

Firewall Penetration Testing

Datrix has been relied upon to secure the perimeter of the UK's critical national infrastructure, including hospitals, government and utilities providers, for more than a decade.



An effective cybersecurity strategy comprises elements of both prevention and protection. A fundamental component of this is identifying and assessing any potential system vulnerabilities through penetration testing.



Penetration Testing (Pen Testing) is used to validate an organisation's security stance, both in terms of its resilience and its compliance with relevant standards.

Also known as ethical hacking, pen testing is an authorised attempt to breach some, or all, of an organisation's systems. Consisting of a simulated attack, pen testing is used to identify any security weaknesses and forms the basis of recommendations for remedial action.

We offer three types of pen testing services:

1. Internal
2. External
3. Wireless

1) Internal

Internal network pen testing is used to assess the security of internal systems and identify any potential vulnerabilities that may be exploited by rogue or unauthorised users. Common issues identified by internal systems testing include weak password policies, unsecured endpoints and poorly managed user access.

2) External

External network pen testing is used to assess how securely an organisation connects to external systems such as third-party applications, cloud services and the Internet. Common issues include poorly configured firewalls, insecure network protocols and unpatched security or operating systems.

3) Wireless

Wireless network pen testing is used to identify unsecured access points or unauthorised devices with access to the private network.



Systems evolve over time, as do external threats. Pen testing should not be considered a "one and done" process.



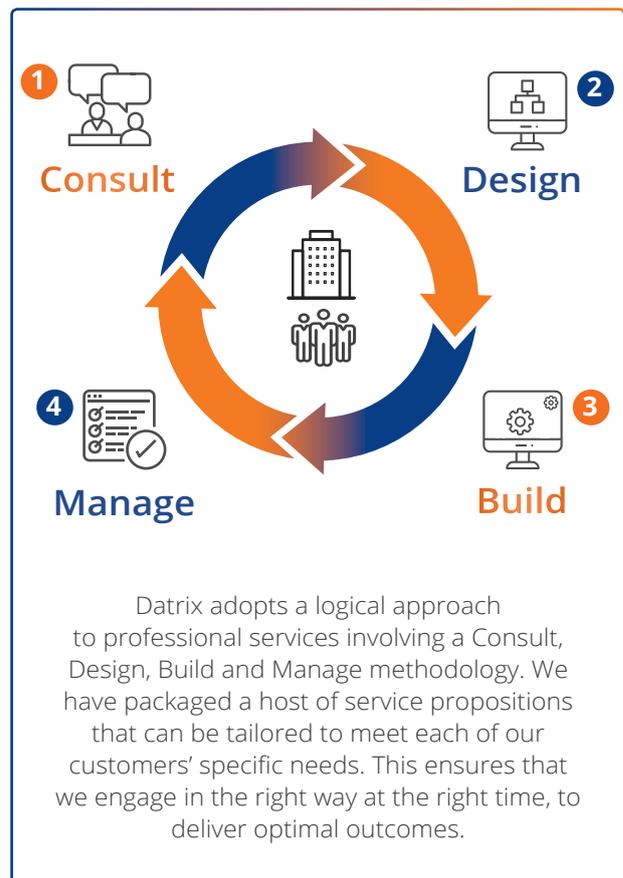
To maintain long-term systems' security pen testing should be carried out on a regular basis. We suggest a frequency of once a year for legacy systems and after the implementation of any new systems of security policies/patches.

Pen Test Reports

Post-analysis, we issue a report detailing your ability to protect your network, devices and applications from both internal and external threats.

Reporting benefits:

- › A list of identified vulnerabilities
- › A risk assessment associated with each vulnerability
- › A severity report highlighting critical fixes
- › Recommendations for remediation
- › An assessment of standards compliance



Datrix is a leading **Smart Infrastructure** and **Cyber Security** Solutions provider.

Established for over 25 years, digital transformation is the driving force behind the evolution of Datrix services and solutions. Our professional and technical services teams adopt a consultative, client-centric approach that sees us design, build and manage superior solutions.

Our critical networking, communications and cyber security solutions are the preferred choice for the nation's key institutions as well as public and private sector organisations seeking to address the business challenges of compliance, performance, availability and affordability.

Gray's Inn House, 127 Clerkenwell Road, London EC1R 5DB

Tel: +44 (0) 20 7749 0800

Email: enquiries@datrix.co.uk

www.datrix.co.uk

SMART Managed Networks
Connectivity
Communications
Insight & Analytics

SECURE Secure Networks
3rd Party Risk Management
Security as a Service



Crown
Commercial
Service
Supplier

DATRIX