



66% of cybersecurity talent are considering bug bounty hunting as a full-time career

BY ANNA HAMMOND · JUNE 1, 2022 · LAST UPDATED ON MARCH 6, 2025

The unique occupation of bug bounty hunting offers a heightened level of freedom and lifestyle that traditional jobs cannot provide, but which today's security professionals' desire. Intigriti set out to explore this trend further.

Intigriti's Ethical Hacker Insights Report 2022

Intigriti's second annual [Ethical Hacker Insights Report](#) reveals bug bounty hunting as a rapidly rising career path amongst cybersecurity professionals in 2022. The market research report, compiled from the survey responses of more than 1,700 ethical hackers, highlights that 96% of ethical hackers would like to dedicate more time to bug bounty hunting in the future, and 66% are considering it as a full-time career.

The pandemic changed what people desire in cybersecurity professions

The biggest appeal of full-time bug bounty hunting to respondents is the money, with 48% declaring this as their number one attraction point. The desire to be their own boss and ability to work their own hours closely follow, with 45% of respondents listing both points as appealing aspects.

Inti De Ceukelaire, Head of Hackers at Intigriti, commented on the shifting career landscape: "The work-from-home culture has made employees desire more independence and has further encouraged digital nomads to pursue a remote working career. Bug bounty platforms can not only facilitate this, but they also allow people to work wherever they want, whenever they want, and without having to rely on a boss to match their talents with customers or be part of a corporate hierarchy."

Education benefits are another key driver of bug bounty hunting

The educational benefits of bug bounty hunting are another key driver in this trend. Concerningly, the survey results indicate that this generation of tech talent isn't getting what they need from employers to keep their skills and knowledge up to date, despite rising cybersecurity threats. For information security, for example, 50% of respondents say they turn to bug bounty hunting to learn the most relevant and useful knowledge, compared to just 11% who gave their job as their first choice.

Security testing through the eyes of the security testers

Around two-thirds (65%) of respondents also have hands-on penetration testing experience. However, taking the opportunity to dive deeper into their opinions on the method's effectiveness, 88% of these respondents agreed or strongly agreed that "a penetration test cannot provide continuous assurance that an organization is secure year-round."

Commenting on this finding, Ceukelaire said: "With most security researchers agreeing that "a penetration test cannot provide continuous assurance that an organization is secure year-round," it's time for employers to question whether they should still rely on them as a standalone too."

Further, Ceukelaire said: "Penetration tests focus on one snapshot in time, whereas bug bounty programs are continuous. As attackers shift tactics, cyber defenses must too. The only way to test their effectiveness is to apply continuous pressure against them. Considering that an organization's security posture will change with each new feature release or update, it's not only a logical step to implement more security testing, but also critical."

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