PentestPeople®

CREST

CHECK
IT Health Check Service

HM Government
G-Cloud
Supplier

We Are PentestPeople

We Are PentestPeople

Formed – December 2017

Head Office – Leeds, West Yorkshire, UK

Pentest People are a UK-based boutique security consultancy focussing on bringing the benefits of **Penetration Testing as a Service** (PTaaS) to all its clients. This innovative approach to security testing combines the benefits of a consultant-led penetration test and vulnerability assurance through a technologically advanced SecurePortal, providing a living threat system to its clients and benefit through the life of the contract rather than just a single point in time.

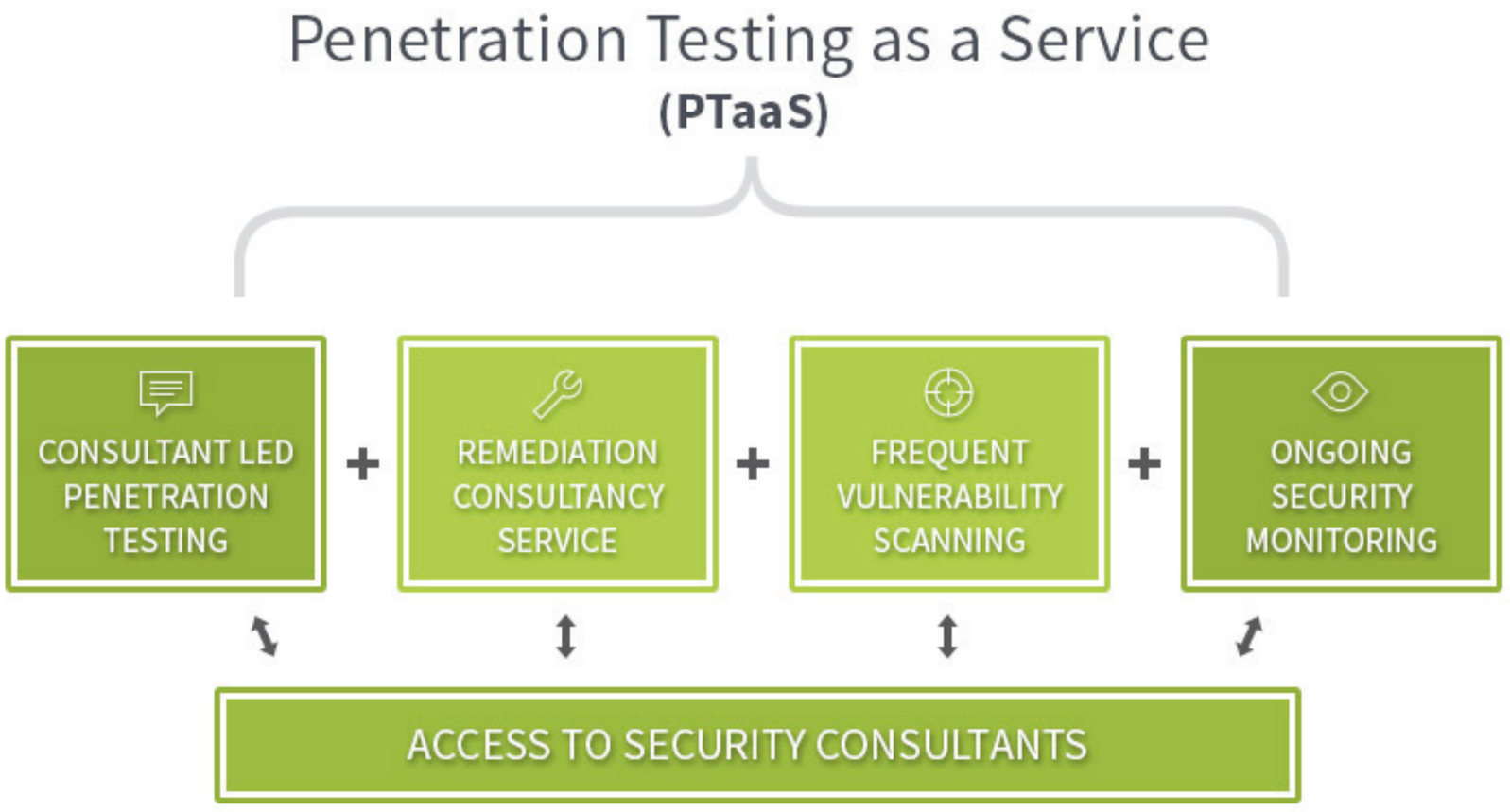
Pentest People are a **CREST** accredited company for its **Penetration Testing** services and have also attained the NCSC **Cyber Essentials** and **Cyber Essentials Plus**.

