CyberSwissGuards

Context

CyberSwissGuards is a boutique Security Technology Consultancy with offices in various European locations. The company is providing security and technology consulting services to a number of high-profile companies within the European region. We compete against world-class consultancy companies and have relentless focus on quality of our services and our people.

The company is looking to create a specialist group in Cybersecurity and is looking to recruit engineers with experience in this domain and with deep IT & networking technical skills who are looking to evolve their career into the security domain.

If you are ambitious and looking for a challenging job in a fast-paced multinational environment, this position is a good match for you. The role offers unbeaten opportunity for long-term professional growth.

Location and Travel

- Position allows for remote work (home office)
- International travel within the European region may be required

Key Responsibilities

- Design and execute Application, Infrastructure and Network Penetration Tests
- Plan and run vulnerability assessments of Application, Infrastructure and Network systems
- Pinpoint methods and entry points that attackers may use to exploit vulnerabilities or weaknesses
- Use manual testing and automated techniques/methods to gain a better understanding of the Identify critical flaws in applications and systems that cyber attackers could exploit
- Develop, test and modify custom scripts and applications for vulnerability testing
- Perform physical security assessments of systems, servers and other network devices to identify areas that require physical protection
- Use automated tools to pinpoint vulnerabilities and reduce time-consuming tasks
- Compile and track vulnerabilities over time for metrics purposes
- Create comprehensive reports and recommendations
- Research, evaluate, document and discuss findings with IT teams and management
- Be sensitive to end-user considerations when performing testing (i.e. minimize downtime, data/system integrity, and loss of employee productivity)

Knowledge, Skills & Experience

- 5+ years of hands-on technical Security experience or in Software Development or Systems Administration
- Experience using modern penetration testing tools and methods
- Deep knowledge of network protocols (IPV6, DNS, HTTP, etc) and accompanying tools (Wireshark, TCPDump, etc)
- Understanding of network administration of Routers and Switching technology
- An understanding of and/or experience developing applications for both on-premises and cloud-based solutions (such as Azure, AWS) and the integration of these platforms
- Experience with the following frameworks: Kali (Linux), Metasploit,
- Adhere to best practices & methodologies (ISSAF, OSSTMM, OWASP, PTES)
- Experience of working within an environment of structured change, release, incident and

problem processes (ITIL)

- Familiar with any of the programming languages: Python, Bash, Java, .NET, C, C++, Ruby
- Fluent in English, other European languages are an advantage
- Pro-active individual who has the ability to “think like the hacker”, being able to see issues and suggest solutions before they arise.

Any of the following certifications (or technical acumen to attend relevant trainings) is an advantage:

- Certified Ethical Hacker (CEH)
- Certified Penetration Tester (CPT)
- Certified Expert Penetration Tester (CEPT)
- GIAC Certified Penetration Tester (GPEN)
- Licensed Penetration Tester (LPT)
- Offensive Security Certified Professional (OSCP)
- Certified Mobile and Web Application Penetration Tester (CMWAPT)
- CompTIA PenTest+
- Experience of ISO27001