SECUINFRA
Cyber Defense. Made in Germany.

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

Als Cyber Defense Analyst begleitest Du unsere Kunden zusammen mit erfahrenen Kollegen bei Analyse und Abwehr von Cyber-Angriffen in unserem Cyber Detection und Response Center (CDRC). Zusätzlich unterstützt Du beim Betrieb der SIEM- und XDR-Systeme unserer CDRC-Kunden.

Konkret erwartet Dich folgendes:

- Tiefe Einarbeitung in die Technologien und Prozesse im CDRC
- Wechselnde Analysetätigkeiten in verschiedenen Detektions- und Abwehrsystemen halten deinen Arbeitsalltag interessant
- Einleiten von Response Maßnahmen zur Abwehr von Cyberangriffen
- Enger Kundenkontakt für regelmäßigen Austausch mit den Security-Abteilungen unserer Kunden
- Durchführung von internen Projekten sowie Spezialisierung in eingesetzten Technologien
- Level 1 & 2 Analysen zur Unterstützung unseres Forensikteams beim Compromise Assessment
- Entwicklung, Implementierung und Optimierung von Detektionsmechanismen
- Gute Work Life Balance im 24/7 Schichtmodell mit Incentives die ein hervorragender Ausgleich zur Schichtarbeit darstellen
- Mentoring von Kollegen mit weniger Berufserfahrung

Anforderungsprofil

- Mindestens 2 Jahre Berufserfahrung im Aufbau und/oder dem Betrieb von Security Operations Centern (SOC) bzw. in angrenzenden Themenbereichen ODER einen Master-Abschluss in einem Studiengang mit klarem Fokus auf IT-Sicherheit
- Eine solide Grundlage in allen Makrobereichen der IT (Networking, Betriebssysteme & grundlegendes Scripting)
- Sehr gute Deutsch- und Englischkenntnisse in Wort und Schrift.
- Optional Reisebereitschaft (wir arbeiten aktuell vorwiegend 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)
    - XDR (z.B. Microsoft Defender, Elastic Defend, Palo Alto Cortex, SentinelOne, CrowdStrike Falcon)
    - NDR (z.B. Corelight, Vectra AI, Darktrace)
    - SOAR (z.B. Microsoft Sentinel, Swimlane, Palo Alto XSOAR)
    - THOR APT Scanner