Cobalt Professional Services

Your Partner Beyond the Pentest

Cobalt

Modern pentesting for security and development teams

Companies of all sizes need manual penetration testing performed on their digital assets to establish trust with customers, comply with regulatory requirements, and improve their security posture.

Traditional pentesting services take weeks to schedule and deliver, work in isolation, and provide written results long after code has been released. This cumbersome and inefficient process does not fit with today's agile development practices, leaving companies exposed to the risk of breach.

Cobalt's Pentest as a Service (PtaaS) platform is modernizing traditional pentesting. By combining a SaaS platform with an exclusive community of testers, we deliver the real-time insights you need to remediate risk quickly and innovate securely.

- **Start Testing Faster:** Launch pentests in days, not weeks with our intuitive SaaS platform and team of on-demand security experts
- **Remediate Risk Smarter:** Accelerate find-to-fix cycles through technology integrations and real-time collaboration with pentesters
- **Make Security Stronger:** Mature your security program through a scalable, data-driven approach to pentesting

Professional Services to Strengthen Your Security Posture

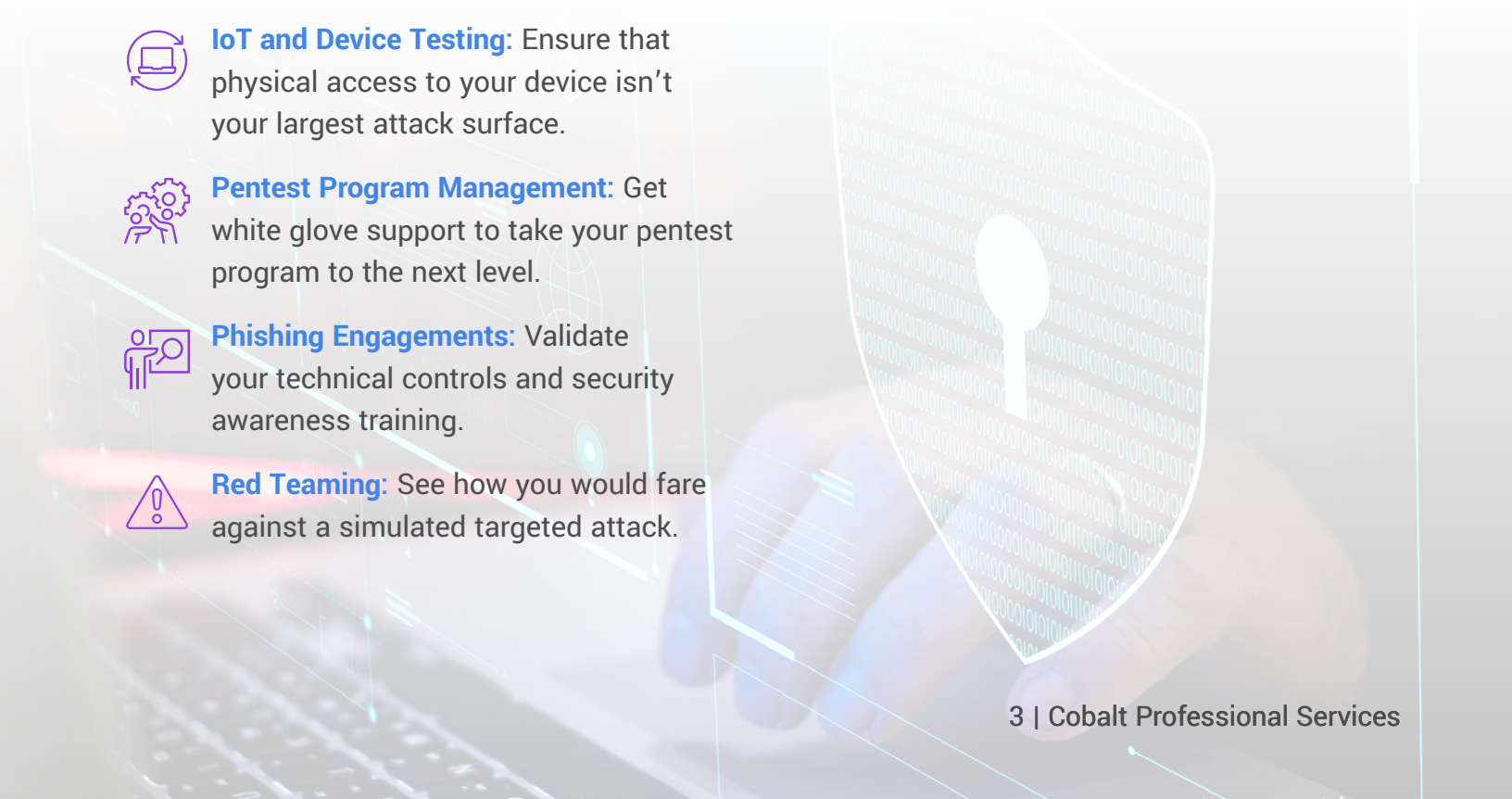
Organizations of every size and industry are seeking ways to improve their cybersecurity posture. At Cobalt, our goal is to be an ongoing resource for our customers and a true extension of their security team by helping them protect their broader IT ecosystems.

