JOB DESCRIPTION – TEAM LEAD (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
- Team Lead (VAPT)

Location
- Kochi

Job Overview

We are looking for a detail-oriented Team Lead (VAPT) to oversee vulnerability assessments and penetration testing across applications, networks, and systems. This role combines hands-on technical expertise with leadership responsibilities to ensure accurate vulnerability identification, effective remediation guidance, and continuous improvement of the organization's security posture. The candidate will also mentor team members and drive high-quality delivery across all engagements.

Job Responsibilities

- Lead end-to-end VAPT engagements across web, mobile, network, and cloud environments.
- Manage and mentor the security testing team, including task allocation, performance monitoring, and skill development.
- Ensure high-quality, accurate, and compliant security testing reports aligned with industry standards.
- Define, implement, and continuously improve VAPT processes, methodologies, SOPs, and reporting standards.
- Act as the primary technical authority and escalation point for all security testing activities.
- Serve as the technical point of contact (POC) for clients and internal stakeholders.
- Identify, track, and escalate risks, delays, and quality concerns to management.
- Assign testing activities based on project scope and team skillsets.
- Perform and review vulnerability assessments, including CVSS scoring, proof-of-concept (PoC), and remediation recommendations.

- Validate and approve final VAPT reports before submission to clients or regulatory bodies.
- Lead client interactions such as project kick-offs, technical discussions, and closure meetings.
- Provide technical guidance and mentorship to junior analysts and interns.
- Support advanced security testing activities across network, web, mobile, and cloud environments.
- Participate in Red Teaming exercises when required.

Technical Skillsets (Mandatory)

- Strong hands-on experience in penetration testing and vulnerability assessments.
- Proficiency with security testing tools for scanning, exploitation, and reporting.
- Solid understanding of frameworks such as OWASP Top 10, NIST, and MITRE ATT&CK.
- Experience in web, API, mobile, and infrastructure security testing.

Technical Skillsets (Preferred)

- Knowledge of programming/scripting (Python, Bash, PowerShell, etc.).
- Experience with SAST, DAST, and DevSecOps practices.
- Exposure to Red Teaming, Threat Hunting, OSINT, and Threat Modeling.
- Familiarity with cloud security assessments and architecture reviews.

Non-Technical Skillsets

- Strong leadership and team management capabilities.
- Excellent analytical, problem-solving, and communication skills.
- Ability to manage multiple projects and meet deadlines.
- Strong report writing and stakeholder communication skills.
- Self-driven and capable of working in dynamic environments.

Education and Certifications

- Bachelor's degree in IT or a related field.
- Preferred certifications: OSCP, CREST, eWPT, GPEN, GXPN, or equivalent.

Experience

3–5 years of experience in VAPT (Application, Network, or Infrastructure Security).

Info Sec Community Activities and Opportunities

- Promote security research that are aligned with the current industry requirements and incepted at HackIT.
- Provide assistance and support for presenting research papers at security conferences across the globe.
- HackIT provides opportunity to contribute back to the information security community.

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