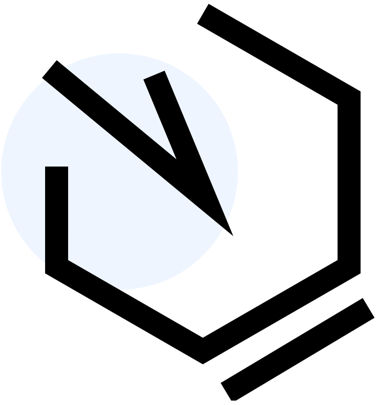
WHITE PAPER

Selecting the Right Penetration Test for Your Organization

GUIDEPOINT®
SECURITY

A few reasons for conducting an offensive style assessment include:

- ✓ Identification of previously unknown security gaps
- ✓ Segmentation testing
- ✓ The ability to demonstrate real-world impacts of vulnerabilities
- ✓ Discovery of Identity and Access Management issues
- ✓ Compliance with regulations such as PCI-DSS, HIPAA, FISMA, FFIEC and more
- ✓ Evaluation of new security tools, processes, procedures and any migration projects



Penetration testing is a critical component of an overall information security strategy and program.

Penetration testing is useful for identifying vulnerabilities in your environment, gaps within your security processes, and compliance risks, as well as evaluating new security tools, processes and procedures. There are different approaches to conducting a penetration test and this paper will examine a few of those methods and help you identify the right fit for your organization. We'll also look at how to evolve your security program to further mature the types of pen test you can effectively leverage to gain the most value.

Before digging into penetration testing, its various styles, use cases and more, it makes sense to establish why this type of work is important. What's the goal of trying to emulate the attackers that we see every day?

Depending on your industry, there may be different drivers.

In highly regulated industries you most likely have regulatory requirements around this capability--at a minimum it's a "check the box" assessment for compliance. Ideally, the motivator extends well beyond mere compliance--since compliance alone doesn't guarantee security.

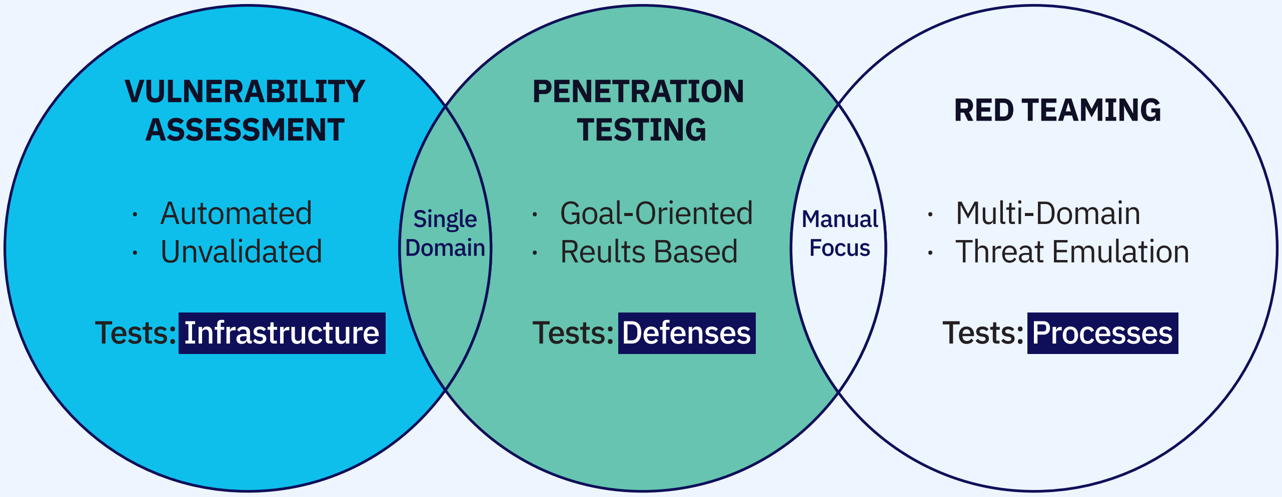
It's important that we consider the defenders' perspective first--the pen test isn't valuable unless we account for their best interests. So, when considering assessments, we should focus on our goals and collective commitment to advancing security maturity.

