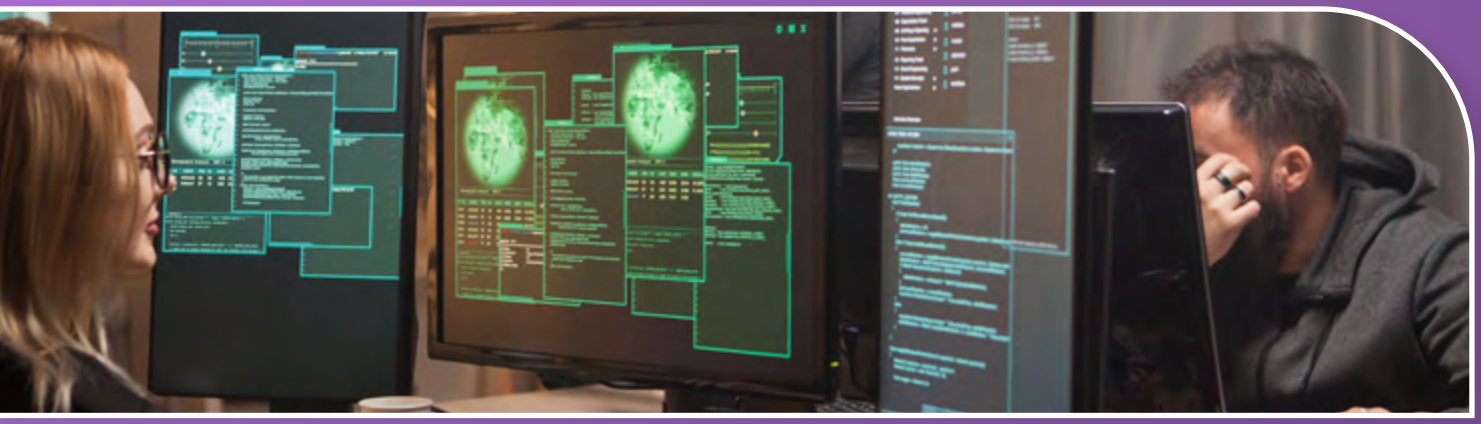
Tailor Made TECHNOLOGIES IT & Communications

Penetration Testing

The cyber threat landscape is always adapting and changing to the latest methods of compromising data, so your cyber defences need to work hard to keep your organisation secure. The TMT range of penetration tests helps you understand and baseline your organisation against the current threat landscape.



What Are Penetration Tests?

Penetration tests are not just designed for protection against direct attacks, they are also the foundation of an effective risk management strategy.

Penetration tests aim to improve the overall security and ensure control of systems, networks, and infrastructure. Regular penetration testing is a constructive method of managing vulnerabilities and ensuring your infrastructure is safeguarded against hackers.

Penetration testing is also a requirement of many security standards, such as ISO 27001 and PCI DSS. Therefore, if you are regulated or accredited in these areas, penetration testing is a non-negotiable business fundamental.

Organisations adopting penetration testing can build a useful cyber threat protection package by embracing services such as (SIEM (Security Incident Event Management)).

TMT's cybersecurity experts will help your organisation manage and mitigate cyber threats by simulating real-world attacks to identify weaknesses and security vulnerabilities in your IT systems and infrastructure. Testing can be done across your complete IT estate, including desktops, servers, and infrastructure devices as well as the business applications that store your most critical and sensitive data. TMT will deliver a comprehensive report on the results of the testing along with recommendations for remediating any identified threats and vulnerabilities.

TYPES OF TESTING AVAILABLE

- **Phishing Assessment -** Both Phishing and Spear Phishing attacks have significantly increased and a primary source of targeted cyberattacks. Our phishing assessment baselines both your employee's awareness of such hacking techniques, as well as providing an ongoing education plan.
- **Remote Working Assessment -** With an increasing number of employees working from home, ensure your networks, applications, devices, and data are protected and fully secured with our bespoke remote working security assessment.
- **Infrastructure Assessment -** Our cyber expects will look to exploit any security vulnerabilities, either via an external cyberattack simulation test and/or an internal one. This helps us to establish if attackers can compromise assets within your systems, such as customer or financial data.
- **Application and API Assessment -** This range of tests offers both automated and manual penetration tests to assess the security of specific applications, and/or code structures.
- **Web Application Security Assessment -** A focused test to identify vulnerabilities in business applications accessed via standard web interfaces, whether internally or externally.
- **WiFi Assessment -** Our wireless penetration testing identifies the security of your internal WiFi network, whether set up for internal use, guest use, or both. The assessment will identify items including unsecured encryption protocols, misconfigurations, and weak access controls.
- **Firewall Configuration Assessment -** This testing checks the configuration of your firewall devices to identify weaknesses or incorrect and sub-optimal setups.