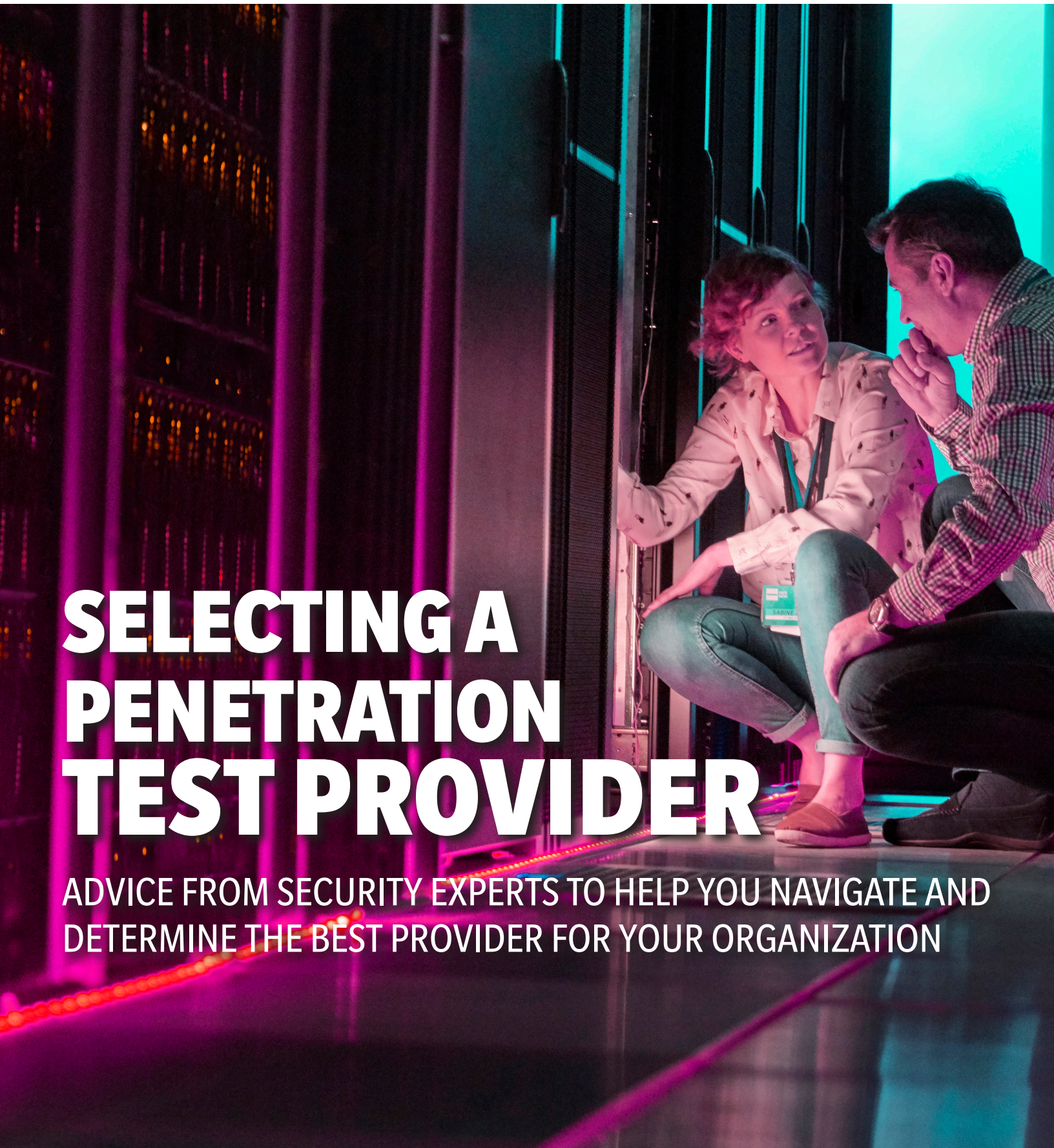
KONICA MINOLTA

DEPTH SECURITY
A KONICA MINOLTA SERVICE



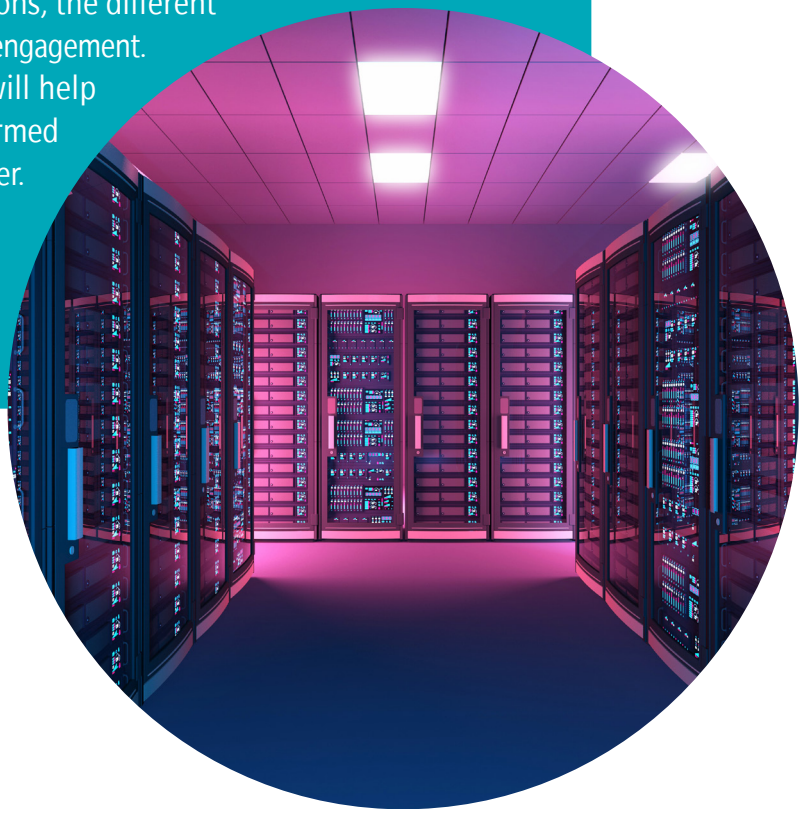
SELECTING A PENETRATION TEST PROVIDER

ADVICE FROM SECURITY EXPERTS TO HELP YOU NAVIGATE AND DETERMINE THE BEST PROVIDER FOR YOUR ORGANIZATION

INTRO

WHEN IT COMES TO SELECTING A PENETRATION TESTING PROVIDER, ORGANIZATIONS CAN OFTEN FEEL OVERWHELMED BY THE NUMEROUS OPTIONS AT THEIR DISPOSAL.

It is important to carefully consider available providers to find a solution that best meets your needs. This eBook provides an overview of the factors that need to be taken into account when selecting a penetration test provider, such as asking the right questions, the different services offered, and the rules for engagement. Understanding these factors will help your organization make an informed decision when choosing a provider.



TESTING THE WATER

Before jumping into the deep end, it's beneficial to select multiple vendors and walk through the scoping and proposal process with them to see the options available. While it is more time-consuming, spending time up-front comparing and testing to see how the relationship feels will help you feel more confident about the choice you make in the end. And be wary: a quick Google search for penetration testing will yield hundreds of companies vying for your business, but just like anything, the firm with the highest marketing budget is not necessarily the firm with the highest quality or value.

Talking to your peers is a better way to find your ideal partner. Word of mouth is powerful, and it works in both directions. For example, firms supplying low-value internal penetration test reports full of low-severity or unexploited findings would be great to know about from an avoidance perspective. Try finding someone you know who has worked with multiple penetration testing firms and ask them which ones have made the most impact. You should ask them to be as candid as possible to help you get a full picture, without breaking any NDAs of course.

