Cyber Security Analyst - Detection Engineer (m/w) 80-100%

Ihr Arbeitsort: Brüttisellen, Chur oder St. Gallen

Innovation, Interaktion, Swissness oder kurz: Inventx. Wir sind der schweizerische IT-Partner für führende Banken und Versicherungen. Mit der vernetzten Innovationskraft von über 250 Spezialisten und mit einer Nähe zum Kunden, die gelebt statt behauptet wird. Mit dem Qualitäts- und Sicherheitsdenken, das höchste Ansprüche erfüllt: BANK ON IT.

In einer vernetzten und digitalisierten Welt wird die Sicherheit von IT-Systemen für Unternehmen immer wichtiger. Die Überwachung und der Schutz der entsprechenden Systeme & Anwendungen werden zugleich komplexer und benötigen hochspezialisierte Fachkräfte. Mit dem Inventx Cyber Resilience Center (ix.CRC) bietet Inventx ihren Kunden die Möglichkeit, diese Aufgaben auszulagern und gleichzeitig den strengen Schweizer Datenschutzvorschriften und Richtlinien für den schweizerischen Finanzsektor zu entsprechen. Wir erweitern im Rahmen des Ausbaus unseres Cyber Resilience Centers die Aktivitäten und die Entwicklungen rund um unser Security Frameworks und suchen ein motiviertes Teammitglied. Als Cyber Security Analyst - Detection Engineer übernehmen Sie dabei eine zentrale Rolle. Sie gestalten den Ausbau unseres Cyber Resilience Centers entscheidend mit. Wirken Sie bei uns als führender Anbieter für namhafte Unternehmen im Schweizerischen Finanz- und Versicherungssektor beim weiteren Ausbau unseres innovativen Security Information and Event Managements (SIEM) mit. Bei uns können Sie mit Herzblut mitgestalten.

Spannende Aufgaben:

- Sie arbeiten an der Weiterentwicklung unseres SIEM (Splunk Enterprise Security) mit und erstellen mit Ihrem Wissen spannende Use-Case basierte Detections und Dashboards für unsere Kunden
- Durch kontinuierliche Wartung unseres Cyber Security Frameworks reduzieren Sie die "False Positive Rate" und passen das Framework der aktuellen Gefahrenlage an
- Sie unterstützen die Cyber Security Analysten und analysieren und bearbeiten Security Incidents und stellen den Security Incident Management LifeCycle (Detection, Analysis & Response) sicher
- Im Rahmen der Threat Intelligence haben Sie unter anderem ein Auge auf relevante Bedrohungen sowie Security-Updates und stossen die notwendige Massnahmen an
- Sie beraten und sensibilisieren unsere System- und Applikations-Verantwortlichen um Veränderungen im Rahmen der Cyber Security frühzeitig zu erkennen

Ihr Profil:

- Informatikausbildung, höherer Fachausweis (HF, FH, Uni) oder langjährige Berufstätigkeit in der Informatik
- Weiterbildung im Bereich IT Security von Vorteil
- Programmier- und Scriptingkenntnisse erwünscht
- Splunk und Splunk Enterprise Security Know How erwünscht
- Gute analytische Fähigkeiten
- Tiefgehendes, technisches Verständnis in den Bereichen Client, Server und Netzwerk

- Durchsetzungsvermögen, Zielstrebigkeit, Einsatzbereitschaft und schnelle Auffassungsgabe
- Grosse Neugier und Motivation, um sich ein fundiertes Cyber Security Wissen anzueignen
- Sehr gute Deutsch- und Englischkenntnisse in Wort und Schrift

Viel zu bieten:
- Kein Tag wie jeder andere: Herausfordernde Aufgaben, viel Verantwortung und Gestaltungsspielraum
- Ein Teamspirit geprägt von Offenheit, Hilfsbereitschaft und Professionalität
- Aktive Unterstützung in Ihrer beruflichen Weiterentwicklung (Projektarbeit und Weiterbildung)
- Arbeitszeiten, die Ihren persönlichen Bedürfnissen entgegenkommen
- Zentrale Lage, auch mit ÖV bestens erreichbar

Haben Sie so richtig Lust auf spannende Aufgaben und Projekte in der Schnittstelle zwischen IT und der Finanzindustrie? Dann freuen wir uns auf Ihre Online-Bewerbung:

JETZT BEWERBEN

Für Stellenvermittler