JOB DESCRIPTION - SECURITY ANALYST (VAPT)

About HackIT

HackIT Technology and Advisory Services is an IT/Cyber Security company, operating since 2009. HackIT is an Indian Computer Emergency Response Team, CERT-IN (www.cert-in.org.in) empaneled provider for IT Security Audit Services. HackIT provides a broad range of security consulting and advisory services to a diverse group of clients, including government organizations, corporations, Military establishments financial institutions and start-up, to name few. Our work spans multiple sectors and industries, including Telecommunications, Defense and Military, ITeS, Financial Services, Aviation, Hospitality, Healthcare and Research. We work end-to-end—from diagnosis to delivery of lasting impact — together generating tangible results that are improving the security posture of organizations worldwide.

Job Title
- Security Analyst (VAPT)

Location
- Delhi

Job Overview

We are seeking a detail-oriented Security Analyst (VAPT) to perform vulnerability assessments, penetration testing, and security analysis of applications, networks, and infrastructures. The role includes developing Proof-of-Concepts (PoCs), providing remediation guidance, preparing detailed reports, and collaborating with clients and stakeholders to strengthen organizational security posture.

Job Responsibilities

- Manual and automated security testing of Web applications, APIs, and Mobile Applications.
- Static and Dynamic testing (SAST & DAST) of thick clients / applications.
- Develop Proof-of-Concept (PoC) for the identified vulnerabilities.
- Provide remediation guidance to identified vulnerabilities.
- Develop and execute security testing project plans.
- Incorporate metrics providing comprehensive insight about the security posture of an organization that will help senior management with decision making.
- Build and maintain strong relationships with key stakeholders.

Technical Skillsets (Mandatory)

- Hands on experience in Penetration Testing.
- Strong analytical and problem-solving skills and the ability to explain complex technical concepts in a clear and concise manner and to provide remediation recommendations.

- Knowledge or experience with both Enterprise and open-source offensive security tools for reconnaissance, scanning, exploitation.
- Sound understanding of security frameworks (OWASP Top 10, NIST, MITRE ATT&CK).

Technical Skillsets (Preferred)

- Proficiency in a programming language(s) (e.g. Python, Ruby, Perl, PowerShell).
- Exposure to DevSecOps, Security Architecture review and Network Security assessment would be a bonus.
- Hands-on experience in Red Team Exercises, Threat Hunting, OSINT and Threat Modelling.

Non-Technical Skillsets

- Estimate Project efforts and meet delivery milestones and deadlines.
- Excellent and effective report writing and verbal communication skills.
- Deliver results within stipulated time-lines.
- Team Player with good interpersonal skills.
- Should be able to work independently with minimum and least supervision in complex, dynamic and challenging environment.
- Self-driven and self-managed technical team leader.
- Communicate project requirements and influence stakeholders with minimal supervision.

Education and Certifications

- Bachelor's degree in IT or equivalent.
- Industry recognized certifications (Eg: OSCP, CREST, eWPT, GXPN, GPEN, Cloud Certifications and other well acknowledged security certifications) preferred.

Experience

1 to 3 years in Application/Infrastructure/Network Penetration testing.

Send your updated profiles to **careers@hackit.co.**