Grant Thornton

Deine Stärken. Unsere gemeinsame Wirkung.

Direkt bewerben!

Consultant als Security Operations Center Analyst/Engineer (m/w/d)

Düsseldorf

Wir nennen unsere Arbeit: Wirkung zeigen. Für Dich bedeutet das ein Umfeld, in dem Du Deine Neugierde, Dein Wissen und Deine Leidenschaft für Exzellenz mit anderen teilen kannst. Weil unsere Arbeit Wirkung zeigt, ist Grant Thornton eine der erfolgreichsten Anlaufstellen für den Mittelstand, für Start-ups und den DAX. Mit uns begleitest Du das Wachstum unserer Mandate regional, national und international und schärfst dabei Deinen Blick für Umwelt, Gesellschaft und Wirtschaft.

Bereit, Wirkung zu zeigen?

- Das Monitoring der Bedrohungslage (z.B. Sicherheitslücken, Angriffskampagnen, Angreifer-TTPs – Tactics, Techniques and Procedures) zur Herleitung von Identifikationsregeln für entsprechende Angriffe sowie jeweils passender Gegenmaßnahmen zählt zu Deinen Aufgaben
- Du automatisierst Abläufe mit Skripten in unserer SOAR-Lösung (Security Orchestration, Automation and Response, z.B. im Umfeld MDR/XDR, SIEM, TI und mehr)
- Du unterstützt beim Monitoring sowie der Erkennung und Abwehr von IT-Angriffen bei Mandanten (z.B. Auswertung von SOC-Alerts/Events, Threat Hunting und ggf. Einleitung einer Cyber Incident Response)
- Für bestätigte Cyber Incidents führst Du Tier-3-Analysen durch (z.B. mittels Host-Forensik, Netzwerk-Forensik, Cloud-Forensik, Log-Auswertungen und Malware-Triage)
- Du wirkst mit bei der kontinuierlichen Verbesserung unseres Managed SOC (Konzepte, Methoden und Technologie)

Stärken, die Dich beruflich auszeichnen.

- Dein Studium hast Du mit passender Fachrichtung (z.B. Digitale Forensik, Cybercrime, IT-Sicherheit, Informatik, Physik, o.ä.) erfolgreich abgeschlossen oder kannst anerkannte Zertifizierungen im DFIR-Bereich vorweisen
- Du hast bereits erste fachliche Erfahrungen als Praktikant/Werkstudent (m/w/d) im DFIR-Umfeld oder im SOC-Umfeld (z.B. Scripting in Python, Threat Hunting und Automatisierung) gesammelt
- Theoretische und praktische Kenntnisse über gängige Betriebssysteme (Windows, Linux und MacOS) sowie IT-Infrastrukturen in Unternehmen (inkl. Sicherheitssysteme und Netzwerkprotokolle) kannst Du vorweisen
- Du verfügst über technisches und methodisches Wissen im Umgang mit Tools für digital-forensische Analysen sowie Tools aus dem SOC-Umfeld
- Du hast ein Grundverständnis für Angriffsvektoren, Schwachstellen und deren Ausnutzung durch kriminelle Akteure sowie Analysen von großen Datenbeständen
- Hohe Professionalität, Eigeninitiative, Teamorientierung, Kommunikationsstärke, Spaß an Technik und eine starke Mandanten- und Serviceorientierung zeichnen Dich aus
- Ein schnelles Auffassungsvermögen sowie eine sehr gute analytische und strukturierte Denkweise setzt Du dazu ein, auch komplexe Fragestellungen und Probleme zu lösen (sowohl eigenständig als auch im Team)
- Deutsch sprichst Du verhandlungssicher und bringst gute Englischkenntnisse mit

Was wir Dir bieten? Die Chance, Deine Zukunft zu gestalten. Und mit uns das Übermorgen zu formen.

Ein vielfältiges Trainingsportfolio, verantwortungsvolle Aufgaben, die Dich wachsen lassen, und ein starkes Team – willkommen bei Grant Thornton! Aktives Talent-Management, Feedback-Kultur und ein wertschätzendes Miteinander leben wir bereits. In Sachen agilem Arbeiten, New Work und digitalem Mindset lernen wir kontinuierlich dazu und entwickeln uns weiter.

Interesse? Wir freuen uns über Deine Bewerbung!

Kontakt

Grant Thornton AG Wirtschaftsprüfungsgesellschaft
People & Culture
T +49 211 9524 8717
E karriere@de.gt.com