Cobalt

The ROI of Modern Pentesting

A metrics-based comparison of Pentest as a Service (PtaaS) and traditional consulting engagements

Table of Contents

Executive Summary

Security and software development professionals almost universally view pentesting (penetration testing) as a critical component of application and network security programs. However, few organizations can perform as much pentesting as they want or need due to limited budgets and inefficiencies (Callout Box 1 on page 4). Additionally, pentesting is a specialized field where demand far outstrips supply, so recruiting and retaining full-time pentesters on staff is very challenging.

The most common approach today is engaging a consulting firm with an IT practice to provide a pentesting team for a specific test project. These engagements provide valuable input, but security teams find them to be slow and expensive, particularly in today's SaaS-driven world where releases happen weekly – even daily.

Pentest as a Service (PtaaS) has emerged as a modern approach that supplies a platform to manage pentest projects and pentesters to perform the testing. The platform automates and standardizes many workflows for defining, scheduling, and tracking tests, matching pentesters to projects, exchanging information between pentesting, security, and development teams, and capturing and reporting test results. Also, PtaaS providers usually have access to a much larger global pool of experienced pentesters than traditional consulting firms.

But how can we measure the impact of PtaaS compared to traditional pentest consulting engagements? Does it allow organizations to start tests sooner or produce results faster? Does it reduce indirect costs? Does it improve security and lower risk? And how large is the ROI?

To answer these questions, we conducted in-depth interviews with a panel of six, seasoned security leaders in different organizations, who have commissioned services from both traditional consultancies and PtaaS providers. We described a common testing scenario and asked them to estimate metrics and outcomes related to time-to-results[1], costs, and security effectiveness.

According to these experts, PtaaS did the following for the **standard pentesting scenario:**

Reduced time-to-results by 50% compared to traditional consulting engagements,

with less than **39.2** elapsed days in the planning, scheduling, and reporting phase of projects.

Reduced management costs by 25%,

saving **$834** per test, and

direct fees by 56%,

saving **$22,900** per test.

Was rated moderately higher on

context and depth of analysis

and much higher on

fit with agile and DevOps, and ease of doing business.

[1] Defined as the time from initiating a pentesting engagement to receiving the test findings.

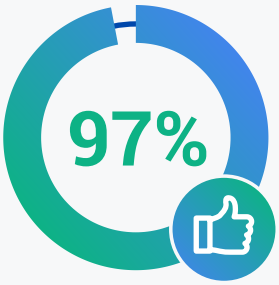
According to the panel, organizations that employ PtaaS enjoy business advantages that include:

- Being able to afford almost twice as many pentests with the same budget.
- Improving security by starting remediation on issues much sooner.
- Integrating pentesting into agile and DevOps application development processes.
- Enabling pentesting to be conducted on short notice for projects such as extra releases of applications, due diligence on potential acquisitions, and unexpected compliance audits.

This report outlines the research process used for the study and explores the results in detail. It also includes explanations from the experts on why PtaaS can provide significantly better results than traditional consulting engagements.

Survey: What is Driving PtaaS?*

Security professionals agree that pentesting **saves money and prevents breaches**

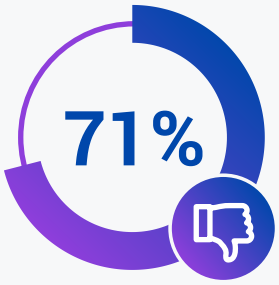


Agree that **pentesting saves their company money in the long run** by preventing security breaches and associated penalties

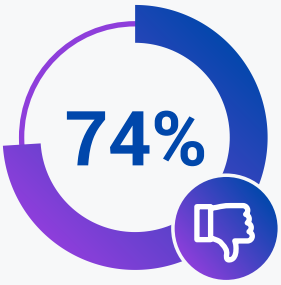
Say that pentesting helps their organization **build better security processes**, and believe that their company should allocate **more budget toward pentesting**

State that **pentest results provide valuable insights** their organization can use to improve developer and security team training

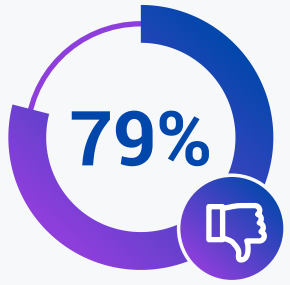
But **budgets and the inefficiencies** involved in traditional pentesting are **holding back its use**



Agree that **the cost of pentesting limits** the ability of their organization to test more frequently



Think that their organizations would test more frequently if the pentesting process was **more efficient or required less management**



Say that their department **loses valuable time** due to inefficiencies involved in the traditional pentesting format

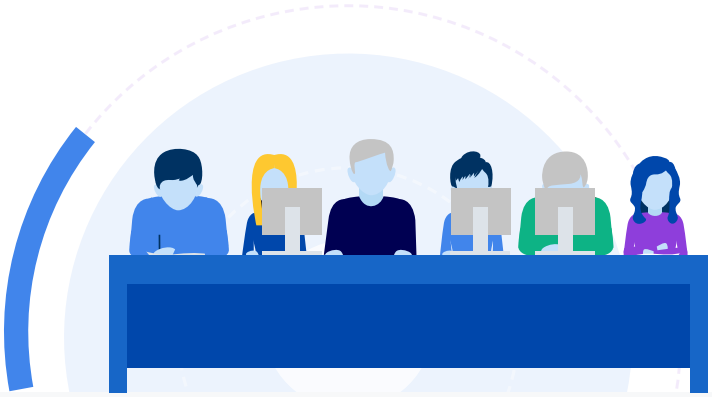
**In tandem with the expert interviews, Cobalt sponsored a survey of 600 IT security professionals in the U.S about the value of pentesting and attitudes toward traditional pentesting services.*

Comparing Consulting Engagements and PtaaS: Our Methodology

Our goal was to quantify and compare measures of value for two types of pentesting services: consulting engagements and PtaaS. Because few people have experience with both, we decided to hold in-depth discussions with a panel of security experts rather than conducting a broad-based survey.

The Expert Panel

For our panel, we identified six security experts who have worked with both types of pentesting services. They include Cobalt customers and Cobalt employees, all of whom have managed or participated in pentesting projects with consulting firms.



The panelists hold security leadership positions and have extensive experience with commissioning pentest services. They manage security programs in vastly different enterprises, such as:

A national marketplace for business catering that serves several thousands of restaurants and caterers.

A creator of an award-winning customer engagement platform used by more than 2,000 global enterprise brands and agencies.

