Possehl Secure

DU MÖCHTEST **BEDROHUNGEN IDENTIFIZIEREN UND EINDÄMMEN?** **DANN BIST DU BEI UNS RICHTIG!**

SOC-ANALYST (M/W/D)

Als SOC-Analyst stärkst du durch deine Fachkenntnisse und deine Leidenschaft für IT-Security die Informationssicherheit unserer Kunden. Du arbeitest in einem motivierten Team, bringst nicht nur deine Erfahrungen in der Analyse sicherheitskritischer Ereignisse ein, sondern trägst auch zur Weiterentwicklung unseres Security Operation Centers bei. Mit Eigenverantwortung und Teamgeist bist du ein unverzichtbares Mitglied unseres Teams, das Bedrohungen identifiziert und unsere Kunden vor vielschichtigen Cyberangriffen schützt.

11 gute Gründe für Possehl Secure

- **Entfalte dein Potenzial in einer flexiblen Umgebung**
- **Leistung wird belohnt**
- **Work-Life-Balance ist uns wichtig**
- **Persönliche Weiterentwicklung**
- **Moderner Arbeitsplatz**
- **Zeit für Erholung & Verpflegung**
- **Gestalte deinen Arbeitsweg neu**
- **Für eine sorgenfreie Zukunft**
- **Gemeinschaft und Zusammenhalt**
- **Fitnessförderung**
- **Corporate Benefits**

Dein Aufgabenbereich

- Du wirkst aktiv am **reibungslosen Betrieb und der kontinuierlichen Weiterentwicklung unseres Security Operations Centers (SOC)** mit. Dabei überwachst und analysierst du präventive, detektive und reaktive Technologien zur Sicherstellung unserer IT-Sicherheit.
- Aktiv beteiligst du dich an der **Weiterentwicklung des SOC**, wobei du unter anderem Elastic- (Elastic Defend, Elastic SIEM) und Microsoft- (Defender for Endpoint und Azure Sentinel) Technologien einsetzt.
- Als Mitglied unseres SOC Teams **analysierst du sicherheitskritische Ereignisse** und leitest entsprechende Schritte im Rahmen von Triage, Investigation & Response ein.
- Du **unterstützt das offensive Sicherheitsteam** bei der Prüfung und Verbesserung von Technologien und Prozessen innerhalb des Purple Team Engagements.
- Die **Definition, Integration und kontinuierliche Optimierung neuer Analytics und Detections** fällt ebenfalls in deinen Verantwortungsbereich.
- Bei **Schwachstellen-Assessments wirkst du aktiv** mit und nimmst an Remediation-Prozessen zur Behebung identifizierter Schwachstellen teil.
- **Systematisch begleitest du Security Incidents auf Basis des PICERL-Ansatzes** und koordinierst Maßnahmen zur effektiven Incident Response.
- Der **regelmäßige Wissensaustausch im Team** und die Integration aktueller Entwicklungen sind für dich selbstverständlich.

Deine Talente

- Du verfügst über **nachweisbare Erfahrungen in der Erkennung, Analyse und Kontrolle von Cyberangriffen**.
- Deine Mentalität ist geprägt von dem **Wunsch, Angreifer und ihre TTPs zu analysieren und zu verstehen**.
- **Mit MITRE ATT@CK bist du vertraut** und kannst die Konzepte und Frameworks effektiv anwenden.
- Du **bewältigst eigenverantwortlich komplexe Aufgaben** und zeigst dabei eine starke Teamorientierung, indem du gerne im kollegialen Umfeld arbeitest.
- Du fühlst dich vorwiegend **im Inneren der Organisation** wohl und ziehst eine Tätigkeit mit geringer Reisetätigkeit vor.
- Du **stehst den Possehl Secure Kunden und Beratern zuverlässig zur Seite** und verstehst die Bedeutung einer kundenorientierten Arbeitsweise.
- Innerhalb von Service-Verträgen bist du bereit, im Team **Rufbereitschaft** zu übernehmen, um flexibel auf Sicherheitsanforderungen reagieren zu können.

PASSEN WIR ZUSAMMEN?

Dann freuen wir uns darauf, dich kennenzulernen.

BEWIRB DICH JETZT

...und gestalte deine Zukunft mit uns!

Wenn du glaubst, das Zeug für diese Position zu haben, aber nicht alle Punkte der Stellenbeschreibung erfüllst, laden wir dich trotzdem herzlich ein, uns deine Unterlagen zukommen zu lassen und gemeinsam herauszufinden, ob du zu uns passen könntest.

Possehl Secure GmbH
Laura Engelhardt
personal@possehl-secure.de | T +49 221 466 195-20
www.possehl-secure.de