# Scaling your bug bounty program: strategic guidance for CISOs and cybersecurity leaders

BY ELEANOR BARLOW · AUGUST 18, 2025 · LAST UPDATED ON JANUARY 2, 2026

## What you will learn

- **How to strategically scale your bug bounty program** by expanding scope, broadening researcher engagement, and aligning with organizational security goals to strengthen testing coverage.
- **How to improve program governance and operations** through adjusted reward structures and internal team readiness that support growth without overwhelming resources.
- **How to measure and optimize success at scale** by tracking key metrics and severity trends to demonstrate program effectiveness.

If you are a CISO or cybersecurity leader looking to scale your bug bounty program but are not sure when the right time to do this is, how to do this in a way that works best for your company or want more insights into the impact scaling will have on your team, then we've got the tips and tricks for you!

## Why scale your bug bounty program at all?

For security leaders, scaling a bug bounty program is a strategic investment that reflects organizational maturity and resilience. Scaling allows for comprehensive testing across all critical assets. But scaling your program is about more than increasing volume; it's a strategic imperative to:

- **Adapt to evolving threats:** Cyber adversaries are constantly innovating with new tactics, techniques, and procedures (TTPs). A diverse and growing global research base helps organizations stay ahead with creative new attack techniques and a variety of skills.
- **Demonstrate security maturity:** Public programs that continue to scale by adding assets to scope signal commitment and transparency to customers, partners, and regulators.

> **"No two organizations are the same. That's why we tailor our support based on your specific security objectives, program maturity, and organizational needs."**
>
> **Rocio Bracero, Head of Customer Success, Intigriti**

## When to consider scaling your bug bounty program

Scaling can have several drivers, including moving from a private or semi-private program to a public program. Key indicators for readiness include analysing the operational bandwidth, consistent quality submissions, and stakeholder alignment.

> **"The kudos of a public program increases exposure of your assets and digital footprint to the full creative power of a large and diverse community. But it can bring its rewards, especially to well-known brands. It reassures your customers that security is a top priority."**
>
> **William Fox, Customer Success Manager, Intigriti**

In addition, the internal team running the bug bounty program can promote their efforts through the organisation, giving reassurance to departments and employees that their assets are constantly being tested for potential threats.

In fact, an expansive and popular program can have so many assets added from different departments and divisions that workflow and reporting lines can become challenging to manage. Expanding a program to include several individual programs can clean up a large volume of submissions that are attributed to different business units.

> **"The initial success of a program, reporting not only numerous findings, but also higher severities, and therefore higher business impact, vulnerabilities, can instigate an appetite to scale bug bounty across an organization's wider digital footprint. Other divisions of a business may want to be part of a bug bounty initiative as they see how departments use continuous testing to mitigate operational risk."**
>
> **William Fox, Customer Success Manager, Intigriti**

# How to scale your bug bounty program effectively

Scaling requires deliberate strategy and strong program governance. Without proper planning, scaling can overwhelm internal teams, frustrate researchers, and cause budget overruns. Without clear forecasting or reward escalation in place, issues such as operational burnout, researcher disengagement, and financial surprises can arise.

Consider the following four pillars to prevent such challenges.

## 1. Expanding scope strategically

Prioritize high-risk assets, APIs, cloud infrastructure, and critical applications before progressively including peripheral systems. This phased approach prevents resource overload while broadening security coverage.

'Understand and respect the testing scope. Active testing on an unauthorized testing scope exposes the tester to legal risks and unexpected damages. Intigriti recommends program owners against rewarding findings on out-of-scope assets if they cannot be formally put in-scope, to drive fairness with other participants that respect the scope and prevent incentivizing out-of-scope testing.'— Intigriti Triage Standards

## 2. Broadening researcher engagement

Transition from invite-only to semi-private or public programs to diversify skillsets and perspectives. This expansion should be supported by clear guidelines and robust communication channels.

‘We help you align your bug bounty program with your broader security goals. Whether you’re a startup just beginning your vulnerability disclosure efforts or a seasoned security team expanding coverage, our experts guide you to the right solution.’
—Your bug bounty journey

### 3. Scaling rewards to match risk and complexity

Transparent and competitive reward structures drive quality research and reduce noise. Adjust your bounty payouts to reflect the criticality and exploitability of vulnerabilities.

‘We believe that transparency is important and public bug bounty write-ups are a valuable source of knowledge for the bug bounty community.’- Community code of conduct

### 4. Preparing your internal teams

Ensure your security operations, engineering, and legal teams have dedicated resources and training to rapidly process vulnerabilities and communicate effectively with researchers.

'A Customer Success Manager (CSM) is assigned to every customer as their single, dedicated point of contact, ensuring continuity, advocacy, and alignment throughout the partnership.'
—Your bug bounty journey

## Metrics to measure program success

Data-driven management is critical.

- To demonstrate responsiveness, it’s best to track time-to-triage and time-to-remediation.
- To assess program effectiveness in finding impactful bugs, track vulnerability severity trends.
- To understand if you have a happy and active researcher community, track researcher engagement levels.
- To identify security gaps, track asset coverage and test frequency.

A bug bounty platform can help provide some, if not all, of these metrics for customers.

“We look at the researcher community as our partners and not our adversaries. We see all occasions to partner with the researchers as an opportunity to secure our customers.” - JeanFrançois Simons, CISO at Brussels Airlines

## Next steps for security leaders

Effective scaling requires expertise, resources, and tailored strategies aligned with your risk and business objectives. Intigriti’s team of security professionals is ready to guide you through every stage of your bug bounty journey.

‘Our team works with you to optimize spending while maximizing program efficiency. By making data-driven recommendations, we help you allocate your resources where they will have the biggest impact.’ –

[How to optimize your bug bounty program]

[Contact Intigriti today] to discuss how to scale your bug bounty program in line with your security goals.

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.