Defining and Differentiating Security Assessments

While there are three types of assessments, all focused on a different objective, Penetration Testing is where there is common ground.

- **Vulnerability Assessments –** These are essentially automated vulnerability scans, with some false positive verification and validation needed to remove those false positives.
- **Penetration Testing –** Far more manual of an assessment, but still focused on a single domain like vulnerability assessments (i.e. testing a specific infrastructure or system itself).
- **Red Teaming –** This is true threat emulation, where you are simulating an adversary's actions. With red teaming, you're not thinking about any specific domain like network or a single application or a phishing exercise--you're thinking about it holistically where all of the different tactics and techniques are combined to achieve an ultimate goal.

FIGURE 1



Common Issues with Penetration Tests

When it comes to assessments, common issues range from lack of qualification of the assessor and/or unfamiliarity with the tools, ego and/or a disregard for the business, proprietary TTPs, point-in-time assessments and misaligned objectives.

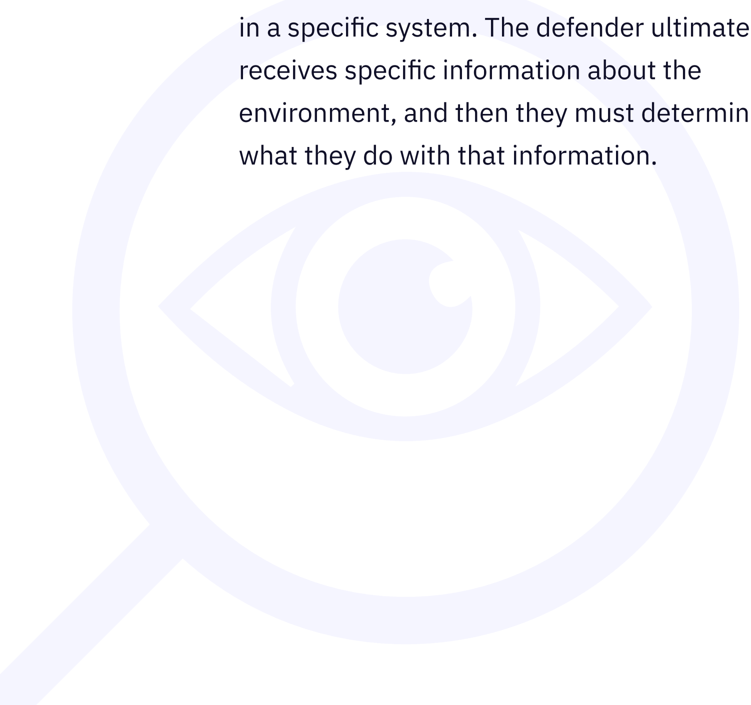
Some of these challenges are rooted in personality traits--let's be honest, we're an interesting bunch--while others require clear definitions from the outset. For example, if your goals are not aligned with those of the defenders or the consumers of the pen test, you will ultimately fail to provide them with the information they need to take appropriate next steps.

Ultimately, these all stem from the crucial issue of communication, which is vital to ensuring the effectiveness and value of performing a penetration test.

Examining Typical Approaches to Pen Testing

We'll divide the common approaches to pen testing into three different categories:

1. **Siloed Autonomous –** This is the traditional pen test, the point in time assessment, that's been performed for a decade or more. This style of pen testing is where the tester or pen test team is working alone and using information they can discover as well as their professional experience to poke holes in a specific system. The defender ultimately receives specific information about the environment, and then they must determine what they do with that information.



