(Senior) SOC Analyst / (Senior) Cybersecurity Analyst (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.
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 Analyst*in bzw. (Senior) Cybersecurity Analyst*in (d/w/m) arbeitest Du als Teil unserer SOC Teams aktiv an der Verbesserung um dem Betrieb unserer SOC Services mit. Dabei hilfst Du unseren Kunden, ihre IT-Infrastruktur gegenüber Bedrohungen von außen und innen zu schützen und bist im Zweifel in der Lage binnen kürzester Zeit auf Sicherheitsvorfälle zu reagieren.
Als Teil unseres L2/L3 Teams entwickelst Du dabei sowohl das System als auch die Services weiter, agierst aber auch selbst als Expert*in für die erweiterte Incident Response im direkten Kontakt mit Betriebsteams und Entscheidern unserer Kunden. Deine Expertise hilft dabei, Angriffe zu erkennen und Schaden von den Betroffenen abzuwenden.

Was du tun wirst.

- Implementierung, Wartung und Betrieb der verschiedenen SOC-Komponenten (SIEM, CTI, IRP, etc.)
- Bewerten und Behandeln verifizierter Incidents in Zusammenarbeit mit den zuständigen Betriebsteams und Kundenverantwortlichen
- Direkte Arbeit mit den Tools zur Analyse und Behandlung verschiedenster Security Incidents
- Entwurf, Erarbeitung und Aktualisierung von Runbooks für den Level 1 & 2 Betrieb
- Identifizierung, Entwurf, Implementierung und Tuning von SIEM UseCases & Alarmregeln
- Anbinden neuer Systeme an die SIEM-Plattform
- Mitarbeit in CERTs
- Verbessern und Erweitern unserer SOC-Services

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

© 2024 CGI Deutschland B.V. & Co. KG

- Durchführen forensischer Analysen im Nachgang eines Incidents
- Übernahme von Verantwortung für den sicheren Betrieb der IT-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, IRP, CTI Systemen
- Du bist in der Lage strukturierte Prozesse und Reportingketten sorgfältig zu befolgen und umzusetzen
- Du bist in der Lage Incidents strukturiert zu analysieren, Angriffsmuster und -vektoren zu erkennen und auch bei neuen Incidents Lösungen zur Behandlung zu entwickeln
- Du kannst Dir grundsätzlich vorstellen Rufbereitschaften zu übernehmen
- 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.
- Sabbatical oder Elternzeit werden unterstützt. Sie sind bei uns kein Karriere-Stopper!

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

© 2024 CGI Deutschland B.V. & Co. KG

- 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

© 2024 CGI Deutschland B.V. & Co. KG