https://dgc.org/it-security-jobs/security-analyst-schweiz/

Security Analyst (m/w/d)

Anstellungsart
Vollzeit

Beginn der Anstellung
Per sofort oder nach Vereinbarung

Arbeitsverhältnis
Festanstellung

Branche
Cybersicherheit / IT-Security

Arbeitsort
Zürich

Wer sind wir?

- Wir sind ein internationales, schnell wachsendes und innovatives Tech-Unternehmen im Bereich Cybersicherheit
- Unser Dienstleistungsangebot umfasst neben einem selbst entwickelten Schwachstellenscanner auch Pentesting, ein Cyber Defense Operations Center, Security Awareness Trainings und Expertise in Blockchain Technologien
- Wir schaffen Bewusstsein für Cybersicherheit im Digitalisierungsprozess
- Cybersicherheit kennt keine Grenzen: unsere Standorte befinden sich heute in Zürich, Berlin, Köln, Abu Dhabi und Flensburg

Was bieten wir dir?

- Ein tolles und heterogenes Team mit unterschiedlichsten Hintergründen und Stärken
- Deine individuelle Balance zwischen Büro und mobilem Arbeiten
- Konzentration auf deine Stärken, um deine Potentiale voll zu entfalten
- Ein gutes Arbeitsklima verspricht dir jeder, hier bekommst du es
- Gute Ideen sind nicht nur gern gesehen, sondern dürfen sogar umgesetzt werden
- Individuelles Onboarding
- Flexible Arbeitszeiten

Deine Aufgaben bei uns:

- Den Aufbau und die Weiterentwicklung eines Cyber Defense Operations Centers (CDOC) begleiten und mitgestalten
- Untersuchung sicherheitsrelevante Vorfälle und Ergreifung entsprechender Gegenmaßnahmen
- Die Tools des Security Operations Centers (SIEM, Schwachstellenscanner, IR, …) einsetzen
- Analyse und Bewertung von Security Incidents in unseren zentralen Sicherheitsplattformen (Threat Hunting)
- Umsetzung und Optimierung der IT Security Incident Response
- Detaillierte Dokumentation der Vorfälle in einem Ticketsystem / SIEM-System sowie Anfertigung entsprechender Reports
- Überwachung und Erkennung von Angriffen und Abweichungen zum normalen Systemverhalten und Einleitung entsprechender Gegenmaßnahmen
- Unterstützung beim Erarbeiten von Konzepten zur Eindämmung und Verhinderung von Angriffen
- Reputationsanalyse von Indicators of Compromise (IOCs)

Dein Profil:

- Erfahrung im Bereich Blue-Teaming (z. B. SOC, Incident Response)
- Idealerweise relevante Zertifizierungen im Bereich (CEH, Securtiy+, CySA+,

…)

- Idealerweise Kenntnisse in zumindest 5 der nachstehend aufgeführten Bereiche: IT-Sicherheit, Security Produkte, Incident Response, Windows, Linux, Netzwerktechnik, Active Directory, Internettechnologien
- Ein abgeschlossenes Studium im IT-Umfeld oder eine vergleichbare Ausbildung mit Berufserfahrung im relevanten Bereich
- Sehr gute kommunikative Fähigkeiten
- Konzeptionelle Fertigkeiten sowie eine analytische, lösungsorientierte Arbeitsweise
- Sehr gute Deutschkenntnisse in Wort und Schrift
- Bereitschaftsdienste sind für dich kein Hindernis

Kontakt und Ansprechpartner:
An einem unserem Standort in Zürich freuen wir uns auf neue Kolleg*innen, die mit ihren innovativen Ideen und Spaß bei der Arbeit unser Team in Vollzeit ergänzen möchten!

Neugierig geworden? Dann freuen wir uns über deine Bewerbung. Bei Rückfragen wende dich gerne an hr-ch@dgc.org oder unter +41 44 288 37 37.

Auf der folgenden Seite findest Du noch mehr Informationen zum CDOC.