Tiberium

DATA SHEET

Tiberium **Penetration Testing**

Tiberium Attack Services

Tiberium Attack services comprise multiple services which suit different businesses at different stages in overall security maturity, project status and of course, the threat and risk levels specific to the business, the sector, or more generally.

It is essential to select the correct service for your organisation to maximise and measure the effectiveness of your Security budget investment.

The services are split into the following categories, although there is some overlap. Tiberium will recommend a programme best suited to the task if required.

THE WEAKEST LINK

Bob got the job!

Bob got phished!

Bob explores the network!

Traditional Penetration testing – This is a full test of your security posture from an external, internal or combined perspective. Carried out by Tiberium's assurance team, this process will result in reliable prioritised recommendations for remediating any issues.

Red teaming – If Penetration testing is akin to an assault by an army, Red Teaming is akin to a 'Special Forces Hacking' affair using preparation, reconnaissance and stealth, aligned to real threat actors tactics and techniques.

Blue teaming – A Blue Team tries to detect a Red Team attack and either stop it in its tracks or defend the target. The tools and techniques available to the Blue Team will be those currently in place at your organisation, or we can rapidly deploy a detection solution.

Purple teaming – This is where Red and Blue teams work together rather than as adversaries to identify issues in detection rules quickly, including applications, infrastructure, people and processes. If you have an in-house

PENETRATION TESTS

Third party penetration tests should be performed by qualified and experienced staff only and are recommended to take place at least once a year by the UK Government

TESTING MODEL

- Engage
- Scope
- Define Special Requirements
- Plan of Action
- Testing
- Reporting

> team, Tiberium can augment it to add knowledge and experience. In terms of training your people, purple teaming is very valuable.

A method of gaining assurance

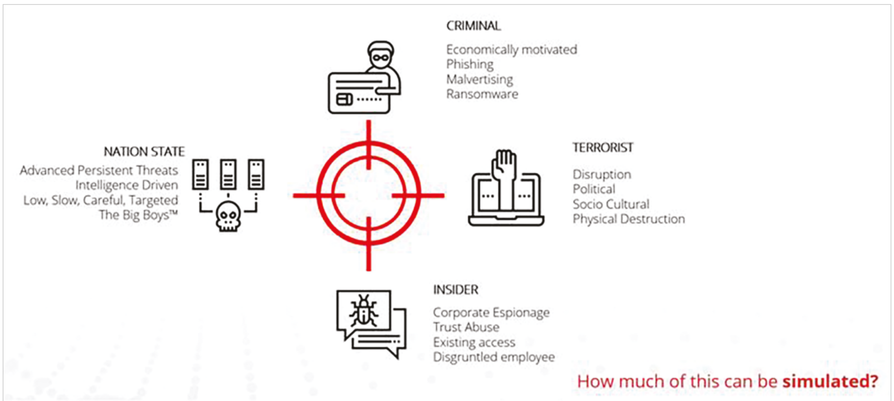
in the security of an IT system **by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might**

What is penetration testing?

The National Cyber Security Center describes penetration testing as the following: "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might".

Penetration tests identify both weaknesses and strengths in the security of your systems and processes, making prioritised recommendations for remediation. As with all Tiberium solutions, prioritised recommendations allow security and IT budget to be best focussed to effectively and measurably improve the security posture of your business, enabling you to protect your assets and ensure business continuity.

Tiberium has extensive Penetration Testing experience for organisations large and small and can justify all recommendations with real-world step by step compromise evidence, demonstrations to reproduce bugs and explanations of risks, business exposure and potential damage (including costs and business impact) to both technical and non-technical staff up to board level if required.



High-Level Tiberium Testing Services Overview

- Web Application Penetration Testing
- Wireless Network Penetration Testing
- Mobile Application Penetration Testing
- Infrastructure Penetration Testing
- Vulnerability Scanning
- Cyber Threat Intelligence (**O**pens **S**ource **INT**elligence)
- Adversary Simulation

> **A Web Application Penetration** test uses manual and automated techniques to identify vulnerabilities and security risks present on internal and external facing web applications, end to end (database, source code, back-end services, API's). Tests are conducted by our team of certified 'ethical hackers'.

ACTIONABLE INTELLIGENCE

Tiberium will always communicate throughout the process and will be here to explain the results, giving actionable intelligence to help you assess vulnerabilities and advise of any solutions required to make your business more secure

Wireless Network Penetration Testing – is required as attackers will try to use wireless networks and devices as an entry point into the organisation. Tiberium uses the latest wireless and RF breach techniques to ensure that your business is not vulnerable.

Mobile Application Penetration Testing – Mobile applications are a way of life and are being very rapidly developed and deployed both commercially and corporately. The pace of Mobile technology makes it a very fruitful hunting ground for hackers. Our testing service will identify any weaknesses in your application code, Android and iOS packages, and supporting systems.

Infrastructure Penetration Testing – Is a non distructive attack against your infrastructure using the same reconnaissance, tools and techniques that an assailant would use to breach your systems, access your data or other intellectual property, cause disruption such as ransomware or leave behind rogue code to facilitate a future attack. All testing is executed without causing any real damage! Used as both an audit point and the foundation and business justification for a security improvement programme, regular infrastructure penetration testing is a vital part of the security lifecycle. Tiberium's experienced, ethical hacking team have many years of experience delivering this service, providing practical, justifiable recommendations.

Vulnerability Scanning – helps to identify potential vulnerabilities in end-user equipment, network devices and applications. Preferably deployed as a continuous, scheduled service, a vulnerability scan, for instance, for Cyber Essentials PLUS, is lower in cost than a Penetration Test but only identifies current areas of risk and not the whole security ecosystem, including processes and procedures. A single scan does also not provide detail into the potential ramifications of a particular vulnerability or series of vulnerabilities. Tiberium uses enterprise-level products for vulnerability scanning to ensure accurate, up to date results. Tiberium recommends regular vulnerability scans to alert on potential exposure to new vulnerabilities and provides this as a managed service (MVIS) to scan external and internal assets regularly.

OSINT – Our team of experts uses open-source intelligence to accumulate information about your organisation from public sources. We will then provide you with a threat assessment based on information that hackers are known to use. With our support you should use this information to make informed decisions to improve internal security awareness, influence decision-makers to look at cyber maturity based on the information provided and accurately address areas where threat actors can take advantage.

Tiberium

Tiberium are at the forefront of intelligence driven managed SOC services combining cloud-native technology and machine based automated.

Tel +44 (0)207 073 2632 • Email contact@tiberium.io

About Tiberium

Our mission is to provide transparent, rapid, and trusted managed security services (MSSP). Our analysts and threat hunters are highly skilled Cyber Security practitioners with decades of experiences in the real-world, we don't do "theory". We aim to reduce the noise experienced by traditional Security Operations Centre's and test your defences to ensure the technology we put have in place is worth the investment. A simple mission with effective results. Find out more at tiberium.io

Tiberium

Partners

Microsoft Partner – Silver Security, Gold Cloud Platform, Silver Application Development

Gold Microsoft Partner

Accreditations

Cyber Essentials Certified Plus • Cyber Scheme • IASME Consortium Gold certified company