How to Select a Penetration Testing Provider

Published 11 September 2020 - ID G00723076 - 19 min read

By Analysts Toby Bussa, Claudio Neiva, Mitchell Schneider

Initiatives: Security Operations

Penetration testing plays a key role in assessing enterprise exposure to vulnerabilities, the ability to meet regulatory requirements and testing security operations. Security and risk management leaders choosing a provider need to plan, apply a structured approach and perform due diligence.

Overview

Key Challenges

- The market for penetration testing providers is overwhelming for many buyers, which makes it challenging to identify and assess the quality of a provider that can meet requirements and fit within budget.

- Many buyers of penetration testing services fail to define their goals and needs prior to engaging with a provider, resulting in engagement outcomes failing to deliver against expectations.

- Buyers are confused by providers offering penetration tests and red team tests, especially as the terms are being used interchangeably by some providers in the market.

- Alternatives to using penetration tests from a single provider are gaining visibility in the market, adding additional complexity to the decision on how to source a test.

- Organizations regularly underestimate the remediation effort required to be performed after the penetration test.

Recommendations

Security and risk management leaders responsible for security operations should:

- Analyze the specific type of tests required and the tests’ goals, scope, requirements and boundaries, as well as how providers define their services, before selecting a provider.

- Compare, assess and select a provider using a structured approach.

- Evaluate and select a provider based on your objectives and requirements; do not rely solely on the provider’s reputation or choose the least expensive firm.
Introduction

Gartner defines penetration testing as going beyond vulnerability scanning to use multistep and multivector attack scenarios that first find vulnerabilities and then attempt to exploit them to move deeper into the enterprise infrastructure.

Penetration tests are an important part of a security team’s compliance and vulnerability management capability. Many security and risk management leaders rely on penetration tests as an independent verification mechanism to assess their organizations’ IT environment’s ability to detect and defend against attacks. The outputs from these tests are used for several purposes as reported by Gartner clients. For example:

- To provide input to the development of security and risk management improvement programs (for example, if the leader is new to the organization)
- To validate the efficacy of security controls and capabilities (for example, using a red team exercise)
- As part of ongoing vulnerability management activities (such as assessing platforms and applications supporting new business-critical initiatives)

For some organizations, these tests are mandatory to perform, for example, in order to comply with PCI Data Security Standard (DSS) requirements. Other organizations may require penetration tests in order to adhere to a specific information security management standard, such as those of the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

Penetration tests can encompass a range of activities and outcomes. Gartner clients using penetration tests typically focus on external and internal network tests, as well as external and critical internal web-based applications. More recently, tests against wireless networks have become more common, sometimes to meet regulatory requirements like PCI DSS, as well as physical tests, depending on the organization’s vertical (for example, utilities or retail). Tests that specifically address phishing and social engineering are seen on occasion.

Red team tests are becoming more visible in the market, which can create confusion with buyers (see “Using Penetration Testing and Red Teams to Assess and Improve Security”). Why the confusion? Because red team tests seem very similar to what may be marketed as an “advanced” network penetration test, but also because some providers are adopting this term to differentiate themselves in the market. The reality is that red teaming is similar, but different from, traditional network penetration testing. Some providers legitimately offer one or both styles of tests, and some providers are really only doing network penetration tests and co-opting the term “red team.”

Selecting a penetration testing provider can be a daunting challenge due to the sheer number of firms offering these services. A Google search for “penetration testing” reveals hundreds of providers of services that vary in many ways, such as organization (and staff) size, geographical...
location, years of experience, and reputation. Providers range in size from large consulting firms with offices located across the globe to custom regional security service providers to individuals working from home. Tester experience ranges from veterans that have completed hundreds of penetration tests to recently certified individuals who have decided to launch a penetration testing practice.

