Security is a continuous process. Here's why your testing process should be too

BY ANNA HAMMOND · JULY 26, 2022 · LAST UPDATED ON MARCH 6, 2025

"Continuous security testing" has recently achieved a top ten spot in the cybersecurity lexicon. At first glance, it appears self-explanatory and very sensible—something like, "An apple a day keeps the doctor away", right?

Well, yes. But what exactly is continuous security testing? How is it different from other cybersecurity approaches, such as penetration tests (pen tests) and vulnerability scanning? If it works, what is the best way to implement it? In this article, we'll answer those questions.

What is continuous security testing?

While there are some differences in how teams approach continuous security testing, there are always four core parts to the process:

1 – **Challenge** your systems, software, applications, assets, and processes.

2 – **Assess** for vulnerabilities

3 – **Optimize** or fix based on what you found

4 – **Repeat continuously**.

Point 4 is what puts the "continuous" in "continuous security testing." But it can be even more than that! The testing becomes proactive by leveraging crowdsourced human inventiveness, as security experts look for *known* and *unknown* vulnerabilities.

How can your business or organization implement continuous security testing?

To get started with continuous security testing, you only need two things:

- The four-part continuous testing plan outlined above
- Small teams of security experts

The security teams perform different roles:

Challengers – security experts, sometimes known as "ethical hackers" or "security researchers", and often crowdsourced through a bug bounty platform. The more, the better, and the higher the skill level, the better, too. Note, in a non-continuous security testing approach, the challengers would be penetration testers or the red team in the red team / blue team approach. However, with bug bounty programs, the Challengers are what many know to be called "bug bounty hunters."

Assessors or Triage – also security experts, but tasked with reviewing the vulnerability reports sent by the Challengers to make sure they are genuine, valid, and unique. When employed by a security company or bug bounty platform, like Intigriti, this testing service is typically known as "triage".

Optimizers – these tend to be the software developers, engineers, or IT departments responsible for wherever the vulnerability was discovered. Their job is to patch the security vulnerability. The reports submitted during continuous security testing can prove an excellent ongoing learning resource for these teams.

Given this diversity of roles, it might come as a surprise to learn that setting up continuous security testing is not only remarkably easy, but also one of the most cost-efficient ways to improve your cybersecurity.

Why bug bounty programs should be part of your continuous security testing

The best way to implement continuous security testing in your organization is to deploy the tool designed precisely to fulfill this role—a bug bounty platform.

You might already be familiar with the idea of bug bounty *programs* that offer rewards (bounties) to ethical hackers for discovering vulnerabilities in software, systems, web services, and other digital assets. The overall aim of bug bounty programs is to reduce your organization's attack surface. Bug bounty *platforms* are the host infrastructure for those bug bounty programs and they are often provided as software-as-a-service.

You can, of course, set up and run your own bug bounty programs. However, businesses typically engage a bug bounty platform. It makes running the programs more manageable and effective in terms of complexity, cybersecurity, and investment. Some bug bounty platforms, such as Intigriti, also offer options to run continuous penetration testing.

How to get started with a bug bounty platform

While we can't speak for other platforms, Intigriti built its platform and managed bug bounty programs to make meeting the requirements of continuous security testing easy. When you set up a public bug bounty program on the platform, for example, you'll instantly have access to a global community of crowdsourced ethical hackers—our Challengers from above.

They'll read your program scope and start hammering at your cybersecurity gates, so to speak. The difference is, if they discover a way in, they won't charge into your premises and wreak havoc as a malicious hacker would. Instead, they send a nicely formatted vulnerability report to Intigriti's triage team.

This team of highly qualified security experts—the Assessors above—will scrutinize the submitted vulnerability reports for validity and ensure you don't receive duplicates. That's *triage*. They'll send the report to you, so your team of Optimizers can patch the vulnerability before malicious hackers discover it. Meanwhile, the platform will handle secure communications between all groups and automate bounty payments.

What's more, unlike a pentest, with a bug bounty program you pay only when a security expert uncovers a bug or vulnerability. It's incredibly cost-effective. If you'd like a deeper dive into getting started with a bug bounty program, check out our four-part series on what to expect from the bug bounty process, from setting up to post-launch.

The best way to maintain top-notch cybersecurity

Cybersecurity can feel like an arms race. Today, the constant threats of malicious hackers make bug bounty programs essential to an effective cybersecurity posture. As long as your program is live, crowdsourced security experts will provide round-the-clock cybersecurity testing and keep you ahead of the hackers. What's more, getting started is simple with a platform, like Intigriti, where you'll get fast access to everything and everyone you need without breaking your budget or sanity!

Learn more

Intrigued by what you have read? Want to know more about bug bounty programs? 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