bugcrowd

DATA SHEET

Aligning With Binding Operational Directive 20-01

Take the fast path to compliance and risk reduction with CISA's VDP Platform powered by Bugcrowd

CHALLENGES

Vulnerability disclosure policies are a federal mandate: Binding Operational Directive (BOD) 20-01, issued by CISA, requires all 100+ Federal Civilian Executive Branch (FCEB) agencies to develop and implement such a policy. A Vulnerability Disclosure Program (VDP) is a highly effective security solution for meeting that goal by accepting and prioritizing vulnerabilities reported by the public under safe harbor – essentially, a VDP is a digital "neighborhood watch" staffed by volunteer security researchers. However, building and maintaining a VDP long-term with internal resources is beyond the capabilities of most organizations, regardless of size.

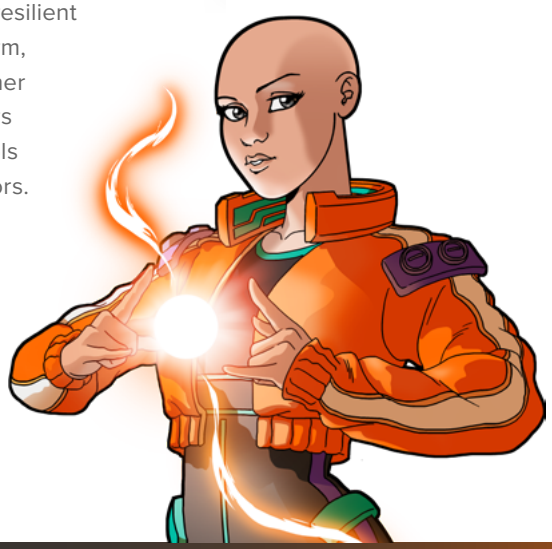
SOLUTION

To help FCEB agencies meet these requirements, CISA has partnered with Bugcrowd and EnDyna to provide a VDP-as-a-service platform that makes adoption an efficient, resilient process with rapid time to value. By adopting the VDP Platform, FCEB agencies can connect with the global security researcher community for scaled testing that goes beyond what scanners can deliver, accessing the diverse skills, perspective, and tools needed to proactively protect agency assets from threat actors.

In 2022, the 40+ agency programs on the VDP Platform received 1,300+ valid submissions (nearly 200 of them being critical), 84% of which have been remediated within 38 days on average (per CISA's *Vulnerability Disclosure Policy Platform Annual Report 2022*).

Key Benefits

- ✓ Proactively reduces risk, typically delivering a 25x increase in vulnerability reports
- ✓ Cuts MTTR, with an average remediation time of 38 days
- ✓ Builds awareness and productive relationships with the security researcher community
- ✓ Streamlines future bug bounty adoption
- ✓ Serves as proof point for mature security culture



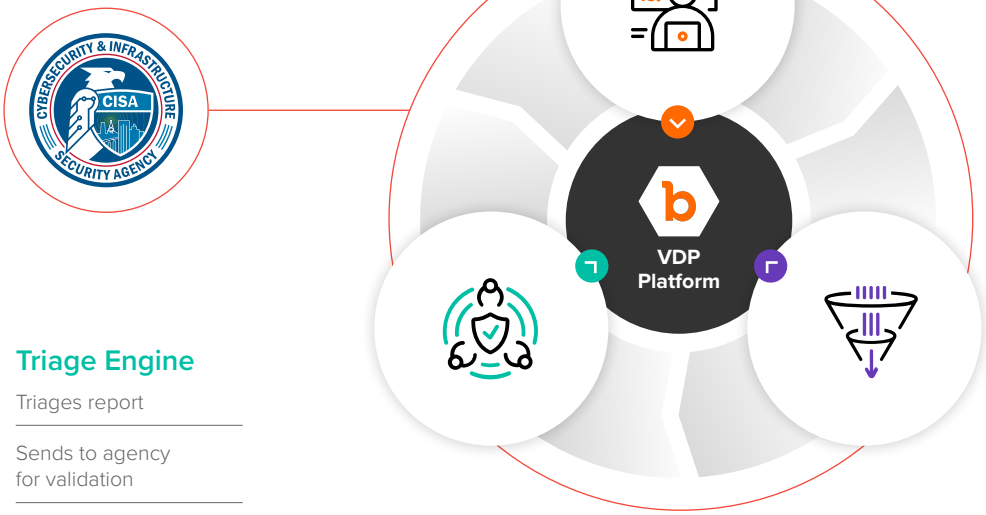
BUGCROWD

DATA SHEET

Key Capabilities

- ✓ Clearly defines vulnerabilities and disclosure policies
- ✓ Generates and submits required metrics for BOD 20-01 reporting
- ✓ Provides human-driven testing at scale to find flaws that scanners miss
- ✓ Intakes, triages, and communicates submissions under safe harbor
- ✓ Integrates with DevSec workflows for fast remediation
- ✓ Offers managed bug bounty and pen testing-as-a-service capabilities on a unified platform for a single view of vulnerabilities
- ✓ Reduces onboarding costs – service is available via CISA free of charge through February 2025

