



Most Frequently

Asked Questions From
Our Partners



HOW MUCH CAN WE RESELL YOUR SERVICES FOR/HOW MUCH MARGIN CAN WE MAKE?



- One of the most common questions we get from our customers (MSSP, MSP's, and VARs) is how much a pentest costs. Before addressing that question, it's important to understand how the cost of a pentest is calculated. Pentest costs can vary significantly depending on multiple variables. Details such as the number of IP addresses, workstations vs servers, complexity & quantity of applications, etc. are key to properly scoping a project. No two projects are the same & asking the right scoping questions is critical to ensure the customer gets the assessment they need. After you have a deep understanding of the scope, the appropriate assessment length can be determined. A very small environment with only a few IP addresses can typically be done (with reporting) in 3-4 days, while large environments can take well over a month.

Once you understand the amount of time needed to provide a thorough assessment, you can then calculate the cost of the pentest. The hourly rate varies depending on the company, but we've found that most firms charge their customers anywhere between \$275 - \$400 per an hour. With this in mind, we've structured our pricing so that our partners can resell our services with the margins they desire.

HOW DO YOU INTERACT WITH OUR CUSTOMERS?



When white labeling our services we make ourselves available for you and your customers. Considering most of our partners view us as an extension of their team, they often include us in key meetings that include discovery/scoping and negotiations prior to contracts being signed. Throughout the assessment, our engagement manager is dedicated to you/your team to ensure any questions that arise from the customer are addressed in a timely manner. After the engagement, we are available to directly help with debrief meetings or, if preferred, help your team prepare to handle it alone.



A common misstep for pentesting companies is undervaluing client communication. A deep technical background is critical for penetration testing, but having the ability to clearly translate that for customers is just as important. Our team is made up of experts with years of customer facing experience so that we can ensure your customers never feel overwhelmed with the results.

HOW LONG DOES AN ASSESSMENT TAKE?



There are many variables that go into determining the length of a penetration test. For an example; consider a small mom and pop shop with only two servers compared to an enterprise network architecture with thousands of servers. The amount of time it'll take a pentester to thoroughly assess each environment significantly differs.



On average, we tend to see our assessments last anywhere between 4 - 12 business days. That said, it takes a serious scoping conversation about the environment to provide an accurate length.

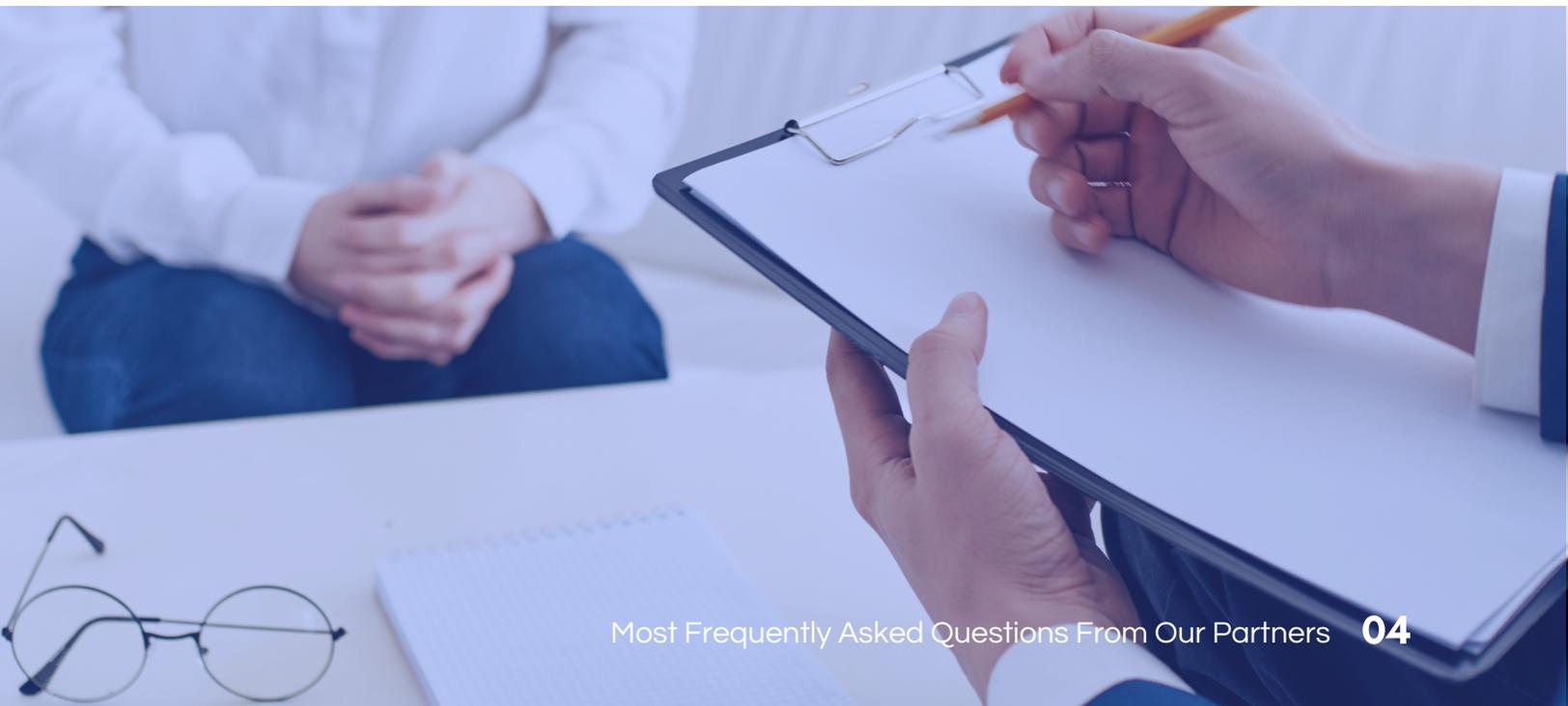
HOW SOON CAN YOU START AN ASSESSMENT?



Penetration testing requirements often have a hard deadline associated with them. We understand that your clients may be pressed for time & require quick results. One of our most commonly asked questions is 'how soon can you start?'



Penetration testing takes planning and preparation, so we try to schedule 2 weeks in advance. That said, we do our best to accommodate urgent requirements and consider ourselves flexible for our customers.



HOW MUCH OF THE TEST IS AUTOMATED/MANUAL



Every penetration test utilizes some variation of automated tools. This allows an assessor to identify low hanging fruit & prioritize where they spend their time diving deep into exploitation. Typically, this is one of the first steps in the pentest process and only accounts for 5-10% of the allotted assessment time. This is a key question you should ask all pentesting companies because many will run basic automated tools and brand the service as a true penetration test.

WHY WOULDN'T WE WHITELABEL YOUR SERVICES INSTEAD OF BUILDING OUT OUR OWN TEAM?



For some, building out your own team might be the right direction. We're happy to provide some guidance as well. That said, most of our partners find it difficult to find penetration testers with the right amount of experience. Cybersecurity as an industry is already a broad subject. Penetration testing requires true subject matter experts with the right type of experience, which is not only difficult to find but also difficult to identify. You might be able to find many people who call themselves pentesters, but even those with years of cybersecurity experience have a challenge distinguishing a good pentester from someone who is simply familiar with a few automated tools. Building out the team is only the start. You'll also need to hire management that has experience working with teams like this, who can also translate the technical findings for your customers.

All of the operational challenges aside, one of the most critical challenges is funding a team like this. The salary & resources required for building a team like this can quickly become larger than anticipated.