2. **Collaborative –** Also known as a purple team assessment where you're working shoulder to shoulder with the defenders (or nowadays using collaborative tools to work in this fashion, but from remote locations). This style is where the objectives are set by the defender, where information is shared freely and the test itself leverages the defender's knowledge. This is true alignment between the attacker and the defender.

3. **Continuous Style Assessment –** This is a newer concept of "as a service" that includes increased automation, tight integration between the attacker and defender, and a very agile process.

SILOED AUTOMATION

The Pros and Cons

PROS

This is the most popular penetration testing option, with some obvious benefits. This method allows for thinking about the current objective from the perspective of the business and/ or the security organization (i.e. if the goal is to tighten the defensive controls of a workstation).

This type of pen test also has a set of predefined expectations. When someone requests a penetration test either to be performed or to see the results, they're expecting a fairly monolithic PDF that has all of the results and the methodology.

CONS

The major con is that again, it's based on a point in time. When you perform a penetration test, especially an annual one, that's 365 days from when the initial assessment was conducted. So while you're examining how to address vulnerabilities that were detected, your entire environment may have gone through dramatic change over that year period. You're always playing catch-up.

It's also a very rigid approach without much if any communication and with very specific results on a specific objective. Of course, the attacker in this scenario can be adaptive, where they're trying to look at different vulnerabilities in different ways. However, it's very much like winding up the toy and letting it go...it's just going to continue in that direction. This is common in a siloed assessment.

COLLABORATIVE

The Pros and Cons

PROS

Collaborative assessments are where the attackers are able to be deeply embedded with the defenders. This method allows for thinking about the current objective from the perspective of the business and/or the security organization. For example, if the goal is to tighten the defensive controls of a workstation, the organization might decide to deploy a new endpoint detection platform. As part of that research process, we're looking across multiple capabilities and multiple functions.

So before a pen test is conducted, we speak with the defenders and with the business to understand their objectives and then determine the proper test plan. The test plan should focus on achieving those identified objectives.

CONS

From there, we can iterate through those objectives in a very meaningful and specific way to ensure that the goals are hyper-focused to maximize that value.

Conversely, because the pen testers are closely integrated with the defenders during the assessment period (typically a week or two), it can disrupt regular day-to-day operations. Consider all of the tasks a defender has on a day-to-day basis--if they have to switch off from those tasks to communicate with the tester, they are losing efficiency with their standard operating procedures. There's a lot of information with a collaborative pen test and a lot of back and forth communication answering questions, talking about technology, or reconfiguring exploitation or vulnerabilities. While everyone's learning, you do have to invest that extra time.

So Which Pen Test is Right for You?

Autonomous or Collaborative?

The reality is that both approaches have value, as they can test incredible aspects based on findings from Open Source Intelligence. They allow you to conduct a real-world assessment of the detection threshold for your external monitoring and alerting systems.

