CYCOGNITO bugcrowd

SOLUTION BRIEF: CYCOGNITO + BUGCROWD

Automated Reconnaissance for Crowdsourced Testing

Drive Efficient Bugcrowd Services with the CyCognito Platform

The Challenge

Most enterprises have a significant number of unknown digital assets exposed to the Internet. Unmanaged and untracked, these assets represent the most common threat vector[1] and are the majority of external risk.

External assets can change 10% per month[2]. Proactive identification, testing, prioritization and remediation are critical to keep pace with risk, but a continuous approach across the full external attack surface is difficult to operationalize and maintain.

The Solution

CyCognito's external attack surface management (EASM) solution combined with Bugcrowd's Security Knowledge Platform provides industry-leading insight and immediate access to the right combination of human-led skills and automated insight to complement every stage of your journey.

Bugcrowd's continuous security approach enables smarter security and faster time to results. Using the CyCognito platform, Bugcrowd customers provide hackers and pentesters working in their crowdsourced security programs with a comprehensive map of the external attack surface along with attribution, business context, and test results for each asset. This significantly reduces time spent obtaining data through manual reconnaissance or waiting for information from stakeholders.

Key Benefits

Automatically map external attack surface, contextualize and test all exposed assets

Leverage hacker ingenuity for pen testing, bug bounty, vulnerability disclosure, and more

Dig in deep to uncover high-impact flaws and hidden risks

Access the right risk skills sets on demand with elastic capacity

[1] 83% of breaches are caused by those external to an organization. Source: Verizon Data Breach Investigation Report, 2023

[2] Source: CyCognito State of Exposure Management Report, Summer, 2023

Business Value

Use Case	Value
Organizational reconnaissance	Automatically find and track previously unknown and unmanaged business entities
Asset discovery	Dynamically maintain a complete external asset inventory, globally
Asset classification and attribution	Understand the criticality of each asset to the business and where the asset resides
Security testing/DAST	Uncover complex issues and validate known issues across all assets, including web application testing/DAST
Targeted vulnerability discovery	Enable hackers and pentesters on the Bugcrowd Platform to find hidden high-impact flaws productively and efficiently
Expanded IT Security skill sets	Access to specific tester skills on demand, with elastic capacity
Real-time access	Real-time visibility into test status and prioritized results and Integration with DevOps tools via turnkey connectors, webhooks, and API

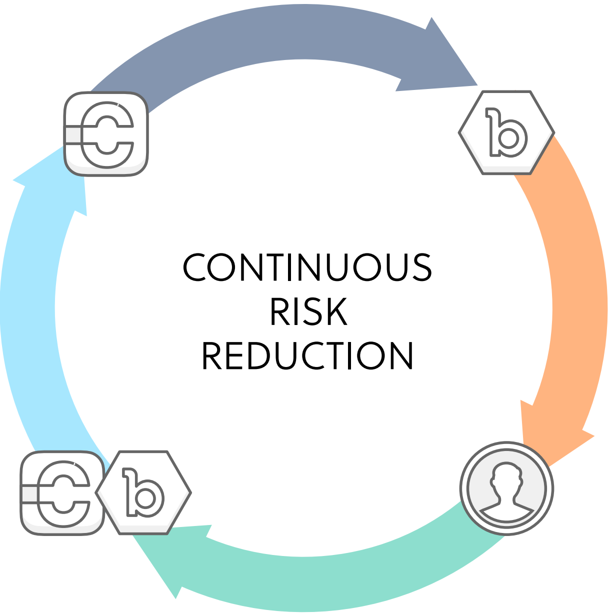
Technical Overview

Together, CyCognito and Bugcrowd invert the asset discovery and risk reduction paradigm.

CyCognito uses machine learning (ML) and natural language processing (NLP) technologies to automatically build a graph data model that represents your organization's business structure. CyCognito uncovers exposed assets, adds attribution and business context, and performs extensive security tests, including DAST for web apps.

The Bugcrowd Platform leverages this continuously updated intelligence for tailored pen testing and bug bounties for your organization. Bugcrowd's precisely curated hackers and penetration testers dig deep; revealing hidden risks that are validated and prioritized by the platform for fast remediation. Bugcrowd's rich analytics and reporting capabilities allow you to see triaged findings in real time and flow them into your DevSec workflows.

To be meaningful, external risk must be assessed frequently and deliver comprehensive results with high accuracy. A manual approach is nearly unachievable on even a modest-sized network. Through the combination of CyCognito and Bugcrowd it is possible to consistently uncover change, validate strengths and identify weaknesses, the latter of which CyCognito calls "the path of least resistance."



Discover & Test

CyCognito performs continuous reconnaissance finding new organizations, assets, and security risks.

Validate & Exploit

Bugcrowd sources the penetration testers on-demand that specialize on the issues uncovered by CyCognito.

Verify

CyCognito will perform an automated revalidation of the issue, and a Bugcrowd tester will confirm manually, providing 100% confidence that the issue is resolved.

Remediate

The Customer will remediate or mitigate the issue.

About CyCognito

CyCognito is solving one of the most fundamental business problems in cybersecurity: the need to understand how attackers view your organization, where they are most likely to break in, and how you can eliminate that risk. It does this with a category-defining, transformative platform that automates offensive cybersecurity operations to provide reconnaissance capabilities superior to those of attackers.

About Bugcrowd

Bugcrowd helps customers deflect cybersecurity threats by activating trusted hackers to take back control of the attack surface. Our AI-powered, crowdsourced security platform is built on the industry's richest repository of vulnerabilities, assets, and hacker profiles, engaging the perfect hacker talent on demand for multiple security goals while providing all the scalability and adaptability needed for present and future threats.

For more details on this unique approach please contact CyCognito at **bugcrowd@cycognito.com** or Bugcrowd at **cycognito@bugcrowd.com**.