Cobalt

Pentesting in 2025 and Beyond

A Strategic Guide to Choosing the Right Security Testing Partner

WWW.COBALT.IO

SAN FRANCISCO · LONDON · BERLIN

Executive Summary

Selecting a pentesting partner isn't as simple as opting for a popular vendor. You're looking for a strategic security ally, empowered with the tools and skills to help you consistently improve your security posture long-term—ultimately reducing organizational risk.

Performed consistently, pentesting evaluates the effectiveness of your defenses, leading you to develop a more effective and efficient security program. Leaning on a trusted partner for your pentesting enables you to build an offensive security program based on the specific needs of your organization, such as software pentesting, network or cloud pentesting, or even building a robust strategy that includes red teaming.

The [2024 GigaOm Radar Report for Pentesting as a Service] paints a clear picture of the evolution of pentesting from a one-time service to an ongoing security partnership:

"The Pentesting as a Service (PTaaS) market is evolving rapidly, driven by increasing cybersecurity threats and a growing recognition of the limitations of traditional penetration testing approaches. We're seeing a trend toward more sophisticated, AI-driven testing capabilities, improved integration with existing security and development tools, and enhanced reporting and analytics features. Vendors are focusing on providing more comprehensive, end-to-end security solutions that combine continuous testing with other security services."

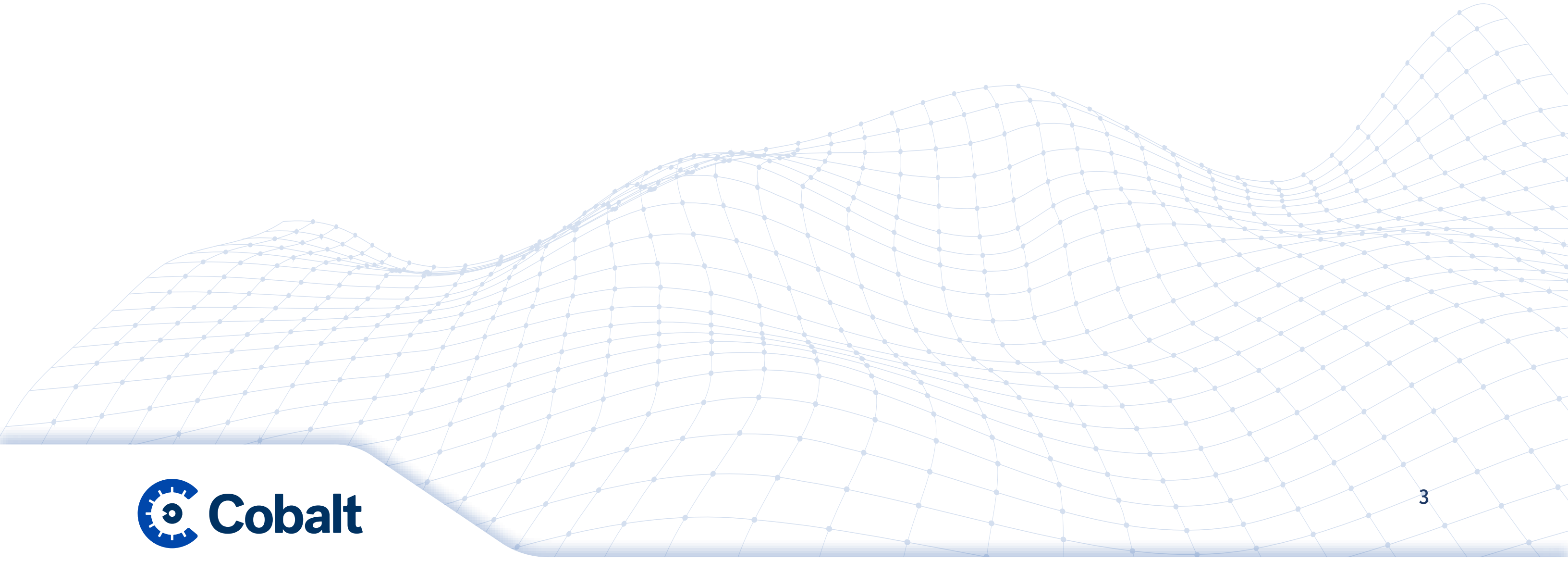
The expanding attack surface, fueled by hybrid operations and interdependent systems, increases the risk of overlooked vulnerabilities and software supply chain issues, making proactive assessments critical. Agile development cycles and continuous deployment introduce frequent changes, creating a constant influx of potential vulnerabilities.

