How can a bug bounty program improve your IT security posture?

BY ANNA HAMMOND · JANUARY 21, 2022 · LAST UPDATED ON JUNE 3, 2025

Rapidly evolving technology has created a world whereby cybersecurity must grow and mature at equal speed. Your IT security posture should anticipate fast change by providing real-world, real-time testing of your cyber defenses for known and unknown threats.

This article looks at how to use a bug bounty program as a cornerstone of this agile approach and how doing so can keep your organization one step ahead of malicious hackers.

What is IT security posture?

IT security posture addresses every aspect of your organization that requires cybersecurity. Like with physical posture, your organization benefits from a good IT security posture. Make it strong, and you can help prevent attacks and deal with security issues quickly when they do arise.

What is a bug bounty program?

A bug bounty program engages ethical, "white hat" hackers to test an organization's cybersecurity defenses. They search for vulnerabilities that bad actors could exploit, then report them to you.

These security experts are usually crowd-sourced and provide a broad range of specializations that test every aspect of your systems. To learn more about the motivations of ethical hackers, take a look at the infographic below.

Bug bounty programs guarantee value too: you only pay for results—unlike pentests and other standardized testing methods.

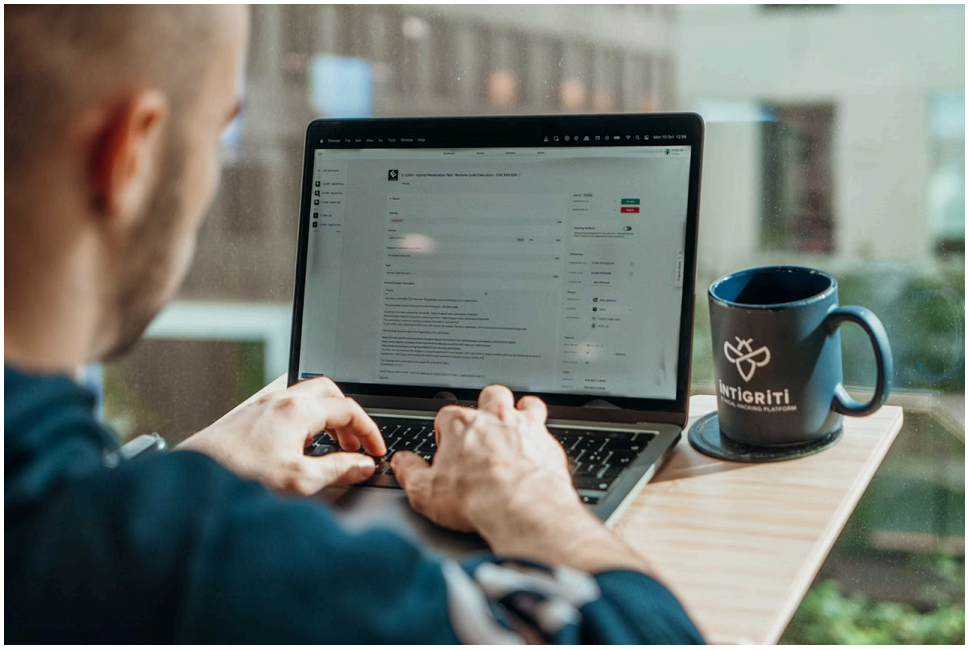
How does a bug bounty program improve IT security posture?

Bug bounty programs exist to address today's non-static, rapidly evolving cybersecurity threats. From enterprise to SaaS startups, from government to small businesses, programs help all types of entities reduce the level of threat on their attack surface.

Benefits for IT security posture

- **Software and technology stacks evolve fast:** Software and technology stacks evolve rapidly, as do cyber threats. Bug bounty programs are agile and respond fast to threats. As a result, you don't have to compromise security in the face of your organization's need to evolve its technologies rapidly.
- **They highlight vulnerabilities quickly:** Programs often reveal vulnerabilities within hours. Therefore, you can get security feedback that is in sync with your development and IT infrastructure deployment.
- **Ethical hackers are creative thinkers:** Ethical hackers think more creatively than automated procedures and pentests. As stated by Thomas Colyn, CISO of DPG Media, by launching a program, organizations "can use the creativity of thousands of ethical hackers' minds — and that is far stronger than using automation or general algorithms to discover difficult to find vulnerabilities."
- **Companies can lean on thousands of experts:** Crowdsourced security delivers a high level of hacker specialization. Hackers with a wide range of skill sets and experiences will work to uncover weaknesses in your attack surface.
- **They offer continuous testing:** Where standard automated tests provide snapshots of your cyber vulnerabilities, bounty programs offer continuous testing for your systems, processes, and software.
- **Your organization pays for impact:** Bug bounties are a win/win value proposition thanks to bounty-based payments. You only pay for results, and you set the price, guaranteeing value.
- **Bug bounty platforms offer real-person support:** Dedicated bug bounty platforms, like Intigriti, provide real person support. For example, the dedicated triage team audits vulnerability reports before relaying them to clients. Therefore, you only allocate valuable resources to dealing with real threats.

Bug bounty platforms also make it easy to track and control your security expenses through expenditure caps and real-time cost reports.



When is the right time to implement a bug bounty program?

Given the long list of benefits, you might be itching to start your program straight away. But to yield the highest, most cost-effective value to your organization, you'll want to optimize the timing. This requires ensuring your organization has a mature security baseline before starting your bounty program. At the least, your IT security posture should have actively incorporated:

- Standardized internal security procedures
- Automated scanning and pentests

These aspects will stop you from paying out bounties for the discovery of easily identifiable or top-level vulnerabilities.

Put simply; you should start your program when you are ready to take your cybersecurity to the next level. CISO of Brussels Airlines, Jean-François Simons,' has been using bug bounty methods for many years. He provides further context around the importance of taking the necessary steps prior to launch:

"I see pentesting as a security test that you take before going to a bug bounty program. It's like a cleanup. If you start with bug bounty straight away, you might be in for an unpleasant surprise. We had done multiple pentests in the past."

Launching a program

Organizations of any scale can easily get started with an effective bounty program.

A bug bounty platform, like Intigriti's, makes setting up and launching your program simple and intuitive, and it doesn't require a high level of security expertise.

Intigriti also provides clear documentation and content on everything from making the business case for a program to writing a vulnerability disclosure policy, or how to maximize hacker engagement, and

more.

Real-person support is also always on-hand and easy to reach. And once your program is up and running, a dedicated team will continue to support you.

Leverage the power of the crowd

Including a bug bounty platform in your IT security posture is a highly effective way to provide continuous security testing for your infrastructure. With the barriers to entry low and the potential for invaluable feedback high, now is a great time to consider the power of crowdsourced security for your organization.

Intrigued by what you have read? Get in touch to request a demo with a member of our team today.

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com