

Penetration Testing



Regular penetration testing remains one of the best methods of measuring the effectiveness of information security controls

With both the frequency and ingenuity of electronic attacks increasing, it's becoming ever more important to regularly test the effectiveness of your information security controls.

Targets are changing too, of course. Theft of confidential data is no longer the sole objective of hackers and web site defacement is now a common goal of individuals seeking to degrade the public image of your organisation.

But these risks can be reduced and penetration testing remains a powerful tool in identifying the vulnerabilities that may exist within your security architecture.

Insight offers three levels of penetration testing services that will help you to:

- Identify both internal and external threats
- Assess and prioritise the potential risk from identified vulnerabilities
- Examine application and database environments as well as networks
- Discover non-technical methods of gaining unauthorised access to your IT assets.

Identifying vulnerabilities

Vulnerability testing is rather like looking for unlocked doors in a building and represents an essential first stage in any security testing strategy.

Our consultants use a proven combination of industry tools and in-house techniques to thoroughly probe and identify vulnerabilities in your Internet-facing IT systems.

And, unlike automated services that typically provide a computer-generated list of every vulnerability that exists on a web or email server, we'll prioritise those that are relevant to your infrastructure and include pragmatic advice on how to overcome them.

Opening the doors

Our next level of service goes further by exploiting the weaknesses we've identified and simulating an actual attack. Using the same techniques as actual hackers, our specialists will conduct activities such as information gathering, network fingerprinting and attempting to bypass access controls.

SIEMENS

Global network of innovation

Insight Consulting

And, with one of the largest penetration testing teams in the UK, we're able to comprehensively check all operating platforms as well as investigate areas such as cross-site scripting, code hacking problems, SQL database injection, XML and web services.

The threat from within

Acknowledging that a significant proportion of malicious attacks originate from within an organisation, our most comprehensive level of service employs advanced testing techniques internally as well as remotely.

Our consultants will review your security architecture to identify potential flaws that would afford a knowledgeable intruder access. We'll also review software builds on servers, examine web application scripts or check compliance to internal security policies.

We can also work with your IT organisation to simulate Denial of Service attacks, test your responses - by both systems and people - to intrusion efforts, attempt access to wireless networks or use social engineering techniques to identify non-technical points of entry into your organisation and its assets.

Regardless of the size of an engagement, though, we'll always develop a comprehensive report detailing the issues we've identified, an explanation of their implications and, importantly, recommendations for either reducing, or eliminating, the risks they pose.

Regular health checks

Insight also offers an ongoing penetration testing service where we'll conduct regular, repeat testing of your infrastructure using a pre-agreed programme of test levels. The table below illustrates our recommended schedule for companies using the Internet for, say, marketing or promotional purposes as well as those making more extensive use of the web for activities such as the selling or purchasing of products.

Our testing teams are also equipped with specialised equipment to provide wireless testing services. This can help you detect rogue Access Points or 'sniffer' equipment that may be attempting to gain unauthorised access to your IT systems. Regular wireless testing can also help identify wireless networks - or devices such as laptops or PDAs that are using wirefree communications - that may have been deployed by legitimate business users but which don't comply with your internal security policy.

Key features

- Choice of three service levels with tailored or fixed price options
- Comprehensive testing of networks, servers, applications and databases
- Detailed reports by testing consultants including solution recommendations
- Annual service option with pre-defined testing schedule
- One of the largest and most respected penetration testing teams in the UK.



Insight Consulting is the specialist security, compliance and continuity unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Research
- Consultancy
- Testing
- Implementation
- Training
- Recruitment
- Managed services

Insight is BS7799 certified, is a GCat and S-Cat (Category 7) supplier and subscribes to the CESG Listed Advisor Scheme (CLAS) and CHECK services.

If you'd like to discuss how Insight could help you manage risk in your organisation, email us at insight@insight.co.uk or visit our web site at www.siemens.co.uk/insight

Insight Consulting

Churchfield House
5 The Quintet
Churchfield Road
Walton on Thames
Surrey KT12 2TZ
United Kingdom

Tel: +44 (0)1932 241000
Fax: +44 (0)1932 244590
www.siemens.co.uk/insight

Summary of test levels and recommended schedule for annual testing service

| Level of testing performed | Internet presence environment | Internet eCommerce environment |
|---|-------------------------------|--------------------------------|
| Remote vulnerability testing | Every three months | Every month |
| External penetration testing | Every six months | Every three months |
| Full assessment including internal and external penetration testing | Every twelve months | Every six months |