Mighty Guides

THE CHALLENGE OF FINDING THE RIGHT PEN TESTING VENDOR

Sponsored by

RISKSENSE

INTRODUCTION

Choosing the right pen testing vendor is challenging because different pen testers work in different ways, and typically there are differences within an organization about what to expect from the pen testing service.

This eBook reviews evaluation fundamentals and provides advice about selecting vendors, including making sure you are dealing with a reputable company that can show how they validate findings. A good pen tester will report on critical findings immediately, before their formal report is completed.

Regards,
David Rogelberg
Publisher, Mighty Guides, Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

MEET THE EXPERTS

VITO SARDANOPOLI
Managing Principal and Owner,
Vantage CyberRisk Partners

PHILLIP WYLIE
Principal Information Security Engineer (Penetration Tester),
US Bank

Vito Sardanopoli, Managing Principal and Owner, Vantage CyberRisk Partners

Vito Sardanopoli, CISM, CISSP, CISA is the Founder and Managing Principal of Vantage CyberRisk Partners, whose focus is in providing information and cyber security advisory and consulting services, including: strategy, architecture, design, delivery, and governance, along with technology and security risk management. They also provide vCISO services. The goal is to provide leadership, strategic direction and practical guidance and solutions tailored for the unique needs of clients.

"However, these testing engagements need to be closely monitored to ensure approach and quality are maintained."

Penetration testing can play a key role in vulnerability management, especially with the faster, more flexible approach to pen testing that is available from some vendors. Choosing the right pen testing vendor, however, can be a challenge. There are many to choose from, and there are different aspects organizations want to focus on that guide the type of service most suited to their needs. This can make finding the ideal pen tester difficult, especially if pen testing plays a key role in understanding risk associated with new technologies and time-sensitive business developments.

When evaluating pen testers, it's important to take a close look at how they work and how they report their results. But what are the key criteria? For Vito Sardanopoli, managing principle and owner of Vantage CyberRisk Partners, pen testers' ability to demonstrate their depth of expertise is critical. "I would like to see a documented outline of their approach that includes how they stand out against competitors in the space. I would follow this by arranging to speak with select business leaders. This includes those that lead the penetration testing services as well as at least one lead practitioner/pen tester. A key focus on these discussions is to have them elaborate on their approach and methodology, as well as specific successful pen testing engagements.

Phillip Wylie, Principal Information Security Engineer (Penetration Tester), US Bank

Phillip Wylie is a penetration tester with over 21 years of experience in Information Technology and Information Security. Phillip is an adjunct professor teaching ethical hacking and web app pentesting at Richland College in Dallas, TX. Phillip is the founder of The Pwn School Project an educational group teaching pentesting and ethical hacking skills. Phillip holds the following certifications; OSCP, GWAPT, and CISSP.

"You want enough detail that someone else besides the original pen tester could duplicate the exploit."

Setting up retainers for ongoing pen testing services is acceptable for pen testings that require periodic (at least annual) testing. However, these arrangements and testing engagements need to be closely monitored to ensure approach and quality are maintained. Obviously, findings need to be thoroughly and satisfactorily vetted prior to publishing in a final report." He also notes the importance of the underlying pen testing technology. "I like to have an understanding of the types of tools they use. The quality and accuracy of pen testing results will reveal whether effective tools and pen testing methodology have been applied."

Phillip Wylie, CISSP, GWAPT, OSCP and principal information security engineer (penetration tester) at US Bank, also underscores the importance of using a reputable pen testing company. He says, "Coming from a consulting background and having seen some bad practices by some consulting companies, my advice is to make sure you are going with a reputable company. There are companies that just run a vulnerability scan and put it in a custom report template. Some will even use vulnerability evidence from the vulnerability scanner they are using. You want to make sure they are validating the findings as well as exploiting those that are exploitable.

Ask to see a sample report. They should be able to give a sanitized report of past pen tests to show the quality and detail of their work." Wylie takes that a step further by suggesting pen testing practices that maximize the value of the engagement. "You should have access to exploit code tools used as well as the details of how systems or devices were exploited," he says. "You want enough detail that someone else besides the original pen tester could duplicate the exploit. If you have a need for a large number of pen testers or fast turnaround time for retesting, you could also schedule the retest time when you are scheduling the initial pen test." He emphasizes the value of timely reports, saying, "During pen tests, you definitely want critical or high findings reported immediately and prior to the report being completed. You need this to prevent possible compromise from bad actors."

For Vito Sardanopoli, an ideal pen test engagement also ties back to risk management objectives shared by all the stakeholders. "In order to maximize the effectiveness of pen testing results, the test objectives need to be clearly outlined and agreed to by all stakeholders prior to commencing testing. Also, these test result objectives should be tied to specific risks or vulnerabilities. This will ensure broad awareness of the pen testing results and benefits for members of relevant business and corporate groups outside of IT as well as members of senior management."

Phillip Wylie believes pen testing needs to be treated as an integral part of a vulnerability management program. He says, "I would recommend doing a pen test at least once a year with a retest of the findings from the first test, twice if your budget allows. If it is not affordable to have a third party test all your assets, then I recommend building your own internal pen test team and supplementing your external pen tests with third-party consultants. Pen testing should supplement your internal recurring vulnerability scanning. Pen testing, vulnerability scanning, and static code analysis should be part of the software development life cycle process for your internally developed software." ■

CLOSING THOUGHTS

Without a doubt, you struggle with prioritizing the plethora of threats and vulnerabilities that hit your organization. Penetration testing findings add to the problem. There are never enough hours in the day, nor enough staff to remediate all of the possible exposure on both your internal and external IT infrastructure.

Shift your thinking. Narrow down the threats and vulnerabilities to the ones that have active exploits, are dangerous with remote code execution capabilities, and are trending with active threats in the wild. This is impossible if you don't have a platform that takes in all of your vulnerability scanner data, across your dynamic attack surface: network, endpoints, database, applications, cloud, and IoT devices. Leverage human intel, combined with AI and machine learning to achieve prescriptive prioritization in minutes. Security and IT teams can focus on what matters the most with a new efficiency to manage cyber risk.

This article illustrates the value of risk-based vulnerability management to predict, prioritize, and take control of your most dangerous vulnerability and risk findings.

Regards,
Srinivas Mukkamala
CEO and Co-Founder, RiskSense

RISKSENSE

RiskSense®, Inc. provides vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness.

The company delivers a fully-informed picture of group, department, and organizational cybersecurity risk with our credit-like RiskSense Security Score (RS3). The RiskSense platform continuously correlates customer infrastructure with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings, and business asset criticality to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation activities to achieve security risk goals.

By leveraging RiskSense threat and vulnerability management solutions, organizations significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, heighten response readiness, lower costs, and ultimately reduce attack surface and minimize cyber risks. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.