KROLL

An Introduction to Agile Penetration Testing

Practice Leaders

Rahul Raghavan

Rob Deane

When it comes to modern application delivery, speed and agility are the name of the game. Customer demands are driving rapid release cycles, pushing development teams to create new products and to update existing ones at a much more aggressive pace.

One may ask, “what is driving this accelerated activity?” High-profile supply chain attacks, increased compliance requirements and customer/end user expectations have all contributed to increased scrutiny on an organization’s ability to release secure-by-default versions of their product. Today, an organization’s ability to effectively demonstrate their strategic application or product security vision is a critical path to earning the trust of their prospects and customers.

Why Point-in-Time Assessments Don’t Work Well for Rapid Development Cycles

Adapting to a dynamic state of software development is difficult for organizations to achieve for several reasons. In addition to ever-more-rapid release cycles, application delivery is contending with adjustments to contemporary technology stacks, varying development styles and the inherent challenges associated with coordinating multiple teams involved in product engineering.

These challenges manifest themselves in different ways depending on the organization. For example, legacy enterprise applications may require limited changes to code or fewer new releases compared to a pure-play Software-as-a-Service (SaaS) platform in the same amount of time. Alternately, organizations that create technology products (like SaaS platforms) may have far fewer applications in development but large deployment frequencies—sometimes releasing and updating multiple times per day.

The goal of security assessments, and of an application security program in general, is to ensure that every product release delivered to the end user has been validated for appropriate risks. In the past, when release cycles tended to be more drawn out, security assessments, such as pen testing, were performed on a “point-in-time” basis prior to release—in a vacuum. But with the acceleration of software development, application security finds itself shifting further left in the process, which means testing needs to be integrated throughout the development life cycle so that the product reaching the customer is delivered with a high degree of confidence stemming from proper validation.

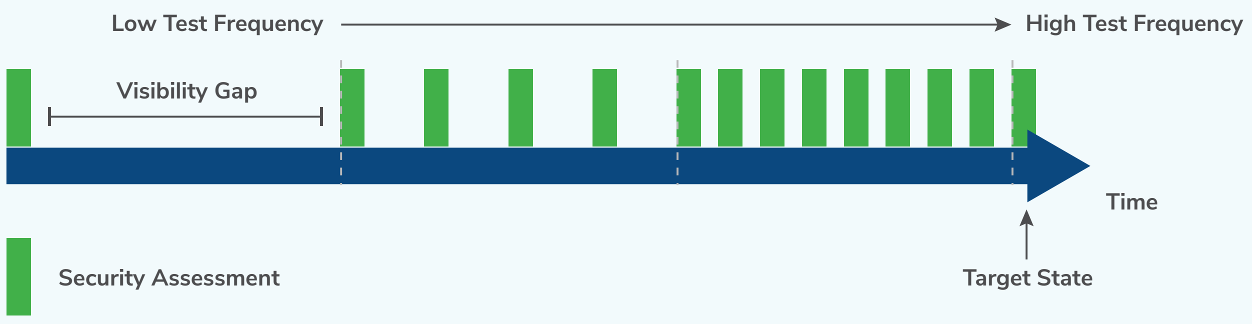
That said, the need to make the application development process more flexible, nimble and collaborative has never been more important, and these changes have led many software development teams to embrace agile methodologies. According to the 15th Annual State Of Agile Report, there has been “significant growth in agile adoption within software development teams, increasing from 37% in 2020 to 86% in 2021.” In addition, 52% of respondents said that either a majority or all their company’s teams have adopted an agile approach.

What Is Agile Penetration Testing and Why Is It Important?

There are several functional approaches to secure software development, each with its own benefits. Within this cadre, agile penetration testing provides a systematic way of including and prioritizing security assessments within every development sprint. Agile pen testing is **not** about performing faster pen tests or only about increasing pen testing frequency. Instead, it’s differentiating advantage centers on security assessments being performed in a programmatic way as close to release cycles as possible. As a result, product teams can verify the security of new product releases on an ongoing basis.

