Cobalt

Cobalt Red Team

Attackers don’t need to find all the vulnerabilities in your environment, they just need one. Simulate attacks with the Cobalt Red Team to better understand the effectiveness of your security controls and discover the impact of a breach.

Red Team engagements from Cobalt simulate threats from real-world adversaries, leveraging the Tactics, Techniques, and Procedures (TTPs) that actual attackers use. Our team of experts will test the effectiveness of your existing security controls and defenses, including your incident response processes. Our goal is to identify gaps in detections, gauge the efficacy of your security operations center (SOC), and discover the true impact of a breach on your organization.

Cobalt Red Team uses techniques from the MITRE ATT&CK framework along with proprietary methodologies to help you understand how a determined and skilled remote adversary might compromise digital assets to achieve a specific objective, like stealing user data and intellectual property.

Red Team Services	Description and Tactics
Initial Access External	Determine the external security posture of your organization to see if an internet-based attacker could break in from the outside. This includes understanding your digital footprint, identifying potential targets, testing publicly accessible systems, and simulating phishing attacks to secure at least one foothold within your environment.
Assumed Breach Internal	Demonstrate the impact an attacker could have once they have access to your systems. This includes establishing a covert foothold, attempting to gain higher privileges, evading internal defenses, seeking out sensitive credentials, mapping and moving through the network, all while maintaining control in an attempt to extract data.
Initial Access and Assumed Breach External + Internal	A combined approach to determine both the effectiveness of your external security posture and perimeter defenses, followed by an assessment of the impact of an attacker once they gain access to your systems.

EXAMPLE RED TEAM OBJECTIVES

- Test perimeter defenses
- Test employees ability to detect phishing emails
- Assess access control effectiveness
- Validate incident and internal threat detection
- Test containment and response
- Assess privilege escalation and data exfiltration prevention
- Meet compliance frameworks including: NIST SP 800-53, CMMC, ISO 27001, PCI DSS, CSCRF, etc.

The Power of Cobalt

Cobalt provides Offensive Security Solutions for programmatic risk reduction by combining technology with human expertise, delivering unmatched speed and scale to reduce risk.

SPEED

Launch with confidence. Cobalt delivers fast, on-demand testing so you can get your ideas to market quickly without sacrificing security

- **24 Hours** to Start a Pentest
- **7 Day** SLA for Retesting

SCALE

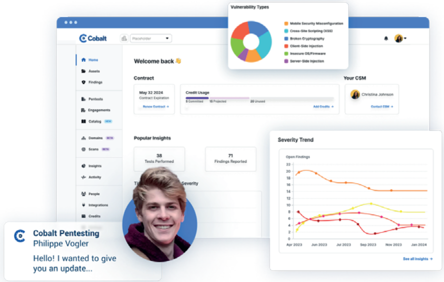
Get the efficiency of automation with the precision of experts. Broad, continuous testing across all assets; enabled by technology, optimized for growth

- **200+** Pentests Live Everyday
- **10k+** Critical or High Severity Vulnerabilities Discovered by Cobalt

EXPERTISE

Protect your business against evolving threats with expert-led assessments that fortify your business

- **450+ Pentesters** in the Cobalt Core
- **11 Years** of Pentesting Experience on Average
- **5% Acceptance Rate** Into the Cobalt Core



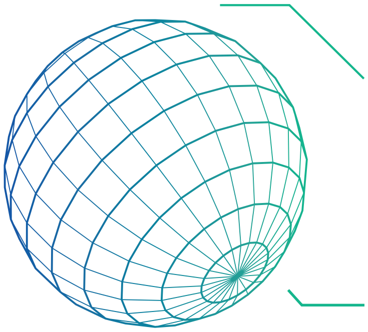
Hello! I wanted to give you an update...

Offensive Security Program

Cobalt Red Teams are a valuable part of a larger security testing program. When paired with External and Internal Network Pentesting, Web Application and API Pentesting, and other offensive security services, your team can ensure coverage with a holistic view of risks and exposures. Combining Red Teaming and Pentesting from a trusted partner like Cobalt ensures a deep understanding of your environment, and the same support you value from our services. This is the most popular approach to red teaming.

Cobalt Core

The Cobalt Core is our community of 450+ rigorously vetted pentesters. These seasoned ethical hackers average 11 years of pentesting experience, and hold certifications such as CEH, CISSP, OSCP, and CREST. Acting as an extension of your security team, the Cobalt Core uses manual and automated offensive security tactics to uncover critical vulnerabilities through pentesting, red teaming, code reviews, and more. Reduce risk, unblock sales and new releases, and enhance your overall security posture with expert services from Cobalt.



5000+
PENTESTS DELIVERED ANNUALLY

450+
PENTESTERS

Ready to test your defenses with the Cobalt Red Team?
Contact your CSM or get started with a demo today at www.cobalt.io/get-started

Cobalt

WWW.COBALT.IO
SAN FRANCISCO • LONDON • BERLIN