For this reason, we offer professional services designed to boost the maturity of your current security program and improve your overall security posture.

- **Advisory Services:** Never let a security question go unanswered due to a lack of time, talent, or resources.
- **Code Review:** Keep the critical details of your applications secure by strengthening their source code.
- **IoT and Device Testing:** Ensure that physical access to your device isn't your largest attack surface.
- **Pentest Program Management:** Get white glove support to take your pentest program to the next level.
- **Phishing Engagements:** Validate your technical controls and security awareness training.
- **Red Teaming:** See how you would fare against a simulated targeted attack.

"Security is very important for StartEngine and we have been able to tackle the job together with Cobalt to demonstrate this commitment to our customers. Cobalt's professional services gave us complete confidence that our security program was shaped to our unique needs."

JOE MATTHEWS
VP of Engineering
StartEngine



Advisory Services

Never let a security question go unanswered due to a lack of time, talent, or resources

Whether you need a second set of eyes on a presentation, help determining which security controls to focus on next, or an explanation of a compliance standard, Cobalt's Security Advisors are standing by to help. Sleep better at night knowing you are just one email away from having your security questions answered by seasoned industry professionals.

Gain quick access to their security expertise with no limit on utilization. Reach out at any time and receive a response within 48 business hours. Complex question? Don't worry, we've got you covered. We'll set up dedicated time to discuss your questions in detail.

Some of Our Areas of Expertise

DevSecOps: The entire industry is looking for ways to "shift left," but no two organizations run DevOps in exactly the same way. Our consultants can get you shifting left in the way that makes the most sense for how your team operates.

Risk Assessment: Carrying out your first risk assessment? Our consultants can provide a methodology, an implementation strategy, and a detailed risk assessment playbook template to guide you through the entire process.

Security Program Design: SOAR, XDR, GRC, VMS. New technologies and acronyms flood the market every day, but how do you know what is the correct next step for your program? Our consultants can help you gauge your program design maturity, and point you in the right direction.

Security Training: Our consultants can help you determine what level of security training is required at your organization and who should be trained on what. They can also provide you with training templates to ensure you're covering all of your bases.

Code Review

Keep the critical details of your applications secure by strengthening their source code

