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.

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

CREST

CHECK
IT Health Check Service

People

Best Practice Security

SAEPIO
INFORMATION SECURITY

SCOPING QUESTIONS

Saepio have access to a large stable of qualified Security Consultants who provide a range of testing services. Regardless of what type of testing you wish to undertake, you can be confident that the consultants Saepio provide will be knowledgeable, professional and easy to work with.

External Penetration Test

- Confirm number of IPs associated with the external perimeter?
- How many of these are live and how many support webservers?
- How many firewalls are there on the external ranges?
- How many VPNs (and which types) are connected to these ranges?

Internal Penetration Test

- How many servers are in scope of an internal infrastructure test?
- Are these servers segregated onto separate VLANs or subnets?
- What flavour of operating systems do these servers run? (e.g. Windows 2012/16, Solaris, RHEL)
- How many of those servers are considered business critical?
- How many desktops/laptops are on the network?
- What locations will need to be visited?

Wireless Penetration Test

- What solution is in place?
- What authentication is required?
- How many user profile types? And with what purpose and what kind of access is provided?
- How many access points?

Web Application Penetration Testing - per application in scope

- What does the application do? (name/description/function)
- What is the URL?
- How complex is it? (e.g. number of functions, unique pages, etc.)
- How many different user types are there and a brief description of the differences?
- Who has access, and what authentication do they require?
- What are the biggest risks if compromise was achieved?
- What technology is the application and its infrastructure based on?
- How many machines and IP addresses is the application hosted over?

CREST

CHECK
IT Health Check Service