Penetration

Testing - What is it?

A penetration test is a simulated attack to identify vulnerabilities in information systems. Our security experts, 'white hat hackers', put themselves in the position of someone determined to gain access to systems and data illicitly – for example, without knowledge of usernames and passwords.

Like a hacker or cyber criminal, they try every trick in the book, every possible plan of attack. They find the ways applications could be modified, and confidential information such as price lists or customer databases stolen or subverted. They then provide a report – explaining how they 'broke in' and how an organization can avoid it happening 'for real'.

Why do i need penetration testing?

A penetration test, carried out by a security expert, tells you whether your environment is secure.

When do i need it?

Penetration testing is recommended annually, and in the event of major changes to your infrastructure.

It is essential for companies holding intellectual property, information linked to personal identities, or financial information such as credit card data – and is often mandated by regulators.