It’s important to note that increased size or global brand recognition does not necessarily equate to better results when it comes to penetration testing. Also, the number of years of experience may not be a good indicator for emerging areas (such as cloud environments) or use cases (such as testing ICS/SCADA environments), where niche expertise is required. Therefore, the experience of the tester is a key factor.

New approaches to penetration testing and red teaming have also emerged in the market (for example, crowdsourced penetration tests, pen test as a service [PTaaS], automated penetration testing tools, and breach and attack simulation [BAS] tools) (see “Utilizing Breach and Attack Simulation Tools to Test and Improve Security”).

Analysis

Analyze the Specific Type of Test Required and the Test’s Goals, Scope, Requirements and Boundaries Before Selecting a Provider

Before starting the process of selecting a provider, review “Understand the Types, Scope and Objectives of Penetration Testing” and “Using Penetration Testing and Red Teams to Assess and Improve Security.”

Once the goals and scope of the penetration test have been agreed on and documented by the security team and key stakeholders, requirements and boundaries need to be defined, agreed on and documented.

Goals may include finding as many weaknesses across assets that could be exploited by attackers to compromise systems, to determine whether an external attacker can get to an organization’s internal network from the internet, whether wireless access points allow for unauthorized access to the enterprise network, and whether an attacker could tailgate an employee in an office and then connect to the corporate network. These spell out how a provider should operate to achieve the test’s goals within the agreed scope.

The requirements need to extend from the scope and the goals, in conjunction with input from applicable stakeholders, especially IT infrastructure and business application owners. Additionally, business leaders outside the IT department need to provide input on their operational risk appetite, in relation to the scope and goals of the exercise, as testing could adversely affect operations.

Examples of questions to answer when defining your requirements and testing boundaries include the following (note that many of these questions overlap, so consider the list as a whole):
What types of assets (devices, hosts, applications, environments and people) are explicitly in scope, and which are off limits, for the testing provider? Are they off limits permanently or only on certain days or at certain times? The assets that are off limits will usually vary, according to the type of test. Lightweight and targeted assessments (white-box and gray-box tests) will usually specify off-limit assets, whereas standard penetration tests (black-box tests) and red team exercises will have few, if any. If a red team style is preferred, is the goal to be stealthy and not detectable by the blue team or not?

What environments are testers expected to test (for example, test or development environments only or all environments, including production)? The type of penetration test employed may drive the choice of environment. For example, a gray-box test against a new platform and application that is not yet externally exposed may be conducted against preproduction versions.

Are cloud services like IaaS, PaaS and SaaS in scope? If they are, most organizations who leverage SaaS and sometimes PaaS are not allowed to perform their own penetration testing, and even for IaaS there are clear demarcations between what the customer can test based on the cloud services shared responsibility model. Are staff that are working from home in scope? Targeting remote workers could be a violation of ISP terms and conditions, as well as cause disruption at private locations and with private devices (for example, if the employee is using their own device). The risk of bringing these assets and people into any penetration tests should be assessed and considered.

Are there operating period restrictions? For example, if a standard penetration test is to be conducted, do you want it to occur only on business days and during office hours, so that, if an exploit crashes an application or a server, IT staff are available to restore normal operations? Are there normal corporate-driven blackout periods (for example, for retailers during holiday periods) when testing should not occur?

Depending on the type of penetration test, how much risk around availability and integrity of assets within scope of the test is your organization willing to accept when the tester employs real-world exploits? If a standard penetration test is to be conducted, will your organization accept the use of real exploits to achieve the test’s goals? Also, it is important to check with the provider to determine how it enforces and monitors boundaries during testing.

Will the tester need to be located within your physical premises or will remote working be acceptable? During disruptive events, like pandemics, remotely delivered pen tests may be the only option offered. How will access, especially remote, be provided, monitored and revoked upon completion of the test? Does the vendor need to deploy its own assets, like a virtual machine or physical laptop, on your network to facilitate internal penetration tests? Usually the type of test determines the tester’s location. A penetration test against a specific system or application may require full access to your internal network. A simulation of an attack that originates outside your organization’s network perimeter may not.
Are there specific requirements on the individuals performing the tests (for example, a specific country where the work will be performed from or security clearance levels required)?