Pentest People are also accredited to ISO:9001 and ISO:27001.

Our specialised team of security consultants hold industry qualifications such as **CHECK Team Leader, CCIE, CISSP** and **CEH** and combine this with many years of industry experience at the highest level working across all industry sectors. It is the aim of our consultants to work with organisations to ensure that their security investment is fully optimised on a 24/7/365 basis.

By building on our front-line network security experience and listening to the day-to-day challenges of our customers we aim to deliver world-class, integrated security risk management solutions that turn security data into security intelligence; simplifies and automates regulatory compliance processes and provides peace of mind for network managers that their IT environment is fully protected.

PTaaS
Pentesting as a Service



Why Penetration Testing as a Service (PTaaS)?

A companies Security Posture is constantly changing in line with the evolving risks faced by multiple sources.
A traditional **Penetration Test** is very much a point in time assessment.

Pentest People have a wealth of experience of building traditional **Penetration Testing** businesses. It is time for the market to evolve and a new solution to be provided that meets the needs of the customer.

PTaaS advocates a continuous cycle of testing and remediation. It suggests that your security posture is always changing so in order to combat this moving target there must be an on-going program of testing, remediation and management. The PTaaS methodology understands that there is a need to test and check the entire platform stack. From the operating system to the SSL certificate, PTaaS is all about establishing a regime of automatic checks and monitoring so that even the smallest aspects of your eco-system are protected.

What do we receive with PTaaS?

Frequent Vulnerability Scanning

As well as the point in time **Penetration Test**, you will also receive access to regular external and internal **Vulnerability Scanning**. This scanning can be scheduled to fit into your environment and timescales to ensure that you are kept informed of newly released vulnerabilities that may affect your infrastructure.

Consultant Led Penetration Testing

A **Pentest People** security consultant will perform a thorough **Penetration Test** based on your exact requirements. This test can include an assessment of your internal and external hosts as well as any Web Applications you may have in use. The Penetration Tests will be scheduled to match your requirements and budget.

Ongoing Security Monitoring

Various **Security Monitors** are available which all run at frequent intervals. These can be used to perform **Port Scanning** of your external infrastructure as well as to check items such as your SSL Certificates in use for your Web Applications and also monitor for JavaScript Security issues on your webservers.

Access to Security Consultants

Depending on the level of service you have purchased, you will receive access to the **Pentest People** team of experienced security consultants. These consultants are available on a helpdesk basis for general security concerns as well as to perform regular security reviews of your **Vulnerability Assessments** and **Security Monitors.**

Key Benefits of PTaaS

- Receive ongoing **Security Management** through an Overarching Managed Service
- Traditional reports are out of date the minute they are delivered. **SecurePortal** is a living system that evolves in line with your network
- Automatically track changes that might affect your security posture with minimal effort
- Consultancy is not enough, keep up with new threats by adopting a **continuous program of Testing and Monitoring**
- With so many attack vectors **PTaaS** allows you to monitor your entire ecosystem so emerging problems can be fixed early

Introducing SecurePortal

SecurePortal is a key component of Penetration Testing **as a Service** and provides customers of **Pentest People** with a live platform of engagement and also managing the current security posture of your organisation based on the information gathered from our penetration testing services.

