NETSPI™

++++

++

How To Build An Effective Penetration Testing and Vulnerability Management Program

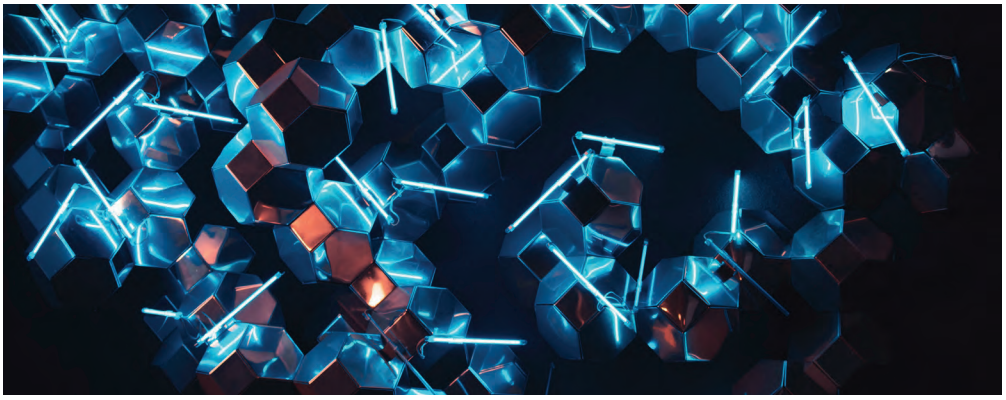
A Four-Part Guide

Introduction

People, processes, and technology are the key ingredients to an effective penetration testing program – but only if you can first create a solid foundation, or plan, on how each can work together to boost your security posture. In this whitepaper, you'll find advice and guidance on how to communicate the need (and get funding) for proactive cyber security to your business leaders, what to look for in a pentesting team, how to gain the most value out of your pentesting program (hint: continuous), and more. With people, processes, and technology at the core of your vulnerability management and pentesting programs, you'll be prepared to better identify and evaluate vulnerabilities and ultimately reduce time to remediation.

Part 01

Making the Case for Proactive Cyber Security Investments



Proactive, or preventative, cyber security measures continue to be an afterthought in today's conversations around breach preparedness. In this Forbes article for example, the author suggests establishing an incident response plan, defining recovery objectives and more, all of which are necessary – but there's no mention of investing in tools and services that boost your security posture in the first place.

Sure, it can be difficult to make a business case for the C-Suite to invest in something intangible that doesn't directly result in new revenue streams. Historically though, we've seen breaches cost companies millions and sometimes billions of dollars, proving that a 'dollars and sense' case can be made. And even when a case has been made to the board and funding is available, security teams struggle to be proactive because they are constantly reacting to the threats already looming in their network, they are lacking adequate staffing, and the pace of vulnerabilities continues to outpace the business. So, how can organizations come together, C-suite and security teams alike, to prioritize the urgency of implementing a proactive cyber security program? How can we communicate that the upfront planning and set up is a proactive investment that will help eliminate the financial and time strain of a reactive-forward program?

The reality is that cyber security breaches today are inevitable and put organizations at grave risk. To help security teams make the case for prevention-based security investments here are three recommendations that will get the attention of C-Suite executives and help security teams remain proactive:

$8.2 M

According to the IBM and Ponemon Institute Cost of a Data Breach Report, the average size of a typical data breach in the U.S. in 2019 was 25,575 records, resulting in an average cost of **$8.2 MILLION** per breach.

1. Translate the Impact of a Breach into Dollars and Sense that the C-Suite will Understand

In today's digital world, data is more valuable than ever, and, at the same time, more vulnerable than ever. So, how can you best communicate this heightened value of data security to your leadership team? By speaking a language they understand. First, shift your mindset from talking about "cyber security and compliance" to "customer safety and quality services;" these terms will resonate better with the C-Suite.

