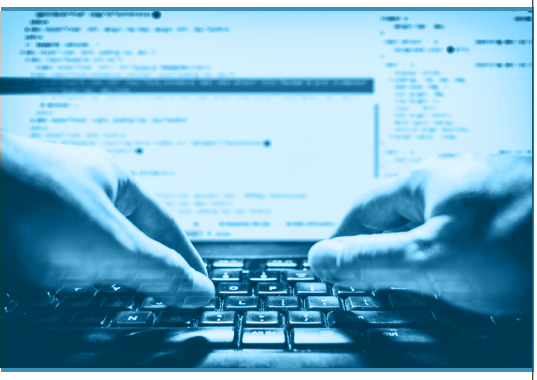
InteliSecure

At a Glance



Three Steps to Finding Your Penetration Testing Provider

1. Understand what type of testing you require.
2. Ensure the provider's skill set meets your requirements.
3. Know the provider's procedures for performing and documenting your testing.

PENETRATION TESTING

Evaluating a Penetration Testing Company

IT'S TIME FOR YOUR COMPANY'S PENETRATION TEST. DO YOU KNOW HOW TO CHOOSE A PROVIDER TO COMPLETE IT?

Penetration testing is a requirement for many kinds of information security compliance, including GDPR and other agency- and industry-specific requirements. In addition, your company may have its own reasons for ordering a penetration test, including:

- Understanding the effectiveness of your security defenses
- Determining the level of risk to your business-critical systems and related processes
- Enabling better security awareness and assurance
- Remediating security weaknesses

Regardless of your company's reasons for requiring penetration testing, a primary factor in your test's success is picking a provider who is capable of meeting your company's specific goals.

WHERE DO YOU START?

As in any industry, there are good and not-so-good security testing organizations out there selling services. When you're faced with selecting a penetration testing provider as a strategic partner, you'll be confronted by questions such as:

- What do you need to know before engaging a penetration testing company?
- How do you find a good testing provider?
- How can you ensure that the provider you choose can perform the engagement to your requirements and meet your business needs?

To answer these questions, use this 3-step guide to define your selection process and narrow down your choices.

STEP 1: UNDERSTAND THE TYPE OF TESTING YOU REQUIRE

To get your selection process started, begin by defining your requirements and goals for penetration testing.

- Are you performing the testing primarily to meet a specific compliance requirement? Make sure your provider understands the importance of meeting that requirement.
- Are you performing the test in response to a change in your security program or for internal governance? Be sure the provider understands the specific goals of your test and the metrics you want to get from it.

Once you have your goals and scope defined, you can talk to the provider about the type of testing that will meet those requirements. Penetration testing is a broad discipline that can cover a lot of ground. Testing can be performed across many different technologies, and can involve external or internal network infrastructure, including physical or virtual servers, workstations, firewalls, network switches, routers, and many IP based devices and applications.

And Also Red…

Attacker perspective is especially important when performing tests known as red team exercises. Red team penetration tests, by their nature, are almost always performed on live systems and can include social engineering tactics against company employees. These tests are typically goal based; the testing team is given challenges to gain access to a specific system, for example, or retrieve a password for a specific type of user within the network environment.

Red team exercises must be pre-planned in agreement with IT security managers to avoid risk and preserve the integrity of the assessment. Only select employees know that attacks are taking place so that genuine defensive responses can be gauged for their effectiveness during and after the assessment. To facilitate successful red team exercises, both black box and white box perspectives may have to exist in parallel to achieve the goals of the testing safely.

Most penetration testing companies also offer a compliance and auditing type of assessment, which can include authenticated build reviews of servers, workstations, firewalls, network security devices, mobile devices, and more. This type of testing isn't essentially penetration testing per se but can be used alongside penetration testing to gain a more thorough and comprehensive overview of risk within the environment. These combined, comprehensive services are often called a "Health Check" and may be adapted and used to meet some compliance requirements, such as PCI DSS and the Cyber Essentials scheme in the United Kingdom.

A RAINBOW OF OPTIONS: CHOOSING THE TESTING APPROACH

A penetration test simulates the actions of an attacker attempting to ascertain and exploit weaknesses of networked computer systems. However, your attacker might execute those actions through a variety of approaches depending on their level of knowledge about your systems and whether they have a specific goal in mind. A wide range of penetration testing approaches exist. The classic testing categories are based on the attacker perspective and are defined as black box, gray box, and white box.

- **Black box** tests are performed without any knowledge of the tested environment. The objective of a black box assessment is to assess the level of security as seen by a third party connected to the internal network or the internet.
- **Gray box** tests are performed with standard access or with only limited knowledge of the tested environment. The objective of a gray box assessment is to assess the level of security as seen by a legitimate user of the environment who has an account and general information about the tested environment.
- **White box** tests are performed with knowledge of the internal structure, design, and implementation of the tested environment.

Typically, organizations think of penetration testing as an offensive methodology in which the attacker could be looking for a way in through multiple areas of an organization, including web applications. Generally, that methodology is best applied through a black box testing perspective in which the attacker is unauthenticated and has limited knowledge of the system. The concept is to attempt to bypass or break authentication in order to gain an initial foothold.

A gray box approach would apply, for example, if a company is looking for vulnerabilities in its network applications. This type of testing assumes the attacker has a minimum set of information to successfully cover the test cases the application naturally presents. Focused application testing differs slightly from a true penetration test as it uses multiple sets of credentials covering multiple roles, assigning the theoretical attacker different levels of trust and access to align with the potential threats the application could pose.