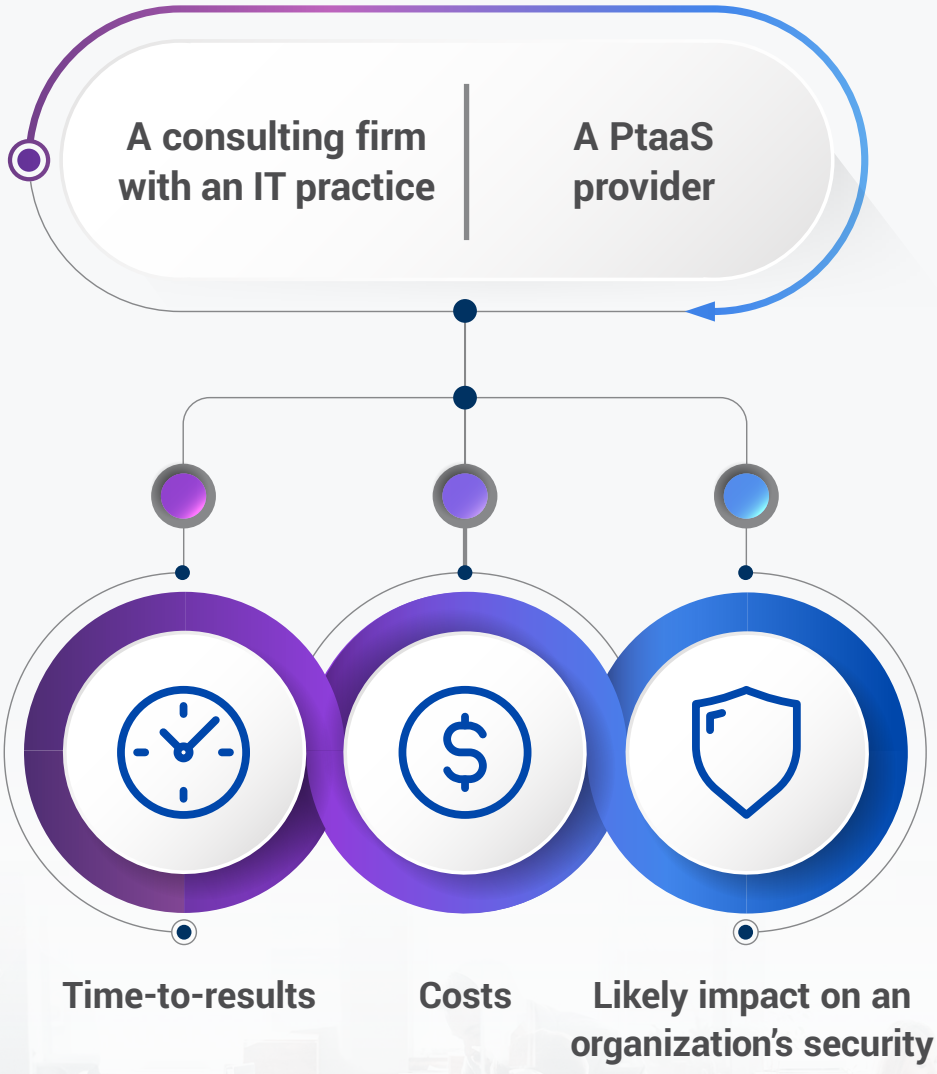
A leading cybersecurity and compliance company that helps more than 3,000 global brands stop targeted threats and make their users more resilient against cyber attacks.

A cybersecurity company that allows security teams at more than 8,000 organizations to reduce vulnerabilities, monitor for malicious behavior and investigate attacks.

The Scenario

To provide a standard basis of comparison, we presented a typical project: pentesting a web application that includes an API, requiring experienced pentesters working a total of 100 hours. This is a common type and size of a project that most security professionals have observed in their own enterprises.

Your organization needs to pentest a web application that includes an API. It will require experienced pentesters working a total of 100 hours. Your CISO has asked you to make some estimates comparing:



Phases of the pentesting cycle

A complete pentesting cycle can be divided into 8 phases. Nevertheless, we wanted our research to focus on the five core phases that tend to be handled consistently across organizations (Figure 1). The time and resources used for the other three phases vary enormously between tests, based on an organization's procedures, the availability of staff, shifting priorities, and many others factors.

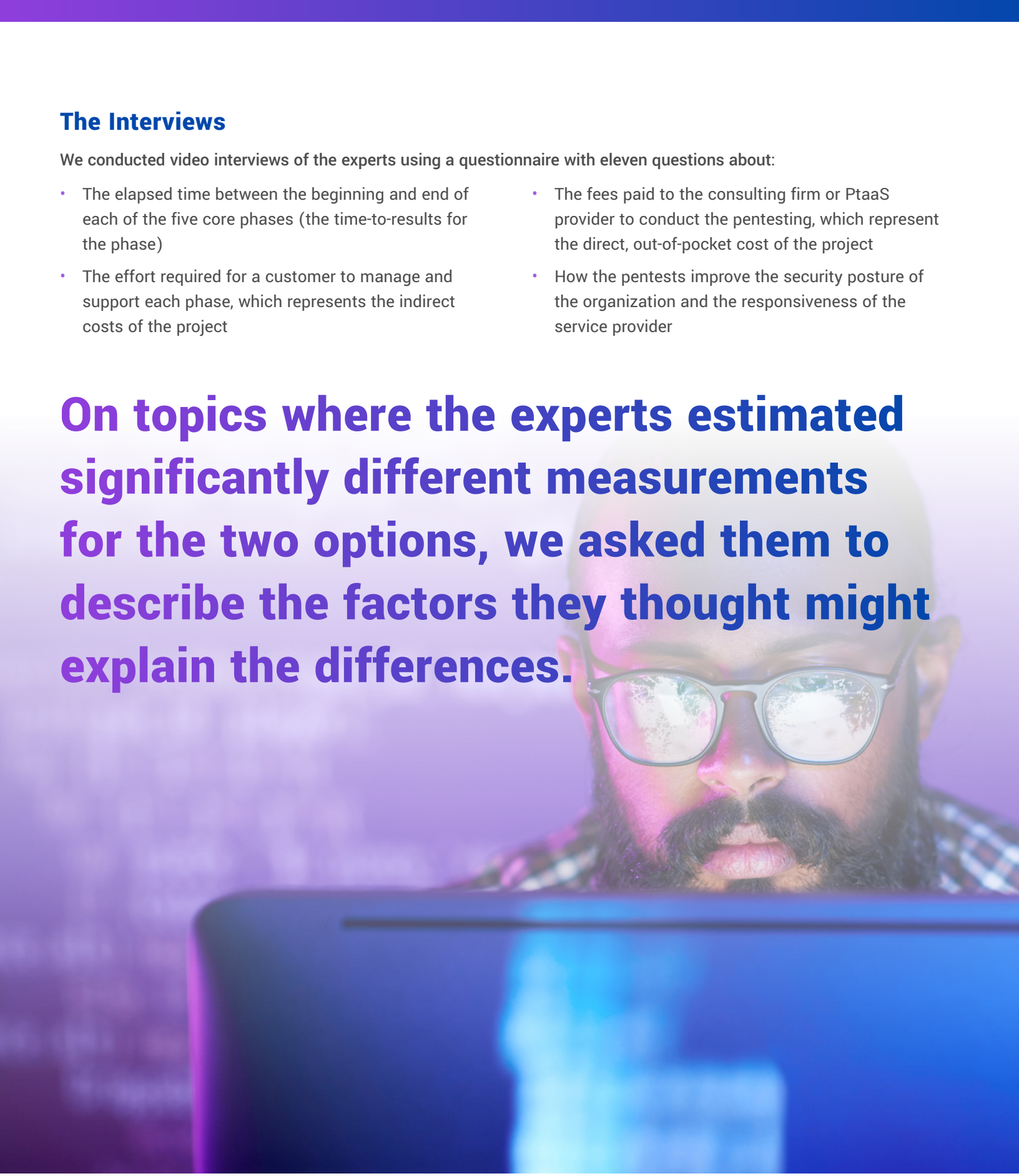
Figure 1: **Phases in a complete pentesting lifecycle.**

