karrierego!

Region: Zürich

Entwickeln Sie Ihre Leidenschaft für CyberSecurity und sicherheitsrelevanten Service! Unser Kunde ist eine „führende Private-Banking-Gruppe der Schweiz“, ausgerichtet auf professionelle Beratung der Privatkunden in der Schweiz und weltweit. Das Unternehmen bietet ein umfassendes Leistungsspektrum und eine erstklassige Dienstleistung an und stellt sämtliche Tätigkeiten unter die Werte „Care – Passion – Excellence“. Für sicherheitsrelevante Aufgaben in der Analyse und der Umsetzung von Lösungen für das Private Banking suchen wir einen

SOC Analyst and Engineer (w/m)

Ihr Verantwortungsbereich Es erwarten Sie verantwortliche und spannende Aufgaben in der Analyse und im Engineering von sicherheitsrelevanten Themen im Security Operation Center (SOC) der Privatbank in der Rolle sowohl als Analyst wie auch als Engineer. Ihre Verantwortungen umfassen die Identifikation und die Analyse von Cyber Security Vorfällen und das Monitoring potentieller Cyber Vorkommnisse. In enger Zusammenarbeit mit dem SOC Team und weiteren Spezialisten der Privatbank besprechen Sie die Vorfälle sowie deren möglichen Auswirkungen und sind für die Erstellung der Reports und der Eskalation an das Management verantwortlich. Ihre Aufgaben als Engineer umfassen die Evaluation der Ergebnisse und die Entwicklung von potentiellen Lösungen. Ihre Erfahrungen mit dem SIEM Analyse und Auditing Lösungstool basierend auf der Splunk Enterprise Plattform setzen Sie erfolgreich ein, um die SIEM Lösungen stetig zu verbessern und den Anforderungen anzupassen. Als Engineer kennen Sie die Dashboards, Suchkriterien und das Security Monitoring der Splunk Plattform und sind in der Lage, diese den Anforderungen anzupassen. Die Unterstützung bei Projekten zur Verbesserung der Überwachungs- und Sicherheitsmassnahmen runden Ihre verantwortlichen Aufgaben ab.

Ihre Persönlichkeit Sie verfügen über eine höhere Ausbildung in der Informatik oder in Business Computing. Spezifische Weiterbildungen in der IT Sicherheit sind von Vorteil. Sie verfügen über mehrjährige Berufserfahrungen in Security Operation Centern und/oder in Bereichen und Unternehmen der Sicherheitsüberwachung oder Sicherheitstechnik. Ihre Erfahrungen und Kenntnisse umfassen die Enterprise Plattform Splunk und die Tools ElasticSearch, Logstash und Kibana (ELK) und/oder ähnliche Lösungen im Bereich des Log Managements. Sie sind interessiert an Sicherheitsthemen, offen für neue Herausforderungen, haben eine hohe Lernbereitschaft und sind fähig, sich als Trusted Advisor in nationalen und globalen Teams zu positionieren. Sie schätzen ein anspruchsvolles Umfeld, sind lösungsorientiert, proaktiv, belastbar und sind eine durchsetzungsfähige Persönlichkeit. Sie sind analytisch und denken zielgerecht. Ihre hohe Eigeninitiative und gute Kommunikation setzen Sie bei Ihrem Einsatz im on-Call Duty Team gezielt ein. Kommunikation auf allen Stufen fällt Ihnen leicht und Sie sind gewohnt zu präsentieren. Diskretion versteht sich für diese Position von selbst. Ausgezeichnete Sprachkenntnisse in Deutsch und gut Englischkenntnisse runden Ihr Profil ab.

Ihre Perspektiven Sämtliche Vorteile einer international erfolgreichen Privatbank. Mitarbeiterentwicklung wird hier gross geschrieben. Das Anstellungspaket entspricht der verantwortungsvollen Position. Wenn Sie diese spannende Herausforderung anspricht, freuen wir uns auf Ihre Bewerbung.

Dorigo AG | Höschgasse 68 | CH-8008 Zürich | www.dori-go.com
Petra Wildemann | Phone +41 43 499 19 09 | petra.wildemann@dori-go.com

dorigo!
Modular Recruiting Services