TEL +41 44 667 77 66
MAIL JOBS@CLUE.CH
WEB WWW.CLUE.CH

SECURITY SERVICES AG
CLUE

Security Analyst

80-100%, Zürich

Wir sind ein Team von passionierten Security Spezialisten, welches sich zum Ziel gesetzt hat,Unternehmen jeder Art und Grösse gegen aktuelle Bedrohungen zu schützen. Dabei entwickeln wir Services, welche zu den Besten auf dem Markt gehören. Wie wir das erreichen? Indem wir ein entspanntes und begeisterndes Arbeitsklima schaffen, wo offene Kommunikation gross geschrieben wird, jeder Mitarbeiter mitgestalten darf und so sein Potenzial voll ausschöpfen kann.

Wir sind bestrebt, innovative und nachhaltige Lösungen für unsere Kunden zu schaffen. Aus diesem Grund unterstützen wir unsere Mitarbeiter dabei, sich stets weiterzuentwickeln und -bilden. In Zürich-Süd, nur 9 Minuten vom Hauptbahnhof entfernt, bieten wir einen topmodernen und zentralen Arbeitsort für kreatives Arbeiten.

Bist du bereit, in einem jungen, aufstrebenden Unternehmen die Weichen für deine Zukunft zustellen? Du misst dein Gelingen am Erfolg des ganzen Teams und hast Spass daran über denTellerrand hinauszuschauen? Du optimierst gerne Arbeitsprozesse und entwickelst so ein konstant effizientes und modernes Umfeld?

Dann bist Du bei uns genau richtig!

Hast du Erfahrung als Security Engineer und möchtest du dich als Security Analyst weiterentwickeln? Ob Senior oder Junior, wir freuen uns auf deine Bewerbung!

Deine Aufgaben

- Überwachung, Analyse und Verarbeitung von IT/OT Security Events im Clue Cyber Defense Center
- Weiterentwicklung und Ausbau der Erkennungsmechanismen von Cyber Attacken auf unsere Kunden
- Entwicklung und Ausbau der Prozesse und Abläufe im SOC sowie von Playbooks
- Unterstützung von Kunden bei Sicherheitsvorfällen auf allen Ebenen zur schnellen Eindämmung und nachfolgender Optimierung der Abwehrmassnahmen
- Mitwirkung bei der Optimierung und Abwehr von Erkennungsmechanismen der Clue Managed Services
- Zusammenführung der sicherheitsrelevanten Informationen aus verschiedenen Threat Intelligence Systemen und anschliessende Korrelation im SOC

Dein Profil

- Sicher im Umgang mit gängigen Security Monitoring Tools wie, SIEM, Network Detection and Response, Schwachstellen Management und EDR
- Erfahrungen im Bereich Incident Response, Incident Management und Arbeitserfahrung aus einem SOC von Vorteil
- Herausragende Kommunikations- und Präsentationsfähigkeiten
- Analytisches Denken und Handeln
- Strukturierte und diskrete Arbeitsweise
- Stilsicheres Auftreten
- Bereitschaft, sich stetig fachlich weiterzuentwickeln
- Sehr gute Deutsch- und Englisch Kenntnisse in Wort und Schrift

Wir bieten dir

Junges, innovatives Team

Zeitgemässe Anstellungsbedingungen, Hybrides Arbeitsmodell

Offene Unternehmenskultur

Entwicklungs- und Weiterbildungsmöglichkeiten

Moderne Büroräumlichkeiten