Bug Bounty Security Testing

Get security checked by ethical hackers!
Want to gain insight on the cybersecurity of your internet connected assets and applications? Kiwa and bug bounty security platform Intigriti proudly present their joint private bug bounty security testing service. This service makes it possible for you to organise (private) bug-bounty programs according to your specific preferences.

Kiwa works together with Intigriti by leveraging their extensive platform of over 40 thousand independent security researchers and ethical hackers. Enable yourself to benefit of the skills, talent, time and creativity of a large and very experienced security audience. Based on your predefined scope these security researchers and ethical hackers will search for vulnerabilities. By leveraging the minds of the many and matching the most skilled and trusted researchers, companies will benefit of high quality vulnerability submissions.

Full control

Kiwa's service allows you to have your assets tested in your own private bug bounty program on Intigriti's platform. We deliver valuable security vulnerability reports which could in turn be beneficial for mending and (re)shaping the cybersecurity of your business or organisation. You as a customer are in full control and will be assisted by Kiwa in every step of the process to successfully complete the program.

Get valuable insights

The basis for the bug bounty program is straightforward: A crowd of ethical hackers and security testers will test your web and mobile applications or other internet connected assets with the intention to find security flaws. The ethical hackers and security researchers are incentivised to perform the tests in the following manner: for every valid vulnerability found they get a reward, also called a bounty. The more severe a found vulnerability, the higher the reward or bounty. This allows for hackers to make full use of their creativeness in order to earn good rewards. If they find a vulnerability they get rewarded whereas your business or organisation gets hold of

Cyber security Certification
Nederland
CyberSecurity.Certification@kiwa.com
+31 (0)88 998 33 70

critical information on a potentially harmful cyber risk. A win-win situation.

Kiwa guides you through every step

Kiwa guides you through every step of setting up and launching a successful bug bounty program on Intigriti's platform. The bug bounty program has a testing period of four to six weeks in which your assets will be security tested according to your preferences and particular requirements. You are in total control of the total amount of available bounty, the bounty table (which contains the different amounts of bounties), the type of researchers and ethical hackers making up the pool of testers etc. The test results and outcomes are also followed up by Kiwa in a report and a debriefing meeting. In the end you will have enough information at hand to improve the security of your asset.

What does a Bug Bounty Security Testing program look like?

Kiwa and Intigriti's program has six important milestones through which we guide and assist you. These milestones are:

Step 1: Content preparations

Understanding goals and expectations to come to an accurate program scoping:

- Define goals and objectives for program scoping;
- What should be included in the scope?;
- How to present customer and program on the Intigriti platform?;

Step 2: Program set-up

Program creation

- Setting up the program scoping;
- Decide what is in-scope and what is out-of-scope;
- Listing out of scope assets and out-of-scope testing techniques;
- Set-up severity level per vulnerability impact and bounty table;
- Additional rules of engagement and guidelines for researchers.

Based upon the scope, the most critical data and test environments the bounty tables are discussed and set. An example of a bounty table can be found below. A success management and triage team is there to validate the found vulnerabilities and discuss them with the client.

Bounties

	Low	Medium	High	Critical	Exceptional
Tier 2	€ 0	€ 100	€ 500	€ 1,000	€ 2,000
Tier 3	€ 0	€ 25	€ 125	€ 250	€ 750

Step 3: Launch!

Cyber security Certification
Nederland
CyberSecurity.Certification@kiwa.com
+31 (0)88 998 33 70

Launch

Program goes live on Intigriti! and will run for 4-6 weeks.

Security researchers are invited on your private program based on your criteria like; geography, ID checked, expertise, skillset, quality, ranking, activity and more.

Submission flow

Researchers begin submitting vulnerability reports via the Intigriti platform;

Intigriti's triage team will handle, review and reproduce all submissions on quality, validity, complete PoC etc.;

Customer receives the valid triaged submissions

Customer reviews and approves/rejects submissions

Step 4: Close Follow-Up

First 24 hours after launch: a close follow-up is performed to adjust where needed;

Check-in call with the customer is performed after 1w-2w (t.b.d.).

Step 5: Operational guidance

In case program activity is not garnering enough results, we start strategies to increase engagement by the participants of the platform.

For example:

Redefine scope, add researchers, in- or decrease bounties;

Additional rights on test credentials;

Program updates.

Step 6: Debriefing

The test and assessment program will be live for 4-6 weeks. After the final week an overview report of activities will be provided. All open submissions will be closed. A debriefing meeting will be held with the customer.

What types of assets can be considered?

First and foremost the assets should be available through the internet. The ethical hackers and researchers use the internet to get access to the assets to further test and look for vulnerabilities. Besides this there are a few more topics we consider to select your assets for a bug and bounty program. Some examples are:

1. The asset is in ownership by you but could be managed by a third party.
2. When the asset is compromised the consequences could be impactful.
3. Test environments and acceptance environments.
4. Discovering vulnerabilities for the asset brings value regardless of the impact of the consequences.
5. Testing credentials, etc.

Included in this program are:

- One program (test period = 4-6 weeks);
- Approximately 25 reports;

Cyber security Certification
Nederland
CyberSecurity.Certification@kiwa.com
+31 (0)88 998 33 70

- Kiwa test summary report (after test period);
- 40 handpicked security researchers (ID checked).

Why Kiwa?

Kiwa is a trusted and independent third party that performs tests to provide the basis for guaranteed quality. Together with Intigriti we offer you a bug bounty service which allows for a thorough check-up of the web and cybersecurity of your assets. As systems and organisations are digitalising so do our means of testing and inspecting. As cybersecurity is an important cornerstone of our digital age, Kiwa is heavily involved in providing high quality, useful penetration tests and services. We are your partners for progress!

Cyber security Certification
Nederland
CyberSecurity.Certification@kiwa.com
+31 (0)88 998 33 70