Public

NEUROSOFT S.A.

Penetration Tester (Cyber Security)

Neurosoft S.A., is a leading software, networking and information security provider in financial, telecommunication, transportation, gaming and government sectors, providing solutions and services aiming to increase operating efficiency and security. Listed in the Italian Stock Exchange since 2009, currently employees 200+ highly skilled professionals with in depth expertise in their field.

We have an open vacancy for a Junior Penetration Tester to join our Cyber Security Services team. The candidate will conduct security testing in terms of technical assessments on web and mobile applications, servers, networks, hardware, advance social engineering and physical facilities to provide high quality of security services to our clients.

Roles' Responsibilities

- Conducts internal and external penetration testing and vulnerability assessments
- Conducts social engineering and phishing attacks
- Supports Red team engagements for specialized scenarios and organizations
- Explains, presents, demonstrates and documents, as needed, the operational impact of any vulnerability
- Develops exploits and tools for assessments or attacks
- Deploys testing methodologies and collects data
- Reports on findings and makes suggestions for security improvements
- Enhances existing methodology material

Professional Experience & Qualifications

- Bachelor's/Master's degree in Information Technology, Information Security or any other relevant field
- 1-3 years of penetration testing experience of systems, web-based applications and networks
- Proven experience of using penetration testing or threat modelling tools
- Good understanding of web technologies and services, networking, operating systems, server services/applications, wireless technologies and hardware
- Knowledge of security technologies such as firewalls, IDS/IPS, application gateways/filters, anti-virus, encryption, security information and event management (SIEM), mobile security, asset discovery, identity authentication management and access control
- Understanding of security community best practices and methodologies such as OWASP and OSSTMM
- Ability to understand complex issues quickly, to apply knowledge to effectively analyze business/IT risks and controls and clearly report findings
- Strong analytical skills, critical thinking and attention to detail
- Good communication skills and a customer-oriented approach
- Ability to work efficiently both independently and within a team
- Fluency in Greek and English languages with ability in technical and business writing

Preferred Skills and Qualifications

- Industry Certifications (e.g. OSCP, OSCE, etc.)
- Writing code with scripting languages such as Python, Ruby, Perl and shells
- Experience with mobile penetration testing applications
- Ability to perform secure code review, reverse engineering and exploit writing

We Offer

A competitive compensation package, a stable and enjoyable working environment, excellent opportunities for professional development and advancement, working on leading-edge technology and industry trends and … A lot of hacking!