

PLEXTRAC EBOOK

Fast Track Continuous Validation

Pave the way to fast, iterative cycles of testing and validation and avoid common roadblocks with workflow automation.



Fast-track to
continuous
validation with
PlexTrac



Harness
repeatable
test plans

Prioritize findings
from proactive
security data
sources

Implement
closed-loop
remediation



Eliminate Threat
Recurrence

Demonstrate
impact on
security
posture


Auto-deliver
findings to
ticketing systems

Introduction

When's the last time you reviewed your security assessment and testing cadence? Chances are, it's been a while. Oftentimes single pentests or vulnerability scans are conducted at a fixed point in time. The results are valuable, but – since the tests are planned – they don't account for business as usual or new high-risk issues.

Assessing continuously, along with your point-in-time tests, provides a more thorough analysis of a security posture. By testing a system or network regularly, you can identify and address vulnerabilities rapidly and assess the effectiveness of security measures. Many would argue that this concept of continuous assessment and validation is the way forward for organizations seeking to truly guard against omnipresent cyber threats. But, like all testing methods, achieving true continuous validation comes with its share of roadblocks.

Continue reading for tips on navigating the most common obstacles and fool-proof methods for fast-tracking your continuous validation strategy.



“ Adequately used continuous security validation – ideally with an extended security posture management approach – not only throws light on hidden gaps in the security posture but can also provide quantified measurements invaluable when talking with executives about cybersecurity risks instead of best guesstimates.”

– “Seeing The Unseen: The Core Merit Of Continuous Security Validation,”
Avihai Ben-Yossef, [Forbes](#)

“ While testing security controls in a traditional way could serve its intended purposes, the company should not feel secure solely based on traditional point-in-time control testing. The reality is that threats and an organization’s systems change on a daily basis, and a traditional control test that was effective yesterday may no longer be effective in mitigating a threat today ... The only effective way to combat this is to think and act like an adversary.”

– Berk Algan, CISA, CGEIT, CRISC, CIPP, [ISACA](#)

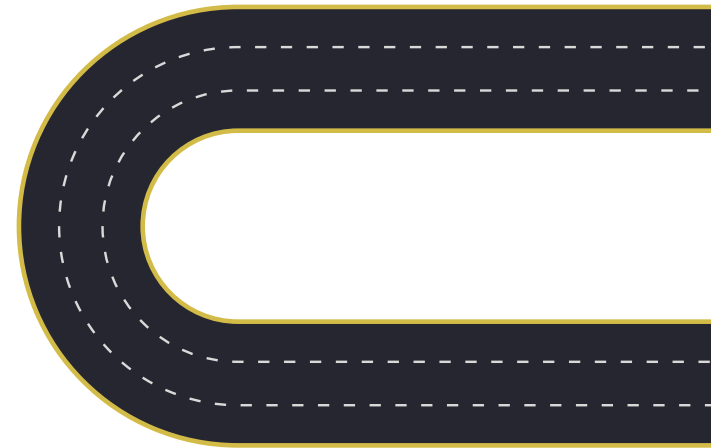
Contents

It's Time to Add Continuous Validation to Your Roadmap	6
The Road to True Continuous Validation Is Rocky – But Worthwhile	7
Overcome Roadblocks	8
Harness Repeatable Test Plans	8
Threat-Informed Pentesting	8
Frameworks and Standards	9
Prioritize Findings From Proactive Security Data Sources	10
Auto-Deliver Findings to Ticketing Systems	11
Real-Time Collaboration	11
Automated Ticketing	12
Implement Closed-Loop Remediation	12
Demonstrate Impact on Security Posture	13
Move Into the Fast Lane With Workflow Automation	14
Shrink Cycle Time With Improved Efficiency	14
Eliminate Threat Recurrence	15

It's Time to Add Continuous Validation to Your Roadmap

The traditional paradigm of annual, point-in-time assessments, is no longer **sufficient to stay ahead of threats**. To maintain the integrity of systems and data, you need to embrace a proactive approach – one that is continuous, dynamic, and adaptable.

A continuous validation strategy helps you move away from a reactive stance by leveraging proactive strategies to testing, fixing, and validating.



