7 ways bug bounty programs can help drive the security development lifecycle

BY ANNA HAMMOND · MARCH 18, 2022 · LAST UPDATED ON MARCH 6, 2025

Software Development Lifecycles (SDLCs) today have to take a huge number of security and privacy realities into consideration with every release — and with the widespread adoption of agile methodologies, release cycles have become more frequent.

Such rapid, large-scale change in how software is produced, delivered and consumed has increased the need for continuous, proactive cybersecurity. In this article, we'll look at how crowdsourced security testing fills that role to improve SDLCs in multiple ways.

What is a software development lifecycle (SDLC)?

A Software Development Lifecycle is an optimized way of working to produce high-quality software. Modern software solutions are the complex products of teams working to meet many requirements. To bring efficiency to such complexity, a methodology is required that clearly defines processes and stages in the development lifecycle.

Waterfall and Agile are two of the best known SDLCs, with Agile now prevalent among many of today's leading software development teams.

The 5 phases of a Software Development Lifecycle

A Software Development Lifecycle is most frequently divided into five key stages:

1. Requirement gathering and analysis
2. Planning and software design (architectural or new features, for example)
3. Software development (writing code to meet the new requirement)
4. Testing new capabilities to ensure they are bug-free and meet the stated requirement
5. Deployment and maintenance of new—and existing—capabilities.

It almost sounds simple when put like that. And it's one of the key benefits to this structured approach to software development—it brings clarity to complex projects. But while SDLC methodologies are a boon to development teams, they don't specify how to integrate security considerations into software development. This gap has created the need for the Security Development Lifecycle (SDL).

What is the security development lifecycle (SDL)?

While Software Development Lifecycles define best practices in the processes of producing software, *Security* Development Lifecycles do the same for security integration, testing and hardening in your development lifecycles.

Ideally, you should be integrating security practices at all five stages of your SDLC. In other words, it's not good practice just to leave security testing until shortly before a release! You might practice risk assessment at the same time you perform requirement gathering and analysis, for example. Or you might have code review practices in place during the software development phase.

It's important that you also have in place is some form of *continuous testing* that checks for vulnerabilities in an ongoing manner. Thankfully there is an innovative approach to continuous security testing that fits well with agile release cycles, and it is simple to integrate into your security practices at any time.

How bug bounty programs can help drive a security development lifecycle

Bug bounty programs are ideally suited to continuous testing of platforms and software against vulnerabilities. They help development and security teams to build, test, and release application features faster without exponentially growing security concerns.

A crowdsourced bug bounty program puts your software under the scrutiny of 1000s of dedicated and highly motivated expert hackers. They will mirror the ways malicious hackers might attack your software, and they'll keep testing as long as you run the program.

Beyond the obvious advantages of being quickly–and privately–notified of vulnerabilities in your software, vulnerability reports increase the level of security awareness in your organization. The reports and associated support are so comprehensive that they make for excellent learning resources, as software developer Showpad discovered.

Showpad's bug bounty program wins

Intigriti customer, Showpad, creates a sales enablement software used by over 1,200 customers in more than 50 counties. Customer trust is critical in a data-intensive app like Showpad, and that means maintaining the highest levels of security and privacy. With their platform constantly and rapidly evolving thanks to their agile Software Development Lifecycle, continuous security testing is a must.

Showpad's security testing background

Showpad have used pentests as part of their cybersecurity practices in the past, but they provided too static an approach for the fast-development world of Showpad's SDLC. So, Showpad went looking for an agile security testing solution that would continuously challenge the platform against vulnerabilities.

Enter crowdsourced bug bounty programs, which immediately provided the continuous testing Showpad needed:

> **“Comparing bug bounty and pentesting is like comparing a photograph to a film. A penetration test is like looking at a picture of what the product looks like in a certain moment in time — but it doesn’t say anything about tomorrow or the next coming weeks.**
>
> **Bram D’hooghe, Director of Security, Privacy & Compliance at Showpad”**

Since launching, Showpad has benefited from a number of high-quality vulnerability reports which they’ve been able to remediate. But they soon realized that a bug bounty program’s benefits go further than catching vulnerabilities. For example, the information-rich vulnerability reports delivered to Showpad by Intigriti have been used as the basis for internal training materials. This has helped improve the engineering team’s knowledge and security programming quality.

Today, Showpad builds application features designed to be secure from the offset. Furthermore, the security and development teams at Showpad now work more efficiently to build, test, and release application features. Bug bounty programs have been instrumental in this improvement, and continue to help improve Showpad’s cybersecurity posture on a day-to-day basis.

7 ways bug bounty programs help secure the software development cycle

Showpad’s experience is not unique. In fact, bug bounty programs can bring significant benefits to all modern Software Development Lifecycles while working seamlessly as part of your Security Development Lifecycle.

Here’s 7 ways they do it:

1. **Uncovering bugs**; known and unknown
2. **Continuous testing** from highly motivated security experts
3. **Efficient and relevant triage** of reported vulnerabilities
4. **Ongoing contact** with the platform’s expert support team, helping explain cybersecurity issues
5. **Use of vulnerability reports** for training, which increases internal team security knowledge
6. **Easy integration** of continuous security testing into any software company’s security culture
7. **Success managers** who proactively reach out to support clients once their programs are live to ensure maximum impact year-round.

Key takeaway

Security is an essential feature of any software. However, with rapid development cycles and increasing complex offerings, software development teams need a way to incorporate up-to-date security knowledge into how they work. Bug bounty program reports and support are an excellent source for such learning, and provide robust continuous security testing at the same time.

Want to know more about bug bounty programs? Then get in touch to request a demo with a member of our team today.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com