PTaaS gives companies ongoing security support, combining a strategic offensive security approach with traditional launch- and compliance-focused pentesting. PTaaS providers collaborate with developers to identify and fix vulnerabilities in real time as the company and its assets evolve.

PTaaS offers scalable access to security expertise, enabling comprehensive security testing. The comprehensive testing model helps organizations maintain trust, meet compliance requirements, and secure their digital assets.

This guide will equip you with pentesting best practices so you can identify the right pentesting partner and strategy for your organization.

Table of Contents



Why Pentest? An Introduction to Pentesting

Pentesting could make the critical difference between a vulnerability being discovered by a friend or an enemy, giving you actionable insights into security weaknesses rather than causing a security breach. It helps your organization assess its security posture, mitigate risks, and proactively improve your defenses. Security teams can use pentesting results as a point-in-time assessment, enhancing the organization's ability to identify and respond to new security threats.

By simulating attacks using the tools and techniques of malicious actors, pentesting helps organizations uncover and fix vulnerabilities before adversaries can exploit them. As cyber threats grow more sophisticated, fueled by advancements in technology and the growing accessibility of malicious tools, pentesting remains a critical defense strategy.

AI Impact on Security

AI represents a sea change in the cybersecurity landscape. While AI tools enhance defensive measures, they also empower attackers to craft more complex and targeted threats on vulnerable or common devices.

Attackers use AI to create more effective spearphishing emails, fake profiles, and other forms of social engineering, dramatically increasing the scale and success rate of their attacks. Yet AI systems themselves are not immune to social engineering tactics such as data poisoning or prompt injection, opening a new avenue for hackers to exploit.

Pentesting has adapted to this new reality, employing tools and techniques designed to simulate attacks on AI-enabled applications and identify vulnerabilities unique to these systems.

Bridging the Skills Gap

As the rate of cyberattacks increase, the demand for skilled security professionals far outstrips the supply, leaving many in-house security teams stretched thin[1]. PTaaS leverages a provider's deep bench of testers to address the talent gap, completing in hours what used to take days. Plus, the rise of PTaaS over one-off tests has further eased the ongoing security burden: where the traditional pentesting model took 10 - 50 pentesters six to eight weeks, the right PTaaS provider can deploy dozens (hundreds, in some cases) of pentesters within 24 hours, allowing organizations to outsource testing without overloading internal teams.

[1] 2024 ISC2 Cybersecurity Workforce Study

Building Beyond Compliance to a Culture of Security

Compliance remains a significant driver for pentesting, as many regulatory agencies mandate security testing to meet regulatory standards like SOC 2, GDPR, HIPAA, and PCI DSS. Additionally, pentesting provides an opportunity to document compliance efforts while demonstrating commitment to user safety and data privacy.

However, limiting pentesting to a compliance use case misses its true value: assessing and fortifying your organization's security posture.

With attack vectors and technology constantly evolving, an effective security response demands continuous adaptation. In 2025, pentesting should transcend the checkbox mentality and become an essential element of a broader proactive offensive security strategy.

Types of Assets to Pentest

Begin your journey by determining which assets to test. We define assets broadly across three categories:

Software Products and Applications

Web applications, APIs, desktop and mobile apps, IoT, and AI language models.

Cloud and Network Testing

Cloud infrastructure, network systems, and foundational IT assets stored inside and outside the organization's physical network.

Information Security and SOC

Incident response processes.

To determine which assets to prioritize for testing, use risk ranking to help you determine the assets that, if compromised, would pose the most serious risk to your organization. Start by taking an inventory to identify critical systems and applications that process PII or other sensitive data and which are web-facing or are otherwise exposed to potential threats. Then you can move on to systems that require testing as part of a compliance mandate.

You may pursue pentesting for various reasons—such as building customer trust and confidence, meeting compliance requirements, or adhering to industry best practices. The most compelling reason for regular pentests is proactive security hygiene. Regularly scheduled pentests bring human creativity and ingenuity to the process, finding the gaps and vulnerabilities a scanner or machine may not recognize. Attackers are human, so it often takes a human perspective to connect disparate data points into a potential attack chain.

