Imagetext / Arbeitgebervorstellung

Die N.O.C Engineering GmbH steht seit 1995 für qualifizierte Ingenieurdienstleistungen in den Bereichen Entwicklung, Konstruktion, Dokumentation, Projekt- und Qualitätsmanagement, Technische Assistenz sowie Soft- und Hardwareentwicklung und Test & Versuch.

In einem Baden-Württemberg flächendeckenden Netz sind wir nah am Kunden und bieten unseren Mitarbeitern spannende Projekte bei den führenden Unternehmen Deutschlands.

Mehr als 200 Projekte pro Jahr – branchenübergreifend; von der Automobilbranche bis zur Medizintechnik. Vom Maschinenbau bis zur Automatisierungstechnik – und mehr als 2000 namhafte Kunden sprechen für sich.

Cyber Security Architect (m/w/d) - Inhouse Consulting

(484)

Standort: Friedrichshafen Anstellungsart(en): Vollzeit Arbeitszeit: 35 - 40 Stunden pro Woche

Aufgaben, Kompetenzen und Verantwortung

- Zentraler Ansprechpartner für Fragestellungen rund um das Thema Informationssicherheit und Cyber Security
- Beratung der internen IT und Fachbereiche in Hinblick auf die Themen Informationssicherheit und Cyber Security
- Erstellung von (technischen) Konzepten und Etablierung von Prozessen auf Basis des Policy Frameworks der Organisation
- Koordination von Schwachstellen- und Penetration Tests und Steuerung externer Dienstleister
- Mitwirkung als Inputgeber bei der Entwicklung und Defi nition von Informationssicherheitsstandards, -verfahren und -richtlinien
- Förderung des Sicherheitsbewusstseins mit dem Ziel der Etablierung einer Sicherheitskultur durch Awareness- und Sensibilisierungs-Maßnahmen
- Unterstützung und Mitwirkung bei umfassenden Cyber-Sicherheitsinitiativen oder -projekten

Fachliche Anforderungen

- Erfolgreich abgeschlossenes Studium im Bereich Informations-/IT-Sicherheit, Informatik oder vergleichbare Qualifikation
- Mehrjährige Berufserfahrung in IT-Security Projekten mit den Tätigkeitsschwerpunkt technische Umsetzung von IT-Sicherheitslösungen und in derAnwendung von IT-Security Standards
- Ausgeprägtes Verständnis sowie Erfahrung in den Bereichen Netzwerk (Netzwerkprotokolle, VPN, Routing, Switching), Firewallsysteme, Public KeyInfrastrukturen, Sicherheitsanalysen / Penetrationstests, Verschlüsselung / Kryptographie, Betriebssysteme (Linux, Windows), Cloud-Umgebungen, etc.
- Spezifi sches Branchenwissen und aktuelles Wissen über moderne Entwicklungen bei Malware, Exploits und Vulnerabilities
- Zertifizierung als CISSP/CCSP/OSCP/TISP oder vergleichbar von Vorteil
- Erfahrung im Bereich im Incident Response, Forensik, Etical Hacking von Vorteil
- Fortgeschrittene Kenntnisse und professioneller Umgang mit agilen Tools (MS Azure DevOps, Atlassin Jira/Confl uence, etc.) von Vorteil
- Ausgeprägte analytische/konzeptionelle Kompetenz/Fähigkeit
- Starke technische Affi nität für IT-Sicherheit und Technik/Technologie
- Ausgeprägte Kunden- und Service-Orientierung, ergänzt durch Ziel- und Ergebnisorientierung
- Überzeugungs- und Begeisterungsfähigkeit bei hoher Kommunikationsfähigkeit
- Teamplayer
- Verhandlungssichere Deutschkenntnisse zwingend erforderlich
- Sehr gute Englischkenntnisse in Wort und Schrift

Arbeitgeberleistungen / Unternehmensangebot

- bis zu 30 Tage Urlaub
- Tarifgebundene Entlohnung mit automatisierter Lohnsteigerung
- Dienstwagen sowie Homeoffice möglich
- Unbefristeter Arbeitsvertrag
- Arbeitgeberfinanzierte Altersvorsorge und Arbeitskontenregelung
- Schulungen, Trainings sowie Fortbildungen
- Gute Karriere- und Aufstiegsmöglichkeiten
- Regelmäßige Feedbackgespräche mit Ihrem Vorgesetzten
- Mitarbeiterevents

Kontaktdaten für Stellenanzeige

Dipl. Ing. (FH) Patrick Günter

Geschäftsleitung

Wir freuen uns auf Ihre Bewerbung an: **guenter@noc-engineering.de**

N.O.C Engineering GmbH
Max-Planck-Straße 11
78052 Villingen-Schwenningen

Tel.: 07721 40 609-11
Fax: 07721 40 609-29
Zentrale: 07721 40 60 9-0

Homepage: http://www.noc-engineering.de

Abteilung(en): Hardwareentwicklung, IT, Softwareentwicklung

Art(en) des Personalbedarfs: Neubesetzung

Tarifvertrag: BAP/DGB **Entgeltgruppe:** EG9+

Impressum