A good penetration testing provider will help guide you to the right testing choices for the environments that are to be tested and should consider the requirements and constraints of the targeted systems. Defense in depth can often be more efficiently scoped and scrutinized by a penetration testing provider depending on what background information they have from the outset.

Also, be aware that attack perspectives can change depending on the information available, so the above categories are not necessarily rigid. Good penetration testing companies will recognize and highlight any relevant issues when such perspectives are not clear or change to best facilitate the proposed penetration testing.

STEP 2: ENSURE THE PROVIDER'S SKILLS MEET YOUR REQUIREMENTS

In addition to evaluating the penetration testing company as a whole, you should also take a close look at the individual consultants who will perform the testing program.

A good penetration testing provider will be able to show you the details of their consultants' professional backgrounds, along with any relevant qualifications or professional certification they may hold individually. Penetration testing has become better known as a specialty in the IT security industry, and many different types of certifications exist to assess an individual's competence in the subject. Certifications offer a way to ensure a baseline level of technical competence and knowledge and understanding of the profession.

However, a consultant who can study a subject and pass an exam, may not have the expertise or experience to competently complete the penetration test to your unique requirements. Limitations of experience can exist within a penetration testing company and top providers will conduct ongoing training and in-house research to continually enhance the skill sets of their consultants.

EXPERTISE

In addition to a degree in computer science, information security, or a related discipline, the consultants you work with will likely hold a variety of penetration-testing industry certifications.

Some of today's most commonly recognized certifications include:

- Certified Ethical Hacker (CEH)
- Licensed Penetration Tester (LPT)
- GIAC Exploit Researcher & Advanced Penetration Tester (GXPN)
- Offensive Security Certified Professional (OSCP)

In the UK, you'll see certifications aligned with the UK National Cyber Security Centre (NCSC) CHECK program, including CREST, Tigerscheme, and Cyber Essentials. The CHECK program deals with government, police, and other sensitive data. In addition, look for continuing education courses and certifications through reputable organizations such as the SANS Institute.

EXPERIENCE

Experience in the penetration testing industry can be extremely broad, and many consultants come to the field directly from university or from another profession. However, it is essential that consultants in a focused penetration testing role have gained direct experience in a variety of areas and built over time throughout their careers.

Most senior penetration testers in the industry—who are likely to be the team leaders who initially scope the penetration test and then lead the assignment—have at least five years of dedicated experience and are certified to senior level qualifications.

You should be able to trace your consultants' experience and see whether they have specialized in a particular area such as red teaming or mobile application testing. Your penetration testing provider can provide your consultants' resumes, and you can review their LinkedIn profiles to verify that they have the right skill set for your assignment.

STEP 3: KNOW WHAT YOU'RE GETTING WITH PROCESS DOCUMENTATION

All reputable penetration testing companies diligently document their processes and procedures and make them available to their clients on request. Typically, a penetration testing company should be able to provide the following information:

- Methodologies (detailing the different types of testing they provide)
- Client Engagement Process
- Data Handling and Retention Policies
- Complaints and Escalation Procedure
- Standard Operating Procedures (detailing the penetration testing execution)
- Quality Assurance Policies
- Information Security Policies
- Liability Insurance Certificates

This level of documentation should be mature, with policies and procedures adhered to within the organization. The company you select should also be able to show that its policies and procedures are regularly audited.

If a provider uses subcontractors when fulfilling a penetration test, they must also document their processes for ensuring standardization across contractors. If your company handles sensitive information, your provider's data handing and retention policies may have to align to your requirements for such data.

Fortunately, most established penetration testing providers are dedicated to providing quality assurance for their services. Some companies go a step further, aligning with organizations such as CREST (the Council of Registered Ethical Security Testers), which has rigorous, effective, comprehensive testing standards and methodologies in place in the UK and globally. This standard could be considered similar to the ISO27001 standard but is more closely focused on the type of security services a company can offer, including penetration testing and incident response.

In order to meet the CREST standard, all policies, methodologies and processes are individually evaluated and have to confirm to a rigorous standard. These companies must also employ consultants with security clearance of at least UK SC level and have been assessed and accredited to the highest standards of security testing. They can be trusted to ethically replicate the actions of threat actors and provide pragmatic advice and direction on how to protect yourself against the constantly evolving threat landscape.

ARE YOU READY?

Penetration testing is a highly valuable tool in your data protection program. It can be the key to eliminating vulnerabilities that threaten your company now—and the foundation for a truly effective data protection strategy that adapts and matures over time. Be sure that the provider you select is able and ready to meet your requirements and goals.

ABOUT INTELISECURE

InteliSecure specializes in making data protection easy, fast, and cost-effective for companies of nearly every size. More than 500 clients with over 2 million managed users rely on our services and specialists to protect the integrity and safety of their sensitive information. With more than 15 years' experience and partnerships with some of the world's biggest names in cyber defense, we make data security and compliance easy by providing effective data protection at a lower cost, eliminating the strain on IT organizations and reducing the risk of confidential information getting into the wrong hands. Unlike other security providers, we focus on business outcomes—providing data and reports that make sense to business and security executives alike. InteliSecure serves clients globally with security operations centers in the United States and the United Kingdom.

InteliSecure

5613 DTC Parkway, Suite 1250 Greenwood Village, CO 80111 | + 1 (720) 227-0990 | sales@intelisecure.com | www.intelisecure.com

1 Lindenwood, Chineham Business Park Crockford Lane, Basingstoke, RG24 8QY, UK | +44 118 976 8960