How security leaders are scaling testing with bug bounty programs

BY ELEANOR BARLOW · JULY 15, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How security leaders use bug bounty programs to scale cybersecurity testing beyond traditional methods** like scans and periodic tests to achieve continuous, real world vulnerability discovery.
- **How to design and launch an effective bug bounty initiative at scale**, including choosing public vs private models, setting reward tiers, and integrating findings into your security workflows.
- **How bug bounty programs improve vulnerability management and ROI** by augmenting internal teams, measuring performance metrics, and strengthening security posture as organisations grow.

For security leaders protecting fast-growing organizations, the pressure is on to identify vulnerabilities before threat actors do. Continuously testing environments, cost-effectively and at scale, is a significant challenge.

This is where **bug bounty programs** are reshaping the security landscape for CISOs, IT directors, and product security leads.

If you are ready to move beyond checkbox compliance into **real-world, proactive defense**, this approach could be your next strategic advantage. Read on for details on how to lead the shift.

What is a bug bounty program?

A bug bounty program is a structured initiative where ethical hackers, also known as security researchers, are rewarded for discovering and reporting vulnerabilities in your software, systems, or applications.

Unlike traditional testing methods, bug bounty programs operate **24/7**, leveraging a **global pool of vetted experts** to find issues before threat actors do. Whether you're running a **private invite-only program** or going fully public, bug bounty programs are flexible and customizable for companies of all sizes.

When traditional tests fall short

Most security leaders are familiar with scanning and **penetration testing** and the many benefits they bring. Issues can arise if traditional tests like these are the sole cybersecurity initiatives in a company, which can mean time-bound, periodic testing, with limited scope and budget. These tests alone do not reflect or replicate the evolving nature of real-world threats.

By combining focused research (like PTaaS) with continuous testing that comes with a **bug bounty,** customers like UpCloud **gain** continuity and scale.

How CISOs use ethical hackers to strengthen security

One of the biggest shifts in mindset in modern cybersecurity leadership is the **strategic use of ethical hackers.** Today's CISOs understand the benefit of tapping into a global pool of security researchers, each with different areas of expertise and skillsets, to:

- Simulate real-world attacks across an expanding digital surface.
- Discover edge-case vulnerabilities missed by internal or automated tools.
- Augment lean security teams with external expertise.
- Build resilience and responsiveness into their vulnerability management process.

As organizations scale, the **power of the collective** becomes a force multiplier; ethical hackers are your eyes and ears across the internet.

How to get started with a bug bounty platform

Modern platforms like Intigriti make it easy for companies to design and launch a program tailored to their needs. Here's how:

- Define the **scope**, such as web apps, APIs, or infrastructure.
- Choose whether to run a public program or a **private bug bounty program** with invited researchers.
- Set **reward tiers** based on severity and impact.
- Receive validated reports directly into your existing workflows.

This ensures you're always in control of researcher access, submission volume, and the triage process, while pushing the heavy lifting away from you and your team.

Cost-effective security with measurable ROI

Unlike traditional security assessments that charge flat, time-based fees, bug bounty programs are **performance-based**, which means you only pay for **valid vulnerabilities**. This makes it easier to show ROI and justify spend to boards and executive stakeholders.

How to run a private bug bounty program

Many organizations begin with a **private bug bounty program**, inviting a handpicked group of researchers to test specific systems. This offers:

- Greater control and lower signal-to-noise ratio.
- The ability to test sensitive assets without going public.
- An easy entry point for scaling later into public programs.

You decide when and how to expand and always retain full control.

How to scale vulnerability management

Bug bounty programs are now a cornerstone of how **CISOs scale** vulnerability management across distributed teams and fast-changing hybrid environments. Key steps include:

1. Integrating bounty findings into SDLC and DevSecOps pipelines.
2. Aligning bounty program insights with internal risk assessments.
3. Continuously tuning the scope and researcher access.
4. Measuring metrics like time-to-remediate and severity trends.

With the right structure, bug bounty programs help transform vulnerability management from reactive to **predictive and continuous.**

Ready to lead the shift?

CISOs and tech leaders, like NVIDIA, are incorporating bug bounty programs as **a core pillar of their cybersecurity strategy.** Whether you're managing a small team or leading a mature enterprise program, platforms like Intigriti help you stay ahead of threats while optimizing resources.

“Our researcher community is the beating heart of our bug bounty platform, identifying hard-to-find vulnerabilities and improving security for our customers. Investing in this community isn’t just something we do; it’s at the very core of how we operate.” – Soti Giannitsari, in ‘Power of the Collective’

Want to learn more about how **bug bounty programs can** support you in achieving your business goals? Contact us today to build a bug bounty program aligned with your risk profile, security posture, and compliance roadmap.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years’ experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.