Next, be prepared to talk financial risk. Annually, IBM and Ponemon Institute release the Cost of a Data Breach Report, which includes a calculator based on industry and cost factors, such as board-level involvement, compliance failures, and insurance, to determine the potential financial impact a breach could cause. Use this resource to calculate your own organization's estimated cost of a data breach. A simple calculation case study: in the United States, if an attacker compromised just 5,000 records, it would cost your organization over $1 million (based on the average cost of $242 per lost record). This case demonstrates the cost of a smaller-scale breach – in fact, the average size of a typical data breach in the United States in 2019 was 25,575 records, resulting in an average cost of $8.2 million per breach. Compare that to the average cost of a vulnerability management or penetration testing program, and your case to the executive team is pretty simple. Notably, loss of customer trust and loss of business were the largest of the major cost categories, according to the report. The study found that breaches caused a customer turnover of 3.9 percent – and heaps of reputational damage.

Lastly, use examples in your respective industry as proof points. For example, if you're in the financial services industry, reference other breaches in the sector and their associated cost. It's important to clearly communicate the reality of what happens when your organization is breached to get the C-Suite on board for additional cyber security spend. Sharing concerning results of *reactive* cyber security strategies will help them to see the benefit of investing in *proactive* security measures to prevent a breach from happening in the first place.

2. Help Leaders Understand Vulnerability Testing's Role in a Crisis Preparedness Plan

A data breach is a common crisis scenario for which every business should plan. It should be discussed in tandem with other risk scenarios like natural disasters, product recalls, employee misconduct, and conflict with interest groups, to name a few. As with any disaster preparedness program, documentation and reporting are critical. Specifically, documentation of your vulnerability testing results and remediation efforts should be viewed as a tool to inform leaders about the organization's exposure to risk, as well as its ability to prevent breach attempts from being successful. Cyber security weaknesses to look for from an organizational standpoint include, lack of continuous vulnerability testing and patching, untested incident response plans, and limited training and security awareness programs. These three key areas can turn into the "Achilles heel" of any organization's security posture if not addressed and implemented properly.

80%

Over **80 PERCENT** of security leaders say lack of resources keeps them up at night, according to a NetSPI survey.

3. Position Your Pentest Team as an Extension of Your Own Security/IT Team

According to a survey we conducted earlier this year, over 80 percent of security leaders say lack of resources keeps them up at night. And for some time now, the security industry has suffered a skills shortage. While companies are eager to hire experts to address the ever-evolving threat landscape and avoid the high costs of a breach, there aren't enough people who can fill these roles. According to the latest data from non-profit (ISC)[2], the shortage of skilled security professionals in the U.S. is nearly 500,000.

Hiring outside resources is one solution to this demand conundrum. Time is invaluable, so if you're proposing to hire new vendors, it's important from the start to position the white hat testers to your executives as an extension of your own team. It is the responsibility of both corporate security practitioners and vendors to find ways to work collaboratively as one team. Pentesting is a great example of this. Traditionally, pentesters complete their engagement, hand off a PDF, and send the internal team off to remediate. With the emergence of Pentesting as a Service (PTaaS), testers not only perform an engagement, but also conduct more deep-dive manual tests, continuously scan for vulnerabilities to deliver ongoing results in an interactive, digital platform that separates critical vulnerabilities from false positives (a time-consuming activity for your in-house team), and serve as remediation consultants for your organization. Make it clear to the C-Suite that vendor relationships *are* changing and vendors can serve as a solution for current cyber security skills gaps within the business.

When the C-Suite and its IT and security departments are disconnected on security priorities, the risk of a data breach increases. Learn to speak the language of your executive leaders and communicate the true value of proactive security measures. Effective communication around the potential financial impact of a breach, where vulnerability testing fits in a crisis preparedness plan, and ways to solve cyber security talent shortages, ought to result in additional budget for key security initiatives.

Part 02
Characteristics of a Successful Pentester

Pentesting has attracted a workforce filled with intensely creative and highly curious technical minds. Ironically, however, we see vulnerability management programs advance and accelerate when creativity is paired with a framework that drives quality and consistency. Is this an indication that our industry has matured to the point that the level of innovation is diminishing? Far from it. In fact, the best cyber security programs and providers incorporate and embrace both innovation and consistency.

Innovation Remains Mission Critical

First, it's important to understand that there are a couple ways to define innovation. The first, of course, is through the lens of creativity and disruption. Attackers don't have any boundaries when it comes to figuring out how to exploit a program or system; neither should cyber security teams. Finding new ways to break things is a critical part of the job.

