Empower your security team to build stronger defenses against cybercriminals [Interview]

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

This interview originally appeared in Cybernews in April 2022.

Trusting your cybersecurity team to identify vulnerabilities in your company's security systems is vital. However, you'll likely sleep better at night by getting a second look from an outsider.

Such is the work that bug bounty hunters (ethical hackers) do. These specialists try to hack into various systems with the aim to find a vulnerability or misconfiguration that, if fallen into the wrong hands, can be exploited for the greater bad. Cybernews reached out to Intigriti's CEO, Stijn Jans, and Head of Hackers, Inti De Ceukelaire, to discover more on this topic.

First things first, what is a bug bounty platform exactly?

Stijn: A bug bounty program engages ethical hackers (at Intigriti, we call them security researchers) to stress test an organization's cybersecurity defenses. Researchers search for vulnerabilities that cybercriminals could exploit and then report them to the organization through their bug bounty program, so that their team can fix them.

Each program comes with a set of guidelines (the scope) that detail the rules of engagement. There is also a table of earning opportunities (bounties), which is based on the impact of the finding.

This proactive approach means organizations get continuous coverage of their digital assets without needing to increase headcount or put pressure on their team internally. Additionally, the programs generate a positive impact on the lives of Intigriti's researchers by offering them a way to make a living on their terms.

There are also many benefits of working with a platform. For example, they come with a large community of already engaged researchers, managed services, and additional customer support. Our programs also offer triage services by default. Triage plays a big role in managing incoming reports and will make sure the program's internal team only receives unique, actionable, and valid reports, meaning they can stay focused on business-as-usual activities.

At Intigriti, we work with organizations of varying sizes, industries, and levels of security maturity.

Which industries should be especially concerned with implementing bug bounty programs?

Inti: If an industry is concerned about cyber threats, chances are, they will also be thinking about cyber defenses — or so they should be! Therefore, it comes down to what type of *company* should be concerned with implementing a bug bounty program rather than industry.

If you have an online presence or digital assets, you're already exposed to hackers. Malicious hackers are obviously a concern, so if there is a vulnerability in your systems that could be exploited, you'd want to know about it, right? This is the exact role of an ethical hacker. Intigriti's role is the facilitator, ensuring you get the right information as quickly as possible.

The takeaway here is that no matter what industry you operate in, actively involving security researchers through a bug bounty program will streamline the reporting process. Importantly, you'll empower your security team to build stronger defenses against cybercriminals.

How did the pandemic challenge cybersecurity worldwide? What vulnerabilities were exploited the most?

Inti: The pandemic meant corporations were forced to expose their internal tools and infrastructure to the outside world as work-from-home mandates started to roll out. For many, this had to be done quickly to ensure business continuity.

As a side symptom, the cybersecurity aspects of this swift transition were disregarded because of the time pressure and uncertainties. Many businesses only expected the temporary measures to last for a couple of weeks and so they made a call that heightened cybersecurity measures weren't necessary.

Later, people realized the work-from-home culture wasn't going anywhere. Even so, many organizations are still using the same insecure systems and configurations that were set up at the beginning of the pandemic. Consequently, we have seen a rise in misconfigurations concerning VPNs, single-sign-on systems, and internal helpdesks.

Even though bug bounty programs have gained momentum over the past few years, why do you think it is still not a widespread practice?

Stijn: The general level of security awareness, and adoption of preventative solutions and technologies is generally good. After all, organizations have hundreds of platforms, vendors and services to choose from. Of course, there are security spot-checks, like penetration tests, that can tell organizations how well their cybersecurity defenses would hold up in the event of a specific type of cyberattack. However, ask any security professional how secure they *really* are on a *continuous* basis, and they will often raise an eyebrow.

Inti: Bug bounty programs have emerged as the next step in security testing, especially in software development lifecycles. The pressure of getting applications, projects, features, and updates to market as quickly as possible can mean security hoops are sometimes skipped. Continuous testing by a wide, diverse, and highly skilled community of security researchers offers a solution to finding security vulnerabilities for organizations that typically don't have the resources or expertise in-house to do this.

Stijn: However, despite them being around for decades, many bug bounty myths linger on, and not everyone trusts the idea of working with someone who has the word "hacker" in their job title. But the sad truth is bad actors won't seek your permission to hack your business – and a simple yet proven method to protect against cyber threats is to invite ethical hackers in to help.

What tips would you give to someone looking to break into the field of ethical hacking?

Inti: Unfortunately, traditional educational establishments are struggling to offer comprehensive and up-to-date training in the rapidly evolving world of cyber threats. But content creators and "Hackademies", like Intigriti's Hackademy, are helping to fill this gap.

As their name suggests, hackademies are online locations where aspiring ethical hackers can come and learn about categories of security vulnerabilities, see real-world examples, and learn how to identify and protect against such weaknesses. It's also worth checking out our Hacker Heroes videos, where we interviewed some of our most successful security researchers on the platform. However, as many of our Hacker Heroes say, the best way to break into the field of hacking is to stop thinking about it, take the leap, and simply start looking for your first bug! Many of our top-performing security researchers have only been bug bounty hunting for one to two years.

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