SecurePortal :

- Eases the administrative burden of planning a Penetration Testing engagement
- Provides digital access to your report
- Tracks the state of your vulnerabilities automatically
- Alerts you when new threats are relevant
- Provides a simple way to filter your report data

Frequent Vulnerability Scanning

SecurePortal provides a single dashboard view of all of the vulnerabilities across your infrastructure.

Receive overview and trend data of all of the current security issues you face in your organisation. Receive useful trend information such as the **top vulnerable hosts**, and the **most common vulnerabilities** within your infrastructure.

Helping you Engage with Pentest People

Customers are introduced to **SecurePortal** early in the sales process and all sales proposals are accessed and downloaded securely through the **SecurePortal**.

Once the agreement to proceed has been made, all of the project management tasks associated with our various **Penetration Testing services** are performed on the **SecurePortal** using various secure web-based forms rather than relying on the unsecured emailing of various documents.

Helping you Manage your Vulnerabilities

Until now, the traditional deliverable from a **Penetration Test** engagement has been a lengthy report. This is usually provided in a PDF file format and can run into the hundreds of pages.

Pentest People have developed a solution to this issue where you interact with your vulnerabilities within the **SecurePortal**. This allows you to quickly search for vulnerabilities rather than scanning through a lengthy document.

Live Vulnerability Updates

SecurePortal updates its vulnerability information every two hours from the **National Vulnerability Database**, providing you with the latest vulnerability details rather than relying on information that was created at the point of your assessment.

Vulnerability Trend Analysis

As well as viewing the results of your latest security assessment, you can also go back and compare the results in each assessment with previous assessments performed on the same hosts. This provides you with a business benefit of understanding if your **security posture is improving**.

Still Allows PDF Reports

SecurePortal still allows you to produce a PDF report if this is what you require, but we have the added benefit of allowing you to select which hosts and in which view format you would like the report, either by host or vulnerability.

The Six Step Methodology

Our proven approach to **Penetration Testing** is based on industry best practice and project management standards. The methodology is broken down into six distinct phases:

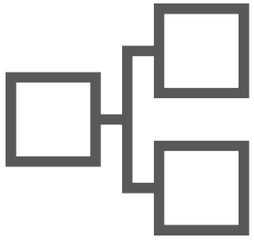
Initial Scoping, Reconnaissance, Assessment, Reporting, Presentation and **Remediation.**

Pentest People believe that these six steps are crucial in performing a thorough and accurate assessment, providing value for the client and ultimately improving the security of the target network. This methodology is cyclical in that the results of the assessment presented to the client, and provided as a report.

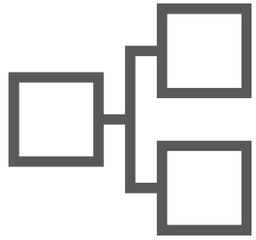
The Six Step Process

This methodology is cyclical in that the results of the assessment presented to the client, and provided as a report, feedback into the scope of additional tests. As security is a process rather than a solution, this methodology is designed to work alongside the ongoing process.

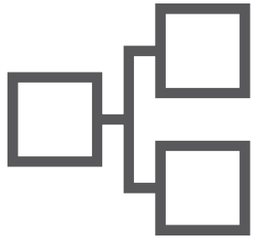
The 6 steps are broad categories and can generally be applied to multiple types of infrastructure assessment, regardless of whether it is internal, external or some other combination.



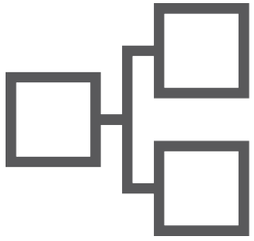
Step 1 – Initial Scoping



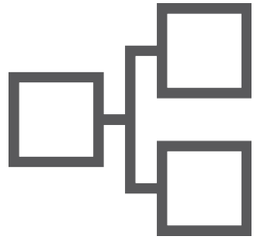
Step 2 – Reconnaissance



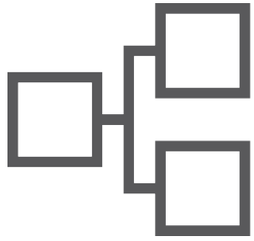
Step 3 – Assessment



Step 4 – Reporting



Step 5 – Presentation



Step 6 – Remediation

If you'd like to see more information regarding each step of the six steps of the penetration testing methodology, then please visit our detailled webpage here at:

https://www.pentestpeople.com/penetration-testing-methodology/

Our Services

Infrastructure Penetration Testing

A **Pentest People** consultant led **Infrastructure Penetration Test** provides a thorough and independent examination of your corporate infrastructure and systems to identify software and configuration based security vulnerabilities**.**