In essence, agile penetration testing is an application security risk mitigation activity designed to ensure that changes to an application or product are validated from a technical security perspective. The scope of an agile pen test within a sprint can be anything ranging from a code walkthrough, architecture review, SAST/SCA scans, a formal penetration test or any combination of these activities. The activity to be performed is dictated by the criticality of the change and the overall impact to the security posture of the application.

When you think about the frequency and speed of releases, the need for a continuous, integrated approach becomes apparent. For example, if your penetration testing schedule only factors one test every six to 12 months, there’s a good chance you’re releasing code into production that hasn’t been thoroughly tested. Agile penetration testing works into your release schedule to make sure most, if not every, release is evaluated before it reaches the customer.



The status quo for typical security assessment cadences has a wide visibility gap. As an agile pen testing program is implemented, the visibility gaps narrow over time.

The result of an agile pen testing approach? Increased secure-product throughput! Every new release has the potential to expose the user to risk and agile penetration testing offers a solution to the question of speed and security within agile development.

The Benefits of Agile Penetration Testing: Efficiency, Flexibility and a More Secure Product

Ultimately, the bottom-line benefit of an agile penetration testing program is that the number of unvalidated releases being pushed to production decreases dramatically. Threat actors are persistent and will eagerly find flaws in code that they can exploit. The 2020 SolarWinds attack was a notable example because it led to a U.S. presidential executive order dictating increased security precautions for software supply chain security, and Congress is also debating bills that will require increased coordination on cybersecurity initiatives between federal, state and local governments, as well as building a federal supply chain security training program.

Regulatory action in addition to the growing concern from customers about the security of the products they trust leads to the need for a way to continuously test and remediate vulnerabilities. Agile penetration testing is setting the stage to address those concerns and needs.

- Agile penetration testing increases the overall product or software security posture at an organization. An agile penetration testing program lays the foundation for a more mature security program and the ability to shift application security even further upstream.
- Investing in agile pen testing leads to increased awareness, skills and capabilities in application security for product engineering teams through consistent engagement with the program. Ongoing collaboration with a provider leads to developer familiarity with the assessment process and secure development practices, leading to more proactive security efforts.
- Ongoing testing and review of security findings enable your team to find patterns in vulnerabilities, assess what worked and what did not and fine tune your model and process, thus resulting in passive security skill enhancement for your product teams.