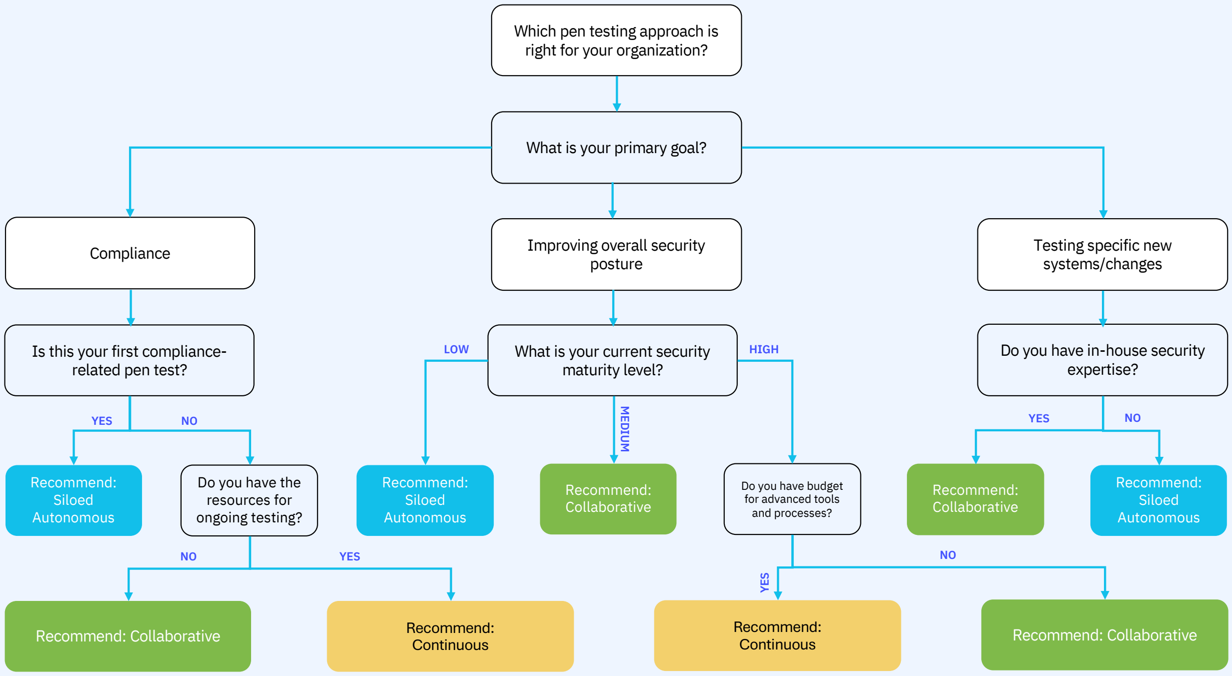
Maybe you have an Managed Security Service Provider (MSSP) that you rely on for security monitoring and you want to keep them honest. By doing this, you may put the internal teams at odds with one another. Collaborative assessments are the emerging way to maximize new value. The important aspect with a collaborative test is that it helps us start to understand and move towards that continuous aspect of assessments. So collaboration enables continuous assessments based off ensuring that those objectives are tightly aligned.

Examining Continuous Assessments

The lifecycle of a continuous assessment is enabled by a lot of the great automation platforms we're seeing emerging in this space. When considering a specific scope, environment, or infrastructure, we must initially approach it from a manual perspective. We're trusting humans, professionals, experience and expertise to understand:

- ✓ The vulnerabilities that are present - what are the avenues or attack paths
- ✓ How an attacker would process the information
- ✓ The Scope of the Assessment

As you get more comfortable with the environment, and as it becomes more baked and exercised, this whole process fits more seamlessly into the groove of normal business operations. The presumption is that it won't change much. From here we can start offloading or augmenting the manual testing with automated tools.


Which pen testing approach is right for your organization?
What is your primary goal?
Compliance
Improving overall security posture
Testing specific new systems/changes
Is this your first compliance-related pen test?
YES
NO
Recommend: Siloed Autonomous
Do you have the resources for ongoing testing?
NO
YES
Recommend: Collaborative
Recommend: Continuous
LOW
What is your current security maturity level?
HIGH
MEDIUM
Recommend: Siloed Autonomous
Recommend: Collaborative
Do you have budget for advanced tools and processes?
YES
NO
Recommend: Continuous
Recommend: Collaborative
Do you have in-house security expertise?
YES
NO
Recommend: Collaborative
Recommend: Siloed Autonomous

Breach and Attack Simulation (BAS)

Gartner introduced the term Breach and Attack Simulation (BAS) to help categorize various tools in this evolving space. BAS has significant potential to enhance the efforts of human penetration testers by automating repetitive or mundane tasks, thereby allowing experts to focus on more complex challenges.