There are two components to **Infrastructure Penetration Tests** and these are Internal and External assessments. It is commonplace to combine these into a single test that covers both the internal and external components of the network.

Internal Penetration Test

An Internal Penetration Test is performed by a **Pentest People** security consultant onsite within your corporate network. This type of assessment looks 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.

External Penetration Test

An External Penetration Test is performed by a Pentest People security consultant whilst remote from your corporate network. This type of assessment is concerned with assessing 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.

Web App Penetration Testing

Web technologies have advanced in recent years and so have the Web Applications that we all use daily. With this advancement and reliance on web technologies, we have also been exposed to security risks associated with these applications.

What are the risks?

External facing Web Applications used by businesses are by nature available to all via the public Internet. 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.

Protecting these applications from new threats is a constant challenge, especially for developers who may not be security aware and who are working towards a performance deadline.

How can we help?

Pentest People have a professional Web Application Security Testing service that can be used to identify vulnerabilities that exist on your web applications. Pentest People have a wealth of knowledge in the area of Web Application Security Testing and their testers have created and contributed to many open source web application security projects.

This **Web Application testing** can be performed remotely for external facing web applications or internally at your premises if the application is an internal application.

IT Health Check

An IT Health Check requires both an External and Internal assessment. Pentest People will assign a qualified security consultant to help with scoping the engagement and delivering the project. Depending on the size of the network and number of devices, sample testing of a minimum of 10 per cent of the estate can be performed and correct scoping is critical to ensure that the service offered meets the CoCo requiremetns without being over bearing and over budget.

How can we help?

Pentest People can provide a full engagement from scoping the assessment and carrying out both the external and internal assessments. An IT Health Check report will be presented as the deliverable of the project that can be used for your Code of Connection application for access to the Public Services Network.

Remediation Consultancy Service

Pentest People offer a Remediation Consultancy Service as part of their **Penetration Testing as a Service (PTaaS)** offering. This service offering completes the Penetration Testing process by engaging with a consultant to provide a tailored prioritised approach to remediating any security issues identified from the testing engagement.

What are the risks?

Fixing identified security issues is a technical task that has to be performed by competent technical consultants who are adept with dealing with such matters. Pentest People specialise in identifying and remediating security issues on all common platforms and applications.

It is important that you assign proper priorities to the identified issues and fix them in a timely manner. Once these issues have been fixed, they have to be retested to ensure that the fix has mitigated the risk.

How can we help?

This Remediation Consultancy Service provided by Pentest People is a two-stage process.

The initial phase involves one of our specialised consultants reviewing the findings of the Penetration Test report and aligning this with your business requirements to create a prioritised approach document that contains remediation advice for all of the identified issues ranked in order of risk.

Once this report is created, the next step is to look at the implementation of this plan to mitigate the risks identified.

GDPR Penetration Testing

How can we help?

Article 32 of the **GDPR** relates to security testing and clearly states that "*a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*" must be in place.

Furthermore, the ICO website makes specific reference to penetration testing "*Run regular vulnerability scans and penetration tests to scan your systems for known vulnerabilities – make sure you address any vulnerabilities identified*."

As it is clear that a common entry point into any corporate network when under attack is through the exploitation of vulnerabilities, Pentest People feel that a properly planned Penetration Test is essential as a part of your **GDPR compliance**.

The service would be delivered as part of the **Pentest People Penetration Testing as a Service (PTaaS**) and full access to the **SecurePortal** and other complementary tools would be provided

Social Engineering Assessments

What are the risks?