The Road to True Continuous Validation Is Rocky – But Worthwhile

Although it's easy to recognize the increasing complexity and sophistication of the threats and even the pressing need to adopt a new strategy, it's difficult to respond at the pace that bad actors take in employing new tactics, techniques, and technologies.

Enacting an organized program of short, iterative cycles of targeted testing and retesting of security controls is the way forward. But achieving this kind of systematic continuous assessment and validation is hard no matter the tools, service, expertise, or resources invested.

That's not to say that it's impossible or that the skills of the good guys and the tools available aren't getting better and better, but change is hard and often expensive. Automation is critical to stretch available resources and expedite processes.

Pentesting-as-a-service (PTaaS) platforms, breach and attack simulation (BAS) tools, and vulnerability scanners are all important and rapidly evolving automation solutions that can begin to bridge the gap between more traditional, less frequent penetration tests, for example. But many teams who have invested in technology to support their attempts at implementing continuous validation are still struggling to close the loop, particularly in the first and last miles.

You might be asking yourself, "Why is it so difficult?" It's not the tools or the people that make achieving true continuous validation cycles so challenging. Rather, the problem is the workflow itself – synchronizing all the moving parts so the engine runs smoothly.

Overcome Roadblocks

The key to unlocking the power of continuous validation and realizing the full value of investments in tooling and testing is a multifaceted approach that leverages a workflow automation solution to:

- Manage collaboration
- Collate data
- Prioritize findings
- Track remediation
- Trigger retesting
- Measure progress

When these processes are managed manually, they impede and slow the cycle. And a cycle that takes too long to complete isn't really continuous.

Harness Repeatable Test Plans

Trouble often starts when determining what to test and how. You might ask yourself, “Where do I even start?”

A systematic approach to planning based on industry best practices is essential. You likely have a sense of your most critical vulnerabilities from traditional testing, but validating those findings can be overwhelming — let alone doing this quickly and repeatedly. The key is to start *somewhere*.



Threat-Informed Pentesting

Threat-informed pentesting (TIP) is an approach to an offensive security strategy that leverages global threat intelligence about specific emerging adversaries to safely test those exact tactics and techniques on your environment. TIP offers a roadmap for short, iterate

testing cycles that ensure your organization is prepared for the attacks bad actors are really using. Building a robust cybersecurity program on a foundation of continuous assessment is possible for teams of all sizes and resources when you leverage threat intelligence as the foundation of your strategy.

“

Organizations need to put a much greater emphasis on continuous pentesting and validation of remediation from known risks, particularly using threat intelligence to inform test plans and activities both from your internal engagements as well as third party pentests.”

— PlexTrac Founder and CTO Dan DeCloss,
OSCP, CISSP

Frameworks and Standards

Not only is industry threat intelligence useful for guiding the direction of a continuous validation strategy, but so are the standards and frameworks based on that intelligence, including NIST, MITRE ATT&CK, ISO 27001, CMMC, PCI-DSS, among others.

Frameworks and standards can direct you on what to look for and what to test against. Berk Algan, in an article for [ISACA](#), states, “In its simplest form, an organization could pick a relevant attack vector (e.g., exfiltration over alternative protocol) from the ATT&CK Matrix and test its cyber defenses to validate that it could withstand that particular attack. They can then review and prioritize mitigation of identified gaps.”

Once you start testing, challenges still remain. How do you use those existing matrices or your own test plans systematically and repeatedly to validate? This is where workflow automation can bridge the gap.

A repository to catalog playbooks and a platform to collaborate on test execution, documentation, and remediation tracking can harness the power of test plan resources and make them systematically repeatable.

Prioritize Findings From Proactive Security Data Sources

Findings from proactive security data sources are a key component of any continuous validation strategy. But when your team is faced with a mountain of data from disparate sources – including your own testing activities, outsourced services, and a variety of tools like vulnerability scanners, PTaaS, and BAS solutions – managing the data produced from all proactive security sources can be a blocker. It takes time and expert analysis to make the most significant findings actionable so they can be passed on for remediation and validation.

The answer is a solution to ingest manual and automated data sources so they can be aggregated, analyzed, and prioritized with significantly less manual effort from your highly-skilled professionals. PlexTrac used as a proactive security workflow automation platform does just that.