CHECK THE CERTIFICATIONS

Be aware that various certifications exist for the security industry, including some offensive-focused specifications.

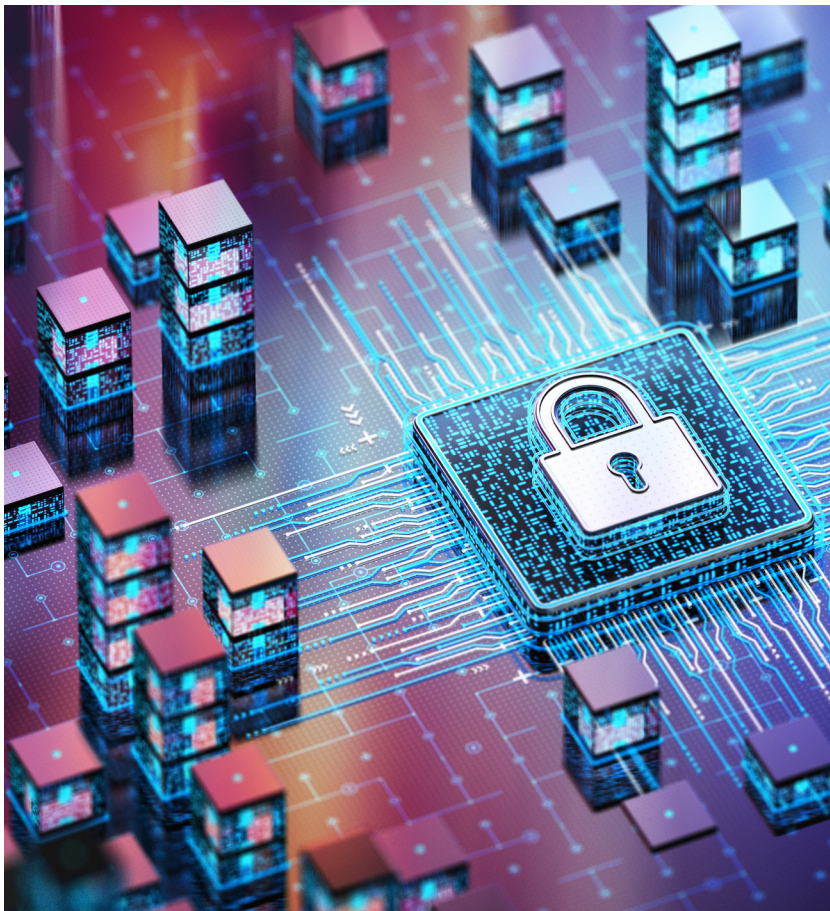
There are some, such as CISSP, CEH, and Security+ that only require unfocused, multiple-choice/multiple-answer, written exams to be certified. None of these have enough offensive security rigor to move the needle in a tester's level of skill.

Instead, look for lab-based certifications such as those from Offensive Security, eLearn Security, and SEKTOR7, which can be good signs that the testing firm not only has the knowledge but has gone the extra mile to validate its claim.

However, there are well-certified penetration testers who do subpar work, and non-certified veterans you would be lucky to have on your project and vice versa. This is why getting to know your testing provider on more than just a superficial level is important.

It just so happens that at Depth Security, a little over 75% of our testers are OSCP-certified. Additionally, 25% are OSCE-certified at the time of this writing, and many have other certs as well. However, it does not directly correlate with seniority, as a couple of our most impressive, most requested testers have no certs. And in contrast, there are those who are certified but never managed to get an external shell in the wild.

It is possible to pass a difficult exam, even a proctored lab-based exam, but have issues applying those lessons in the real world. When evaluating testing providers, certifications are only one piece of the puzzle; they should not be used as absolutes or as gatekeeping devices.

