Für den Bereich IT Service , Abteilung Netzwerk & Security suchen wir einen :

Security Operations Center (SOC) Analyst (m/w/d)

Köln (mit Remote) | Vollzeit | ab sofort

DAS SIND IHRE AUFGABEN

- Aktive Mitwirkung beim Aufbau, Betrieb und der kontinuierlichen Weiterentwicklung des Security Operations Centers (SOC)
- Analyse, Bewertung und Bearbeitung sicherheitsrelevanter Incidents sowie Erkennen von Anomalien und Abweichungen vom Normalbetrieb
- Eigenverantwortliche Administration und Weiterentwicklung der SOC- und SIEM-Tools mit klarem Schwerpunkt auf IBM QRadar
- Konzeption, Implementierung und Optimierung von Use Cases, Korrelationen und Alarmierungslogiken im SIEM Tool
- Durchführung von Root-Cause-Analysen sowie Ableitung und Begleitung geeigneter Gegenmaßnahmen
- Strukturierte Dokumentation von Sicherheitsvorfällen und Erstellung aussagekräftiger Reports und Management□Auswertungen
- Mitwirkung bei der Entwicklung von Präventions□ und Reaktionskonzepten zur Abwehr aktueller und zukünftiger Bedrohungen
- Durchführung, Auswertung und Aufbereitung von automatisierten Vulnerability-Scans
- Kontinuierliche Weiterentwicklung von Analyse□ und Erstanalysewerkzeugen
- Enge Zusammenarbeit mit Security□, Prozess□ und Fachabteilungen zur Optimierung von SIEM□ und Incid
- Überwachung der SLAs sowie Reporting zu SOC□Services (Level 1 & 2)
- Steuerung und Nachverfolgung der Incident□Behebung in Abstimmung mit den verantwortlichen Organisationseinheiten
- Nutzung von Informationen aus Threat□Intelligence□Quellen (z.□ CERT□Verbünde, N□CERT) zur Erstellung aktueller Sicherheitslagebilder
- Teilnahme an der Rufbereitschaft

DAS ERWARTEN WIR VON IHNEN

- Abgeschlossenes Studium der Informatik, IT‑Sicherheit oder eines vergleichbaren Studiengangs oder eine einschlägige Berufsausbildung, z.‑B. Fachinformatiker Systemintegration
- Fundierte Praxiserfahrung im Betrieb, der Konfiguration und Optimierung von SIEM Systemen (Use Cases, Offenses, Korrelationen, Dashboards, Reporting) vorzugsweise IBM QRadar
- Erfahrung im SOC‑ oder CERT‑Umfeld sowie in der Security Incident Analyse und -Bearbeitung
- Kenntnisse im Betrieb von Security Services, wie z. B. SIEM, PAM, IAM, Schwachstellenscanner
- Verständnis für IT‑Service‑Management‑Prozesse (idealerweise ITIL)
- Sehr gutes Verständnis von Angriffsmethoden auf Applikationen, Systeme und Netzwerke
- Breitgefächertes IT‑Know‑how (Betriebssysteme, Netzwerke, Protokolle, Applikationen, Log‑Quellen)
- Ausgeprägtes Risikobewusstsein und analytisches Denkvermögen
- Selbstständige, strukturierte und lösungsorientierte Arbeitsweise
- Hohe Eigeninitiative sowie schnelle Auffassungsgabe bei komplexen Sachverhalten
- Teamfähigkeit, Kommunikationsstärke und ausgeprägte Service‑ und Hands‑on‑Mentalität
- Bereitschaft, bei kritischen Sicherheitsvorfällen auch außerhalb regulärer Arbeitszeiten aktiv zu werden
- Sehr gute Deutsch‑ und Englischkenntnisse (mindestens B2)

DAS KÖNNEN SIE VON UNS ERWARTEN

- Moderne Unternehmenskultur mit individuellen Arbeitsplatzkonzepten
- Sehr gutes Betriebsklima und ein wertschätzendes Miteinander
- Faire Bezahlung (Entgeltsystem) und Förderung der Betrieblichen Altersvorsorge (bAV)
- Home Office / Mobile Office Möglichkeit und flexible Arbeitszeiten für eine gesunde Work-Life-Balance
- Workation innerhalb der EU
- Weiterbildungs- und individuelle Entwicklungsmöglichkeiten (SoCura-Karrierekonzept / Talent Management)
- Überdurchschnittliches Angebot im Rahmen der Gesundheitsförderung (Mobile Massage, Entspannungsraum, Check-ups etc.) sowie betriebsärztliche Betreuung
- Zeitgutschrift für Arztbesuche und Behördengänge
- Gute Verkehrsanbindung (Job-Ticket, Company Bike, Tiefgarage)
- Arbeitgeberzuschuss zur Kantinennutzung
- Hundefreundliches Unternehmen
- Mitarbeitervergünstigungen, Events und vieles mehr

Erleben Sie unsere Vielfalt und entdecken Sie Ihre Möglichkeiten!

WIR FREUEN UNS AUF IHRE BEWERBUNG

Jetzt bewerben!

Ihre Ansprechpartnerin

0221 - 6909 0

Rückfragen per E-Mail

Personalleiterin

Birgit vor der Wülbecke