Stellen ID: 159873

IT-Security Engineer m/w/d

Zurück Bewerben PDF

Das Klinikum Wolfsburg zählt mit 547 Planbetten, 20 Kliniken und Instituten zu den größten Krankenhäusern Niedersachsens. Rund 2.200 engagierte Mitarbeitende aus über 60 Nationen sorgen in professionellen Teams für die Gesundheit unserer Patient*innen. Wir sind mit dem MedizinCampus Wolfsburg (MCW) klinischer Ausbildungsstandort der Universitätsmedizin Göttingen und verfügen über eine eigene Berufsfachschule Pflege.

IT-Security Engineer

Unsere Vielfalt ist unsere Stärke! Wir setzen auf Chancengleichheit und Diversität. Daher freuen wir uns über Bewerbungen von Menschen aller Altersgruppen, unabhängig von Geschlecht, sexueller Identität, Herkunft, Religion, Weltanschauung oder einer möglichen Behinderung. Bewerber*innen mit Schwerbehinderung oder Gleichstellung werden bei gleicher Qualifikation und Eignung bevorzugt berücksichtigt.

Was können Sie vom Klinikum Wolfsburg erwarten?

- Unsere Vorteile - Das Klinikum Wolfsburg - ein attraktiver Arbeitgeber
- Eine Vergütung - je nach persönlicher Voraussetzung - **bis zur Entgeltgruppe E11** des Tarifvertrages für den öffentlichen Dienst TVöD (Besonderer Teil Krankenhäuser)
- Ein multiprofessionelles Team, interkulturelle Zusammenarbeit und individuelle Förderung
- Eine angemessene und strukturierte Einarbeitungszeit

Als Krankenhaus der Schwerpunktversorgung und Teil der kritischen Infrastruktur ist der Schutz unserer IT-Systeme, Patient*innendaten und medizinischen Prozesse von zentraler Bedeutung. Für unsere IT-Abteilung suchen wir eine technisch versierte Persönlichkeit, die Informationssicherheit nicht nur konzeptionell begleitet, sondern vor allem praktisch und operativ in der IT-Infrastruktur umsetzt.

Die Position ist in der IT-Abteilung angesiedelt und arbeitet eng mit dem Informationssicherheitsbeauftragten, dem Datenschutzbeauftragten, der Krankenhausleitung, den IT-Fachbereichen, der Medizintechnik sowie externen Security-Dienstleistern zusammen.

Der Schwerpunkt der Tätigkeit liegt ausdrücklich auf der technischen IT-Sicherheit: Betrieb, Konfiguration, Härtung, Überwachung und Weiterentwicklung sicherheitsrelevanter Systeme sowie die technische Begleitung von Sicherheitsmaßnahmen, Schwachstellenmanagement und Incident Response. Wenn Sie Freude daran haben, Sicherheitsmaßnahmen praktisch umzusetzen, Systeme zu analysieren, Schwachstellen zu beheben und technische Security-Lösungen weiterzuentwickeln, freuen wir uns auf Ihre Bewerbung.

Das ist Ihr zukünftiges Aufgabengebiet:

Technisch-operative IT-Sicherheit

- Betrieb, Konfiguration und Weiterentwicklung sicherheitsrelevanter IT-Systeme, zum Beispiel Firewalls, VPN, IDS/IPS, SIEM, Endpoint Protection, EDR, PAM, MFA und Monitoring-Lösungen
- Technische Umsetzung von Sicherheitsvorgaben in enger Abstimmung mit dem Informationssicherheitsbeauftragten

- Analyse, Bewertung und Behebung technischer Schwachstellen in Server-, Client-, Netzwerk- und Applikationsumgebungen
- Organisation, Durchführung und Nachverfolgung von Schwachstellenscans, Sicherheitsanalysen und Penetrationstests
- Technische Koordination und fachliche Schnittstelle zum externen Security Operations Center
- Unterstützung bei der Analyse und Bearbeitung von Security Events, Incidents und Verdachtsfällen
- Mitwirkung bei Incident-Response-Prozessen, forensischen Erstbewertungen und technischen Maßnahmen zur Eindämmung und Wiederherstellung
- Planung und Umsetzung von Projekten mit Sicherheitsbezug, zum Beispiel Netzsegmentierung, Zero Trust, MFA, Systemhärtung, Protokollierung, Monitoring und Berechtigungsmanagement
- Beratung und Unterstützung der IT-Fachbereiche sowie der Medizintechnik bei sicheren Systemarchitekturen, Konfigurationen und Betriebsmodellen
- Technische Begleitung von KRITIS-Prüfungen, Audits und Nachweisprozessen gemäß den geltenden Anforderungen