The Interviews

We conducted video interviews of the experts using a questionnaire with eleven questions about:

- The elapsed time between the beginning and end of each of the five core phases (the time-to-results for the phase)
- The effort required for a customer to manage and support each phase, which represents the indirect costs of the project
- The fees paid to the consulting firm or PtaaS provider to conduct the pentesting, which represent the direct, out-of-pocket cost of the project
- How the pentests improve the security posture of the organization and the responsiveness of the service provider

On topics where the experts estimated significantly different measurements for the two options, we asked them to describe the factors they thought might explain the differences.

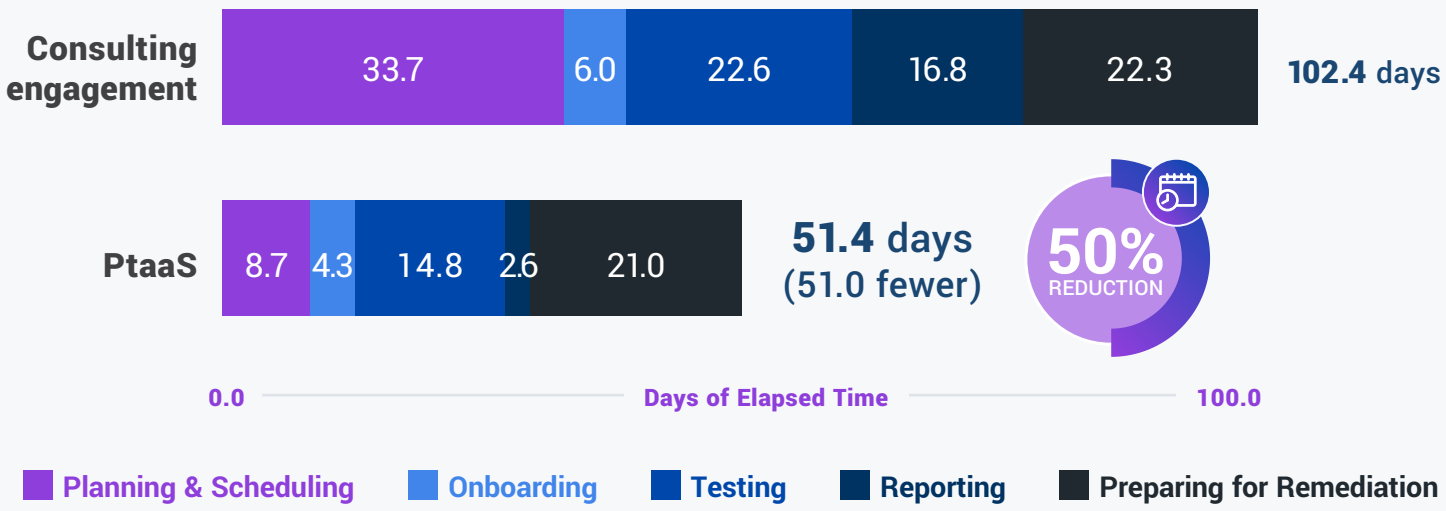


Section 1: Time-to-Results

Traditional pentest consulting engagements have a reputation for taking a long time to schedule and a long time to complete. Is this reputation justified? Does PtaaS perform better on this metric?

Figure 2 suggests that the answer to both questions is a definite "yes." Based on their experience with both types of pentesting services, the experts suggested that PtaaS projects are completed with a 50% reduction compared to conventional consulting engagements.

Figure 2: Time-to-results for traditional consulting engagements and PtaaS projects



The value of faster time-to-results

Today's dynamic IT environment requires software releases and infrastructure changes to be implemented on short notice. Long pentesting lead times can delay these enhancements, or worse, tempt development teams to release them without proper testing which can expose the organization to a greater number of threats.

Organizations that identify and remediate issues faster shorten the window of exposure that attackers can exploit, which reduces the number and severity of successful attacks. Shorter pentesting lead times also contribute to faster time-to-market and greater agility for the business as a whole.

[2] For a thought-provoking discussion about pentesting in agile and DevOps environments, read the Cobalt white paper: Pentesting in DevOps: A How-To Guide.

Fast time-to-results is especially important in situations such as:

- New software features demanded by major internal or external customers
- Due diligence on the IT systems of potential acquisitions
- Compliance audits that require pentest results
- Security assessments of major supply chain partners

Finally, faster time-to-results is essential for agile and DevOps practices. In these environments, developers accustomed to two-week sprints or daily releases are likely to ignore pentest findings on two-month-old builds. But findings that begin coming in shortly after a release will find much greater acceptance and use.[2]

Time-to-results by pentest phase

To compare time-to-results, we asked the experts to estimate the elapsed time, in work days, between the start and finish of the five core phases of a pentesting project.