The people and process element of security is often overlooked when allocating budget to Penetration Testing engagements. It is no surprise that attackers are also aware of this and looking at some very high profile attacks it is clear that Social Engineering techniques were utilised by the attackers as a way to extract reconnaissance information or to gain access to physical locations.

How can we help?

Pentest People's Social Engineering experts are adept at discovering and exploiting operational weaknesses in corporate policies and procedures that can unwittingly lead to unauthorised access to restricted systems.

Using the Open Social Engineering Framework methodology, our consultants can set up a covert Social Engineering project aimed at testing the robustness of your internal systems and provide practical advice on what changes are needed to prevent a real attack succeeding.

VPN Configuration Assessment

Virtual Private Networks (VPNs) are the modern way to allow remote employees to access resources on the corporate network. These VPN systems have replaced traditional dial-in and other types of remote access. There are many types of VPNs using differing technologies offered by a lot of technology vendors.

The configuration of these VPNs can be quite troublesome with a lot of companies relying on both site-to-site VPNs for third party access as well as Remote Access VPNs for remote workers who need access to corporate resources when on the road or working from home.

What are the risks?

A VPN device normally straddles the external Internet and internal corporate network. Any security vulnerability or misconfiguration can lead to an external hacker being able to access corporate resources as if they were physically connected to your network.

How can we help?

Pentest People can perform a full VPN Security Assessment of all of your external facing VPN infrastructure. One of our qualified consultants will use industry leading techniques to identify and assess the configuration of the VPN device, looking for any weaknesses that may lead to compromise.

Firewall Ruleset Review

A **Pentest People** consultant led Firewall Ruleset Review provides a thorough and independent examination of your firewall configuration with the aim of discovering issues that could leave your network vulnerable to a security breach.

These issues may include problems due to overly permissive rules, historic rules, badly configured rules or rules that have been added to provide a workaround that now should be removed. Firewalls evolve over time and procuring a regular rule-set review provides you with the peace of mind that your firewall is continuing to operate as intended.

What are the risks?

A Firewall device acts as the gatekeeper to the corporate network and often is the first and last form of defence for most organisations who do not employ a multi-layer of security. An incorrectly configured firewall or one that exhibits a software vulnerability due to lack of patching can seriously affect the security posture of your organisation and allow a hacker total access to the corporate network.

How can we help?

Pentest People can perform a full Firewall Ruleset Review of all of your external facing Firewall infrastructure. One of our qualified consultants will use industry leading techniques to identify and assess the configuration of the Firewall, looking for any weaknesses that may lead to compromise.

Network Device Security Review

A **Pentest People** consultant led Network Device Security Review provides a thorough and independent examination of the configuration of your network devices, such as routers and switches with the aim of discovering issues that could leave your network vulnerable to a security breach.

Our experienced team of Penetration Testers have identified that the network infrastructure is often overlooked on corporate networks and it is very common to find these devices installed in a default state with issues such as default admin credentials still configured.

What are the risks?

The whole corporate network is running on this key infrastructure and having the ability to gain access this allows a potential attacker the luxury of being able to eavesdrop all of the traffic or to cause a Denial of Serice (DoS) attack at their will. There are so many devices and vendors on the corporate network and these are usually outside of the corporate patching policy, leaving both software and potential configuration vulnerabilities ready to be exploited.

How can we help?

Pentest People can perform a full Network Security Device Review of your internal network infrastructure. One of our qualified consultants will first map out the internal network and identify the devices in use before using industry leading techniques to identify and assess the configuration of these devices, looking for any weaknesses that may lead to compromise.

CYBER ESSENTIALS

Pentest People are a Cyber Essentials Certifying Body and can help you at all stages of your Cyber Essentials accreditation journey.

Cyber Essentials is a UK Government led and industry-backed scheme that helps organisations of all sizes protect themselves against common cyber-security threats.

The scheme is based on the correct implementation of five technical controls that are designed to protect your organisation.

