QUESTIONS TO ASK PENTEST COMPANIES

INTRO:

MSP’s, VAR’s, and security solution integrators have a massive opportunity within cybersecurity. Penetration testing is a niche service that allows a company to identify vulnerabilities and gaps within their security posture. After completing the assessment, a good penetration test provides recommendations to remediate the findings; opening up further opportunities for the partner to sell other professional services & products.

The challenge of offering pentests to your customers is that it’s a very specialized skill set that is hard to build out internally. It’s also difficult to find high quality penetration testing companies that understand the complexities of working with the channel. Below we outline key questions you should be asking penetration testing companies prior to doing any work together.

1. WHAT KIND OF WORK HAVE YOU DONE WITH MSP’S & MSSP’S IN THE PAST?

Why you should care: A key detail that you should be eager to learn is what kind experience they have working with the channel. If you’re working with a penetration testing company, you’ll want them to understand your business model & how you prefer to work with your customers. We’ve seen penetration testing companies that don’t understand whitelabeling reports or even flat out refuse. Many penetration testing companies don’t provide channel discounts & deal registration discounts, instead they provide full price quotes to partners expecting them to make razor thin margins on top of that.

When it comes down to it, many penetration testing companies are ran by pentesters who lack the necessary channel experience to fully support partners. You want to ask this question to ensure your partner understands your business & the complexities of working together.

What you should look for: Ideally, your penetration testing company will let you know that they only operate through the channel. This is unlikely and isn’t necessarily a hard requirement, so below are some key details & potential red flags to look for.

- Do they outline how their process changes from typical work with end customers? The sales process, the project management, and the post engagement support should be handled differently when working with channel partners.
- Do they talk about discounts & margins? You operate on margins and your pentest partner needs to understand that.
- Red Flag: Do they skate over this question? It's key to ask about the kind of work they've done with the channel instead of only if they've done work with the channel. If the question is met with a quick 'yes we've worked with plenty of channel partners' then you should aim to dive deeper into the details.

Conclusion: Overall, it's important that your penetration testing partner understands the difference between working directly with customers and partnering with the channel. This should be a focus in your discussion with penetration testing companies.

2. WHAT IS THE SIZE OF YOUR PENETRATION TESTING TEAM?

Why you should care: There are no hard requirements to call yourself a penetration tester, and there are no hard requirements to start a penetration testing company. What we've seen is that many of the pentest companies are ran & operated by a single individual. You'll want to ensure your pentest partner has a team large enough to handle multiple projects at once, while also having the capability to support your sales reps in the sales process. If an individual is in charge of everything, including the pentest, you must ask yourself if they have the experience outside of pentesting to provide your team the support they need. Additionally, there are several different types of penetration tests that your customers will need. Application penetration tests, network penetration tests, social engineering, etc. Each of these require a unique skillset & years of experience to become proficient. Many full time pentests dedicate themselves to one craft. Ultimately, you want to know that the pentest partner you work with isn't a one person run-of-the-mill operation.

What you should look for: This one is fairly simple. Ask about the individuals on the team. Who handles the customers throughout the sales process, who handles project management, and who is performing the assessments? Do the individuals on the assessment team have specialties? Be curious about the individuals & in the end you'll know your customers are in good hands.

Conclusion: Ultimately, the point of this question is to understand who you're working with. While this seems simple, many make the mistake of only getting to know the company they're working with while neglecting the individuals performing the work.

3. WHAT IS YOUR REPORTING PROCESS & OUTPUT?

Why you should care: When penetration tests are performed, there is only one thing your customer walks away with; the report. We've heard horror stories of companies having hard deadlines, being told by the pentest company the testing would be completed within that hard deadline, and then having to wait weeks after the testing was complete (and after the deadline) for the final report to be delivered. One other reason you should care about the reporting process is because many pentest companies might not be open to putting it on your paper. For one reason or another, pentest companies aren't the most flexible when it comes to white-labeling their work. You should also inquire about report delivery. Pentest reports always contain extremely sensitive information & should never be simply emailed to customers. That said, it's shocking how often this is the case. Overall, you want to make sure you and your customers know exactly what to expect when it comes to the final reports.

What you should look for: There is no definite answer to this question. In fact, the way the answer is presented is just as important as to what the answer actually is. Someone experienced in pentesting who also knows how to consult with customers should first break down the meaning of both types of pentests. Only after ensuring the customer fully understands the difference should the person provide their answer & the reasoning. Every customer has a different need, so the truth is that no answer fits all. In our experience, most customers end up somewhere in the middle of the two options. Some critical information should be provided to the assessors so that they can be thorough while also being efficient. On the other hand, if no information is provided at all, time will be wasted discovering that information on our own & the results will be limited.

Conclusion: This question is about evaluating how the pentest company will interact with your customers. Pentesting is about consulting & advising customers so that they can limit their security gaps. The technical work is important, but communicating those results & how to fix them is just as important. Your pentest partner needs to be able to step into an advisory role with not only your customers, but your team as well.

4. WHAT IS YOUR REPORTING PROCESS & OUTPUT?

Why you should care: When penetration tests are performed, there is only one thing your customer walks away with; the report. We've heard horror stories of companies having hard deadlines, being told by the pentest company the testing would be completed within that hard deadline, and then having to wait weeks after the testing was complete (and after the deadline) for the final report to be delivered. One other reason you should care about the reporting process is because many pentest companies might not be open to putting it on your paper. For one reason or another, pentest companies aren't the most flexible when it comes to white-labeling their work. You should also inquire about report delivery. Pentest reports always contain extremely sensitive information & should never be simply emailed to customers. That said, it's shocking how often this is the case. Overall, you want to make sure you and your customers know exactly what to expect when it comes to the final reports.

What you should look for: First & foremost, you should listen for the company to mention some type of secure portal for the delivery of reports. You and your customers need to know that security is of utmost importance at every step of the process. They should also give you an expectation on when you receive a report after the testing is completed. Pentest companies with good experience should include the creation of the report in the overall timeline. If the testing will take 5 business days, and the report 3 business days, then the total time of the assessment should be 8 business days.

Conclusion: Overall, you should have a good understanding of what the reporting process is. Ideally, you should have the option to whitelabel the pentest reports so that the output is from a company your customer is familiar with. Most importantly, make sure you have seen a sample of the output.