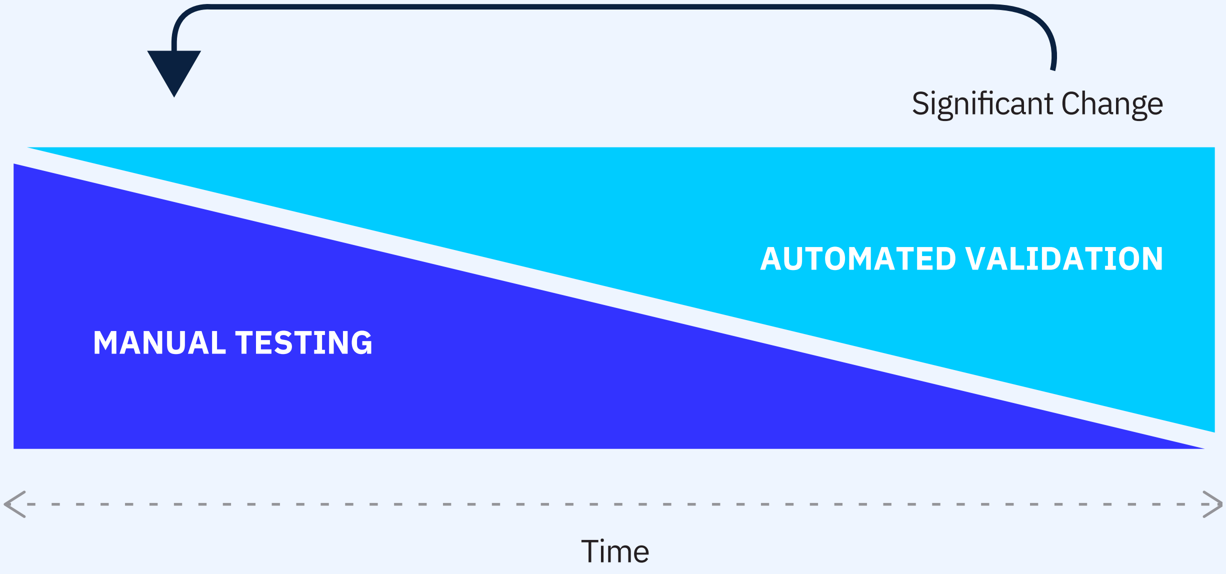
There's a great play here for both humans and automation to be able to work off each other, and maximize the value during an assessment.

As we move through time towards automated validation (Figure 2), we can streamline more processes as we understand more about the environment. If there is any change in that environment, such as a new system being deployed, then there needs to be a kickback to identify that change and recommend more manual testing for either that specific change or the system holistically.

This is how you would ultimately understand the overall impact of that change. It doesn't just need to be with the environment itself, as it could also be with a significant vulnerability that was only publicly released, or it could be with a new tactic or exploitation technique and existing vulnerability.

An example like this should be classified as a significant change and introduce additional manual testing until things stabilize. At this point, we can iterate back into higher levels of automation.

FIGURE 2: Continuous lifecycle that leverages both automation and manual testing



The Pros and Cons

PROS

The pros and cons of continuous pen testing, by definition are that it's always on. Additional pros are that you can maximize your budget by offloading the tediousness of some manual aspects of pen testing to automation, while also allowing those manual testers to focus on the things that only humans can do. Automation is used to give full tireless coverage of the hundreds, if not nearly thousands, of different avenues for an attacker to potentially exploit.

With continuous pen testing, there's this great idea of instant, zero-day feedback. Not too long ago, a large hospitality provider announced a large breach. Every other vendor in that industry should have been asking themselves or asked by others, how susceptible were they to that type of breach. BAS platforms can facilitate continuous assessments alongside human pen testers who can quickly leverage newly disclosed tactics, and then quickly give you a sense of how you're doing as an organization. You're very rapidly, if not instantaneously, gaining information to answer those questions. Since the assessments are continuous, you can also take snapshots to show trends over different periods of time as far as vulnerability detections. Regardless of the KPIs defensive teams measure, continuous pen testing is probably the most data-rich way to go.