Dokumentation und Zusammenarbeit

- Erstellung und Pflege technischer Sicherheitsdokumentationen, Betriebshandbücher und Nachweise
- Unterstützung beim Betrieb und bei der Weiterentwicklung des Informationssicherheitsmanagementsystems aus technischer Sicht
- Mitwirkung bei Schulungen und Awareness-Maßnahmen mit Fokus auf technische Sicherheitsaspekte
- Enge Zusammenarbeit mit internen Fachbereichen, externen Dienstleistern und Prüfinstanzen

Sie passen besonders gut zu uns, wenn Sie über praktische Erfahrung in der technischen IT-Sicherheit, IT-Infrastruktur, Netzwerksicherheit oder Systemadministration verfügen und gerne direkt an Systemen, Plattformen und Sicherheitslösungen arbeiten.

Damit überzeugen Sie uns:

Erfolgreich abgeschlossenes Studium der Informatik, Wirtschaftsinformatik, IT-Sicherheit oder einer vergleichbaren Fachrichtung
oder alternativ eine erfolgreich abgeschlossene Ausbildung im IT-Bereich, zum Beispiel als Fachinformatiker*in für Systemintegration, Informatiker*in, IT-Systemelektroniker*in oder vergleichbar

- Mehrjährige praktische Erfahrung in IT-Infrastruktur, Netzwerksicherheit, Systemadministration oder operativer IT-Sicherheit
- Sehr sichere mündliche und schriftliche Kommunikationsfähigkeit in deutscher Sprache, mindestens Niveau C1 GER
- Fundierte Kenntnisse in mehreren der folgenden Bereiche: Firewalls, Netzwerksicherheit, SIEM, IDS/IPS, Endpoint Security, EDR, Active Directory, Windows Server, Linux, Virtualisierung, Netzwerksegmentierung, VPN, MFA oder Berechtigungsmanagement
- Erfahrung in der Analyse und Behebung technischer Schwachstellen
- Verständnis für Security-Monitoring, Log-Analyse, Incident Response und technische Schutzmaßnahmen
- Analytisches Denken, Hands-on-Mentalität und eine eigenständige, lösungsorientierte Arbeitsweise

Wünschenswert sind:

- Erfahrung im KRITIS- oder Gesundheitsumfeld
- Kenntnisse relevanter Normen, Gesetze und Anforderungen, zum Beispiel BSI-KritisV, IT-Sicherheitsgesetz, DSGVO, KHZG, B3S Medizinische Versorgung oder NIS2
- Zertifizierungen wie BSI IT-Grundschutz-Praktiker, CompTIA Security+, CISSP, CEH, Microsoft Security, Cisco Security oder vergleichbare Nachweise

- Erfahrung in der Zusammenarbeit mit einem Security Operations Center oder Managed Security Service Provider

Für nähere Details zur Tätigkeit sowie weitere Fragen:
Robert Dietrichs
IT-Teamleitung
Tel. +49 5361 80-3110
E-Mail: robert.dietrichs@klinikum.wolfsburg.de

Bewerbungen absenden ausschließlich über den Button "Jetzt bewerben"

Wir freuen uns Sie kennenzulernen!

Klinikum Wolfsburg

Ansprechpartner für weitere Informationen

Robert Dietrichs
IT-Teamleitung
+49 5361 80-3110
robert.dietrichs@klinikum.wolfsburg.de

Steckbrief Stelle

- Berufsgruppe:
  Verwaltung
- Gewünschte Qualifikation:
  Informatiker/in
  Fachinformatiker/-in
- Beschäftigungsart:
  Teilzeit/Vollzeit
- Anstellungsverhältnis:
  Unbefristet
- Stellenbesetzung:
  ab sofort

Einsatzort

Wolfsburg