Penetration Testing

For MSP's, MSSP's, VAR's, and
the rest of the partner community

Here we'll outline why channel partners (MSP's, MSSP's, VAR's, etc.) might benefit from offering penetration testing to their customers. You'll learn more about what penetration testing is, the business drivers behind why your customers may be doing them, and the benefits of offering pentesting services to your customers. In our experience, the most successful partners within the security industry are the ones who remind customers that they are more than just 'IT help' but that they are business & technology strategists to be viewed as a virtual CISO. Let's get down to why penetration testing is the way to earning that trust.

What is pentesting

Penetration testing is a niche corner within cybersecurity that requires a specialized skill set for identifying & exploiting vulnerabilities. Once the impact of those vulnerabilities is discovered, customers are given the results ranking in severity so that they can fix those findings. The most common types of penetration tests are external network pentests, internal network pentests, and web application pentests.

External Network:

Exploits vulnerabilities that could be performed by an external user without proper access and permissions.

Internal Network:

Exploits vulnerabilities that could be performed by an internal user within your network. This could be an outsider who has compromised the external network to gain access to the internal network.

Web Application Assessment:

Most commonly performed on SaaS products, a web application assessment exploits vulnerabilities that could be performed through a webapp.

WHY YOUR CUSTOMERS NEED PENETRATION TESTS

There are a number of reasons that your customers might need, or are already performing, penetration tests. The three most common reasons are compliance & regulatory requirements, third party requirements, and as a security best practice.

Regulatory Compliance

Customers have many regulatory requirements that they are subject to. Many compliance requirements include language that outlines the need for regular penetration tests. This means that your customers might already be performing pentests on an annual or quarterly basis with another firm. Unsure of what kind of regulatory requirements your customers are subject to? Think about the type of data they handle, or just ask!

The list of regulations that require penetration testing is long, but here are a few common ones that we see:

- Companies that handle health information (PHI) such as blood type, prescription details, SSN,
- Companies that handle credit card information (PCI) such as credit card #, expiration date, CVV #, etc.
- Companies pursuing SOC2 compliance.

Third Party Requirements:

Do you customers sell their services or products to large enterprises? Often, large enterprises require their vendors to perform penetration tests on an annual basis. The enterprise may even have their information security team review the penetration test results prior to signing contracts..

Security Best Practice:

This one is simple. Some of your customers perform penetration tests because they are doing the right thing. A penetration test helps identify weaknesses in your security posture, which in turn reduces the likelihood of a company being subject to a compromise.

WHY YOU MIGHT CONSIDER OFFERING PENTESTING

Looking back, we've reviewed what pentesting is & why your customers are performing them. The final missing detail is why your organization might benefit from offering pentesting services. After working with channel partners for many years, we've found that the most successful ones have relationships that transcend transactional purchases. Penetration testing helps you with that because it puts you in an advisory role for your customers, where they look towards you for strategy & planning a roadmap. You help them identify the security gaps, demonstrate what could happen if those gaps aren't closed, and then you help them close them.

As part of that, penetration testing can help you identify opportunities that eventually lead to additional purchases by your customer. If the pentest identifies that your customer has no way of blocking data exfiltration, then part of the recommendations would be deploying a DLP solution. Down the road, you can help facilitate that purchase.

While helping your customers purchase DLP solutions is great for business, those renewals only happen every few years. Another key benefit of offering pentests to your customers is that it keeps you regularly engaged with your customers. At a minimum, companies perform penetration tests once a year. That said, we've seen companies who perform monthly pentests so it varies from company to company

SUMMARY

MSP's, MSSP's and channel partners are leaving money on the table by not offering penetration testing services. The service offers high margins, recurring revenue, and positions you as your customers' trusted advisor.

If your company is interested in offering penetration testing services to your customers, but don't have the expertise to build out a pentest team internally, reach out to us for a deeper discussion.