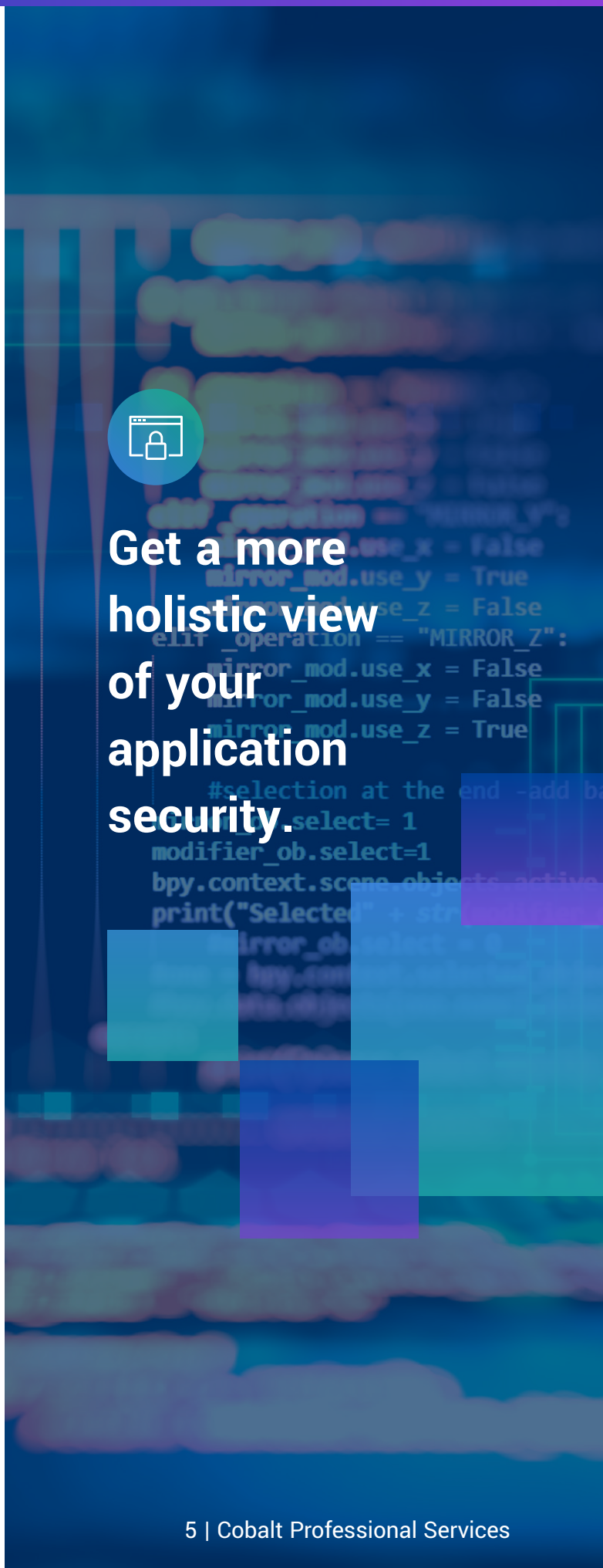
Not only does it contain all of the critical details of your application's functionality, it also holds insights into hidden, exploitable vulnerabilities.

Software Engineers work in fast-paced, agile environments where speed is critical. This can inevitably lead to coding mistakes that introduce vulnerabilities and increase your cyber risk. Our experienced engineers can skillfully review your code to identify these vulnerabilities and prevent a future breach.

Adding a Code Review to a Cobalt Pentest gives pentesters the necessary context they need to dig even deeper and provide even more coverage, resulting in a more detailed, comprehensive view of your application security.

Key Benefits

- Find hardcoded issues within your source code
- Discover vulnerabilities at their source
- Understand the risk associated with your source code being leaked



IoT and Device Testing

Ensure that physical access to your device isn't your largest attack surface

Internet of Things (IoT) devices are often part of a more complex ecosystem, each component with its own unique vulnerabilities. Many of these vulnerabilities can be discovered through traditional pentesting of the IoT infrastructure, APIs, and associated applications. However, that level of testing leaves the most potent attack vector uninspected — the device itself.

With years of experience in IoT and physical device testing, including medical, military, and government equipment, our highly qualified team of security consultants goes beyond normal network and application pentesting techniques and focuses on hardware, firmware, and radio communication vulnerabilities.

Whether you need assurances that your device won't fall victim to relay attacks, or you want us to disassemble the unit and attempt JTAG debugging, we can help ensure that physical access, or proximity, to your company's IoT devices doesn't leave you unnecessarily vulnerable. Additionally, if you need the entire IoT ecosystem tested, we can help there too.

Key Benefits

- Gain a holistic view of your IoT ecosystem's security posture
- Understand the unique risks associated with physical device access
- Ensure, within reason, that your device isn't the cause of a wider network compromise
- Hedge against supply-chain attacks with firmware testing

Experience in IoT and physical device testing, including medical, military, and government equipment.

