AUSTRIAN POWER GRID

Das Energiesystem der Zukunft: Voller Spannungen, Bewegungen und Chancen. Uns treibt der Stolz auf das, was wir für Österreich bewirken. Gestalter:innen der Energiewende zu sein, fordert uns. Hochgesteckte Ziele erst recht. Einzigartiges Fachwissen, volles Vertrauen. Eigene Entscheidungen, volle Verantwortung. Das ist unser Spielfeld. Das ist APG.

Security Operations Engineer

#energiewende #frauenpower #poweron

Das Security Operations Center der APG ist ein junges, engagiertes Team mit einer starker Mission. Als Teil dieses Teams stehen Sie zwischen dem wachsenden Risiko von Cyberangriffen und der sicheren Energieversorgung Österreichs. Durch Ihre Unterstützung im Bereich der Automatisierung von Security Operations Prozessen können wir unsere Reaktionszeiten weiter optimieren und die Tool Integration vorantreiben.

Aufgaben

- Weiterentwicklung und Automatisierung von SOC Playbooks (Anreicherung, Analyse und Automatisierung von Aktionen)
- Entwerfen, Dokumentieren und Warten von Integrationen zwischen Security Tools, Threat Intelligence und sonstigen 3rd Party Tools
- Unterstützung im Bereich Detection Engineering, Case Management und Automatisierung
- Regelmäßige Unterstützung im Bereich Vorfallserkennung und Reaktion auf Sicherheitsvorfälle (Incident Response)
- Aufbereiten von Cyber Threat Intelligence aus internen und externen Quellen zur Anreicherung von Sichereitsereignissen im Rahmen der Automatisierung
- Enge Zusammenarbeit mit anderen Bereichen im Team (Detection Engineering, Schwachstellenmanagement, etc.) sowie im Unternehmen (IT-Betriebsverantwortliche, ISMS Team, OT Security)
- Bereitschaftsdienst für Sicherheitsvorfälle

Anforderungen

Must-Haves:

- Abgeschlossenes Studium mit dem Schwerpunkt IT (Master/Dipl.-Ing) ODER abgeschlossenes Bachelorstudium mit dem Schwerpunkt IT und mindestens 3 Jahren Berufserfahrung
- Erfahrung im Umgang mit SIEM-, SOAR-, IDS/IPS- und/oder EDR-Systemen
- Grundlegende Kenntnisse in Python, PowerShell, Perl oder anderen Scripting Sprachen sowie APIs
- Gute Deutsch- und Englischkenntnisse in Wort und Schrift (Deutsch mindestens B2 Niveau)
- Ein hohes Maß an analytischem sowie vernetztem Denkvermögen und Einsatzbereitschaft zur gesamtheitlichen Weiterentwicklung der APG
- Schnelle Auffassungsgabe und Teamfähigkeit

Nice-to-have:

- Themen wie TTPs, Pyramid of Pain oder MITRE ATT&CK sind Ihnen ein Begriff
- Erfahrung in der Erkennung und Bewältigung von Sicherheitsvorfällen

Das bieten wir:

Das Gehalt (zuzüglich einer leistungsorientierten Entlohnung) für Ihren neuen Job richtet sich nach Ihrer konkreten Qualifikation und Erfahrung. Das kollektivvertragliche Mindestgrundgehalt beträgt für diese Position Euro 4.192,13 brutto im Monat.

Vielfalt bei unseren Mitarbeiter:innen ist ein wichtiger Bestandteil unserer Unternehmenskultur. Wir sind auf der Suche nach motivierten Menschen und achten bei Ihrer Bewerbung auf Chancengleichheit. Uns ist der Mensch wichtig, das Engagement und Ihr Wille mit uns gemeinsam die Energiewende zu gestalten.

Kontakt

Für Fragen steht Ihnen Leonidas Moissidis gerne telefonisch unter +4366488342883 zur Verfügung.

Machen Sie sich einen Eindruck von Austrian Power Grid AG auf www.apg.at