CONS

1. **Your industry maturity level, or potentially lack thereof when it comes to this topic, is not insurmountable, but it does add complexity.** The adoption curve for BAS solutions is early stages, where organizations are beginning to investigate the technology and how best to integrate them into their existing defensive controls and processes. The integration alone can be challenging to figure out where the obstacles are, what things don't play well with each other, and so on.

2. **Complacency setting in is another potential con.** With more automation, there's more potential to let it run in the background and focus on other areas. This honestly goes beyond continuous assessment--complacency is an issue when it comes to the use of any security tool. With security staffs overloaded with work, the eye can easily move off of the ball, where you're not maximizing the value of the solution.

   For continuous assessments, we need to ensure that they're still actively reviewed, that there's feedback to improve the scope or the methodology, and that we're not left pen testing individual trees as opposed to the overall forest.

How to Plan for a Continuous Pen Test

Generally speaking, more mature security organizations (defensive teams that are used to working in an iterative way) are in a better position to take advantage of continuous, collaborative pen testing. When planning for continuous pen test, two things come to mind immediately:

1. **Set clear goals and objectives –** In order to truly maximize the value of a pen test, communication is critical. Set the common goals and objectives from those involved, and ensure the feedback during a test is instant. There has to be a method that allows the defenders and the attackers to communicate back and forth, and adjust as necessary.

2. **Ensure collaborative threat modeling –** This is a fundamental step that forms the basis for virtually any penetration test. In a siloed, or autonomous assessment, the red team must conduct the threat model themselves to understand what they can find about an organization and then pair that with what they know. To do that threat modeling in a collaborative or continuous assessment, it's important to leverage the experience and expertise of the defending team, which knows the crown jewels--what is critical and core to the business that those attackers are trying access. The most effective threat modeling is when the red and blue teams are working together to understand both perspectives.

Conclusion

We've examined the three primary types of penetration testing to help you determine which approach best suits your organization's needs. Ideally, you will continue to mature your security program and process and as part of that explore how to gain more value out of your penetration testing efforts.

As mentioned earlier, the most effective penetration test assessments combine both manual human elements and automated technologies. Take the MITRE ATT&CK framework, for instance; it encompasses hundreds of different aspects that need to be addressed and is widely adopted as a standard by many organizations.

Pen testers, constrained by time and budget, find it challenging to cover all the various components within the typically narrow parameters they are given. Leveraging, for example, a vulnerability assessment solution to help with that through automation is a more feasible way to perform the test in the time allotted. \

By extension, BAS solutions can similarly extend the reach of human pen testers to be more effective and thorough.

To maximize the value of your penetration test, it's critical to foster collaboration between offensive and defensive teams, set clear and holistic goals, and identify tasks that can be automated versus those requiring manual effort.

ABOUT THE AUTHOR

Victor Wieczorek

Victor Wieczorek, Vice President, is an information security professional with a broad range of experience in both defensive and offensive security roles. His prior work included delivering various security projects to a wide spectrum of clients with a primary focus on penetration testing, vulnerability assessments, and security architecture design. As a penetration tester holding both the Offensive Security Certified Expert (OSCE) and Offensive Security Certified Professional (OSCP) certifications, he has helped organizations identify a multitude of weaknesses with a focus on root cause remediation.

Before joining GuidePoint Security, Victor consulted for a global firm where he worked to mature and standardize their security assessment practice while leading various penetration testing engagements. Before that, he was a Systems Security Engineer focused on secure architecture design for multiple federal organizations. Victor has developed skills in effective communication with client stakeholders to detail security issues, illustrate business impacts, and consult on remediation efforts.

Victor holds a Bachelor's degree in Computer and Information Technology from Purdue University, as well as multiple professional industry certifications including Certified Information Systems Security Professional (CISSP), Payment Card Industry Qualified Security Assessor (PCI QSA), and Certified Information Systems Auditor (CISA).

GUIDEPOINT®
SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132