Pentest Program Management

Get white glove support to ensure you get the most out of your pentest program

Whether your organization has tens, hundreds, or even thousands of applications, keeping track of your assets and the teams responsible for their development, maintenance, and security can be an operational nightmare.

That's where our Pentest Program Manager comes into play. From day 1, you'll be partnered with a seasoned security consultant to help with asset identification, prioritization, pentest setup, integration support, recurring security roundtables, strategic planning, and more. Consider your Pentest Program Manager an extension of your security team.

Key Benefits

- Optimize the end-to-end pentest process with team onboarding, technical scoping, strategic planning, and more.
- Improve overall security posture by maturing your pentest program
- Reduce tribal knowledge by capturing key asset information within the platform and onboarding new teams and team members
- Ensure that pentesting is not done in a silo, but is informed by your wider security strategy

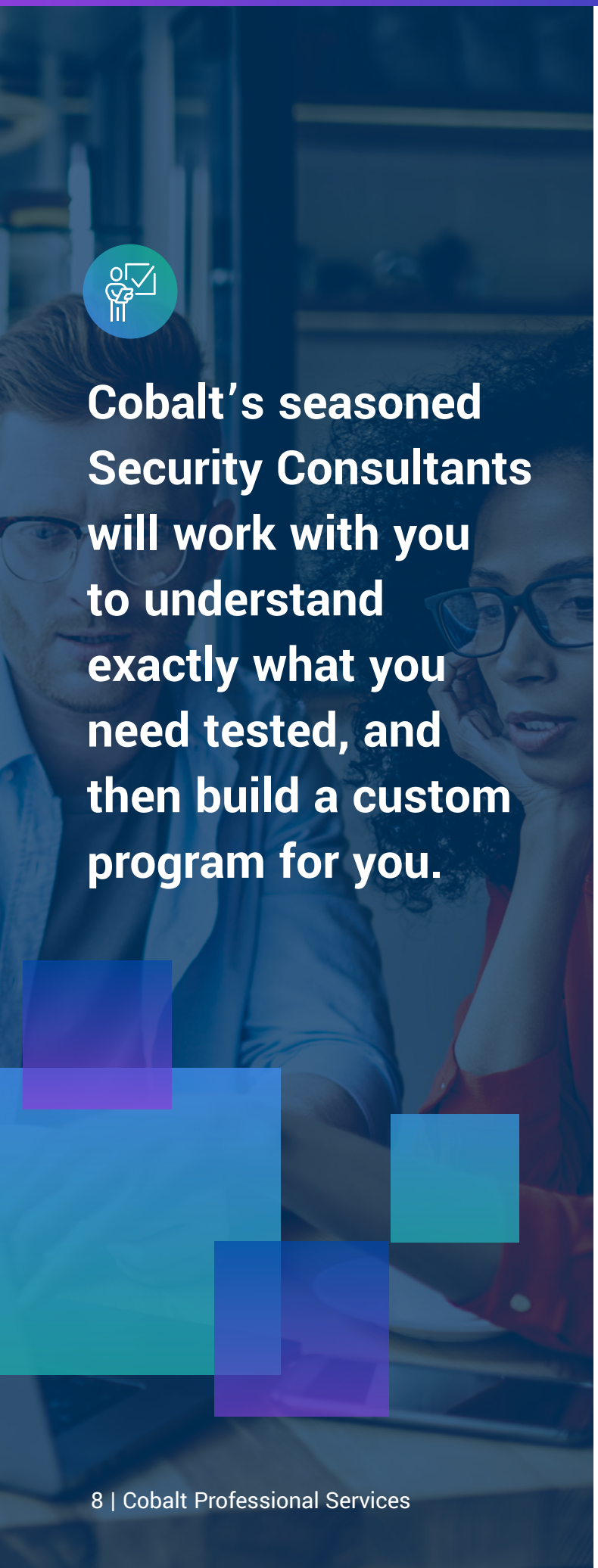
Offering Details

Onboarding for All Teams: From account setup to platform walkthroughs, we'll ensure your teams have the information they need to succeed. Additionally, we'll be available to provide comprehensive platform walkthroughs for your teams in a group setting.

