Senior Security Engineer

Gubra is looking for an experienced**Senior Security Engineer**to strengthen our Security Operations capabilities and work closely with the Lead Security Operations to build and mature our technical security capabilities across infrastructure, cloud, digital platforms, research systems, and business applications.

You will be a key hands-on technical contributor in the Security Operations team, helping operate, improve and build security capabilities across Gubra. Working closely with the Lead Security Operations, you will turn security priorities and requirements into practical technical solutions, while taking ownership of defined security engineering and operational areas.

This is a hands-on role with significant technical responsibility. You will work across security operations, incident response, vulnerability management, security engineering, detection and security monitoring, while collaborating closely with colleagues from Infrastructure & Platform Engineering, Software Engineering, Data Engineering, Digital Workplace and Quality teams.

You will work under the technical direction of the Lead Security Operations, while being expected to operate independently, take ownership of technical problems and proactively identify opportunities to improve Gubra's security capabilities.

Key responsibilities

- Work closely with the Lead Security Operations to operate, mature, and continuously improve technical Security Operations practice.
- Investigate and respond to security alerts, incidents and suspicious activity, supporting containment, remediation and recovery.
- Develop and improve security monitoring, detection rules, alerting and operational playbooks.
- Support vulnerability management, security hardening and remediation activities across Gubra's technology environment and to reduce manual work.
- Build, configure and operate security capabilities across Microsoft 365, Azure, AWS, SaaS platforms, identity and hybrid infrastructure.
- Collaborate with Infrastructure & Platform Engineering, Software Engineering and Data Engineering to implement security controls, secure development practices DevSecOps capabilities.
- Participate in threat modelling, security assessments and technical risk analysis for new solutions and infrastructure.
- Help identify security gaps and translate them into practical technical improvements aligned with Gubra's security requirements and standards.
- Evaluate and recommend improvements to security tooling, technologies and technical practices and work with external IT security partners where specialist expertise is required.

Must-have experience

- Strong hands-on experience within Security Engineering, Security Operations or Cyber Security.
- Experience operating security capabilities across Microsoft 365, Azure, AWS, or hybrid environments.
- Strong understanding of identity security, endpoint security, networking and infrastructure security.
- Experience with vulnerability management, incident response, security monitoring and

technical security control.
•Comfortable working across infrastructure, cloud platforms and engineering teams.
•Strong analytical and troubleshooting skills, with the ability to investigate complex technical security issues.
•Excellent communication skills with both technical and business stakeholders.

Preferred experience
•Experience with SIEM platforms and security monitoring and developing security use cases.
•Experience with Microsoft Defender XDR, Defender for Cloud or similar security platforms.
•Experience with security automation, scripting, security integrations and support for Platform Engineering, DevOps or DevSecOps practices.
•Experience securing cloud-native platforms, Kubernetes or containerized workloads or modern enterprise platforms such as Datadog, or Databricks.
•Experience with threat modelling and technical security assessments.
•Experience within biotech, pharma, healthcare or other regulated industries.
•Relevant certifications such as SC-200, AZ-500, GCIH, GCIA, CISSP or similar is an advantage.

Ideal candidate
You are a pragmatic, hands-on security professional who enjoys solving operational security challenges.
You move confidently between investigating security incidents, analysing vulnerabilities, engineering security controls, improving detection capabilities and collaborating with infrastructure and engineering teams to build and solve security problems.
You enjoy building and improving security capabilities and understand that effective security is achieved through automation, collaboration, and practical engineering.
You are comfortable working under the technical direction of the Lead Security Operations while taking ownership of your own technical areas and proactively identifying opportunities to improve the security posture to help establish a modern Security Operations capability that grows with the organization.

Application and deadline
Please apply no later than September 27, 2026 by uploading your motivated cover letter, resumé, and relevant diplomas on our website.
For questions about the position, please contact Robin Hansen, Cyber Security Specialist at rha@gubra.dk
We are looking forward to receiving your application.

About Gubra
Gubra is a disease-agnostic techbio company specialized in peptide-based drug discovery and development as well as preclinical contract research services striving for excellence at all levels. We insist on doing things efficiently – and often differently - to reach the results we aim for. Our vision is to become leaders in the path towards a more sustainable and healthier world. We do that by facilitating the discovery of new medicine, and by acting and inspiring others to fight the ongoing climate and biodiversity crises.
Gubra’s activities are focused on the early stages of drug development and are organised in two main highly synergistic business areas: Biotech and CRO Services. We generate our revenue by performing research for life science companies as well as by partnering

projects from our discovery and development pipeline.
Our therapeutic focus is within metabolic and fibrotic diseases, and we specialize in in vivo pharmacology, ex vivo assays, drug profiling, histology, stereology and whole brain and organ imaging. In addition, we offer a full palette of advanced transcriptomics. Our ML/AI-driven peptide drug discovery platform streaMLine enables us to rapidly develop a peptide hit into a non-clinical candidate ready for development. Through a constant focus on high quality, scientific excellence, speed, and solid teamwork we have established ourselves as a highly professional and competent partner in the market.
People are our greatest asset, and our team consists of around 300 employees of which many are located in Hørsholm, Denmark. The mix of people from different cultures and educational backgrounds combined with our entrepreneurial mindset have greatly impacted our working environment, which is characterized by entrepreneurial drive, scientific curiosity, and teamwork – we join forces!