> “While compliance checks help, they don’t provide a full picture of potential vulnerabilities, making expert pentesting essential to uncover hidden risks. Annual tests not only ensure compliance but also drive critical security discussions that shape our approach.”
>
> AVIAD NOAH
> DIRECTOR OF CLOUD SECURITY, CENTRALREACH

Choosing the Right Provider

Choosing the right pentesting provider is key to the success of your security initiative. Start by selecting the right provider category, then pick the best vendor in that category that fits your needs.

Provider Categories

Pentesting providers typically fall into five categories, each category has its own strengths and considerations.

1. Traditional Pentesting
2. Bug Bounties
3. Automated Tools
4. Boutique Testing Firms
5. Offensive Security and PTaaS

Traditional Pentesting

These are large, well-established firms that offer security testing as part of their broader service offerings. They have access to vast resources, experienced staff, and industry expertise. They provide pentesting in a structured, often compliance-focused approach.

PROS

- ☑ Offer lengthy, comprehensive pentesting solutions.
- ☑ Own access to extensive resources and expertise across various areas.
- ☑ Provide detailed reports with both technical and business insights, ideal for executives and IT teams.
- ☑ Can offer additional cybersecurity services like SOC implementation, data backup and recovery, encryption management, etc.

CONS

- ☒ Long lead times, sometimes measured in months, means pentesting needs can't move at the speed of your business.
- ☒ Premium pricing and extra retesting fees may be too costly for programmatic usage.
- ☒ Longer testing periods and reporting timelines due to bureaucracy.
- ☒ Inflexible testing methodologies may hinder effective assessments in evolving or unique environments.
- ☒ Pentesting is just one of many services, so organizations may not get the specialized attention of smaller, dedicated firms.

Bug Bounty Crowdsourced Security Platforms

On crowdsourced security platforms, organizations can turn to a global community of bug bounty hunters for vulnerability discovery. Companies register their program, and bounty hunters compete to find and report security issues to earn rewards or payment.
These organizations often offer pentesting in addition to their bug bounty programs.

PROS

- ☑ Ongoing bug bounty programs provide continuous monitoring and quick identification of bugs, especially related to usability.
- ☑ Cost-effective with a minimal annual subscription and pay-for-results model, ensuring organizations only pay for verified vulnerabilities.
- ☑ Pentesters from bug bounty programs are often the highest-scoring bounty hunters within their organization.
- ☑ Large pool of bug bounty hunters—sometimes measuring in the millions of participants.

CONS

- ☒ Shallow assessments with many bounty hunters focused on one type of testing that is fast and repeatable across many different bug bounty programs.
- ☒ Limited depth for comprehensive risk analysis.
- ☒ While the pool of bounty hunters is large, the active participants in the community are generally much smaller, and the group that will perform pentesting is even smaller still—usually only a fraction of the overall pool.
- ☒ Inconsistent result quality due to varying skill levels and experiences of security experts conducting pentests.

Automated Pentesting

The tools in this category excel at the speed and efficiency because they are automating pentesting techniques. Automated systems perform initial vulnerability scans simulating and emulating real-world attacks by using the adversaries’ tactics, techniques, and procedures as observed in the wild.

PROS

- ☑ Automated tools speed up vulnerability discovery and reduce the time needed for initial assessments.
- ☑ Access to automation reduces costs and human error.
- ☑ Automated tools can handle large, complex environments, making them attractive for organizations of all sizes.

CONS

- ☒ Automated tools may miss sophisticated attack vectors or business logic flaws, even with human review.
- ☒ Requires skilled human reviewers to interpret results, which can strain resources for smaller teams.
- ☒ Does not meet regulatory requirements for manual or in-depth testing in industries with strict compliance standards.
- ☒ Tend to be noisy with large numbers.

Boutique Testing Firms

Small pentesting firms are specialized cybersecurity companies offering tailored security assessments. They stand out for their focus on personalized service and deep expertise over speed and affordability.

PROS

- ☑ Customized, personalized evaluations of your environment.
- ☑ Ability to adapt methodologies to the specific needs of your organization.
- ☑ Direct access to seasoned experts, clear communication, and a deep understanding of findings and recommendations.
- ☑ Detailed reports with actionable insights for effective remediation.

