Vulnerability Analyst and Penetration Tester

Job Description:

The Vulnerability Analyst & Pen-Tester (VAPT) is responsible for identifying threats and vulnerabilities and their associated security risks within True Digital by performing vulnerability testing and penetration testing across the MDR Centre constituency and provide advice on how to remediate the vulnerabilities discovered. The VAPT team owns the vulnerability testing plans and keep current on security attack risks and methods.

Key Responsibilities:

- Performs security vulnerability assessment and penetration testing of internal, perimeter, external and wireless network and web and mobile applications.
- Identifies security weaknesses and vulnerabilities, and non-compliance within the MDR Centre constituency.
- Characterizes threats and provides recommendation for remediation.
- Advises appropriate business units on technical configuration and process changes, remediation and best practices to adapt to changing threat, vulnerabilities and new attack methods.
- Conducts follow up assessment to ensure proper action has been taken.
- Researches and develops testing tools, technique and process.
- Maintains, executes and refines processes to monitor, collect and update information about threats and vulnerabilities.

Qualifications:

- Bachelor degree in a related field such as information security, management or computer engineering.
- Experience in security incident management and response, threat modelling, penetration testing and/or secure application development.
- Active OSCP, OSCE, GPEN, GWAPT, GXPN, CEH, ECSA, LPT certifications good to have.
- Other relevant certifications (such as GCIH, GCIA, GCFA and others) desirable.
- Experience in architecture design and assessment (manual approach to penetration testing).
- Good working knowledge of security concepts for both Windows and Unix related operating Systems.
- Familiar with application and infrastructure vulnerabilities.
- Experience with exploit research and mitigation.
- Good working experience using various assessment tools, such as scanners, administrative utilities, local proxies, debuggers, fuzzier, etc.
- Good working knowledge of web technologies, solutions and attack vectors that apply to application technologies, such as OWASP.
- Experience with threat modelling methodologies.
- Experience with security source code review or development experience in C/C++, C#, VB.NET, ASP, or Java.
- Familiar with application reverse engineering techniques and procedures.
- Good working knowledge of IDS and AV evasion techniques.