IT Security Consultant

Do you have a solid consultancy background and an extrovert positive attitude, then you might be the colleague we are looking for.

For our passionate team of highly skilled consultants, we are looking for a consultant who has a proven track record of working with Enterprise customers and thrive in a dedicated market-leading, cutting-edge team where your colleagues are hardcore experts in defensive and offensive security whom live and breathe IT security.

We expect that you are experienced in- and passionate about infrastructure penetration testing, web application testing and red teaming. Having experience with handling incident response cases is also a plus.

Your focus:

You will be part of our consultancy team. Your responsibility will include various consultancy related tasks primarily, but not limited to, penetration testing of web applications and infrastructure, investigation of customer networks for signs of compromise and from time to time running phishing campaigns, advising clients on windows security and giving recommendations on how to harden a network. Our consultants also take part in handling incident response cases where we work on everything from smaller ransomware cases to targeted threats and compromises of entire large network with tens of thousands of machines.

Your experience:

We are searching for a candidate with at least 4 years of focused work experience in offensive security.

We have a team of reversers standing by to help you with any malicious code you find, so reversing is not a requirement, but you need to be confident with dynamic malware analysis.

Minimum qualifications:

- Knowledge of both Windows and Linux security
- Penetration testing of web applications and infrastructure

- Knowledge of enterprise network setups, network and windows domain
- Understanding business demands
- Ability to translate IT security risks into business risks and present them to non-technical people
- Be available to travel with short notice
- Fluent verbal and written communication skills in English

We would also appreciate:

- Experience with the full incident response process
- Relevant certification(s) (GPEN, GCFA, CISSP, OSCP, GCIH, GCIA)
- Experience with code review
- Experience with large scale intrusions (10.000+ devices)
- Network forensics
- Memory forensics
- Knowledge of EDR, SIEM and NIDS systems
- Knowledge of using a SIEM system
- Good communication skills in Danish

Working for us you will:

- Become part of a strong, talented, diverse and passionate international team of colleagues
- Be part of an inclusive, ambitious yet relaxed environment with exceptional people
- Be given both responsibility and flexibility to reach your goals
- Work in a financially-independent company

- Have a competitive salary and personal benefits package

Type:

Full-time and permanent position available immediately

Other:

This position is currently open in our Consultancy team, located in Copenhagen, Denmark.

It is a requirement that you can show and uphold a clean criminal record. Also, it is an advantage if you have been security cleared by your National intelligence and security authority at level "Secret".

Relocation to Denmark will be required if the applicant is currently located elsewhere.

Contact:

To apply for this position, please e-mail your resume and a cover letter to: CSIS HR at hr@csis.dk

About CSIS:

Founded in 2003, CSIS Security Group A/S (CSIS) is a leading provider of advanced cybersecurity capabilities, focused on actionable and intelligence-driven detection and response services. We are the preferred cybersecurity partner to notable organizations across various sectors, including Banking & Financial Services, Energy & Utilities, Manufacturing, Transportation & Logistics, as well as, Government & Public Sector. We are a trusted adviser to law enforcement agencies (including the FBI, NCA, Europol) and are also sought-after speakers for public and closed-community conferences around the world. Additionally, our depth of expertise and distinguished reputation ensure that we are regularly called upon as expert commentators on cyber topics for the media.