Strategic Planning: Starting with your end goals in hand, we'll help you build out an optimal testing plan based on asset criticality and business needs. We'll also provide ongoing scheduling guidance to enhance your pentest program's effectiveness.

Technical Remediation Guidance: We'll partner with your internal teams to help track and manage remediation efforts. While your internal teams will make the fixes, we'll provide guidance every step of the way, as well as follow up on a regular cadence to help track remediation versus target.

Quarterly Maturity Assessment: Utilizing objective scoring and concrete guidance, we can help take your program to the next level. Each assessment will be done using Cobalt's framework for maturity, which is based on data from our 900+ customers.



Cobalt's seasoned Security Consultants will work with you to understand exactly what you need tested, and then build a custom program for you.

Phishing Engagements

Validate your technical controls and security awareness training

One of the most common causes of a breach is a successful phishing campaign. Whether it is a targeted campaign against your C-suite (whaling) or a spray-and-pray campaign, it is important to understand how your controls and users stack up to this increasingly regular attack method.

Cobalt's seasoned Security Consultants will work with you to understand exactly what you need tested, and then build a custom program for you. We can test your technical controls through a complex campaign or dial the complexity back and test your end users.

At the end of the campaign Cobalt will supply you with a detailed anonymized report. We do not believe in naming and shaming those who failed the test. Instead, we focus on important statistics and concrete remediation guidance. The more regularly you test with us, the more valuable our data and the tests themselves become.

Key Benefits

- Test your technical security controls to validate efficacy
- Gauge the effectiveness of your security awareness training
- Make data-driven decisions around the most common method of data breach
- Ensure your environment is holistically tested for vulnerabilities

Red Teaming

See how you would fare against a simulated targeted attack

Understanding what vulnerabilities exist in your environment is just the beginning. Red teaming gives you a clear look at what a motivated attacker can do when exploiting these vulnerabilities. By simulating the movements of an adversary, we are able to understand your most critical risks and actively test your defenses.

Our experienced consultants work closely with you to design the perfect attack plan and rules of engagements to meet your unique goals. While the engagements may be custom, the methodologies are not. We always design our attack plans to use known tactics, techniques, and procedures that malicious attackers are using in the wild.

Whether you want to test your security defenses or see what could happen if you were targeted, we are happy to help.