PtaaS performs for planning, scheduling, and onboarding

The "Planning and Scheduling" phase represents the number of days from deciding to have a test performed to having it scoped and scheduled with a pentesting service provider. Activities include: describing the testing, setting objectives, scoping the work, and scheduling the test with the service provider.[3]

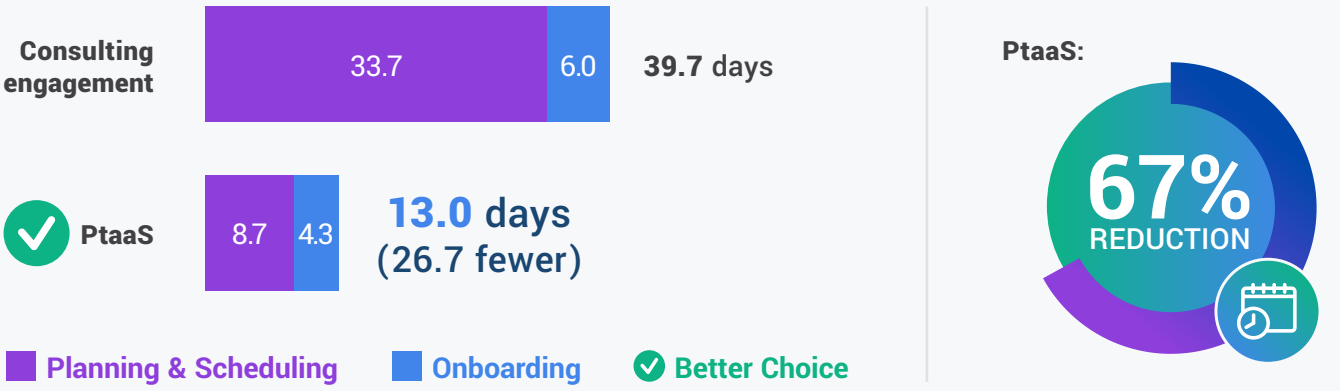
The experts estimated that planning and scheduling the pentest in the scenario would take nearly 34 days for the consulting engagement but less than 9 for PtaaS. On average, the time savings from PtaaS was 74%, or 25.0 days to be precise! (Figure 3)

The experts were unanimous in describing long waits between initiating contact with a representative of a consulting firm and being able to start the onboarding process and testing. They attributed this to two factors:

1. Consulting firms have long, daunting processes with sales representatives for estimating each pentest, negotiating a fee, and scheduling — often with a lot of paperwork. On the other hand, PtaaS providers allow tests to be scoped, costed, and scheduled online.

2. Consulting firms have a limited bench of pentesters and financial incentives to keep them continuously employed, leading to full schedules and wait times of a month or more for qualified personnel PtaaS providers can draw from a much larger pool of talent, including vetted independent pentesters with immediate availability.

Figure 3: Elapsed days for the planning and scheduling and onboarding phases



Onboarding involves activities such as preparing briefing materials, setting up the test environment and user accounts, and onboarding the pentesting team. Estimates for this phase also favored the PtaaS option, which represents a savings of 1.7 days or 28%.

The difference of 26.7 elapsed days, or an average 67% reduction can greatly improve an organization's ability to respond to unexpected events and to integrate pentesting with agile and DevOps processes.

[3] This phase does not include evaluating service providers or receiving internal funding approval, which are not part of this analysis.

Points to PtaaS for testing and reporting

Estimates for time-to-results in the testing and reporting phases also showed a major contrast between the two project types. The estimates are shown in Figure 4.

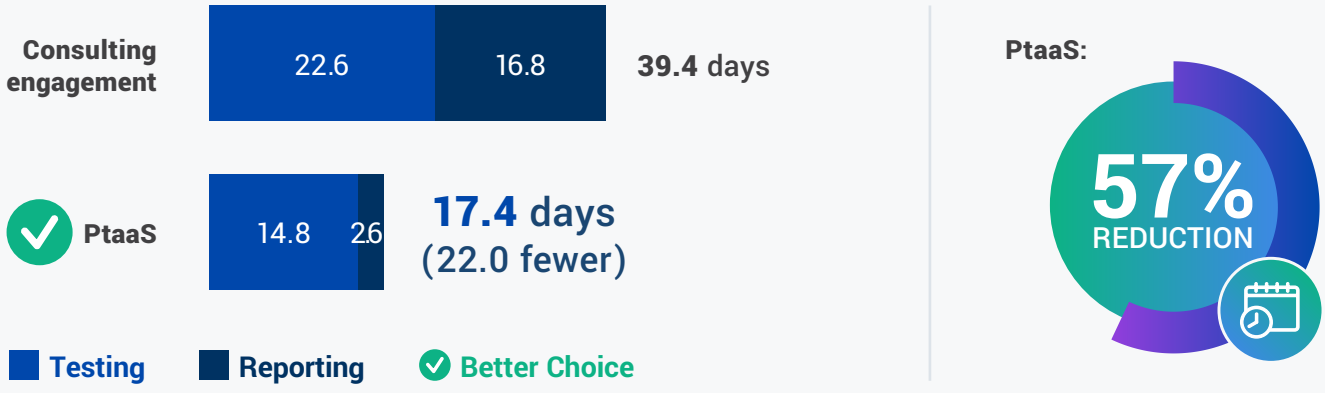
During the testing phase, pentesters perform the assigned tests and assess results with support from security and development teams. **For PtaaS, testing was estimated to take 14.8 days, compared with 22.6 days for the consulting engagement, a reduction of 35%.** The experts noted that PtaaS providers usually assign a team of three pentesters to a project of the size specified in the scenario, whereas most consulting firms assign one or two.

The divergence was even more dramatic for the reporting phase, which covers documenting test findings and writing up recommendations for remediation in a report or in online notes. For consulting engagements, pentesters typically complete the testing stage and then go off for two or three weeks to prepare a final report with all findings and recommendations. However, PtaaS pentesting teams capture findings and recommendations on the platform as they work through the tests, and send them to the customer in real time. Then, the final consolidated report is presented two or three days after the end of the testing phase. In effect, the testing and reporting phases overlap rather than being sequential. The average savings works out to **14.2 days, a reduction of 85%.**

The panelists cited the faster reporting of the PtaaS projects as particularly valuable because it enabled them to start remediating issues several weeks before the report from the consulting engagement would have been available.

The totals for the two phases **combined were 39.4 elapsed days** for the consulting engagement and **17.4 for PtaaS**, working out to a **difference of more than three weeks, or 56%**.