A second way to define innovation is more pragmatic. While companies need to address large volumes of vulnerabilities and develop strategies to remediate them, most security teams are faced with doing more with less due to budget restrictions, lack of resources, and other constraints. The only way to accomplish this is to adopt some level of automation. Moreover, automation is critical for handling mundane or repetitive processes to free up time for humans – pentesters, developers, and others – to exercise their creative minds. As in any industry, automation enables people to perform at their highest potential, and when used correctly, it becomes a force multiplier.

Consistency Plays a Vital Role, Too

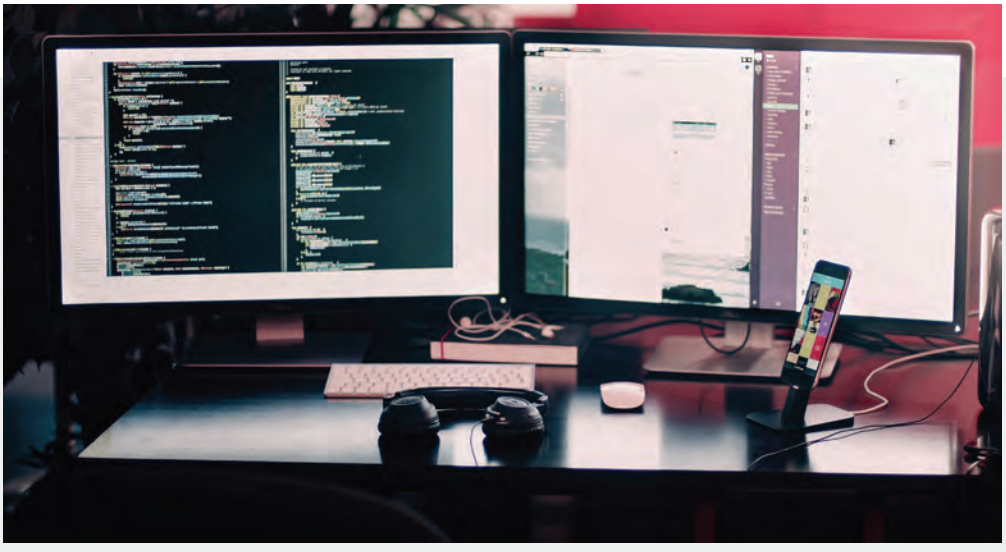
As partners to large corporations and other organizations that have extensive testing programs, NetSPI must have consistency in our testing approach. When we find a new vulnerability within one client's environment, our consistent, systematic process enables us to add that one vulnerability to a checklist for each and every test we do in the future, regardless of the individual tester. This process frees up time for our team of pentesters to be more innovative in finding ways to exploit a program or system, while also ensuring as much coverage as possible.

Another way to approach consistency is through more regular testing for vulnerabilities instead of performing a pentest on your network as an annual compliance tool that results in static PDF reports with out-of-date vulnerability information. As a best practice, vulnerability management measures should employ continuous monitoring, with real-time reporting that enables companies to remediate vulnerabilities as quickly as possible. This new paradigm, known as Penetration Testing as a Service (PTaaS), employs both automated scanning and manual tests that dive deeply into applications and networks.

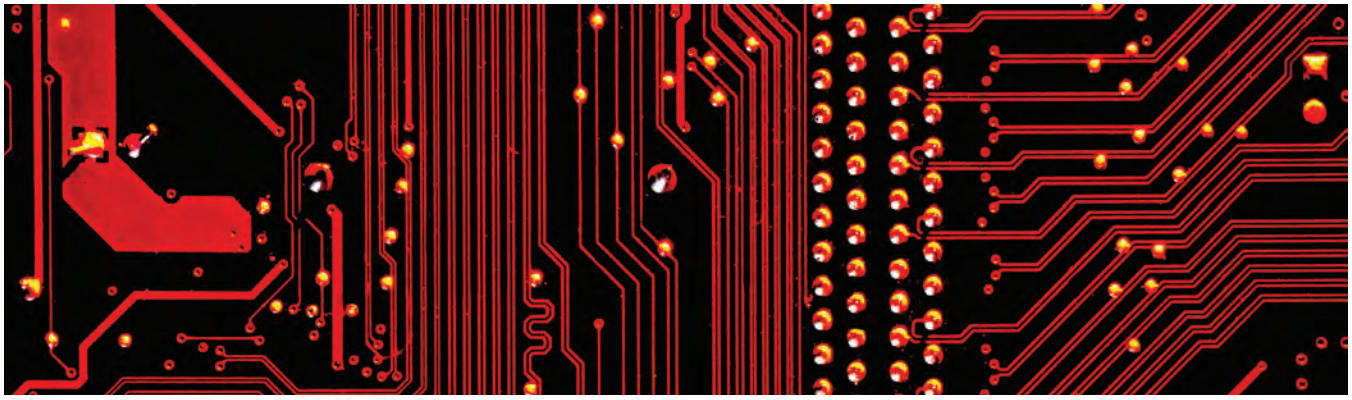
Striking a Balance Between Innovation and Consistency

