Deloitte.

Technology & Transformation
Cyber: Attack Surface Management (ASM) | Senior Executive

What impact will you make?

Every day, your work will make an impact that matters, while you thrive in a dynamic culture of inclusion, collaboration and high performance. As the undisputed leader in professional services, Deloitte is where you'll find unrivalled opportunities to succeed and realise your full potential.

The Team

Deloitte helps organisations prevent cyberattacks and protect valuable assets. We believe in being secure, vigilant, and resilient—not only by looking at how to prevent and respond to attacks, but at how to manage cyber risk in a way that allows you to unleash new opportunities. We put cyber risks at the start of strategy development for more effective management of information and technology risks.

Work you'll do

As a part of our Technology & Transformation team, you'll build and nurture positive working relationships with teams and clients with the intention to exceed client expectations. You'll:

- Work on projects with clearly defined guidelines as team member with responsibility for project delivery
- Work under general supervision with few direct instructions
- Perform cyber security assessments which includes vulnerability assessment & penetration testing, network security architecture review, secure configuration / code review, etc.
- Understand basic business and information technology management processes.
- Demonstrate knowledge of firm's methodologies, frameworks and tools
- Participate in practice development initiatives

Required skills

- Understanding of basic business and information technology management processes.
- Good knowledge of TCP/ IP and Networks including Firewall, IDS/IPS, Routers, Switches, and network architecture.
- Experience of Web Application Security Testing, Infrastructure VAPT, API testing.
- Experience on Mobile Security Pen-Testing (iOS and Android).
- Experience in conducting config reviews of Windows, Linux, UNIX, Solaris, Databases, etc.
- Experience with Vulnerability Management tools: Kali Linux, Acunetix, AppScan, Nexpose, Qualys Guard, Nessus, Nmap, Metasploit, Fortify etc.
- Experience in basic scripting such as: Shell, Python, PERL, etc.
- Basic knowledge of Technologies such as: IPSEC, SSL, SSH, VPN, Ethernet Token Ring, WAP, SMTP, FTP, Frame Relay, WAN, ATM, FDDI, DSL, ISDN, HP Openview, Sun NetManage, Cisco Works, Radius, Big Brother, F5.
- Experience on End Point Security, Threat Profiling, Configuration Review
- Experience on Firewall and Network Devices Configuration Review.
- Strong analytical and communication skills (written, verbal and presentation)
- Open to learn new tools and technologies as per the project requirement
- Interactive with team members and confident during client meetings, under the guidance of senior members of the project
- Initiative & drive
- Deadline-oriented and quality-focused
- Familiarity with industry standards and frameworks such as OWASP, CIS, NIST ISO/IEC 17799, etc.
- Basic knowledge of security and privacy controls and risk management processes

- Basic knowledge in one or more Cyber Threat Management domains such as: Threat Management, Cyber Operations/Fusion Managed Services, Malware Analysis, Collective Threat Intelligence and Cyber Risk Sciences, Incident Management and Forensics, Data Protection solutions.

Qualifications

- Bachelor’s degree is required. Preferred in Computer Science, Cyber Security, Information Security, Engineering, Information Technology.
- Candidate should have a minimum of 3+ years of experience in Cyber Security covering Application Security and Infrastructure Security
- Candidates must possess security certifications such as CEH, LPT etc
- Security certification for OSCP, GPEN would be an advantage

Kindly send your CV on mucareers@deloitte.com