CONS

- ☒ Smaller firms may struggle to handle large-scale projects or multiple engagements simultaneously.
- ☒ Personalized services may result in higher fees.
- ☒ Limited resources might challenge scheduling, with longer lead times for initiating and completing assessments.
- ☒ Specialization results in limited capabilities beyond their area of expertise.
- ☒ Often boutique firms specialize only on specific asset types and techniques.

Offensive Security and PTaaS Providers

Providers use cloud-based platforms to streamline the process and offer fast execution, collaboration, and actionable security insights. Unlike traditional providers, PTaaS makes pentesting more agile, accessible, and affordable.

PROS

- ☑ Faster onboarding and execution compared to traditional methods. Pentests can begin within 24 hours, with results in seven days.
- ☑ Real-time reporting to minimize delays in identifying and addressing vulnerabilities.
- ☑ Cost-effective payment options, like subscription-based pricing, make pentesting affordable for organizations of all sizes.
- ☑ Flexible scopes for targeted, frequent or continuous testing to keep up with development teams.
- ☑ Direct communication with pentesters during testing for clarity, faster resolutions, and flexibility to adjust the scope.
- ☑ Capable of meeting accelerated timelines to speed up vulnerability detection and remediation, especially in urgent situations like post-breach evaluations or compliance deadlines.
- ☑ Massive scalability. Providers in this category can scale up or down as needed, with some providers running over 200 pentests concurrently.
- ☑ Support for your security team’s needs when additional offensive security services make sense for your organization (such as a red teaming engagement).

What is Offensive Security?

Offensive security involves proactive, adversarial cyber-security techniques such as penetration testing, red teaming, and attack surface monitoring (ASM) to simulate real-world attacks. These tactics are used to identify vulnerabilities and weaknesses in systems, networks, or applications and to evaluate the effectiveness of existing defensive controls.

Offensive security provides organizations with actionable insights, helping them prioritize and address vulnerabilities, ultimately strengthening their overall security posture by continuously testing and improving their defenses.

CONS

- ☒ PTaaS platforms may focus on specific types of pentesting (e.g., web apps, APIs) and offensive security capabilities but lack the broader services of enterprise consulting firms such as SOC services.
- ☒ Many PTaaS providers leverage a contractor model for efficiency and scale. If full-time employees are a requirement for your organization, this may be a distinction to consider.
- ☒ Many PTaaS providers can support location requirements, such as US-based pentesters, but this is something to consider as you investigate PTaaS platforms.

Questions to Ask a Pentesting Provider

When evaluating potential pentesting providers, you can ask questions to help determine if the solution in question serves your organization’s needs. Here are a few suggestions:

Speed and Agility

Top PTaas platforms are able to kick off new pentests in 24 hours or less, communicate vulnerability reports in real time, and offer rapid retesting once your developers address any findings.

- □ How quickly can I start a pentest?
- □ How long does it take to get a report?
- □ Are findings delivered in real-time to enable faster prioritization and remediation or does the pentester only share a final report?

Expertise and Pentester Quality

The advantage of PTaaS is that it can offer a network of experienced pentesters with a range of expertise, making it possible to support niche technologies without the overhead and risk of hiring full-time employees.

- □ How many pentesters are active in your community? This should not include participants in a bug bounty program.
- □ How many years of experience do your pentesters have on average?
- □ What is the vetting process for pentesters? What certifications (e.g., CEH, CISSP, OSCP, or CREST)?

Collaboration and Transparency

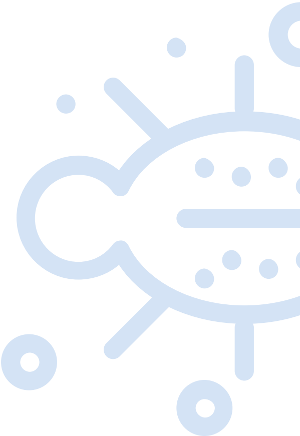
Direct collaboration between testers and developers can lead to more efficient retesting, faster results, and a more secure final product. Ensure your testing partner works collaboratively.

- □ Do you enable direct collaboration between security teams and pentesters?
- □ Do you provide transparency through features like progress checklists and detailed methodologies?
- □ What happens if there is a critical finding; how is this communicated?
- □ What if my team has questions about the findings?
- □ How do findings get into my team’s backlog? Are findings integrated into existing tools?

Retesting and Validation

If your testing partner only communicates findings in a final report, you will have to fix and retest all vulnerabilities at once. Real time collaboration allows this to be a more efficient and ongoing process.