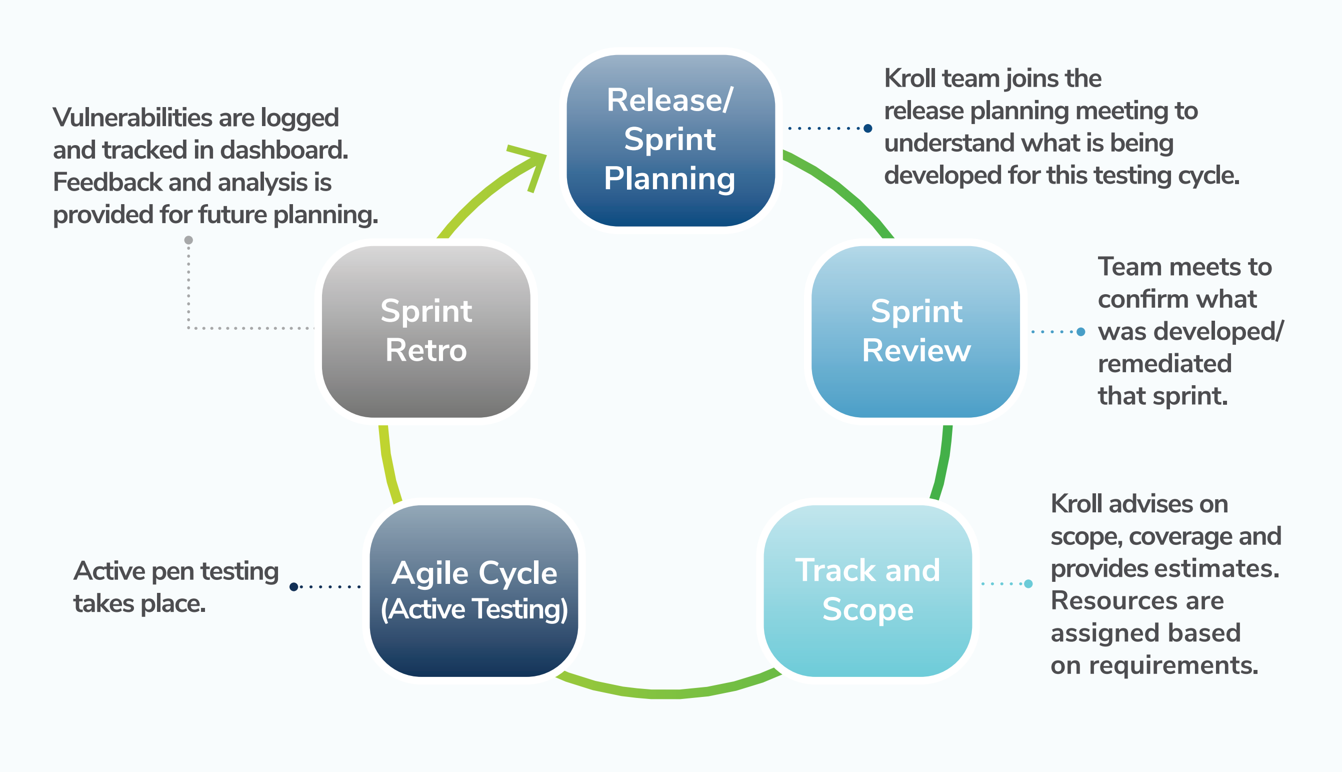
What Does an Agile Penetration Testing Program Look Like?

Agile software development programs are common among app development teams, but penetration testing largely remains an activity performed apart from the product release schedule. An agile, or continuous, testing approach that is seamlessly incorporated into your software development life cycle, will reduce the amount of time between product updates and security assessments to ensure that an application does not go live with unidentified risks.

Let's get into what an agile pen testing program looks like in practice.

The Agile Assessment Life Cycle

A view into a standard deployment of the agile penetration testing program.



Kroll team joins the release planning meeting to understand what is being developed for this testing cycle.

Team meets to confirm what was developed/ remediated that sprint.

Kroll advises on scope, coverage and provides estimates. Resources are assigned based on requirements.

Active pen testing takes place.

Vulnerabilities are logged and tracked in dashboard. Feedback and analysis is provided for future planning.

Team Structure

The foundation of an impactful agile pen testing program is built upon appsec *domain expertise and effective program management*. A good appsec service provider will assign a technical program manager (TPM), lead technical consultant (LC) and additional consultants specializing in specific areas.

The TPM is a security project manager who has a firm grasp of product management. The TPM should engage closely with your product management team to understand the product, your team structure, your release schedule and any pressing needs to address immediately.

The lead consultant (LC) is an appsec subject matter expert who supports the TPM. It should be the LC's primary aim to understand your application or product's security posture, the tools you have, your product architecture, your technology stack and any other information needed to build a successful agile pen testing program.

