Microsoft Sentinel)
    - THOR APT Scanner