“

Continuous security validation’s offensive testing components shine a bright light on the shadowy paths a cyberattacker could exploit to wreak havoc on your environment or stealthily loot your data, IP or other crown jewel and sneak out with the booty. Whether relying on basic; comprehensive; or advanced sets of security validation tools, offensive testing is a way to enter the mind of potential attackers; impersonate them; and, through running production-safe attacks, see precisely how many critical gaps are open to exploit and how far an intruder could travel within the environment.”

— Avihai Ben-Yossef, [Forbes](#)

Auto-Deliver Findings to Ticketing Systems

Much like collating data from proactive security sources, moving key findings through to rapid remediation is another bottleneck on the road to continuous validation. Siloed teams, processes, and tooling creates inefficient and ineffective hand-offs when it's time to remediate, reconfigure, or address the results of the offensive testing.

**NO EFFECTIVE WAY
to prioritize or
create tickets**

The problem is twofold. First, visibility into the offensive testing activities is lacking for the

defensive team who will ultimately have to fix the findings. Second, actioning the findings by creating, assigning, and tracking them to closure is a painfully manual process for most teams.

Real-Time Collaboration

Many teams struggle not with performing offensive testing but rather with communicating the result in an effective way. Static reports, whether from internal teams or external service providers, are onerous to work with and leave context gaps for those tasked with remediating.

Cross-team collaboration, preferably during the testing phase, can provide visibility into what to fix and how to fix it. “Collaboration across all teams, both offensive and defensive, is critical to ensure that organizations stay focused on resolving their most critical vulnerabilities. Organizations that focus on collaborative exercises through purple teaming and adversarial simulation are improving their security posture faster and with greater visibility,” said Dan DeCloss, Founder/CTO of PlexTrac, Inc.

Better collaboration between offensive and defensive teams is another area where workflow automation can make an exponential difference. PlexTrac Runbooks is a feature designed to facilitate collaboration between teams from test planning to execution to remediation tracking. When all team members have visibility into the issues, they are able to resolve them faster with less back-and-forth communication.

Automated Ticketing

Regardless of where your offensive findings are coming from, making them actionable for remediation is a sticking point. But it doesn't have to be. Workflow automation can ease this pain point with internal ticketing capabilities and integrations with key ticketing systems already used by the defenders – systems like Jira and ServiceNow. Streamline the full process with one platform to manage data, facilitate collaborative exercises, and deliver findings to ticketing systems. With PlexTrac you can automatically deliver findings – with

key information like evidence and criticality scoring attached – into the preferred ticketing platform and assign tickets to specific analysts for remediation. By eliminating the work of manually creating tickets from static PDFs or Word documents, remediation can begin immediately.

Implement Closed-Loop Remediation

In its simplest form, closed-loop remediation is reporting the completed tickets back to the testing source for validation. It may seem obvious that this reverse hand-off is necessary to achieve continuous validation, but, again, this point in the cycle is often blocked by technology.

The tools and technologies preferred by offensive and defensive teams are very different and don't automatically communicate. Historically these teams



are siloed so, like the process for creating tickets, the process for communicating when tickets are closed is also manual. This lack of remediation tracking creates another inefficiency that can slow or halt continuous validation efforts.

Automating remediation tracking creates the appropriate triggers to keep the cycle flowing. With notifications for closed tickets occurring automatically, offensive teams can more quickly retest to validate the effectiveness of the fix and move on to the next cycle.

Demonstrate Impact on Security Posture

In addition to the value derived from continuous validation on improved security posture is the visibility it provides. The results of traditional point-in-time pentests delivered via a static report are valuable for compliance but the results are outdated almost

immediately. Measuring – and demonstrating to organizational leaders – progress in real-time is only possible with continuous assessment and validation.

Continuous validation cycles allow for targeted testing based on specific threat vectors.

Programs with processes for continuous validation in place

are agile enough to quickly assess their vulnerability to the latest zero-day making headlines, for example. Not only that, they can apply regression testing techniques to their offensive security practice by constantly retesting to identify any vulnerabilities that crop up due to changes in the environment.