These are:

1. Use a firewall to secure your Internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware
5. Keep your devices and software up to date

From the 1st October 2014, the **UK Government** requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the **Cyber Essentials** scheme.

There are currently two levels of certification, **Stage 1** which is the basic level and **Stage 2** which is also referred to as **Cyber Essentials Plus**. Pentest People can help you with the full certification at both levels including performing the certification assessment.

Recieve a **UK Government** recognised Security Accrediation for your business

Be listed on a **Government Directory** of organisations awarded Cyber Essentials

Attract new business with the promise you have cyber security measures in place

Cyber Essentials Stage 1 & 2

Cyber Essentials (Stage 1)

The initial level of Cyber Essentials certification is delivered through SecurePortal as a self-assessment questionnaire that covers the five technical controls and then an external vulnerability scan of your external facing network.

You are assessed against the answers to your questionnaire and the results of the external vulnerability scan. Stage 1 certification awards the Cyber Essentials accreditation and associated use of the logo.

Cyber Essentials (Stage 2)

The more advanced level of certification relies upon the same protections as Stage 1 but the certification is carried out on your business premises and also includes an internal vulnerability scan of a common workstation build.

Your antivirus protections both via the web and email are manually tested whilst onsite to ensure that your tools of choice are protecting the level of protection required to achieve Cyber Essentials Plus.

You are assessed against the answers to your questionnaire and the results of the external vulnerability scan. Stage 2 certification awards the Cyber Essentials Plus accreditation and associated use of the logo.

In order to achieve Stage 2 certification, you have to first achieve Stage 1 certification.

Want to learn more?

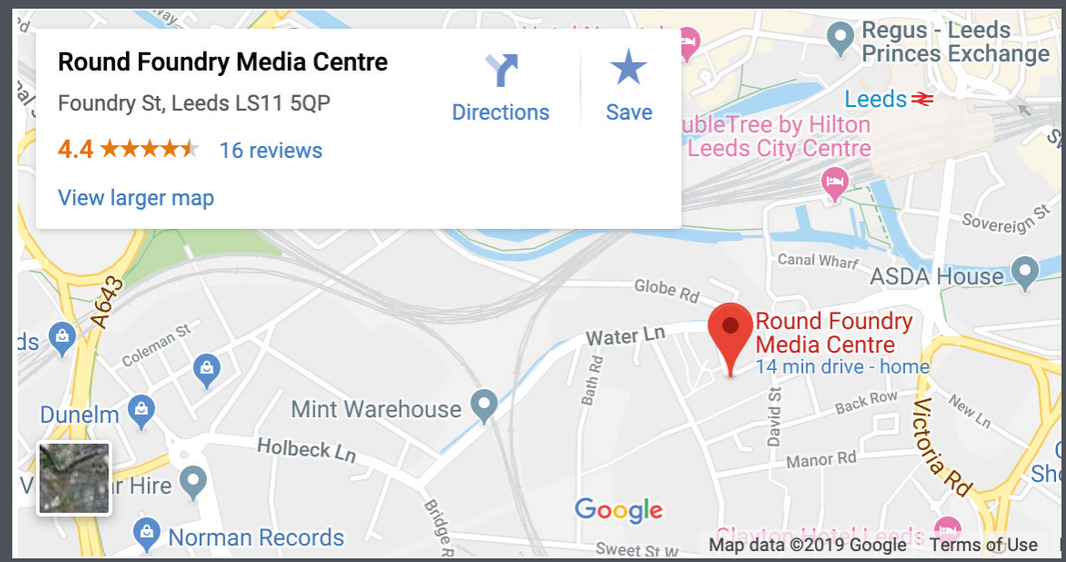
Don’t hesitate to get in touch

If you would like to learn more or speak to one of our sales team about any of our services please contact us via email or telephone.

Email: info@pentestpeople.com

Phone: 0330 311 0990

Address: Pentest People, The Round Foundry Media Centre, Foundry St, Leeds, LS11 5QP, UK



Thank You For Your Time

We Hope This Information Was Helpful