What is the escalation plan? Relying on email communications and meetings is not appropriate in all circumstances. You need a detailed communication and escalation plan. Both parties must agree on a “no assumptions” policy, for example, if a system becomes unresponsive, a significant vulnerability is discovered or there is evidence of a breach. Communications must be timely and crisp in their details (for example, what has happened, what was identified, the severity of the issue, whether a breach is active or there is indication of past activity, and what artifacts indicate a breach).

How much independence are you willing to give the test provider? Understanding this is crucial. Will you allow it to employ social engineering techniques (for example, in phishing emails and phone calls)? Will you grant physical access to achieve the test’s goals? The more autonomy you give a provider, the higher the risk, but the more comprehensive and thorough the results are likely to be.

Compare, Assess and Select a Provider Using a Structured Approach

Once you have documented your goals, scope, requirements and boundaries, develop a shortlist of penetration testing providers. Providers range in size from individual consultants to global consultancies. Sources of identifying potential vendors to use include peer recommendations, existing relationships with IT service providers and consulting firms, providers experienced with specific regulations like PCI DSS, and providers associated with related accreditation and certification schemes like CREST. Once you have a shortlist of providers, it’s advisable to issue an RFP.

At the introduction to the RFP, the goals, scope and boundaries of the test must be provided. It’s also important to be very specific and provide enough details for a provider to determine whether it can achieve your goals and operate within your boundaries. Some consultants and firms are likely to decline an engagement based on these factors. For example, some firms want only to conduct standard penetration tests remotely and lack the resources to conduct on-site tests.

Your aim is to issue an RFP that enables, as far as possible, a consistent comparison of the providers’ strengths and weaknesses. Give the providers some leeway to explain their differentiation, but phrase the questions in such a way as to elicit clear answers and responses. Your RFP should include four core parts, which are described in more detail below:

1. Your organization’s details, relevant background information, drivers for the engagement, and the scope and goals of the penetration test

2. Relevant requirements and boundaries (or “guardrails”)

3. Specific questions that providers need to answer in their response to the RFP
4. Standard RFP procurement information and questions, including the format for the RFP response, contact details, commercial details, customer references and due date for responses

The first part should include brief background information about your organization and the drivers of the engagement. Be as specific as possible within what is organizationally acceptable to share externally. This is an important component of the document and is frequently not given enough attention when constructing the RFP.

The second part should include a description of the engagement’s goals and scope. Once the goals and scope have been stated, the engagement’s boundaries should be described. Next, provide a numbered list of your specific requirements, such as remote versus physical presence, and allowed hours of testing (for example, between 6 p.m. and 6 a.m.). Document communication methods clearly. Also, it is necessary to be very clear on requirements that may limit a tester’s ability to adhere to their methodologies and practices (for example, when requirements dictate the toolset or host to be used to perform the tests).

It’s also important to define an expected completion date for the engagement, by which the tester should deliver a final report and recommendations. Even if attackers have almost unlimited time, a penetration test has to be finite, as organizations don’t have unlimited budgets. If the engagement will include retests, clearly state the number of additional tests required and the decision and authorization criteria for them.

The third part should include questions designed to establish the providers’ capabilities and to make it easier to compare them. Listed below are suggested questions. Parts below marked “Note” provide additional explanation of the question or request and should be removed if being used verbatim from this document. We also recommend that questions focused on staff, testing methodology, engagement management and reporting be mandatory. Answers to these will be key during the comparison and final selection phase.

Suggested questions:

- To whom will you assign this engagement? What are the skills, experience and qualifications of the testers who will be assigned? What is the average number of years of experience per tester? Please provide biographies as supplements.

