VAPT Engineer

Responsibilities:

- Conduct Vulnerability Assessment and Penetration Testing and configuration review for network, web application , mobile application and thick -client application
- Conduct configuration reviews for OS , DB, Firewall, routers, Switches and other security devices/components
- Involved in performing manual and automated penetration testing.
- Conduct source-code review using automated and manual approaches
- Work with implementation partner to see project on track
- Provide required detailed reports to management and client
- Ensure timely delivery of status updates and final reports to clients
- Handle the project as well as BAU operations
- Ensure high level of systems security compliance
- Coordinate with and act as domain expert to resolve incidents by working with other information security specialists to correlate threat assessment data
- Analyze data, such as logs or packets captures, from various sources within the enterprise and draw conclusions regarding past and future security incidents
- Involved in vulnerability scanning and assessment for various projects.
- Involved in setting up the process for vulnerability management.
- Experience in scheduling scans and processing the vulnerability reports
- Keep oneself updated on the latest IT Security news ,exploits, hacks
- Prepare Threat Intelligence reports for newly discovered threat agents, exploits, attacks

Requirements:

- Minimum 3 years of experience in VAPT
- One or more security certifications: OWASP,CEH, Security , GSEC, GCIH, etc
- Experience in Vulnerability Assessment and Penetration testing of web applications, thick client applications, mobile applications, API and network.
- Understanding of web-based application (OWASP Top 10) vulnerabilities.
- Understanding of TCP/IP network protocols.
- Working knowledge of industry standard risk, governance and security standard methodologies
- Expertise on skills like NIPS, WAF, SIEM, Nessus, CEH, Qualys guard, Vulnerability Assessment and Penetration Testing, Network Security, Web Application Security
- Proven ability of incident response processes (detection, triage, incident analysis, remediation, and reporting)
- Proven attention to detail and organizational skills and ability to coordinate input and develop relevant metrics
- Ability to multitask and work independently with minimal direction and maximum accountability

Additional Information:

- Office based in KL Eco City
- Walking distance to LRT Abdullah Hukum
- Office Hours: Monday - Friday, 9am - 6pm
- Smart Casual Fridays
- Benefits: Dental, Medical, Optical
- Parking Allowance