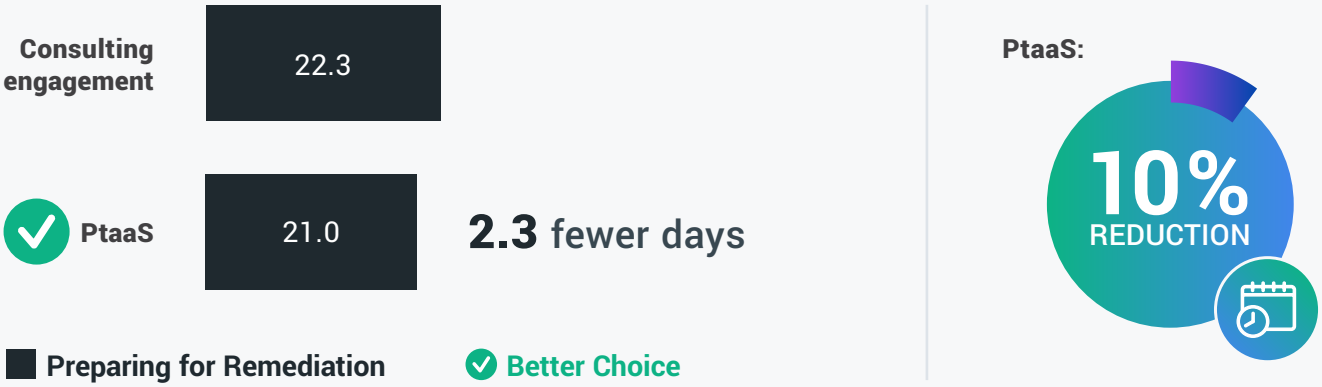
Figure 4: **Elapsed days for the testing and reporting phases**



Preparing for remediation

Preparing for remediation involves security and development teams converting notes and reports into tickets, then triaging and prioritizing them. It often includes discussions between internal teams and the pentesters about threats, security issues, and alternative methods of blocking attacks. Elapsed days to prepare for remediation are shown in Figure 5.

Figure 5: **Elapsed days for preparing for remediation phase**



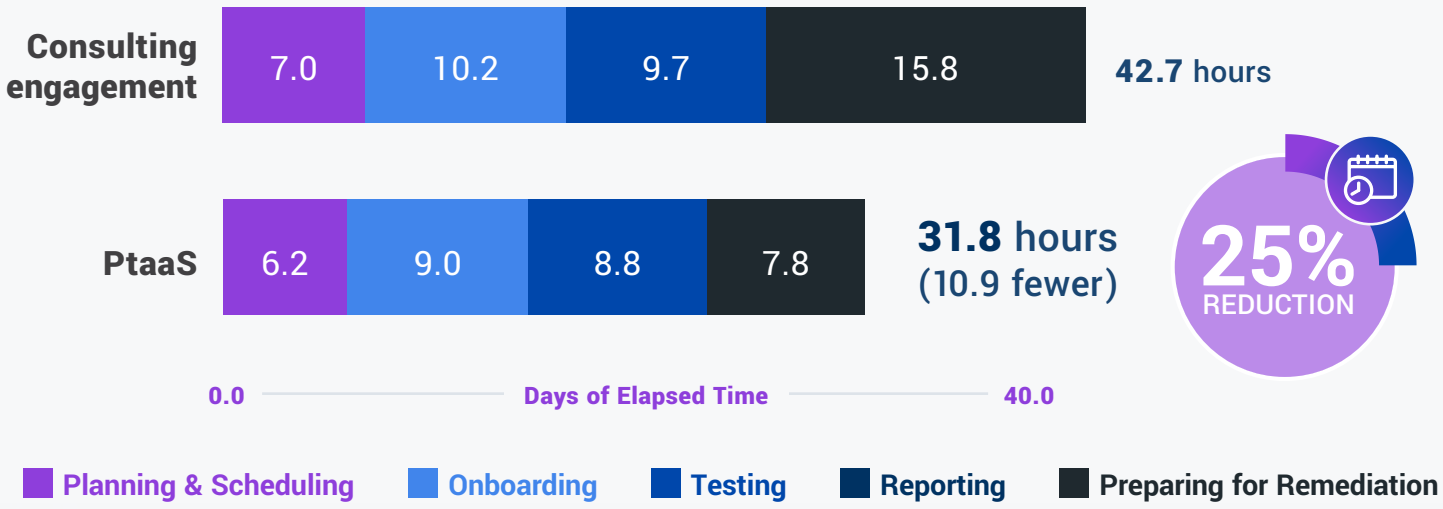
In this instance, the elapsed days differed by only 10% between the two options. The experts believed that time required to prepare for remediation was determined more by the availability and priorities of the people performing the tasks (the customer's security teams) than by the characteristics of the pentesting service providers.

Section 2: Cost of Managing Pentests

Our analysis covers two types of costs: indirect costs to manage a pentest project are discussed here, and direct costs of fees paid to the consulting firm or PtaaS provider are addressed in the next section.

How do traditional pentest consulting engagements and PtaaS compare to the work required to plan, manage, and support a pentesting project? Figure 6 summarizes the estimates of our panel of experts, broken down by the five core phases of a pentesting project. It shows that PtaaS requires 25% fewer hours.

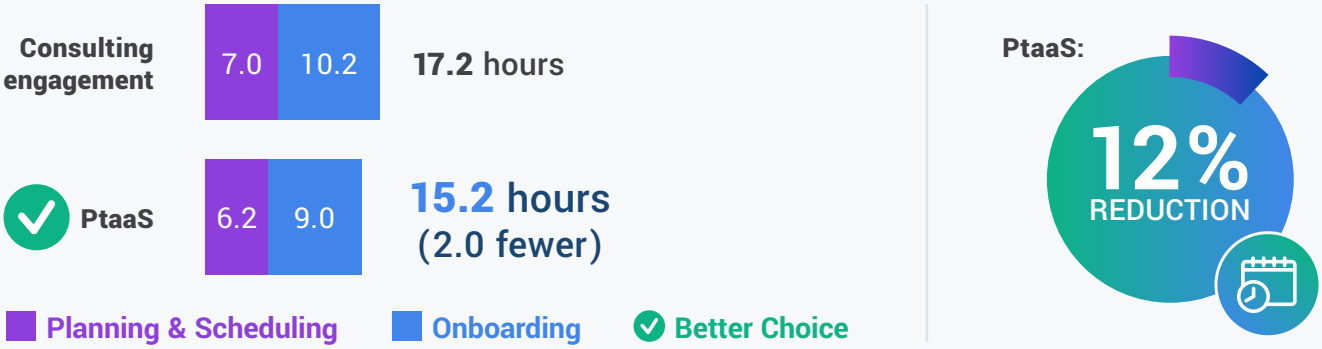
Figure 6: **Hours of work to plan, manage, and support a pentesting project**



Planning, scheduling, and onboarding: an edge for PtaaS

We asked the experts to estimate "how many hours of work would you and your colleagues expect to perform to support each phase." The average of their answers for the planning and scheduling and onboarding phases is shown in Figure 7.