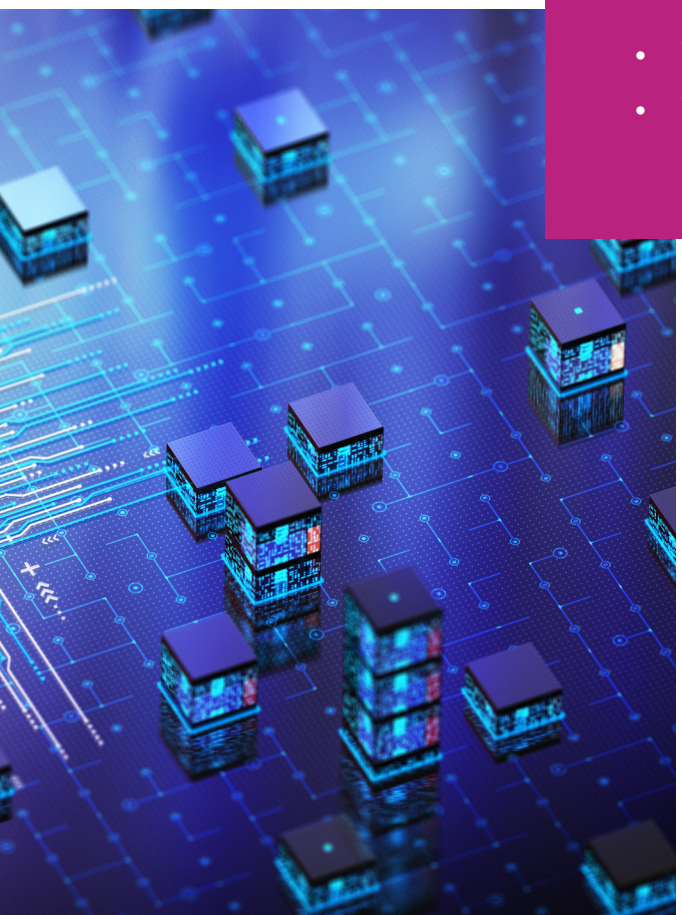


ASKING THE RIGHT QUESTIONS

During the scoping period, you should first be asked fundamental questions, and later, more specific ones. The proper scoping of engagements ensures appropriate coverage of targets by allotting a proportional amount of time to test them.

