Penetration Testing

Overview

Penetration Testing (often referred to as pentesting) is a valuable component of an organisations vulnerability management programme, the objective of a pentest is to simulate the actions of a malicious threat actor in order to identify vulnerabilities within applications and services, put simply a pentest is about gaining access, reaching the point of simulating a malicious act and highlighting to the business what was achieved and how the vulnerability was exploited.

Many businesses believe that simply conducting vulnerability scans is sufficient to understand their vulnerabilities; however, a scan is exactly that – an automated process to find common vulnerabilities, a pentest is generally more focused and works against all elements (people, process and technology) and generally provides a more informed output.

In the pentest world a Red Team act as the attackers, while the Blue Team are the defenders, using a pentest to allow a blue team to conduct threat hunting is a useful opportunity that can 'gamify' and enthuse your network defenders to look out for malicious activity.

Pentesting is a complex activity, there are different types of pentest, with each bringing slightly different results.

- ***Vulnerability identification in bespoke or niche software*** – most commonly used against web applications
- ***Scenario driven testing aimed at identifying vulnerabilities*** – The penetration testers explore a particular scenario to discover whether it leads to a vulnerability in your defences
- ***Scenario driven testing of detection and response capability*** – In this version of scenario driven testing, the aim is to also gauge the detection and response capabilities your organisation has in place, detecting and watching a threat move around your network can be extremely challenging and deciding what to do and when is best practiced before a 'real event'

Capita

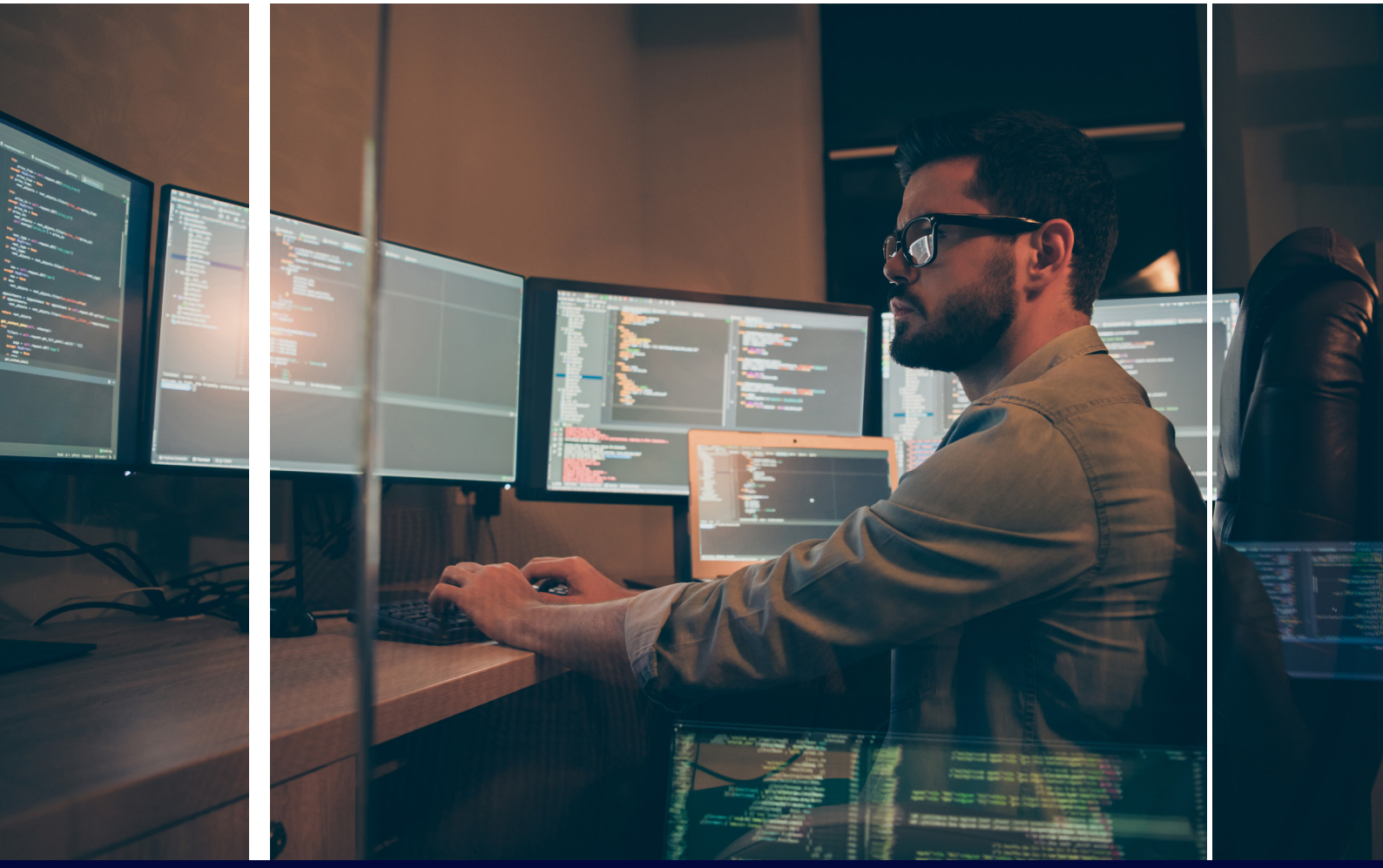
Our approach

Using our Capita trusted third parties we will :-

- **Scope** – out the parameters of the pentest to be conducted, this includes the technical boundaries, the timeframe and amount of effort, the scenarios you want explored and any specific requirements needed (such as test accounts or specified logins to use) and most importantly the written approvals for us to proceed;
- **Testing** – conduct the test and maintain technical points of contact throughout;
- **Reporting** – Issue a comprehensive pentest report which outlines the security issues found, an assessment as to the level of risk relating to each vulnerability and a method for resolution
- **Severity Rating** – all our reports utilise a CHECK definition (such as High, Medium, Low and Informational) which will aid you to prioritise each vulnerability

Markets / Industries

- All



For more information please contact:

Jim Fox CISM, MBCS, MSyI
James.fox2@capita.com

Capita