

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

Als Junior Cyber Defense Consultant begleitest Du unsere Kunden zusammen mit erfahrenen Kollegen bei 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 eine Berufsausbildung in einem IT-Beruf ODER einen Bachelorabschluss in einem Studiengang der Informatik \*
- 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
- Idealerweise erste Berührungspunkte und Kenntnisse in einem oder mehreren der folgenden Produktsegmente:
  - o SIEM (z.B. Elastic SIEM, Microsoft Sentinel, Splunk Enterprise Security, QRadar)
  - o EDR (z.B. Microsoft Defender for Endpoint, Elastic Defend, CrowdStrike Falcon)
  - o NDR (z.B. Corelight, Vectra AI, Darktrace)
  - o SOAR (z.B. Swimlane, Palo Alto XSOAR, Microsoft Sentinel)
  - o THOR APT Scanner