Cobalt
Pen Testing as a Service

3 Signs It's Time to Rethink Your PCI Pen Testing Strategy

The Payment Card Industry (PCI) security standard encompasses a set of technical and operational security requirements for all organizations that handle payment transactions and also extends to software developers and manufacturers of the applications and devices used for payment processing. Touching just about any company involved in payment processing, PCI is one of the most recognizable, and arguably influential, standards impacting data security.

PCI's origins date back to the early 2000s when it became clear that the emergence of online shopping also came with significant and costly increases in credit card fraud. Significant losses and limited success in their individual efforts to stem them led the major credit card issuers to unify existing security guidance under a single, mandatory standard. The first version of the PCI standard debuted in late 2004 and it has been maintained and updated by the PCI Council as both payment technologies and attacks against them have evolved.

Given it is one of the more mature security standards, many companies have significant experience in managing PCI compliance programs. Even companies new to payment processing, and thus, PCI, have a good deal of guidance to help drive the development of their compliance programs. In fact, many companies have streamlined a number of PCI's security and reporting requirements through automation.

However, one area that continues to challenge is the PCI penetration testing requirement (requirement 11.3). Unlike vulnerability scanning, which can be fully automated, pen testing relies on skilled researchers to perform manual testing and can take a fairly significant effort. The latest version of the standard, PCI DSS 3.2, specifies that pen testing should be based on industry-accepted approaches and cover the entire Cardholder Data Environment (CDE) using testing from both inside and outside the network. Some companies may use network segmentation to essentially "wall off" the CDE, which does reduce the required scope of testing. However, penetration testing of the segmentation strategy will still be required. Companies must perform both internal and external penetration at least annually, and also test after any significant upgrades or changes to the technology environment that might impact the security of cardholder data. Further, exploitable vulnerabilities found must be fixed and re-tested to confirm remediation.

The inclusion of penetration testing in the PCI standards is a direct reflection of its value in network defense. Manual testing by skilled researchers is the best way to simulate a real-world attack and see how far into the network an adversary can get and what information they can compromise. This helps security teams understand their exposure and bolster their defense. Yet, despite the well-understood value of penetration testing, it remains one of the more challenging PCI requirements to implement.

However, while penetration testing will always require more effort than automated scanning, it need not overwhelm your security team or distract from other priority efforts. In fact, if you are experiencing any of the following three effects when you schedule your PCI penetration test, it is time to take action:

1. A noticeable sense of dread overtakes the office

Does a gray cloud descend over the office when it is time to perform a PCI-mandated pen test? Done well, pen testing can take a fair amount of effort. This can include defining the scope and educating testers on the systems, supporting and monitoring researchers and network performance during testing, and handling post-test remediation, retesting and reporting. Often this involves working with an expensive team of consultants or redirecting internal security researchers to ensure a PCI-compliant test.

Penetration testing should take effort, but it should not be painful. Unfortunately, despite its flaws, the delivery model for penetration testing had remained largely unchanged over the past decade. Finding skilled testers, both as employees or consultants, is the first challenge. Once you've found them, getting them up-to-speed on your testing requirements, risk assessment and network architecture is a time-consuming process that needs to be repeated every time you bring in a new tester.

Further, even when you and the tester have performed due diligence, issues arise during testing that you often don't learn about until presented with the final vulnerability report. These can include wasted time testing a threat model that does not apply or creating an overwhelming number of individual vulnerability reports for a pervasive issue that could have been better addressed at the architectural level. Further, though most testers are able to conduct testing without creating adverse system effects, sometimes unforeseen issues can occur such as application instability. These can be easily addressed, but any lag in communication between the testing team and devops can create headaches.

