Unser Kunde gehört zu den größten IT-Dienstleistern im Raum Südwestfalen. Das Unternehmen bietet Dienstleistungen rund um die Informationsverarbeitung im Gesundheitswesen sowie dem öffentlichen und dem sozialen Bereich an. Zu seinen Kunden zählen sowohl Krankenhäuser (in nahezu allen Trägerschaften) wie auch kirchliche Einrichtungen aus den Bereichen Diakonie, Caritas sowie der evangelischen und katholischen Kirche. Für diesen Kunden suchen wir im Rahmen der Festanstellung am Standort Wetter (Ruhr) zum nächstmöglichen Zeitpunkt einen:

SOC / Security-Analyst (m/w/d)

Job-ID: CF-00007686
Job-Ort: Wetter (Ruhr)
Remoteanteil / Home Office: 60%

Das Security Operation Center (SOC) ist ein essenzieller Bestandteil der Informationssicherheitsorganisation des Unternehmens. Ziel ist es, Sicherheitsvorfälle frühzeitig zu erkennen und wirksam darauf zu reagieren. Hierzu gehören Konzeption und Implementierung moderner Sicherheitslösungen, Entwicklung effizienter Abläufe und kontinuierliche Überwachung der IT-Systemlandschaft.

Ihre Hauptaufgaben:

- Technische Analyse von Angriffsmustern (Thread-Hunting)
- Weiterentwicklung der SOC-Plattformlösung
- Weiterentwicklung der SOC-Services und Prozesse
- Erstellung/Weiterentwicklung von Playbooks bzw. Prozessabläufen
- Bewertung und Eskalation von Sicherheitsmeldungen
- Koordination und Unterstützung bei der Mitigation von Sicherheitsvorfällen
- Steuerung unserer Security Dienstleister und Beratung internen Gremien und Boards
- Unterstützung bei regelmäßigen Reportings an Stakeholder

Ihre fachlichen Voraussetzungen:

- Erfolgreich abgeschlossene IT-spezifische Ausbildung oder entsprechendes Studium
- Mehrjährige, fundierte Erfahrung im Bereich der IT mit Fokus auf IT-Security
- Fundierte technische Kenntnisse zur Analyse in den Bereichen:
  - Netzwerksicherheit
  - Serversicherheit
  - Clientsicherheit

  - Applikationssicherheit
  - Systemadministration
- Erfahrung mit technischer IT-Security-Prüfung und IT-Infrastruktur wie:
  - SIEM
  - Vulnerability Management
- Kenntnisse in den Bereichen:
  - SQL-Injection
  - Pass the Hash
  - Buffer-Overflow
  - Spear-Phishing
- Technisches Verständnis zur Bewertung von veröffentlichten Schwachstellen, deren potenziellen Auswirkungen sowie dessen Mitigation
- Fundierte Kenntnisse in folgenden IT-Technologien:
  - Netzwerk
  - Sicherheitssysteme
  - Firewall / Web-Application-Firewall
  - IDS / IPS
  - Anomalieerkennung

Ihre persönlichen Voraussetzungen:

- Akquisitionsstärke und Verhandlungsgeschick
- Eigenverantwortlichkeit und Flexibilität
- Strukturiertheit und Zuverlässigkeit

Unser Mandant bietet:

- Intensive Einarbeitung
- Firmenfahrzeug
- Weiterbildungsmaßnahmen
- Fortbildung an der hauseigenen Akademie
- Flexible Arbeitszeiten und mobiles Arbeiten
- Hochmoderne Ausstattung der Arbeitsplätze
- Sozialleistungen
- Betriebliche Altersvorsorge
- Jobradleasing
- Nutzung der konzerngetragenen Einkaufsplattform
- Betriebliches Gesundheitsmanagement
- Zuschuss zum Deutschlandticket als Jobticket



Your Contact Person:
Adrian Weinast
auteega GmbH
Kaiserring 14-16
68161 Mannheim

Phone: +49 170 2175 230
E-Mail: adrian.weinast@auteega.com
Apply now