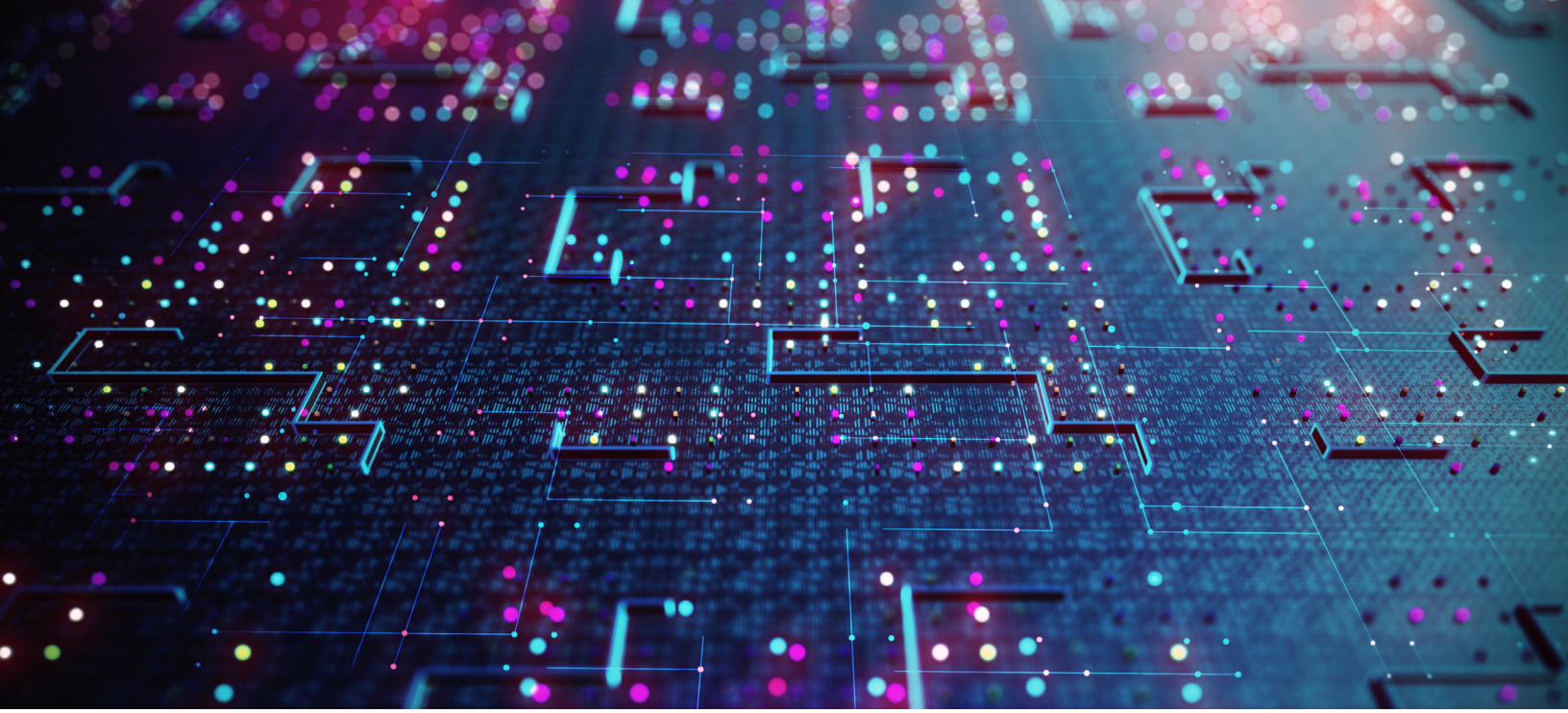
FOR EXAMPLE

- Do you want to test your entire network or just a single application?
- Are you worried about internal or external perspectives?
- Authenticated or without credentials?
- Wireless or wired?
- Are social engineering attacks such as phishing more concerning?
- Or are you worried about server-side attacks where none of your people even come into play? Maybe both?
- What is a worst-case scenario for your organization?
- What is the reason for the test in the first place?



More specifically, if you are asking for application penetration testing, they should be inquiring, **"What kind?"** and **"What size?"**. And follow-up questions about a mobile app should be different from questions about an API or a browser-based application.

It can feel good to receive a quote without having to answer a bunch of questions about testing targets; we're all busy. However, this is a red flag that a firm is arbitrarily pricing its engagements without a solid understanding of how long it will take them to get thorough coverage. You might check an audit box with this approach, but three days of testing against a target set that required 13, is still negligent.



GENERAL QUESTIONS FOR PROSPECTIVE PROVIDERS

- Do you offer free remediation testing later after bugs are fixed?
- Are all testers full-time employees with the firm, or are they just 1099 contractors?
- Will testing traffic be sourced from the US or are testers global?
- Have the team members released any public research regarding bugs or tooling?
- Can I communicate directly with my tester(s), or must I go through a project manager? What about questions after a project ends?
- What kind of certifications does the team hold? What percentages of the team have these certs?
- What web application/API coverage level is provided on network penetration tests?
- What would a typical final report look like?
- What percentage of your tests result in a documented attack narrative containing remote code execution or significant levels of remote access?

ALLOW YOURSELF TIME FOR SCHEDULING

With increasingly high demand outstripping the supply of qualified testers, testing firms are often 2-3+ months booked out.

