Market Insight Report Reprint

Coverage Initiation: Cobalt aims to modernize traditional penetration testing with its pentest-as-a-service model

June 15 2021

by Aaron Sherrill

The provider is aiming to modernize the traditional penetration testing model by delivering programmatic, on-demand, manual penetration testing services for web, mobile and desktop applications, APIs, and internal and external networks.

451 Research

S&P Global
Market Intelligence

Introduction

Enterprises have traditionally relied on compliance-focused third-party assessments and audits to test and assess their defenses, applications, networks and workflows to meet regulatory, customer and partner demands. Constrained by scope and limited by the amount of time, resources and expertise allocated to the assessment, traditional annual penetration tests conducted by consultancies often fail to meet the testing demands of modern, fluid IT ecosystems underpinned by ongoing digital transformation and frequent software releases and updates.

Cobalt Labs, a pentest-as-a-service (PtaaS) provider, is aiming to modernize the traditional penetration testing model by delivering programmatic, on-demand, manual penetration testing services for web, mobile and desktop applications, APIs, internal and external networks. Integrating people and technology into a SaaS platform, the company is focused on empowering organizations to remediate risk quickly and innovate securely.

THE 451 TAKE

Data from 451 Research's recent Voice of the Enterprise: DevOps, Organizational Dynamics survey shows that a growing percentage of organizations (41%) are accelerating or newly introducing initiatives to add security to DevOps workflows. However, organizations are finding that traditional annual penetration testing engagements often fail to deliver the outcomes needed for rapid development cycles. Providing only a point-in-time snapshot of an enterprise's risks, weaknesses and vulnerabilities, traditional assessments typically offer little to no interaction with testers during or after testing activities, provide limited retesting capabilities to ensure issues have been fully remediated, and fail to deliver the insights needed for a data-driven security program. Continuous, collaborative, on-demand penetration testing capabilities, like those offered by Cobalt, can help organizations improve their application security posture amid frequent releases, updates and changes.

Context

Originally headquartered in San Francisco and now fully remote, Cobalt was founded in 2013 by CEO Jacob Hansen, Esben Friis-Jensen, Jakob Storm and Christian Hansen, all self-identified as outsiders to the cybersecurity space. With 200+ employees, 300+ penetration testers and 800+ customers, the privately held company reports it has experienced 70% year-over-year revenue growth. The company's client base, spanning a variety of industries, includes HubSpot, Vonage, MuleSoft, Verifone, Zuora and SolarisBank.

In August 2020, Cobalt announced it had raised a $29m series B round, bringing its total funding to $37m. The round was led by Highland Europe, a global venture capital firm whose portfolio includes Malwarebytes, Nexthink, Adjust, ContentSquare and WeTransfer.

According to Cobalt, security is the outcome of the unpredictable decisions and actions made by many different people and groups throughout the organization, including security engineers, developers, and IT and network engineers. At the same time, organizations are finding that traditional penetration testing is too slow and static to be highly effective in continuous development pipelines. As a result, the company has developed a PtaaS platform coupled with a community of vetted penetration testers to deliver on-demand security testing that produces interactive, real-time, prioritized insights and findings, helping organizations reduce risk and remediate vulnerabilities.

Platform and services

Cobalt describes its PtaaS platform as a penetration testing management and orchestration system that delivers the people and process innovation required to drive better security. Positioned to align with agile and DevOps development practices, the platform enables organizations to quickly configure penetration tests that can begin executing in 24 hours. This approach contrasts with traditional penetration services that can take weeks to months to schedule, execute and deliver, as well as crowd-sourced 'bug bounty' programs that are crowd-powered and rely on a 'pay for results' model.