- Note: Targeted and standard penetration tests are driven predominantly by the attributes of the tester, not by the tools and methods used. It’s important to review the capabilities of staff that are used by the provider as differentiators. The provider should be able to understand the test’s requirements (if it doesn’t, it should ask you for clarification) and know who it will assign. Look for testers that have several years of experience and, optionally, recognized certifications such as those from CREST, Global Information Assurance Certification (GIAC) and Offensive Security.
For standard penetration test engagements, it's worth spending a few minutes searching online to see if the provider's staff are visible members of the information security community. For example, do they present at conferences and publish exploits, and are they credited for vulnerability discoveries? Do they blog about their research?

If a provider will not indicate whom it will assign to your engagement at this stage, be sure to ask the provider for a final list of staff, with the option of approving any substitutions, before you sign any agreement.

How do you vet staff? Are you using resources outside the country?

Note: Providers should conduct regular background checks on the staff who perform penetration tests. However, the nature and regularity of these checks will vary by country, as laws differ. Consider whether the use of resources outside your country creates any policy compliance or liability concerns for your organization.

How much manual, as opposed to automated, testing do you typically conduct?

Note: Initial testing usually uses automated tools to map a network and gather detailed information about potential targets, but depending on the test's scope and boundaries, a good provider may rely more on manual testing. The amount of manual testing is likely to influence the engagement's duration and cost, so understanding the relative proportions of manual and automated testing could help to explain cost differences between providers.

Describe your experiences and provide examples of your engagements, covering similar goals.

Describe your experiences with similarly sized organizations and IT environments.

Describe how reports are written and findings are presented.

Note: This is one of the most important questions to ask, and it's important for the provider to supply real-world reports (with details redacted, where necessary). The final report will be the product you receive, and it will be what you use to determine whether the engagement has achieved its goals.

Specific questions that could be asked include: Are your reports written by the testing staff themselves or by dedicated writers? Do you use a standard template or are report formats unique to each engagement? Does the report contain an executive summary, a detailed technical description of findings, remediation guidance, and a listing of the methodologies and tools used and the tests executed? Are the results contextualized in a risk-based approach, including level of complexity required to remediate a vulnerability? Are recordings made available to demonstrate how an exploit was performed? Provide examples of reports for similar engagements.
Regarding the presentation of findings, questions include: Is an executive briefing provided? Is it possible to have a debriefing meeting with the technical resources where technical staff can ask the testers questions about their actions and findings?

Additionally, a penetration test should be the start of a remediation program of works. We see clients regard penetration testing as a one-time event or something that is compliance-related only. Providers should be preferred that provide guidance on priorities of issues as well as any guidance and indications of what kinds of work would be required to perform these remediations. This is critical, as it is often the case that remediation work can be more costly and time consuming than the test itself. Having a provider help you describe the implication of findings in a way that can be delivered as a program of work is very helpful.

How will you manage the engagement? How will you communicate status updates and findings to the customer during the engagement?

Note: It's important to manage the engagement as a project. Holding regular, even daily, meetings during the engagement to address issues or urgent findings, as well as weekly check-in meetings to assess progress, will help achieve a successful outcome.

Do you sign confidentiality agreements? How do you securely store customer data to prevent unauthorized disclosure? What are the retention periods for raw data and reports? Who is authorized to view the results, both from the provider and client? How is data destroyed and what verifications do you provide?

Note: The provider will collect information about your IT assets, especially hosts, security devices, networks and applications. More importantly, it will record vulnerabilities and weaknesses. It is of paramount importance that the provider agrees to keep all information confidential, that it has processes and tools in place to protect your information, and that it destroys this information after a specific period. Providers must offer this protection to their customers.

Supply two or three customer references for engagements with similar scopes and goals.

Note: Customers providing references need not necessarily be formal reference customers whom you can speak to, but their references should enable you to confirm that the provider has completed similar work with customers of similar size in the same or a similar industry. If you can speak to the customers providing references, take that opportunity.