How our industry maintains the balance between innovation and consistency should start with our people. While it may seem easier to screen for skills versus personality, the goal is to look for people that can not only think like an attacker, but also excel within a framework that supports individual agility, and leads to a consistent and high quality outcome. A tip? Search for individuals who have an interest in information sharing and bettering the larger security community; those who develop new tools (or improve existing tools) and participate in continuous learning in their free time typically have the capability to be extremely innovative. With a well-rounded workforce and mindset, organizations can gain an edge on their competition, disproving the notion that who you get determines the quality of the services delivered.

To be successful in the world of vulnerability management and pentesting, it's critical that providers offer a balance between creative disruption and methodical, systematic structure. Together, both right-brained and left-brained talent and solutions result in the very best tests that help organizations stay ahead of ever-changing attack surfaces.



Part 03
Four Elements of an Always-On Cyber Security Program



39

A University of Maryland study says that hackers attack every **39 SECONDS**.

Let's face it. The chefs in our lives were right when preaching the "clean as you go" philosophy while cooking. Keeping counters and utensils washed and put back in place helps thwart the influx of bacteria and spread of cross contamination that could make us sick. Shouldn't that same philosophy apply to cyber security, too? Foregoing a "clean as you go" program and conducting a penetration test just once each year may check a compliance box, but ultimately prove to be unsuccessful when it comes to protecting your network and assets from the potential "bacteria" that can enter at any time.

Systems and applications in any organization become alarmingly vulnerable if monitored under a one-and-done scenario. An ongoing and continuous vulnerability management or penetration testing program is an important guard against the potential threat to your technology assets that hackers pose nearly every second of the day. In fact, a University of Maryland study says that hackers attack every 39 seconds (on average 2,244 times a day). Think of how vulnerable your technology assets are in this environment if only tested once a year.

As an aid to help put structure around a continuous penetration testing program, here are four core considerations that should be a key part of an always-on security program.

70%

Nearly **70 PERCENT** of CISO security leaders are concerned about network vulnerabilities after implementing new security tools, according to a NetSPI survey.

1. Prevent Breaches with an 'Always On' Testing Mentality

There's no doubt about it: attack surfaces grow and evolve around the clock. With network configurations, new tools and applications, and third-party integrations coming online constantly, an atmosphere is being created that opens the possibility of unidentified security gaps. This whitepaper points to the fact that cyber-attacks can affect your business and are, unfortunately, almost as prevalent as natural disasters and extreme weather events. And we know from our own NetSPI research that nearly 70 percent of CISO security leaders are concerned about network vulnerabilities after implementing new security tools.

And those CISOs' concerns are not unfounded: take for example, the recent announcement from the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). It published security advice for organizations that may have rushed out Office 365 deployments to support remote working during the coronavirus pandemic. A ZDNet article says that CISA warns it continues to see organizations that have failed to implement security best practices for their Office 365 implementation. It is concerned that hurried deployments may have led to important security configuration oversights that could be exploited by attackers. With continuous pentesting in place, security leaders can identify high risk vulnerabilities in real-time to ultimately close security gaps faster.

2. Automation is a Tool; Human Logic is Critical

It's a fact that good pentesters use automated scanning tools (ideally from many different sources) and run frequent vulnerability discovery and assessment scans in the overall pentesting process. Scanning is generally considered an addition to manual, deep dive pentests conducted by an ethical hacker. When correctly understood, manual pentesting leverages the findings from automated vulnerability and risk assessment scanning tools to pick critical targets for experienced human pentesters to: 1) verify as high-fidelity rather than chasing false-positives, and then 2) to consider exploiting as possible incremental steps in a serious effort to eventually gain privileged access somewhere important on the network.