Designed to accelerate the cycle of detecting and remediating risks, the platform enables security and developer teams to collaborate with testers in real time, promoting transparency and helping organizations better understand findings and how to resolve issues. The platform also blends into the organization's software development lifecycle (SDLC) process, providing bi-directional integration with Jira, Github and Slack, enabling developers to seamlessly manage findings through their preferred workflow system. Integrations help development teams establish accountability for each finding, a key factor in ensuring that identified weaknesses do not go unaddressed. The ability to initiate (unlimited) retesting to validate that a weakness or vulnerability has been fully addressed can be automated as part of the integrated remediation process.

In June, Cobalt launched its public API, giving organizations the ability to automatically integrate data from assets, penetration tests and findings into the rest of their technology stack, including GRC platforms and other development tools.

Cobalt says its curated penetration tester community, known as the Cobalt Core, is the platform's greatest asset. The group is composed of over 300 vetted penetration testers with a broad range of specialized testing skills and 5-10+ years of penetration testing experience on average. Cobalt says that less than 5% of applicants pass its in-depth interview and vetting process, which includes extensive technical assessments, soft skills assessments and background checks. In addition, pentesters are continually evaluated on communication skills, technical skills and overall performance by customers and other pentesters in the Core community as well as Cobalt's own team members. The company believes the breadth and depth of skills of pentesters in the community give it the scale to deliver on-demand skills and expertise needed to match any given customer's specific technology stack.

In 2020, the company introduced a new delivery model to standardize costs with a unit of work and increase the flexibility of consumption for its customers. With the new model, called Cobalt Credits, customers can consume on-demand pentesting services that match the specific needs, priorities and budgets of the organization. The company believes the model is differentiated, standing in contrast to both the traditional 'all in scope' assessment model of traditional penetration testing firms and other PtaaS providers that typically charge a set monthly or yearly fee for a defined scope of pentesting services whether they are used or not.

In April, Cobalt announced the launch of its partner program. With options for both referral and reseller partners including consultancy firms, managed service providers and professional service firms, Cobalt believes its partner program will quickly become a significant part of its sales approach.

Competition

Competition in the broader security testing space is escalating as firms go to market with capabilities and flexible services that modernize traditional penetration testing. Although many traditional security testing firms, technology vendors and service providers are adding a variety of testing capabilities to their existing tools and services, most providers in this space tend to be primarily focused on either automated or manual security testing.

Cobalt competes with an abundance of traditional global and regional consultancy and penetration testing firms including PWC, BishopFox, Caliber, Accenture, Cigital, IOActive, Optiv and the NCC Group. At the same time, the company faces competition from firms such as BugCrowd, HackerOne, ZeroCopter, Synack, Intigriti, NetSPI, Pcysys, Passpoint and other providers seeking to modernize traditional penetrating testing models with a variety of continuous or automated delivery, service platforms, bug bounty and crowdsourced approaches.

SWOT Analysis

STRENGTHS

Organizations of every size and industry are seeking to improve their cybersecurity posture; however, access to frequent security testing has been beyond the scope of expertise and resources of most organizations. Cobalt's flexible, tailored and integrated approach to on-demand, programmatic security testing is designed to meet the needs of both rigorous testing approaches and organizations that are just beginning their security testing initiatives.

WEAKNESSES

Cobalt provides in-depth, flexible, on-demand security testing services focused primarily on the organization's application tier. The company's services do not fully address penetration testing needs for the organization's broader IT ecosystem, although Cobalt has plans to address this gap via the rollout of professional services offerings planned for later in 2021. In the meantime, a comprehensive approach to penetration testing will require organizations to leverage multiple penetration testing providers.

OPPORTUNITIES

The newly launched partner program should prove to be a force multiplier for the company enabling partners such as consultancies and MSPs/MSSPs to bring Cobalt to a broader audience while enabling partners to deliver greater value to their customers with penetration testing services.

THREATS

While programmatic penetration testing is becoming increasingly pivotal, especially in light of recently well-publicized attacks and breaches, many organizations are reluctant to leave their traditional testing partners and embrace a more modern approach to penetration testing.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence