People

Best Practice Security

SAEPIO
INFORMATION SECURITY

DATASHEET

Penetration Testing

How do Cyber criminals decide who to target? Like any opportunistic attacker, they look for low hanging fruit first. By using readily available tools to scan the health of websites, applications, wireless networks & endpoints, they find and focus on weakness.

How can you help to protect yourselves? Conduct regular Penetration Tests. Ethical hackers systematically probe for vulnerabilities in your applications and networks by launching benign attacks to uncover any weaknesses before the bad guys do.

Whether you are looking to comply with a security framework like Cyber Essentials Plus or ISO27001, a compliance standard like PCIDSS, or just looking to test the integrity of your security posture, Penetration testing is a great way to baseline or ultimately prove your security posture from a product maturity, configuration and operational standpoint.
Working with our teams of external, CREST accredited Penetration Testers, Saepio can supply a wide range of services – External, Internal, Wireless, Web App, Red Team, Social Engineering and more

ABOUT SAEPIO?

Saepio is an Information Security advisor that helps organisations reduce their cyber risk and improve security posture.

Saepio believe Security is more than technology. Best practice policy and process direct a successful security strategy. Products and people help to enforce it

CYBER ESSENTIALS PLUS

"Pen testing services from Saepio have been professionally delivered and of a very high quality, 100% we would use them again" – CISO, Wealth Management Firm

Essential Testing

External Penetration test
Assess the external, Internet-facing infrastructure of your corporate network. The level of access to these resources would be the same as an external hacker trying to break into your corporate environment.

Internal Penetration Test
Assess for security issues and vulnerabilities on the inside of your corporate network with the same physical access as a member of staff or other type of employee who has access to the building

Wireless Penetration Test
Assess for WLAN weaknesses before attackers take advantage of them. Regular testing of your wireless network can identify and close any security holes before an attacker can slip through.

Web application Penetration Testing
Assess the external & internal applications that you host. Their complexity and availability have made them an ideal target for attackers and there have been many publicised data breaches that have been caused by insecure web applications.

Advanced Testing

Social Engineering/ Red Teaming
Assess for the Social Engineering techniques used by attackers as a way to extract reconnaissance information or to gain access to physical locations. Test the robustness of your internal systems and provide practical advice on what changes are needed to prevent a real attack succeeding.

Breach Simulation
Use software to test your network's ability to cope with pre-exploitation stage threats in Email, Browsing, and WAF. Analyse your ability to respond to real incidents with post-exploitation detection for lateral movement, Endpoint and Data Exfiltration