

**Be Part of our  
Security Journey!**

## **Bist Du bereit für eine neue Herausforderung?**

Für unser national agierendes Security Operation Center (SOC), welches von unseren ausgewiesenen Spezialisten mit hoher Expertise betrieben wird, suchen wir für den nächstmöglichen Zeitpunkt Verstärkung in Form eines SOC-Analysten (m/w/d).

### **SOC-Analyst (m/w/d)**

#### **Was Dich erwartet:**

- Du bist verantwortlich für die Überprüfung von Alarmmeldungen und deren Bewertung nach Dringlichkeit und Relevanz.
- Als Teil des Incident Response Teams bearbeitest du gemeinsam mit unseren Spezialisten entsprechende Vorfälle.
- Du überprüfst die Ergebnisse von Schwachstellen-Scans und unterstützt bei der Erstellung von Korrekturmaßnahmen.
- Du wirkst bei der Weiterentwicklung und dem Betrieb von Automatisierungsprozessen im Rahmen des Security Incident Prozesses mit und sorgst für die kontinuierliche Verbesserung und Wirksamkeitsprüfung.
  - Du unterstützt das Team bei der Erstellung von Security Use Cases und Regelwerken in unserem Security Information Event Management (SIEM) System.

#### **Du bringst folgende Qualifikationen mit:**

- Ein erfolgreich abgeschlossenes Studium der Informatik oder eine vergleichbare Berufsausbildung.
- Kenntnisse der APT-Akteure bzgl. ihrer Werkzeuge, Techniken und (TTPs).
- Erfahrung von TTP-Methoden und -Rahmenwerken.
- Sicher im Umgang mit der TCP/IP-Kommunikation und Kenntnisse darüber, wie gängige Protokolle und Anwendungen auf Netzwerkebene funktionieren, einschließlich DNS, HTTP und SMB.
- Berufserfahrung in der Analyse von IT-Sicherheitsvorfällen sowie fundiertes Wissen von SIEM- und Analyse-Tools, wie z.B. QRadar oder Splunk.
- Erfahrung zu standardisierten Empfehlungen wie IT Grundschutz (ISO 27001 & ISO 25999).
- Kenntnisse im Compliance-Bereich sind von Vorteil.
- Kommunikationssichere Deutsch- und Englischkenntnisse runden dein Profil ab.

#### **Was wir Dir bieten:**

- Ein ambitioniertes und motiviertes Team sowie eine offene „Du“ Kultur.
- Unbefristeter Arbeitsvertrag.
- 30 Tage Urlaub.
- Vertrauensarbeitszeit.
- Betriebliche Altersvorsorge.
- Interne und externe Weiterbildungsangebote.
- Mitarbeitererevents & Kaffee-, Wasser und Tee-Flatrate, Obst.

**Karriere ...  
mIT Sicherheit!**