Cobalt is different. We've modernized the delivery model for penetration testing to support your needs every step of the way. We match you with the right testers for your application stack and provide you with a platform that allows real-time monitoring and reporting on the testing effort. You can flag any scope issues as soon as they arise, be immediately alerted to any testing or network issues during the testing process, and add comments or notes as the tests progresses to help support the researchers and ensure the final product meets your needs. Everything is captured on the platform simplifying both the reporting and remediation needs, and streamlining future tests by Cobalt even if the researchers themselves change. After the test, you can collaborate directly with the security researchers on fixing the vulnerabilities and re-testing - and give the overall penetration test a quality rating. From the initiation of the engagement to final reporting, the Cobalt pen testing process is transparent, collaborative, and efficient which helps make fulfilling PCI pen testing requirements as easy as possible.

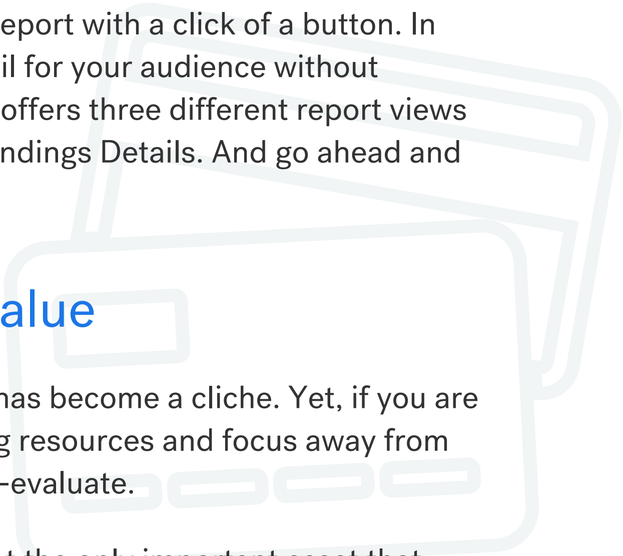
2. You're having to stock up on printer paper

Okay, maybe you've moved beyond actually printing reports. But lengthy, static PDF reports prepared by expensive consultants with long lists of vulnerabilities and descriptions are still all too common deliverables from pen testing teams. Working through test results begins with a lengthy read-out call with the testing provider, and then companies are essentially left on their own to prioritize remediation, report findings to management and other stakeholders, and communicate needs to the development team, usually via emails and more conference calls. They also have to track remediation process and ensure re-testing is completed and documented. This process is time-consuming at best, and confusing and cumbersome at worst.

If this has been your experience, it is time to modernize your penetration testing workflow. Cobalt's penetration testing-as-a-service enables real-time reporting via a modern application security platform that supports a complete find-to-fix workflow. Cobalt delivers all its findings clearly and concisely with integrated messaging to allow you to ask questions throughout the process.

Our platform integrates with GitHub + JIRA to allow you to send issues to your development team with a simple click. All activity is automatically tracked so you can check in at any time to monitor progress and resolve issues.

And don’t worry, you can still create a PCI-compliant report with a click of a button. In fact, you can create reports with the right level of detail for your audience without spending time cutting, pasting, and re-writing. Cobalt offers three different report views including Attestation, Full Report, and Full Report + Findings Details. And go ahead and print them too, if you’d like.



3. Checking the box is the only value

The concept that compliance does not equal security has become a cliche. Yet, if you are feeling that your compliance program is actually taking resources and focus away from your most effective security operations, it is time to re-evaluate.

While securing cardholder data is a clear priority, is not the only important asset that security teams need to consider. Intellectual property, employee information, and financial data are just some examples of other assets that may be at risk from attack vectors entirely unrelated to your PCI compliance efforts.

PCI and other required standards often receive a greater focus from management and higher budget priority than other necessary, but not mandated, security efforts. Security teams have long struggled to create a balance between the needs of various stakeholders, compliance requirements, and risk-driven security requirements. A less cumbersome, more streamlined PCI security program and reporting strategy is the best way to ensure this balance and avoid distraction.

If the penetration testing requirement of your PCI program is feeling more like a means to check a box then a valuable part of your security program, then it is time to modernize your testing process and rethink your pen testing mindset.

Contact Cobalt today to learn more about how its innovative penetration testing delivery model and transparent, collaborative, and efficient find-to-fix workflow can help you address your most pressing PCI penetration testing challenges.

Visit Cobalt.io to learn more about our Pen Testing as a Service Platform