Purely automated tools or highly automated testing activities cannot adequately perform testing of the business logic baked into the application under the test. While some tools claim to perform complete testing, no automated technology solution on the market today can perform true business logic testing. The process requires the human element that goes well beyond the capabilities of even the most sophisticated automated tools.

3. Reporting Doesn't Have to be Mundane

We can all agree that there isn't much enjoyment in reading pages and pages of testing data presented in static excel or PDF documents. Now picture what the paperwork might look like if it is a once-a-year penetration testing report. Gulp! Much like many of us consume the daily news headlines, so too should CISOs view the daily "headlines" of their vulnerability management programming through the display of live pentest results.

Under this scenario, less time is spent analyzing report data, opening up valuable time to give to the important work of remediation. Insist on the following report deliverables in your pentesting program:

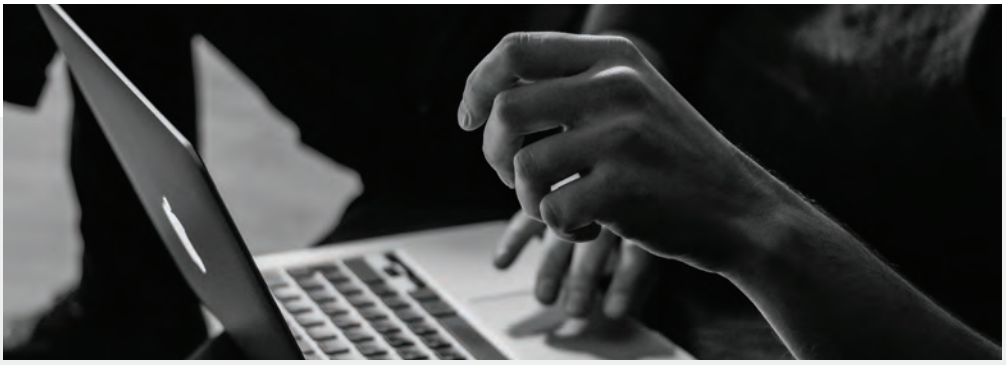
1. Actionable, consumable discovery results to automatically correlate and normalize all of the data collected from multiple open source and proprietary tools.
2. High quality documentation and reports related to all work delivered, including step-by-step screen-capture details and tester commentary for every successful manual attack.

4. Stay Ahead of the Attacks Through Remediation

To stay ahead of the every 39-second hacks every day, it's important to enable fast and continuous remediation efforts to keep a threat actor at bay. This goes hand in hand with testing, analyzing, and reporting: if you're not continuously testing for vulnerabilities, it's highly probable that the issues remain unresolved. Layer in these remediation best practices into your pentesting program:

1. Industry standard and expert specific mitigation recommendations for all identified vulnerabilities.
2. Traceability and archiving of all of the work done to make each subsequent round of testing for your organization more efficient and effective.

Factoring these considerations—always on testing, manual testing, real-time reporting, and remediation—into the planning and design of penetration testing programs will significantly minimize the risk of damage or disruption that could occur in an organization, and dramatically boost the security of your cyber assets.



Part 04

A Checklist: How to Get the Most Value Out of Your Testing and Vulnerability Management Strategy

You have leadership buy-in to invest in a proactive cyber security program to better protect your organization from security breaches that could put your organization at grave risk. And you've committed to building an ongoing and continuous vulnerability management program to guard against the potential threats to your assets. Now what?

Putting a successful vulnerability management program in place needs careful consideration up-front to ensure your organization is set up for success to remediate vulnerabilities for each application and system you have. For a quick overview of the process, our *Best Practices for Your Vulnerability Management Program* tip sheet can be used as a guide. The following checklist breaks the best practices process down and provides you with a planning road map to getting the most value out of a testing and vulnerability management program.

Penetration Testing Program Plan of Attack

STEP ONE: THE PLAN

ELEMENTS OF SUCCESS

Develop a plan that puts structure and strength around cyber security to include continuous vulnerability testing and patching, incident response plans, and training and security awareness programs. The ultimate goal? Decrease time to remediation and to close security gaps in your network.

Clearly define the scope, objectives, identification of testing, and the order in which they are to be performed.

Build a vulnerability management team. This could include both in-house talent as well as industry analysts or consultants. When choosing a pentesting service provider, ask about the credentials of their pentesting team, beyond technical competencies. Will your team be comprised of a dedicated work group or an outsourced group who haven't previously worked together, for example. Team structure has implications on streamlined communications and in knowing who is inside your network.