Central Oversight & Governance



Researcher

Easy access to participating agencies' VDPs through VDP Platform dashboard

Searches for vulnerabilities and submits reports through the VDP Platform

Agency

Receives alert from the VDP Platform on vulnerability submission

Receives triaged report from Bugcrowd and validates it

Remediates valid vulnerabilityreports

Triage Engine

Triages report

Sends to agency for validation

Coordinates with researcher

CDAO

87% of researchers believe that reporting a critical vulnerability is more important than trying to make money from it[1].

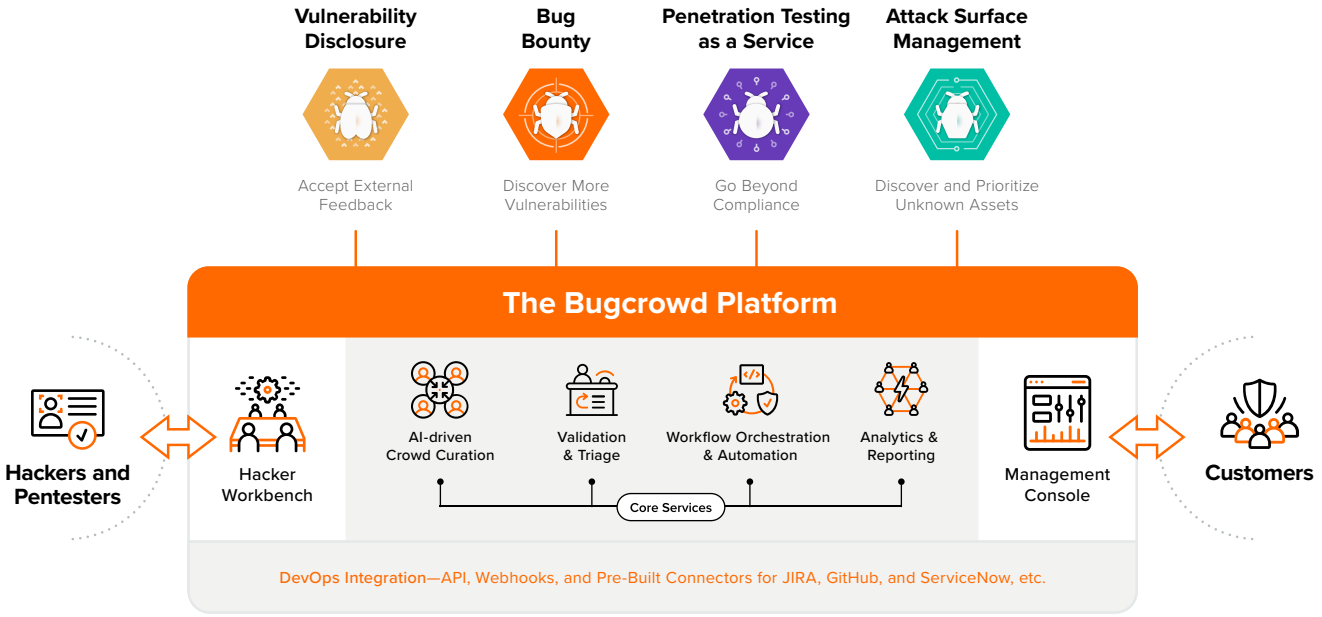
[1] Inside the Mind of a Hacker Report (2023)

BUGCROWD

DATA SHEET

Why Bugcrowd

The Bugcrowd Platform helps customers defend themselves against cybersecurity attacks by connecting with trusted, skilled hackers to take back control of the attack surface. Our AI-powered platform for crowdsourced security is built on the industry's richest repository of data about vulnerabilities and hacker skill sets, activating the ideal hacker talent needed on demand, and bringing scalability and adaptability to address current and emerging threats.



BEST SECURITY ROI FROM THE CROWD

We match you with trusted security researchers who are perfect for your needs and environment across hundreds of dimensions using machine learning.

INSTANT FOCUS ON CRITICAL ISSUES

Working as an extension of the platform, our global security engineering team rapidly validates and triages submissions, with P1s often handled within hours.

CONTEXTUAL INTELLIGENCE FOR BEST RESULTS

We apply over a decade of knowledge accumulated from experience devising thousands of customer solutions to achieve your goals for better outcomes.

CONTINUOUS, RESILIENT SECURITY FOR DEVOPS

The platform integrates workflows with your existing tools and processes to ensure that apps and APIs are continuously tested before they ship.

TESLA indeed credit karma Pinterest mastercard ATLASSIAN

Start your stress-free managed migration to Bugcrowd

Make Moves