What is the estimated cost of this engagement? Please provide a breakdown of the total costs per day and hour (across resources if there are different rates for different skills, such as tester or project manager). If the engagement runs longer than estimated, how are change orders handled and what is the rate for additional engagement time (per day and per hour)?
The final part of the process is to send the RFP, along with your organization’s standard procurement collateral, to a manageable pool of potential providers — not too many but enough that analysis of RFP responses is feasible without too much difficulty. Gartner clients procuring penetration testing services usually will select between three to five providers for their shortlist. Know that, even after choosing one provider, some organizations retain a pool of other providers, according to their strengths and specializations (such as in web application testing and attack simulation). Depending on the type of testing, they may draw on these other providers’ services if their principal provider cannot perform a test in the required time frame or to get different perspectives.

Evaluate and Select a Provider Based on Your Objectives and Requirements

The next stage is to analyze the providers’ responses to the RFP. Focus on the critical selection factors to achieve a successful penetration test (see Figure 1). Then consider their answers to the other questions, as these will add context to the crucial answers.

**Figure 1: Critical Factors to Address for a Successful Penetration Test**

### Critical Factors for a Successful Penetration Test

- **Engagement Management**
- **Communication Channels**
- **Boundaries**
- **Expertise and Experience**
- **Outputs**
- **Penetration Test Success**
- **References**

Source: Gartner (September 2020)
ID: 383103 © 2019 Gartner, Inc.

**Outputs**

Review the sample reports and any additional materials. Ask yourself which providers have supplied “canned” reports, rather than reports that are more oriented to your engagement and
organization specifically. Context can be missed, and they might solely focus on content alone. Is the content of the reports sufficiently detailed? Is the information provided useful? Is it detailed enough to help prioritize the remediation of weaknesses, both immediately and in the long term? Do you have the ability to influence the provider's output or report format, or do you have to take its default version? Which providers are willing to work to your requirements and within your boundaries?

Engagement Management and Communication Channels

Also consider how the engagement will be managed. Is there a dedicated project management resource supporting the testers, or are the testers expected to also manage the engagement? Are communications channels and cadence adequate for the complexity of the engagement. For example, if the testers cause a suspected impact on your environment or if the testers find evidence of an active or past breach, will both parties know whom to notify and how? These are crucial elements that should be documented in the provider's response and/or statement of work.

Expertise and Experience

Selecting a provider based solely on cost is not recommended. The old adage of “you get what you pay for” is applicable when selecting a penetration testing provider.

Focus first on the quality of the response, the provider's work, and its ability to meet objectives, then compare prices. When comparing prices, pay special attention to the number of days allocated to assessment, project management and report generation. Differences in the days allocated to these activities often explain why providers’ prices diverge widely. If vendors differ markedly in the number of days they project for the engagement’s completion, discuss this matter with those providers. Recognize that the amount of time spent on assessment is crucial. A noticeably shorter engagement duration can indicate a less thorough test. For example, more automation may be used to try to discover more vulnerabilities to demonstrate value to the customer, although the vulnerabilities may be low-value and hide the fact that more significant vulnerabilities went undiscovered.

Evidence

1 Some Gartner clients report changing penetration test providers every year or every other year to ensure they are getting a fresh review of their environment.

2 Sample of end-user guidance for performing pen tests where cloud services providers could be in scope:

- AWS
- Google
- Microsoft
- Oracle

Gartner, Inc. | 723076
Recommended by the Authors

Understand the Types, Scope and Objectives of Penetration Testing
Using Penetration Testing and Red Teams to Assess and Improve Security
Ensuring a Successful PCI DSS Assessment

Recommended For You

Microsoft's Indirect Access Rules Risk Increased Liability and Licensing Costs
Summary Translation: Three Steps to Hyperautomation
Improve Key Account Management Results Through Targeted Compensation Plan Design
Deliver Strategic Business Value With Your Seat at the Table
Increase IT Value: Shift Your Seat at the Table

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."