- □ Can retesting be done on a per-finding basis to ensure critical vulnerabilities are resolved quickly?
- □ What is the service level agreement or average turnaround time for retesting to confirm fixes?
- □ Is retesting included at no cost?
- □ What is the retesting window?



Scalability and Flexibility

PTaaS providers are typically larger organizations, allowing diverse testing support and scalability. Leading providers offer complementary support like external attack surface monitoring (ASM) and dynamic application security testing (DAST) to deliver a continuous view of organizational risk.

- □ Do you have a flexible pricing structure that allows us to adapt our strategy as vulnerabilities are found?
- □ Do you support specialized expertise for pentesting APIs, mobile apps, IoT, or LLM applications?
- □ Can you scale to meet the needs of growing organizations with multiple concurrent tests? How would you handle testing 50 applications at one time?
- □ What additional capabilities do you provide to complement pentesting efforts?

Customizable Reporting and Insights

Pentest findings are useless if your team can't easily read and understand them. Ensure your testing partner has the capability to produce custom reports and insights that fit your organizational needs instead of trying to slog through blocks of templated text.

- □ Does the platform offer customizable, interactive reports tailored to compliance needs, board-level summaries, and customer attestations?
- □ Are reports designed to provide actionable insights to both technical and non-technical stakeholders?

Do you need an AI pentest?

Organizations of all sizes are integrating AI into their software products. While AI offers a new world of innovation, it also introduces new threats and vulnerabilities. Understanding if your pentesting partner can provide an AI pentest, and asking about the qualifications of testers and soundness of methodologies are worthwhile when it comes to selecting the right provider.

To Rotate or Not to Rotate?

Historically, rotating pentesting providers was seen as a best practice because many firms only had a handful of experienced, specialized pentesters. With the changes in the pentesting space, these assumptions deserve a closer look. With the changes in the pentesting space, these assumptions deserve a closer look: modern pentesting companies recognize the need for deep partnerships and fresh perspectives, which is why their solutions combine the best of both strategies.

- **Large talent pools**:
  Some providers have hundreds of skilled, vetted, and certified pentesters that can be rotated to bring a new perspective and find new vulnerabilities with every test.

- **Strategic insights**:
  There's value in analyzing a few years of pentesting data over time—especially if you are a larger firm that tests multiple times a year (testing new app releases, for example).

- **Costs of rotating providers**:
  It takes effort to set up integrations and ensure your team is remediating based on findings. By rotating pentesting teams but remaining consistent with the provider, you can avoid those setup costs while getting a fresh perspective.

A long-term partnership with a capable provider that offers tester rotation can provide the best of both worlds: fresh perspectives and accumulated knowledge of your systems.

Why PTaaS Is the Right Choice for Most Businesses

Cyber threats evolve rapidly, but traditional pentesting models are too slow and rigid to keep up. Scheduling can take weeks, and by the time findings are reported, the attack surface has already changed. Security teams need a faster, more adaptable approach that aligns with modern development cycles and integrates into broader security workflows.

PTaaS addresses these challenges by delivering on-demand, scalable testing with faster execution and real-time collaboration. Unlike traditional pentesting, which operates in silos, PTaaS ensures findings are actionable and remediation happens quickly.

A modern pentesting program should prioritize:

Speed and agility

Some providers can launch pentests within a day and validate fixes in hours, minimizing risk exposure.

Actionable insights

Security reports should be structured, customizable, and delivered in a way that allows developers, security teams, and executives to act quickly.

Scalability on demand

PTaaS allows companies to increase testing frequency, rotate experts as needed, and maintain access to specialized security talent.

Real-time collaboration

Pentesting should be a two-way process, with security teams working closely with testers to resolve access issues, clarify findings, and request retesting. Direct communication keeps testing and remediation on track.

Testing aligned to business needs

Organizations should have the flexibility to test new features, infrastructure changes, or emerging threats like Log4j without committing to rigid, lengthy engagements.

PTaaS’s modern approach to pentesting doesn’t just find vulnerabilities—it enables a programmatic approach to identifying risk, speeding remediation, and ultimately strengthening security posture over time.

Building a Sustainable Offensive Security Program

A mature offensive security program starts with a programmatic approach to pentesting, creating a continuous feedback loop to assess and improve defensive controls.