Making Strategic Decisions

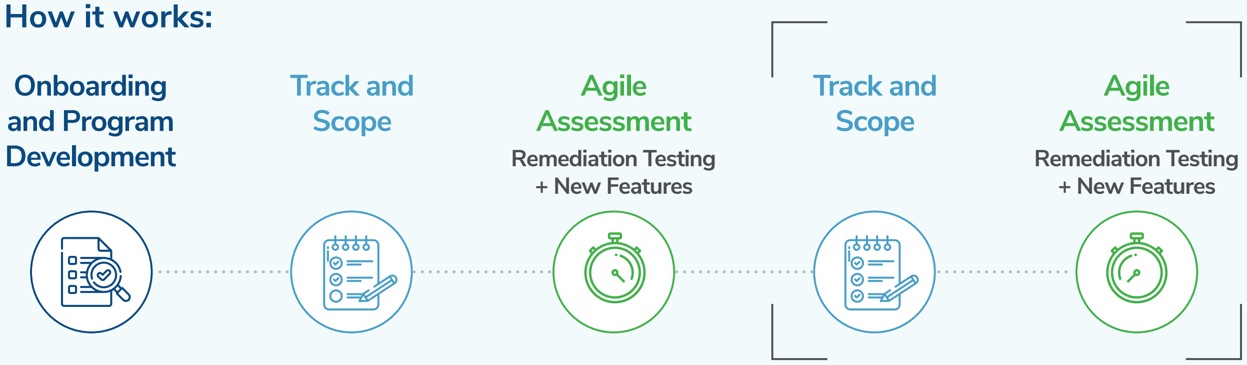
While pen testing is naturally at the heart of an agile penetration testing program, the LC and TPM should prioritize assessments and the appropriate level of validation required for each release. A customized security prioritization matrix is designed that prescribes the nature and the depth of assessment mandated for a specific release. For example, a minor user interface change might not require the same kind of security assessment as the replacement of an existing microservice. Since each assessment is tailored to the specific needs of each respective release, not every release may require a full-fledged pen test.

The core of such a program is in building upon technology and processes to replicate and scale success. For example, the provider might use available SAST/SCA or DAST toolsets as part of the assessment program as required and defined by the prioritization matrix. Similarly, using engineering platforms such as Confluence to log abuse cases/threat models or bug trackers such as JIRA or Azure DevOps to log vulnerabilities or findings within the release cycle helps streamline the agile pen testing program as part of mainstream product engineering. By maintaining this dual focus in direct partnership with the customer's product team, the service provider becomes an extension of the internal team's skills and capabilities, rather than a replacement. This positions the service provider to scale involvement as needed, thus democratizing the assessments both internally and externally.

Moving Forward with Agile Penetration Testing

At Kroll, we believe that every product release, be it a minor bug fix or a major feature release, can and should be vetted from a security perspective. Kroll brings together our strengths in application security, security assessments and program management to make this possible.

How it works:



Onboarding and Program Development

Track and Scope

Agile Assessment

Remediation Testing + New Features

Track and Scope

Agile Assessment

Remediation Testing + New Features

These steps will be repeated as updates and changes are made to the software throughout product life cycle

An agile penetration testing program with Kroll consists of four key phases:

- **Onboarding and Program Development:** Your TPM and LC gather contextual knowledge of your organization and apps, security requirements, release cadence and cycles, to conduct roadmap planning.
- **Management:** During the track and scope phase, each test is carefully considered and managed by our team, including tracking frequency, priority and coverage, assigning resources and consistently monitoring progress.
- **Agile Assessments:** We conduct the relevant type and level of assessment of new features to identify underlying vulnerabilities in new versions of code.
- **Tracking and Reporting:** We provide detailed reports and recommendations tailored to your needs and the interests of key stakeholders, including vulnerability tracking and prioritization, remediation testing and tracking, budget and effort tracking, KPIs and metrics and trend analysis.

> **“Kroll’s agile penetration testing team has worked in the software development industry. The team understands the methodology behind software development and knows how to ask the right questions and integrate with clients’ processes.”**
>
> – Director of Cyber Risk at a banking and finance firm

Why Kroll?

- Our team conducts 100,000 hours of cybersecurity assessments every year and carries well over 100 security certifications encompassing offensive security, cloud, penetration testing, mobile and web testing.
- Senior team members have each spent decades working in cybersecurity and our award-winning penetration testers are certified to some of the highest global industry standards, including CHECK, CREST (CCT/CRT), and SANS (GIAC).
- Kroll boasts deep application security domain expertise across assessments, strategy and program implementation for clients across the globe.
- Our adaptive software security programming approach and methodology are backed by a dedicated team focused on continuous research and development.

For more information about agile penetration testing and how Kroll can help you release secure software continuously, contact us today.

Contact Us

KROLL

For the latest insights, threat intelligence, and analysis from Kroll check out kroll.com/cyberblog

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.