

Cyber Security Engineer

Do you have a strong interest in cyber security and enjoy turning new insights and knowledge into ways of improvement? At Collectia, we are looking for a hands-on security professional with the ability to work across a broad technical remit and help move our security programme forward.

In this role, you will be the main contributor across a range of cyber security initiatives, working closely with experienced colleagues in DevOps, Engineering and IT Support, as well as external specialists. The position covers infrastructure, cloud, identity, endpoints and operational processes, combining technical security engineering with governance and compliance. You will help define effective controls and make sure they are implemented in practice.

Your key responsibilities

- Own and continuously develop our CIS 18 framework, including gap assessments, prioritised action plans, implementation follow-up and maturity reporting.
- Own and improve our Microsoft Secure Score and drive relevant security improvements across Microsoft 365 and Azure.
- Act as a central technical partner for ISAE 3000 activities, including audit preparation, evidence collection, control walkthroughs and remediation.
- Establish, document, maintain and test internal IT and security controls, ensuring that control design and evidence remain practical, consistent and traceable.
- Perform security risk assessments and drive remediation plans through to completion in collaboration with relevant colleagues.
- Plan, coordinate and carry out penetration tests and attack simulations together with external security experts and ethical hackers, and translate findings into concrete improvements with our technical teams.
- Investigate and implement technical security improvements based on developments in threats, vulnerabilities and defensive capabilities.
- Support the handling of security incidents, including investigation, containment, lessons learned and improvements to controls, monitoring and procedures.

Security domains in scope

The role spans identity and privileged access management, multifactor authentication, vulnerability management, logging and detection, incident management, endpoint and network security, server hardening, and cloud security across Microsoft 365 and Azure. It also includes security controls, risk management and audit readiness.

You will be part of

You will join our DevOps department in a role with significant influence on how security is designed, implemented and operated. You will work closely with technical colleagues and relevant business stakeholders, with direct access to decision-makers and opportunity to shape our security roadmap and ways of working.

We offer high professional standards, short decision paths, and opportunities for continuous professional development and knowledge sharing. Benefits include a lunch scheme, pension, health insurance, an in-house hairdresser and masseur, carwash and fitness subscription.

How we imagine you

Above all, you have a strong interest in cyber security. You are curious about emerging threats, new technologies and security developments, and you enjoy investigating how things work, and turning that knowledge into practical improvements.

We are open to different levels of experience. If you are earlier in your cyber security career but have a strong technical foundation, the right mindset and the ambition to grow

into broader ownership, we would still be very interested in hearing from you.

You bring:

- Hands-on experience in cyber security, infrastructure security or a comparable technical security role.
- An interest in working across multiple security domains, with the initiative to investigate unfamiliar issues and involve the right colleagues or specialists when needed.
- An understanding of Microsoft security capabilities across Microsoft 365, Entra ID and Azure, including Secure Score, identity protection and privileged access.
- A practical approach to risk, balancing security, operational impact, cost and business priorities.
- The ability to take ownership, manage several initiatives at once and follow actions through to completion.
- Strong communication skills with the ability to work effectively with both technical specialists and non-technical stakeholders in Danish and English.

Experience with control frameworks such as CIS 18, and with audit preparation or remediation in an ISAE 3000, ISO 27001, NIS2 or similar environment is an advantage.

You do not need to be a specialist in every security domain from day one. What matters most is that you enjoy being hands-on, stay curious, challenge existing configurations constructively and work with others to implement sustainable improvements.

Ready to join our team?

Please send us your CV. We will review applications and invite candidates for interviews on an ongoing basis and will hire as soon as we find the right person.

For questions, please contact Oliver Pedersen, Team Lead DevOps by phone (+45) 30 29 07 22.

Location and terms

- Full-time, 37 hours per week, based in Brøndby
- Salary will reflect your qualifications and experience
- Clean criminal record and no registrations with credit information agencies

Want to get to know us better?

Start by watching a short video about Collectia, and then explore our mission, vision, and values.

We look forward to receiving your application.