As organizations refine their security posture, they can expand beyond pentesting by incorporating red teaming to simulate real-world adversaries, ASM to continuously identify external exposures, and DAST to uncover vulnerabilities in live applications. The impact of this approach is a stronger, more resilient security posture that enables organizations to stay ahead of attackers rather than reacting to breaches after they occur. By layering offensive security tactics, companies reduce risk exposure, improve detection and response capabilities, and build confidence with customers, stakeholders, and regulators.

Ultimately, this strategic shift transforms security from a reactive necessity into a proactive business enabler, ensuring long-term resilience in an increasingly complex threat landscape.

Components of an Offensive Security Program

Attack Surface Management (ASM)

Automated process that helps security teams discover shadow IT, misconfigurations, and potential entry points in internet-facing assets before attackers. When combined with pentesting, ASM helps organizations secure their expanding digital footprint.

Dynamic Application Security Testing (DAST)

Continuous scanning that simulates real-world attacks to identify vulnerabilities in an application while it is running. DAST combined with pentesting can help provide a comprehensive view of application security risks.

Red Teaming

Relies on human testers who mimic real-world cyberattacks to probe an organization’s defenses. As part of a comprehensive program, Red Teaming helps organizations identify blind spots, improve incident response, and train blue teams to detect and respond to threats.

Key Offensive Security Features to Evaluate in a Pentesting Partner

Effective offensive security programs adapt and grow as new techniques and technologies become available. Key features to evaluate in a potential pentesting partner are:

□ Scheduling and remediation speed

Pentests should move at the speed of your business. If you are testing a software release, you need a partner who can spin up a test in 24 hours and give you real time results and collaboration. Your pentesting partner's timelines for both scheduling and for retesting should fit within your expectations.

□ Real-time collaboration

A collaborative testing partner can directly engage with your team through in-platform messaging or your company chat tool (think Slack) while transparently tracking test progress with a coverage checklist. This allows your team to resolve access issues, clarify findings, and request fast retesting, keeping your pentests on schedule.

□ Customizable reporting

Customizable reporting helps your team meet the informational needs of all stakeholders, whether they be customer attestation letters, summary reports, or detailed findings descriptions—making results easy to understand for your security team, developers, executive decision makers, and end users.

□ Breadth of expertise

Different asset types require different approaches, and working with a provider that offers a range of methodologies ensures you get the testing you need. Where a single-approach provider often has one solution to many problems, a partner with a broad and diverse bench of pentesters and rigorous attention to methodologies is more likely to identify and execute the right approach for your company.

□ Scoping considerations

A good pentesting partner is one that can meet the scale and scope of your project without allowing the project to creep. Define the scope and parameters of your pentest quickly and consistently, ensuring everything is in one place, and your test can start on time (or even tomorrow).

□ Integration support

Not all platforms are built the same, and insights that are hard to access are rarely actioned. Find a pentesting partner that can support your workflow and integrate with your systems rather than having orphaned results languishing in PDFs and inboxes. Your partner must deliver their findings to the right team (in the right format) to best resolve issues and improve your risk posture.

□ Rotating experts on demand

With the right pentesting partner, you have access to a deep bench of experts, meaning you can rotate the individual testers without losing the relationship, integration setup, and institutional knowledge that comes with a long-term partner.

Conclusion

You now have the tools and questions needed to make informed decisions about your pentesting program. With the right partner and strategy, pentesting can serve as a cornerstone of your organization's journey toward sustainable security excellence and help you protect your business.

At Cobalt, we strive to be that partner:

SPEED

Cobalt can initiate pentests within 24 hours of onboarding. Plus, we provide real-time reporting and quick retesting for pentesting that matches your organization's pace.

SCALE

Regardless of your needs, Cobalt can craft a pentesting strategy that matches your business goals. No engagement is too small or large for our team to tackle, and our goal is to make security accessible, affordable, and aligned with DevSecOps best practices.

EXPERTISE

We're proud to employ the Cobalt Core, a team of vetted, highly skilled pentesters with deep expertise across diverse technologies, industries, and disciplines.

Ready to experience the benefits of PTaaS?

Level up your pentesting strategy with Cobalt's agile, scalable, expert-driven pentesting services. Cobalt's pentesters have you covered.

GET A DEMO AND SEE COBALT IN ACTION

GET IN TOUCH WITH A PENTESTING EXPERT