Figure 7: Hours of work to plan, schedule and onboard the pentesting team

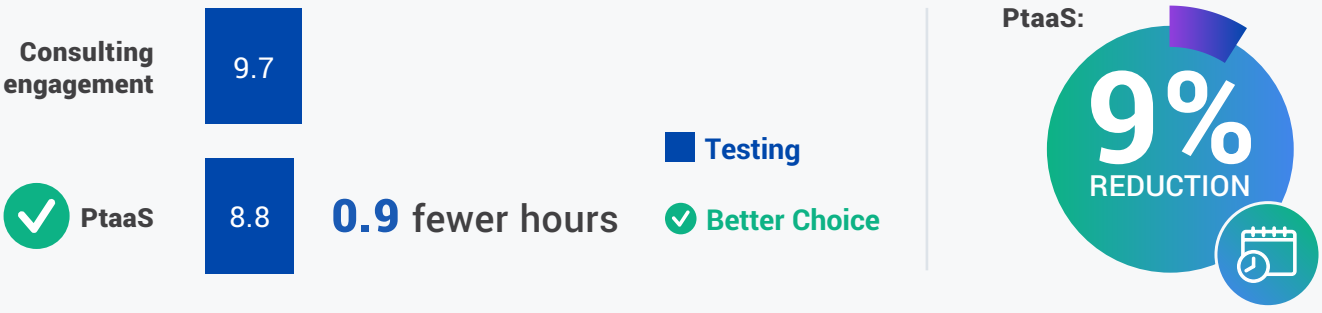


The experts estimated that their team typically spends about 7 hours planning and scheduling a pentest when working with consulting firms, and 6.2 hours with a PtaaS provider. For onboarding, an average of 10.2 hours was required for consulting engagements and 9.0 hours for PtaaS. The differences were attributed to the ease-of-use and data sharing capabilities of PtaaS user interfaces, which make it easier to collect and share information about the assets to be tested, the objectives of the test, and the test plans.

Testing and reporting: Close

Our experts agreed that no significant support was needed while the pentesters were documenting their findings and recommendations. However, they were called upon to support the pentesting team during the testing period. Pentesters were available to answer questions about the applications, the environment, and for administrative tasks like adding user accounts. They also needed to track the progress of testing for their own management. The hours required for this averaged 9.7 when working with consulting firms and 8.8 with PtaaS. This works out to .9 hours or 9%. (Figure 8)

Figure 8: Hours of work to support testing and reporting

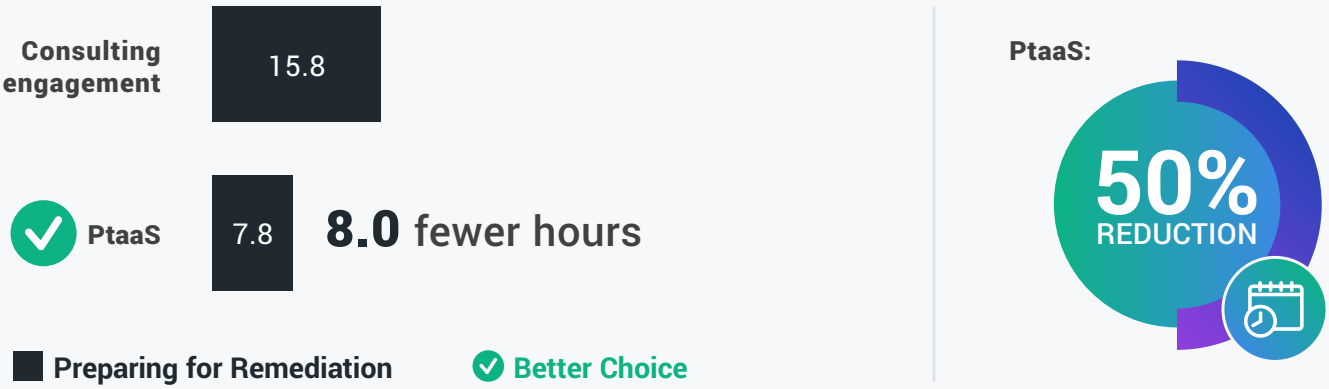


Where did the difference in time come from? The PtaaS platform made it easier for all parties to collaborate and answer each other's questions about the assets and the ongoing tests, which made the entire process more efficient.

Preparing for remediation: A PtaaS API provides a significant advantage

Preparing for the remediation phase involves converting test findings and recommendations for fixes into tickets, then triaging, prioritizing, and assigning the work to be done. The panel's estimates of work hours needed for this phase are shown in Figure 9. The savings in work hours from PtaaS averaged 50%.

Figure 9: **Hours of work to prepare for remediation**



Why the big difference?

The most tedious and error-prone task in this phase is converting findings and recommendations into tickets. When the job is performed manually, someone must copy and paste information and screenshots from static PDF reports, emails, text messages from pentesters, and other sources onto fields in an issue tracking application like JIRA.

Some PtaaS platforms include an API that sends pentest results and recommendations to ticket and issue tracking systems, formatting them into actionable entries.

The experts who had experience with this type of API indicated that it cut the work hours required to prepare remediation by almost two-thirds (63%).

Calculating and comparing indirect costs

To calculate the indirect costs of planning, managing, and supporting the pentest in our scenario, we multiplied the work hours by the fully burdened hourly cost of a security engineer (that is, the cost to the organization of an hour's work, including compensation, benefits, and taxes).[4] The result is shown in Figure 10.

Figure 10: **Cost of work to support the scenario based on average security engineer cost per hour**

Based on our scenario, PtaaS will yield a savings of $834 for each pentest. If an organization conducts one comparable pentest a month, the annual savings would total just over $10,000.

Of course, in many organizations, the time of the security team is a resource that is even more scarce than budget. For such an organization, saving 10.8 hours each month would free up 130 hours of valuable time over a year, or just over 3 work weeks (assuming 40-hour weeks).

If an organization conducts one comparable pentest a month, the annual savings would total just over $10,000.

