Zum Klienten:
Weitere Informationen zum Klienten und laufend neue Jobchancen erhalten Sie nach Ihrer Anmeldung und dem Onboarding durch Ihren Fachberater per Mail oder online. Wir freuen uns, Sie persönlich kennenzulernen!

Arbeitsort:
Zürich (X Kilometer und X Minuten von Ihrer Wohnadresse entfernt)

Jobbeschreibung:
Sr. PKI, HashiCorp Operations Engineer (w/m/d)

Ihr Aufgabengebiet:
- Implementierung und laufender DevSecOps-/Operations-Support für einen globalen Secrets-Management-Service mittels Certificate Lifecycle Management/PKI-Lösungen und weiteren Datenschutztechnologien
- Laufender Support für ein globales Information Security Cryptography Services-Programm inkl. Verschlüsselung, Key-/Secrets-Management, Tokenisierung und Datenschutztechnologien
- Mitwirkung als technischer Lead im Team der Secrets-Management-Engineers
- Mitwirkung bei der Erstellung, Bearbeitung und Prüfung von Dokumentationen (Verfahren, Standards) zur Sicherstellung einer gut verwalteten, reifen Sicherheitsinfrastruktur
- Aktive Rolle in Engineering, Implementierung und Betrieb von Sicherheitsmassnahmen zum Schutz von Systemen, Netzwerken und Informationen
- Unterstützung bei Disaster-Recovery-Planung, -Betrieb und Datensicherungen
- Tägliche Administration und Support der Infrastruktur für API, Applikationssicherheit, Firewalls, Verschlüsselung, Intrusion-Detection-Systeme, PKI, Secrets-Management, Vulnerability-Scanning, Sicherheitsmonitoring, Penetrationstests, Authentifizierung, Web-Filtering, Identity- und Access-Management sowie zugehörige Logs/Prozesse
- Enge Zusammenarbeit mit Information Security Program Manager, Scrum Master und Architekten zur Kommunikation technischer Auswirkungen auf Entwicklungs-/Engineering-Zeitpläne und Risiken
- Selbstständige Identifikation von Verbesserungspotenzialen für Security, IT und weitere Funktionsbereiche
- Zusammenarbeit mit Information Security Architects, Engineers und API-Entwicklern zur Programmumsetzung
- Zusammenarbeit mit Information Security Leadern zur Weiterentwicklung von Secrets-Management-Standards in der Organisation
- Fungieren als Fachexperte für andere Teammitglieder in der Information Security Organisation
- Durchführung von Zertifikatsmanagement-Aktivitäten, u.a. Lifecycle-Management (SSH, TLS-Zertifikate), Policy- und Prozessentwicklung, Dokumentation, Nutzerbetreuung, Monitoring/Reporting, PKI-Infrastrukturmanagement und PKI-Performance-/SLA-Reviews

Was Sie ausmacht:
- Bachelor in Informatik/Engineering oder verwandtem Bereich, alternativ High-School-Abschluss mit mind. 4 Jahren Technologieerfahrung, davon mind. 5 Jahre in Information Security
- 5+ Jahre Erfahrung in PKI und HashiCorp Operations
- Erfahrung in der Führung und Steuerung von Remote-/Offshore-Teams und Deliverables

- Gute Erfahrung im Kundenmanagement, lösungsorientiert mit Fähigkeit zur Umsetzung komplexer Lösungen
- Zertifizierungen in Audit, Big Data, Cloud, Cybersecurity, Governance, Information Security, Privacy oder Risk von Vorteil (z.B. AWS, Cloudera, GCP, GIAC, ISC2, ISACA)
- Ausgezeichnete mündliche und schriftliche Kommunikationsfähigkeiten sowie Präsentationsstärke bei komplexen Themen
- Fundierte technische Praxis mit API, AWS, Cloudera, Docker, Verschlüsselung, HashiCorp Vault, Kubernetes, Java, Linux, Perl, PKI, Protegrity, Python, Secrets-Management, Thales/Vormetric, Tokenisierung von Vorteil
- Fähigkeit, mehrere Prioritäten zu organisieren und sich flexibel an wechselnde Geschäftsanforderungen anzupassen
- Starke analytische und lösungsorientierte Fähigkeiten mit methodischem Vorgehen bei komplexen Problemstellungen
- Erfahrung in DevOps, Engineering und/oder Operations von Vorteil
- Kreativität, eigenständiges Denken sowie Team- und Eigenverantwortungsfähigkeit
- Kenntnisse in Problem- und Incident-Management, Change-Management sowie im Betrieb und Unterhalt von Infrastruktur
- Praxiserfahrung mit modernen Programmiersprachen wie Python, API-Entwicklung, CI/CD-Pipelines, Jenkins sowie Cryptography-Management-, Secrets-Management- und Tokenisierungstechnologien
- Verständnis verschiedener Cloud-Deployment-/Servicemodelle aus Entwicklungs-, Infrastruktur- und Sicherheitssicht

Was diese Stelle ausmacht:

- Zahlreiche individuelle Benefits