Augment with careful preliminary risk planning with contingency plans should any services be unintentionally disrupted.

Resources:

- Cloud penetration testing
- Application penetration testing
- Host-based penetration testing
- Network penetration testing

REQUIREMENTS

- ☐ Develop a high-level vulnerability management plan – be sure to include non-negotiables such as scalability and continuous testing
- ☐ Present your case to business leadership; gain agreement on budget
- ☐ Refine plan and define ownership and scope of your program to include personnel and their roles and responsibilities
- ☐ Develop policies, standards, and procedures
- ☐ Determine merchandising strategy – to bring visibility to the program's successes

Penetration Testing Program Plan of Attack (CONTINUED)

STEP TWO: SCANNING AND ASSESSMENT

ELEMENTS OF SUCCESS

Layer in automated scanning functions that deliver results that can be easily sorted and acted upon with human capital to find and fix vulnerabilities.

Create an enumeration (list and count) of suspected vulnerabilities that are enumerated only after using multiple automated tools over time, not just one single tool.

Build in further analysis of suspected vulnerabilities using specialized tools and manual techniques as required.

REQUIREMENTS

- ☐ Identify all assets you want to scan
- ☐ Define vulnerability landscape:
  - Common vulnerabilities and exposures (CVEs)
  - Common configuration and enumeration (CCEs)
  - Architecture
  - Design
- ☐ Define actionable reporting structure of vulnerabilities
- ☐ Deploy automated vulnerability scanning, use authenticated mode to scan high-value resources
- ☐ Prioritize pentesting cadence, beginning with an external network penetration test followed by internal network testing
- ☐ Commence manual pentesting

STEP THREE: PREPARING FOR RISK-BASED REMEDIATION

ELEMENTS OF SUCCESS

Develop a risk-based remediation plan commensurate with your program's maturity level and appetite for business risk.

Employ a comprehensive verification of high-risk vulnerabilities including but not limited to safe exploitation of these vulnerabilities using both automated and manual processes, including the injection of malicious code when called for.

REQUIREMENTS

- ☐ Rank vulnerabilities through an established remediation timeline. For example:
  - Critical = 7 days
  - High = 2 weeks
  - Medium = 1 month
  - Low = Patch driven updates
- ☐ Assign application and system remediation owner
- ☐ Build in business leadership approvals for long lead remediations

Penetration Testing Program Plan of Attack (CONTINUED)

STEP FOUR: ONGOING REPORTING AND IMPROVEMENT

ELEMENTS OF SUCCESS

Automate your vulnerability management program as much as possible: spreadsheets, emails, and document sharing portals are insufficient for most organizations, large ones in particular. Automation enables 24/7 visibility with business leadership and continuous improvement.

Find a reporting platform that is engaging and customizable to showcase what is most important to your business, one that can track and compare data over time.

REQUIREMENTS

- ☐ Build a reporting framework – for the pentesting team and for business leadership
- ☐ Identify continual improvement opportunities
- ☐ Use comparison data to showcase progress over time and highlight successes

All organizations should aspire to have the people, processes, and tools necessary to effectively execute an ongoing vulnerability management program. Failure to do so may result in poor tool selections, testing mistakes, and faulty interpretation of results that often lead to a false sense of security and could put the enterprise at risk. By building out a vulnerability management plan, as depicted above, you can dramatically increase the security of your enterprise and can be better assured to reach your ultimate goal: to decrease time to remediation and close any security gaps in your network.

DOWNLOAD THE CHECKLIST NOW

Conclusion

How To Build An Effective Penetration Testing and Vulnerability Management Program

Repeat: people, processes, technology. Combined, they are the key to success in vulnerability management. Find ways to make the three core elements work seamlessly together in the planning phase of your vulnerability management and pentesting strategy and you will find a quicker path to remediation. To recap, here are the next steps to take on your journey to a robust pentesting program.

1

Win over your leadership team

2

Choose your team

3

Find ways to keep tabs on your network 24/7

4

Get the most value out of your strategy

Learn more about NetSPI's services

Schedule time to talk with one of our team members

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest health care companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster. Follow us on LinkedIn, Twitter, and Facebook.