All these benefits make attestation to leadership much easier ... if you can consolidate and easily report on the results. Providing documentation, particularly in a form less technical stakeholders like board members or executive leaders can easily understand, is still a



sticking point. PlexTrac solves for this with robust reporting automation that enables practitioners to rapidly create reports tailored to the needs of a variety of audiences. Additionally, analytics provided within the platform and visualizations offer instant insight into progress over time.



Adequately used continuous security validation – ideally with an extended security posture management approach – not only throws light on hidden gaps in the security posture but can also provide quantified measurements invaluable when talking with executives about cybersecurity risks instead of best guesstimates.”

— Ben-Yossef, [Forbes](#)

Move Into the Fast Lane With Workflow Automation

[Gartner](#) predicts that by 2025, 70 percent of organizations will implement automation for flexibility and efficiency. This is not a surprising statistic. The trouble is that automating proactive security efforts is only half the battle. PTaaS, BAS, and continuous validation solutions can effectively supplement traditional pentesting and assessment for more consistent and targeted testing; however, only leveraging these solutions isn't enough to close the loop and achieve continuous validation.

Shrink Cycle Time With Improved Efficiency

Automation in the testing phase is not enough because teams lack the resources to efficiently manage the data

produced at a speed that can constitute a “continuous” cycle. In fact, oftentimes only one type of offensive assessment is used to achieve continuous validation. As more proactive tools are added to the mix, it becomes more difficult and cycles take longer to complete.

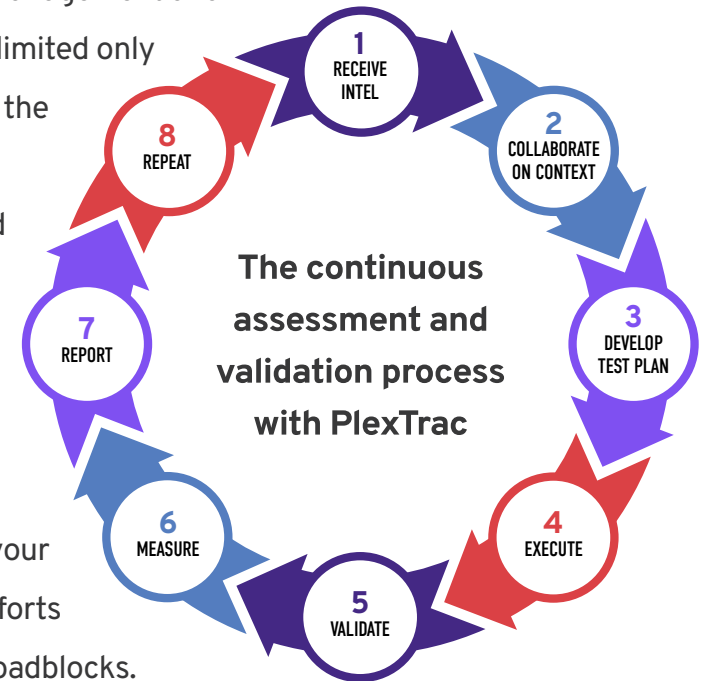
PlexTrac automates and consolidates the entire workflow to dramatically improve efficiency and effectiveness and significantly reduce cycle times – helping teams realize full value from their investments and make measurable progress.

Eliminate Threat Recurrence

At the end of the day, continuous validation exists to ensure that proactive efforts are, and remain, effective despite an ever-changing environment. Short iterative cycles not only help cover a wider attack surface but also prevent recurring vulnerabilities that are all too common in traditional security strategy.

[NIST Special Publication 800-137](#) on continuous monitoring states, “The end result [of information security continuous monitoring] is improved organization-wide risk management and continual improvement limited only by the speed with which the organization can collect information and respond to findings.”

Automating and managing the complete security life cycle with PlexTrac will fast-track your continuous validation efforts by removing workflow roadblocks.



Are you ready to shift into high gear?

Let us help you conquer the last mile of continuous validation.

REQUEST A DEMO TODAY



PlexTrac is the premier penetration test reporting, collaboration, and management platform designed to automate planning, documentation, communication, and remediation tracking, allowing service providers to enhance margins and client outcomes and enterprises to demonstrate the value of internal pentesting efforts and improved security posture.

www.plextrac.com © 2023 PlexTrac, Inc., all rights reserved.