

(Senior) SOC Engineer (m/w/d)



Du bist Teil unseres stark wachsenden Unternehmensbereichs "Defence & Intelligence" am Standort Köln. Zum Kundenstamm zählen neben vielen großen Unternehmen aus dem Rhein-Ruhr-Gebiet auch öffentliche Auftraggeber und Kunden aus dem Verteidigungsbereich.

Das gibt dir die Möglichkeit, in verschiedenen Teams und Konstellationen zu arbeiten. Du kannst dein Wissen und deine Fähigkeiten anwenden und vertiefen – und fortlaufend Neues lernen. Bring deine eigenen Ideen ein und gestalte deine Karriere!

Die Cybersicherheit von Unternehmen, Organisationen und Staaten liegt Dir am Herzen?

Du kannst Dich dafür begeistern, IT-Landschaften gegenüber einer sich ständig ändernden Bedrohungslage abzusichern? Dein 32" Screen zu Hause ist Dir ohnehin langsam zu klein?

Als (Senior) SOC Engineer arbeitest Du als Teil unserer SOC Teams an der Implementierung und kontinuierlichen Verbesserung SOC-Services mit. Dabei hilfst Du unseren Kunden, ein Security Operation Center oder unseren Managed Service auf ihre Anforderungen aufzubauen und zuverlässig zu betreiben. So können unsere Kunden sicher sein, dass ihre eingesetzte Lösung ihnen dabei hilft mögliche Vorfälle schnellstmöglich zu erkennen und effektiv zu behandeln. Als Teil unseres Ramp-Up- und Betriebsteams begleitest Du unsere Kunden von Anfang an bis zur Übergabe in den produktiven Betrieb und darüber hinaus im täglichen Doing. Du bist maßgeblich daran beteiligt unsere Lösung, das Tooling und die verwendete Alarmregeln permanent zu erweitern und zu verbessern. Deine Expertise hilft dabei, Angriffe zu erkennen und Schaden von den Betroffenen abzuwenden.

Was du tun wirst.

- Implementierung der verschiedenen SOC-Komponenten (SIEM, EDR, CTI, IRP, etc.) und Prozesse sowie ihrer Schnittstellen zum Betriebsteam, zu anderen relevanten Stellen und Behörden.
- Bewerten existierender SOC Lösungen und Aufzeigen von Schwachstellen und Verbesserungspotenzialen
- Direkte Arbeit mit unseren SOC Architekt*innen und dem Team des Kunden
- Entwurf, Erarbeitung und Aktualisierung von Alarmregeln, Dashboards und Reporting
- Implementierung neuer Werkzeuge und Anbindung neuer Logquellen für die Auswertung

Du willst mehr erfahren?
Dann besuche unsere
Karriereseite und
be part of our story.
#ExperienceCGI

CGI Deutschland B.V. & Co. KG
Ettore-Bugatti-Straße 6-14 | 51149
Köln

valeria.feist@cgi.com
01737817713

cgi.com/de/karriere



- Entwicklung neuer Parser und Normalizer für die Auswertung der Logdaten
- Verbessern und Erweitern unserer SOC-Services
- Übernahme von Verantwortung für die sichere Implementierung der SOC-Infrastruktur unserer Kunden im exponierten Umfeld

Was wir suchen.

- Du verfügst über fundierte Erfahrung im Bereich SOC / SIEM / Incident Response / Cybersecurity
- Du hast ein Verständnis und Gefühl für die Cyberbedrohungslage und bist vertraut mit MITRE oder vergleichbaren Frameworks
- Du bist vertraut im Umgang mit SIEM, EDR, IRP, CTI Systemen
- Du kannst flexibel auf Kundenanforderungen eingehen und dich innerhalb kurzer Zeit in sich ändernde Kundenlandschaften und -anforderungen einarbeiten
- Du bist in der Lage, strukturierte Architekturen, Prozesse und Reportingketten zu implementieren
- Du kennst die verschiedenen eingesetzten Werkzeuge und deren Eigenheiten, wie z.B. Query Languages
- Du sprichst und schreibst fließend Deutsch und Englisch

Was wir bieten.

- Bei uns findest du Kolleg:innen, mit denen die Zusammenarbeit Spaß macht. Wir begegnen uns offen, duzen uns über alle Positionen hinweg und denken nicht in Hierarchien oder Silos.
- Du arbeitest meist direkt an deinem Heimatort – weil wir Kundennähe wörtlich nehmen und uns Work-Life-Balance am Herzen liegt.
- Du profitierst von flexiblen Arbeitszeiten und hast je nach Kundensituation die Möglichkeit, von zuhause zu arbeiten.
- Die richtigen Trainings und Zertifikate bringen deine Weiterbildung voran. Unsere E-Learning-Plattform Academia ermöglicht dir das Lernen, wo und wann du willst.
- Einen Teil deines Bruttogehalts kannst du in CGI Aktien investieren – bis maximal 3 % des Monatsgehalts geben wir für jeden Euro einen weiteren hinzu.
- Außerdem beteiligen wir dich am Unternehmenserfolg: Du erhältst eine Gewinnbeteiligung, die sich nach deiner individuellen Leistung richtet, sowie danach, wie wir als Unternehmen unsere finanziellen Ziele erreichen konnten.
- Wir bieten verschiedene Modelle, damit du mobil sein kannst: wie Bahncard, Dienstfahrrad oder Firmenwagen.



Du willst mehr erfahren?
Dann besuche unsere
Karriereseite und
be part of our story.
#ExperienceCGI

CGI Deutschland B.V. & Co. KG
Ettore-Bugatti-Straße 6-14 | 51149
Köln

valeria.feist@cgi.com
01737817713

cgi.com/de/karriere



- Sabbatical oder Elternzeit werden unterstützt. Sie sind bei uns kein Karriere-Stopper!
- Wir sind an deiner Seite, auch wenn es einmal nicht so gut läuft: Du kannst Sonderurlaub nehmen, und unsere Beratungshotline steht dir immer zur Verfügung.
- Eine Vielzahl an gemeinsamen Events und Freizeitaktivitäten stärkt deine Verbundenheit mit deinen Kolleg:innen.



Du willst mehr erfahren?
Dann besuche unsere
Karriereseite und
be part of our story.
#ExperienceCGI

CGI Deutschland B.V. & Co. KG
Ettore-Bugatti-Straße 6-14 | 51149
Köln

valeria.feist@cgi.com
01737817713

cgi.com/de/karriere