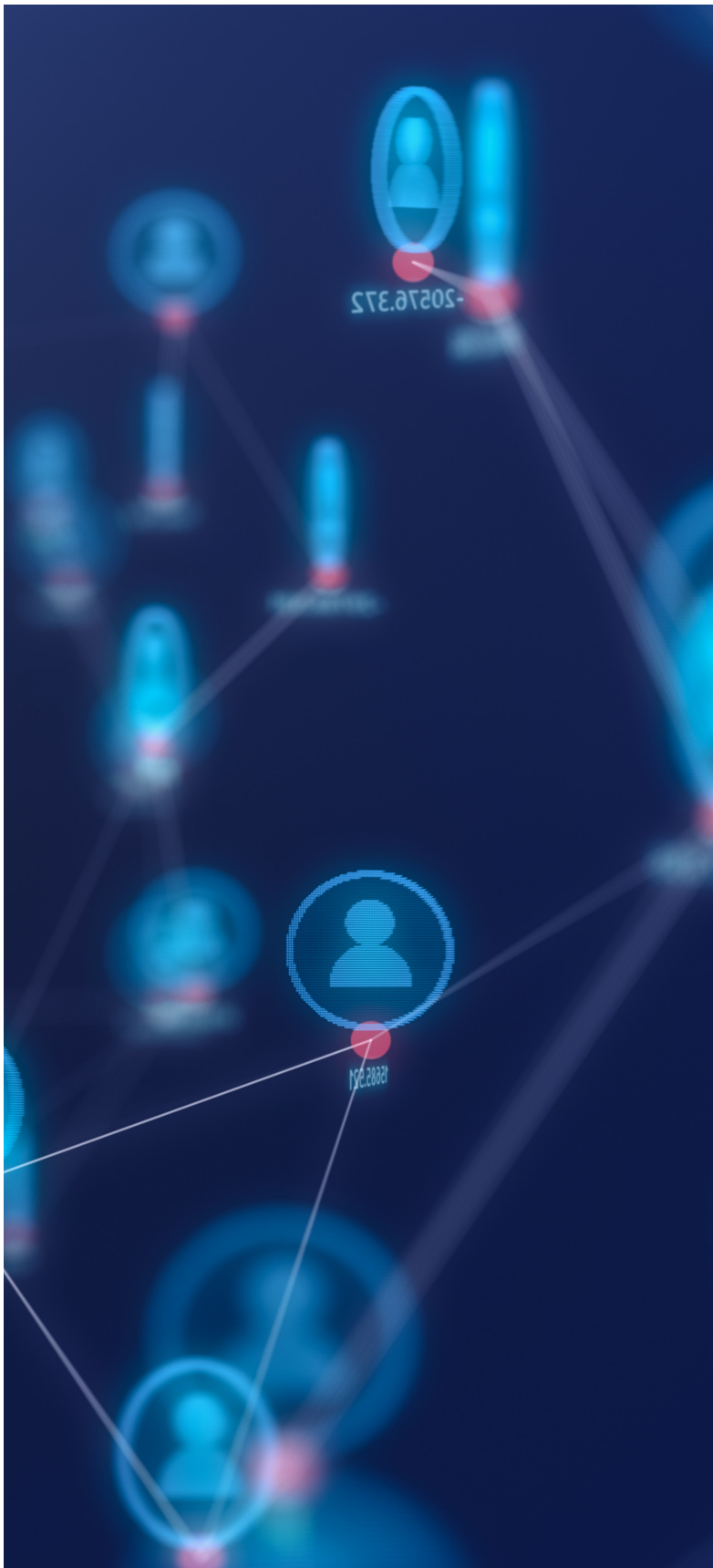
Therefore, being proactive and planning for offensive services is especially important. Attempting a last-minute emergency penetration test is an invitation to get overcharged, or end up with a low-quality test.

At least in the U.S., Q4 is frequently known as a busy period for penetration testing, as organizations empty the last of their budgets, completing work that had annual deadlines after first procrastinating all year...don't worry, it's not just you! Conversely, Q3 and the summer months tend to slow down, with many project stakeholders inevitably taking their vacations.

If a firm you are considering is available immediately for an engagement, take time to think about what that means. Sometimes, it is possible that a customer backed out and a spot opened up, but it could also indicate they don't have much business, which should start ringing alarm bells.