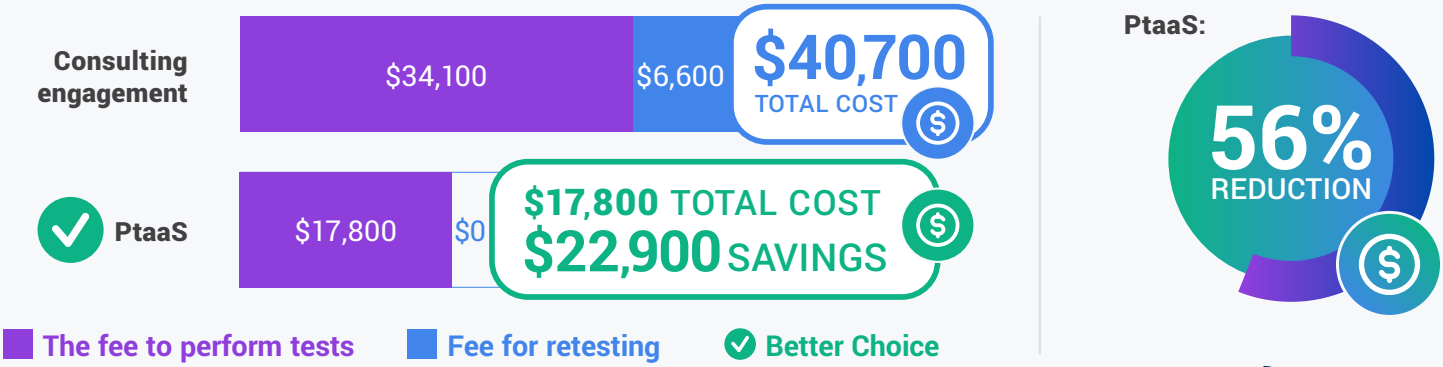
[4] Average Security Engineer salary in the U.S.: $111,675 (Glassdoor) x burden rate of 30% = fully burdened annual cost of $145,178. Hours worked per year: 235 days x 8 hours = 1880 hours per year. Hourly cost: $145,178 / 1,880 = $77.22.

Section 3: Service Fees and Total Cost

Direct costs

We asked the panel of experts about the fees they would expect to pay a service provider to pentest a web application that includes an API, requiring experienced pentesters to work a total of 100 hours. The average estimates are shown in Figure 11.

Figure 11: **Fees paid to the service provider for a 100-hour project**



Note: These estimates are based on the panel members' experiences at their current and prior employers with projects of this type and size. Actual fees will vary based on many factors, including the number of assets being tested, the types of assets (applications, APIs, networks, etc.), the depth of the testing, special skill requirements, and the pricing policies of the service providers.

Obviously, these are very significant cost differences. The fees paid to a PtaaS provider are estimated to be roughly half the fees for a consulting firm. The difference is even more pronounced when fees for retesting are considered. Some PtaaS providers include retesting in the price of pentest services, while consulting firms often charge up to 40% extra for retesting.

The average estimates from the panel indicate that when retesting fees are added in, the total cost of the PtaaS project is on average $17,800, which is 56% lower than the consulting engagements.

Why is the difference in costs so large?

The scenario specifies that both types of service providers deliver 100 hours of testing by experienced pentesters. So how could there be such a dramatic difference in fees for performing essentially the same testing? The experts pointed to two factors.

First, PtaaS automates many repetitive tasks and enables data sharing and reuse. For example, PtaaS platforms capture tests scoping information, asset descriptions, intelligence about vulnerabilities and attack techniques, and test findings. They make it easy to find and reuse this information for later tests of the same assets and similar assets. Report generators can repackage final test reports into different formats tailored for security teams, executives, and auditors. Features like these increase the productivity of the pentest teams, allowing the PtaaS provider to lower fees.

Second, the two types of service providers have different business models when it comes to hiring and compensating pentesters. According to the panel:

Consulting firms compete for a relatively small number of experienced, full-time pentesters, and must pay them both when they are working for customers and when they are between projects.

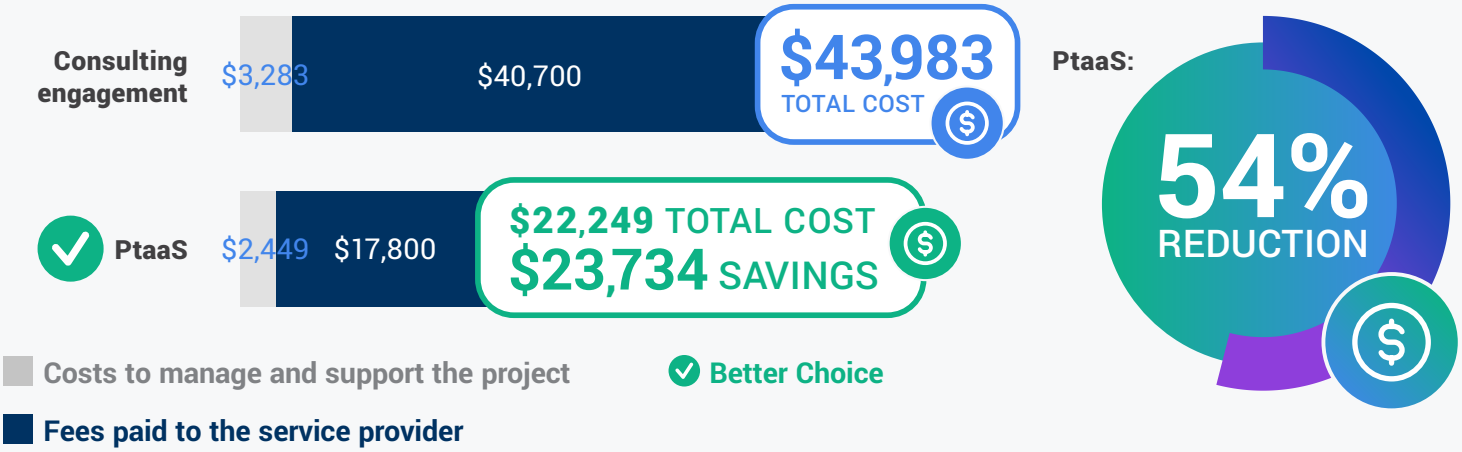
PtaaS providers can draw from a much larger talent pool. The pool includes experienced and certified pentesters who prefer to work on a per-project basis. Many of these professionals have full-time positions on security teams, with roles ranging from security engineers to managers, and sometimes even CISOs. Because they are freelance contractors, PtaaS providers only pay them when they are working on customer projects.

PtaaS platforms capture tests scoping information, asset descriptions, intelligence about vulnerabilities and attack techniques, and test findings.

Total Costs

Figure 12 shows the panel's estimates of the combined cost of the project. The figures are noteworthy. The combined cost of PtaaS projects is less than half the cost of traditional consulting engagements.

Figure 12: **Estimates of combined costs for the project**



The experts made an interesting observation about how most organizations leverage savings that come with using PtaaS. They do not shift people or budgets to other programs. Instead, they use the same staff and budget to pentest critical assets more than once a year and to pentest a wider range of assets.

Another way of looking at these estimates is that PtaaS gives organizations that have been using consulting firms an opportunity to double the ROI of their investment in pentesting services. Either they can achieve the same reduction in risk at half the cost, or they can double test coverage with their current budget.