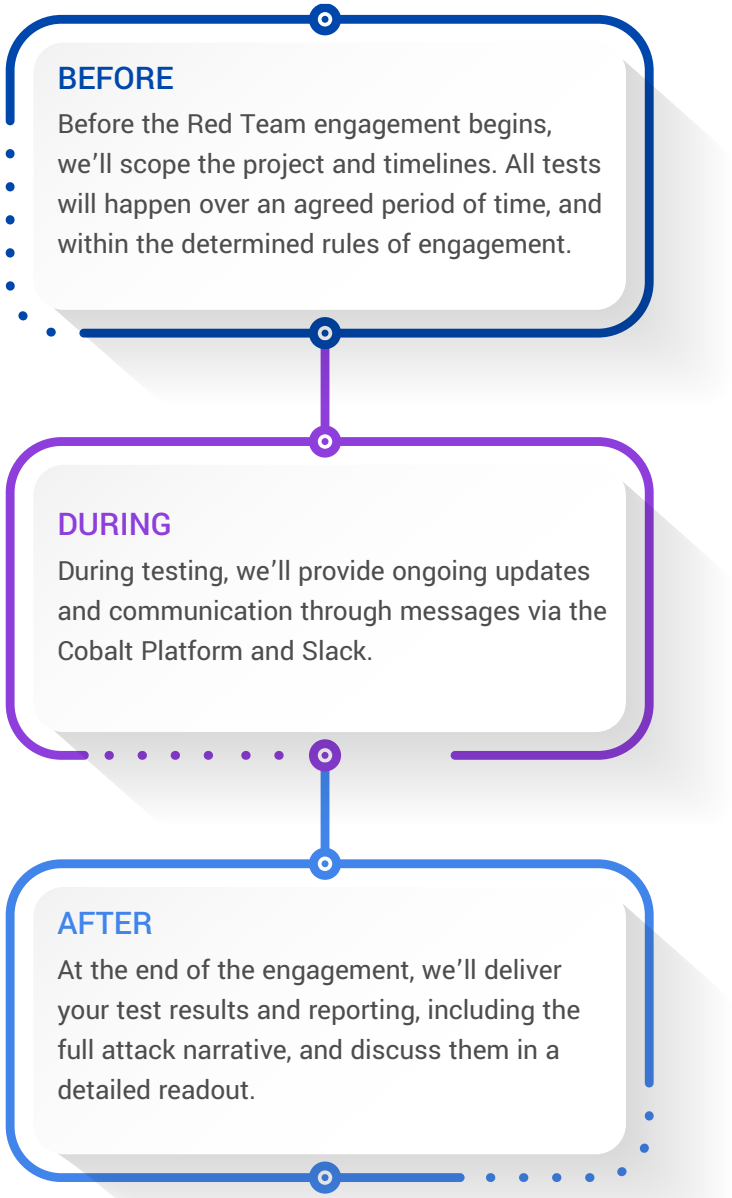
Key Benefits

- Test the strength of your defenses
- Better understand your unique technical risk
- Safely simulate a breach
- Validate your security posture to executives
- Ensure the effectiveness of your Incident Response playbooks

How It Works

Cobalt's Red Teaming services are an extension of Cobalt's modern streamlined pentesting platform. Our security experts will define the scope of work and timelines before kicking off the testing process. Testing is transparent and collaborative – you'll have consistent communication through Slack and Cobalt's platform.

At a high level, here's what you can expect from a Red Team engagement:



The Power of PtaaS

Talent: No two applications are the same, so we bring the right combination of skills, performance, and experience to fit your pentesting needs.

Speed: With the Pentest Wizard, you can easily set up a pentest in four guided steps. We'll review your submission and assign pentesters with skills best suited to your needs.

Collaboration: Collaborate with Cobalt pentesters through real-time, in-app vulnerability findings. Get quick status updates and discuss details throughout the process with our Slack integration.

Integration: Integrate into your SDLC with Jira and GitHub, or use the Cobalt API to sync with your remediation teams and fix findings faster.

Results: Customize reports to best suit your audience. We offer a variety of templates, including a full pentest report with finding details, a customer letter, and an attestation.

Validation: Close the remediation loop by submitting your fixed findings for [free] unlimited retesting. Direct retesting efforts with thoroughly documented pentest data.

Progress: View findings data over time to improve security outcomes with the Insights feature. Analyze trends by pentest type, status, criticality, time to fix, and more.

"The main benefits that we get from Cobalt are speed, scalability, and repeatability. We're able to quickly launch and execute pentests; and beyond that, we're able to see individual findings in real time and relay them to the engineering team so they can start triaging immediately."

ERIC GALIS, VP of Compliance & Security at Cengage

PtaaS versus Traditional Consultancies

Pentests start in days, not weeks. You receive a notification as soon as a vulnerability is found. Manual security testing supports DevOps sprints and helps to prevent breaches without slowing down releases. It's not a dream – it's Pentest as a Service.

Traditional Consultancies		VS		Pentest as a Service
Static, encrypted results and reporting (e.g. PDF)		DELIVERY		Real-time results and reporting via a cloud platform
Tests can start in 4-7 weeks		START TIME		Tests can start in 24 hours
A limited pool of in-house pentesters, constrained by location		TALENT		A large, diverse group of freelance pentesters, available to work remotely
Daily or custom pricing		PRICING		Flexible SaaS model
No integrations or technology-enabled collaboration workflows		COLLABORATION & INTEGRATIONS		Technology workflows improve interactions between teams
No analytics from previous tests, difficult to review		ANALYTICS		Analytics and insights from pentest data
Manual knowledge transfer from one test to another		DATA REUSABILITY		Platform retains knowledge of past and ongoing tests
Charged extra		RETESTING		Included, unlimited

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

San Francisco | Berlin | Boston

cobalt.io