PROJECT-BASED, CONTINUOUS AND CROWD-SOURCED OFFERINGS

While most penetration testing engagements are still point-in-time and project-based, many firms offer "continuous penetration testing" services. This commonly amounts to a less frequent (annual or quarterly, for example), real, manual penetration test, followed by recurring automated scanning. In a worst-case scenario, this involves scheduling a recurring scan and sending you the PDF with no manual attention, exploitation, or post-exploitative activities – which, let's be clear, is not penetration testing.



Continuous offerings may or may not be valuable to you if you are already performing in-house vulnerability scanning. Do not be afraid to ask how much of their service involves an actual penetration tester (and if they're not telling you directly, get the SLAs; they should be defined there). If the firm claims "machine learning" or "AI," don't be afraid to ask, "How?", and uncover if the technology is there to help enhance the offering, or if it is more along the lines of buzzwords they think clients want to hear. Defensive responses, including words like patented, proprietary, bespoke, etc. could indicate evasion of tough questions.

Crowd-sourced penetration testing is available too. This involves platforms that tout a streamlined vetting process for onboarding testers, engaging them for projects, triaging reported findings, and usually paying testers per bug, similar to how researchers get paid in bug bounties. If you're considering this, ask about how the workflow is enforced across disparate researchers.

How do they keep people from wasting time retesting the same addresses, parameters, and pages? How is full target coverage ensured? Is there a methodology they follow, and how is that distributed? How many person-hours can be expected to be spent? How easy is it to communicate with the individual testers on short notice? Are the testers 1099 contractors or full-time employees?

Ultimately, there is no right or wrong type of offering – it is asking the questions and getting the answers that match best what you need that will guide you forward here.

PROJECT KICKOFF & RULES OF ENGAGEMENT

Once a project is scoped and agreed upon by both parties, the engagement is typically scheduled along with a kickoff meeting.

The kickoff meeting should be held at least a week before testing and will outline the type of testing to be performed, targets to be tested, and rules of engagement.

Any access to targets such as VPN connectivity, user accounts, MFA enrollment, and such should be handled during this meeting so as not to impede the testing schedule. Typically, the tester and their project manager will attend the call. Do not underestimate the importance of the kickoff meeting: a lack of a kickoff call or having it scheduled after the start of testing could indicate an unorganized or disengaged firm.

THE TESTING PROCESS

Once testing starts, the tester should begin the process of information gathering and threat modeling for targets. Vulnerabilities will be identified, exploited, and privileges escalated according to the rules of engagement agreed upon during the kickoff meeting.

The results of these activities are then documented in a final report. A good report should leave little doubt about what the issues are, why they are important, in what ways they can be remediated, and which ones to prioritize.

Reports often lay out the testing results at different levels for different audiences. However, there are typically at least two major sections: An Executive Summary and Technical Details. Any claimed exploits should be well-documented, usually in step-by-step, narrative form, with supporting evidence including screenshots within the technical details. Sometimes a table-formatted list of findings is also included for those in charge of keeping track of individual instances.

PROJECT WRAP-UP

Finally, it is common to schedule a project wrap-up meeting to go over the firm's final report – included in the project cost, of course). In addition, some firms charge to test for remediation status after you think you have resolved the issues that were most concerning to you. Others offer it for free within a certain time window.

Regardless of what firm or offering you go with; the importance of finding the right provider cannot be stressed enough for you. Often you are testing an application or network that is critical to your business, and sometimes your livelihood too – this is not an area to jump into without doing your due diligence.

For more information on how Depth Security can help provide organizations like yours with real-world visibility into threats facing their infrastructure and applications,

GET IN TOUCH HERE

START A CONVERSATION WITH ONE OF OUR INFORMATION SECURITY EXPERTS

sales@depthsecurity.com
https://depthsecurity.com

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446
CountOnKonicaMinolta.com

Item #: Depth_Sec_eBook
8/23-B