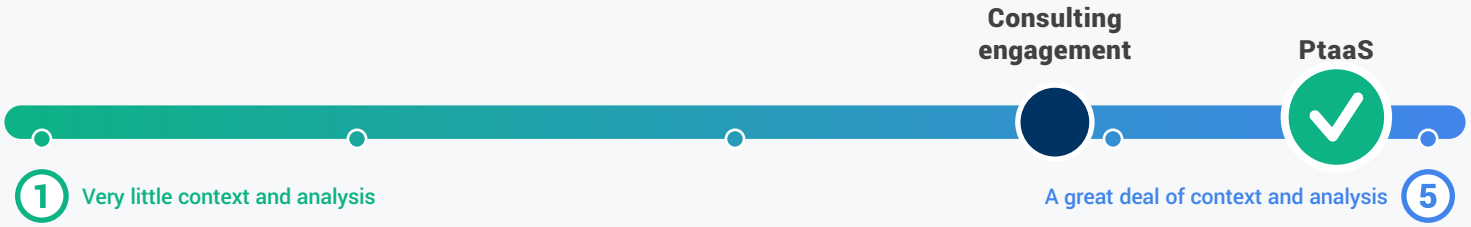
Section 4: Security Effectiveness

The final section of our research asked the panel about factors that affect how much the two types of pentesting services help organizations improve security and reduce risk.

Pentester knowledge

We asked the experts to rate the amount of context and depth of analysis provided by the pentesting teams on a scale of 1 to 5. (Figure 13)

Figure 13: **Context and depth of analysis**



The panelists stated that they had been impressed by the knowledge and experience of the majority of the pentest teams on both sides. They gave PtaaS a slight edge in terms of effectiveness because the online communication channels made it easier to find and share context and analysis.

Fit with agile and DevOps and responsiveness to unexpected needs

We asked the experts to rate how the pentesting service options fit with agile and DevOps processes and their responsiveness to unexpected needs on a scale of 1 to 5. In these areas, PtaaS was assessed as far ahead of traditional consulting engagements, with ratings 2.4 points higher. (Figure 14)

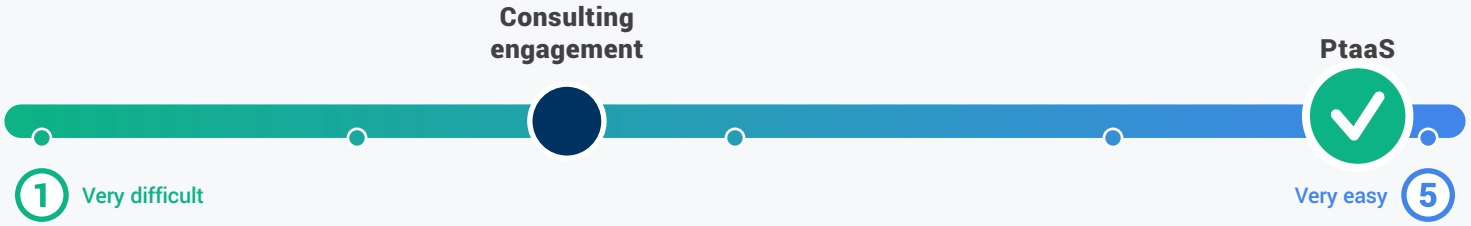
Figure 14: **Fit with agile and DevOps and responsiveness to unexpected needs**

The panelists agreed that lengthy delays scheduling pentests coupled with the long testing and reporting cycles of traditional consulting engagements don't align with agile and DevOps processes. PtaaS is a much better fit because test results and remediation recommendations are available as tests proceed. Similarly, when unexpected needs arise, PtaaS providers can respond faster because they draw on a large pool of vetted pentesters available on demand.

Ease of doing business

We asked the experts about the ease of doing business with service providers, in the sense of working with them on tasks such as negotiating agreements, planning, and scheduling pentests, responding to requests for information, and changing plans and schedules. (Figure 15)

Figure 15: **Ease of doing business**



The panelists shared the view that it is much easier to do business with PtaaS providers, saying they are more flexible about changing plans and schedules. In addition, the PtaaS platforms include tools that speed up communication and collaboration, so the pentesting teams respond faster to requests for information. Finally, consulting firms tend to require a lot of work to scope and negotiate every project change, while many **PtaaS providers allow tests to be scoped, cost, and rescheduled online with minimal time and effort.**

Testing frequency

Testing frequency can have a major impact on security by reducing the time that vulnerabilities and security issues remain undiscovered. We asked the experts to estimate how often they would pentest critical assets if their organization used the two types of pentesting services. (Figure 16).

Figure 16: **Frequency of testing critical assets**

The difference was dramatic. With consulting firms, the vast majority of organizations (83%) would test critical assets only annually. With PtaaS, the vast majority would test them either twice annually (50%) or quarterly (33%).

The panel explained this wide difference partially because of the flexibility of the PtaaS model, but even more because of the lower costs of testing. In our discussion of total costs, we mentioned that the low cost of PtaaS enabled organizations to double test coverage with their current budget. That appears to be reflected in the panel's views here.

Conclusion

Organizations that want to strengthen their IT security programs frequently turn to pentesting services, ranging from consulting firms to PtaaS providers. Both can provide knowledgeable and experienced pentest teams and manage projects from start to completion. **Our panel of six security experts who have worked with both options have identified several areas where PtaaS has demonstrated better performance**:

The time-to-results of PtaaS is about half of traditional consulting engagements, meaning you can accomplish just as much in half the time. This makes PtaaS a much better fit for organizations that use agile and DevOps methods, and for those that want the flexibility of quickly scheduling tests for unexpected needs.

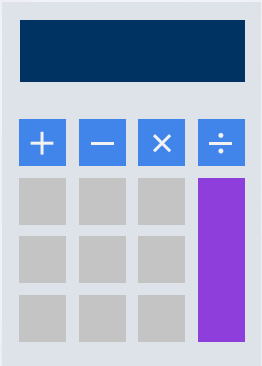
The panel estimated that PtaaS could cut the total cost of a standard pentest project by 54% (See pages 17 and 19) compared with traditional consulting engagements. This enables organizations to reduce the same amount of risk for half the cost, or get twice the coverage for the same budget.

PtaaS reduces the hours of work required to plan, manage, and support pentesting projects by about 25%, freeing up the time of security and development teams to address other critical tasks.

The experts rated PtaaS significantly higher on a variety of criteria related to security effectiveness, responsiveness, and ease of doing business.

Security and development teams that want to achieve similar results are invited to explore the premier PtaaS offering from Cobalt.

Use our calculator to learn how much Cobalt can improve your pentesting ROI, or **schedule a demo** to get started today!



Calculate your ROI

Schedule a demo

Cobalt

Learn more about how we can **transform your pentest process** at cobalt.io

San Francisco | Berlin | Boston

cobalt.io

102921