Who are We?

Security is not just something we are good at and we deliver, it is something we enjoy, and we breathe and speak security. At core, we are a bunch of geeks who love learning and reading about security. We love to nerd it up, we build new stuff and try to break them just for the fun of it. Customer Loves us for it! Do you want to build a tool to automate Penetration testing? We are happy to give you time to succeed. Sounds like you? Read further…

We are seeking a driven and motivated Senior Penetration Tester reporting to the Managing Director to lead the Security technical team.

We have a wide portfolio of clients from SME's to national corporate businesses, who trust us and respect and listen to us, we love that relationship with them. We love helping them in managing and improving security posture by delivering red team (offensive) and blue team (defensive) engagements and advisory service.

The Role

- Lead the Vulnerability and Penetration Testing team Practice
- Grow and build the practice capabilities by Contribute to the development, review, and maintenance of Cyber Security registers, standards, procedures, and related documentation
- Develop Penetration Testing program for both BAU and Project workstreams, run red/ purple team testing, and define & manage findings
- Work with a diverse range of customers to identify and solve security problems.
- Lead and deliver Infrastructure Penetration Testing
- Lead and deliver web application penetration testing
- Ability to present findings to a wide type of audience including both technical and non-technical.
- Perform incident responses services as required

This job requires a mix of deep hands-on technical skills as well as soft skills

About you

- Previous experience in a similar role
- Ambitious and motivation to drive and grow the security practice
- 5+ years' experience in infrastructure Penetration testing and/or
- 5+ years' experience in Web application Penetration testing
- Solid understanding of one or more security concepts, e.g.
    - Web Application Security
    - Infrastructure security (windows and/or Linux)
    - Security architecture
- Experience in a large number of tools under your arsenal (Metasploit, PowerSpolit, BurpSuite, Responder, etc…)
- Solid understanding and experience in Windows environment

- One or more offensive security certification (or near completion) such as OSCP, CREST, GWAPT, GPEN, or other
- Familiar with one or more offensive coding languages (Python, Ruby, C#) is highly desirable
- Excellent attention to detail as well as communication skills
- Understanding of red teaming, blue teaming and purple teaming engagements
- Can lead and manage concurrent red teaming project

Preferred

- Deep understanding of API security
- Experience and/or certified in Azure
- Experience and/or certified in AWS
- Experience in Windows PowerShell
- Experience in one or more commercial vulnerability scanners such as Qualys or Nessus
- Active in the security community (B-sides, AISA, OWASP, other)

In Return

- Flexible working hours/ work remotely or from home
- Large budget for training and R&D
- Employee stock options vest to own shares in the company.
- Ability to experience with the vast types of technology and cross multiple customer environments.
- Potential for growth and own shares in a Start-up company

Call 1300 20 90 23 for a confidential discussion.