What is an ethical hacker? And why do companies hire them?

BY ANNA HAMMOND · MAY 27, 2021 · LAST UPDATED ON MARCH 6, 2025

Ask someone to define the word 'hacker' and it's almost guaranteed to spark a debate. Yet, hacking isn't a new concept. In fact, it's been around for decades. Throughout the sixties, hacking simply meant optimising systems and machines to make them run more efficiently.

Since then, the world's fear and fascination with black hat hackers have clouded the term 'hacker', and as a result, many choose to differentiate between malicious hackers and ethical hackers. In this article, we're going to focus on the latter.

1. What is an ethical hacker?

Like malicious hackers, ethical hackers are driven by an overriding goal to break through a target's cyber defences. However, as the name suggests, an ethical hacker operates within the law and will alert a company to the vulnerabilities they've found within their assets. Some ethical hackers choose to work independently, but many businesses employ or partner with them too.

> "Ethical hacker definition:
>
> **A security expert that specialises in the testing of computer and software systems or processes to evaluate, strengthen and improve security.**
>
> **The Ethical Hacker Insights Report 2021, Intigriti "**

Mainstream media coverage of hacking tends to associate it with something criminal — feeding into the stereotype of a dark clothed anarchist hunched over a laptop. But ethical hacking is quite the opposite. In 2021, becoming an ethical hacker is a popular ambition amongst information security professionals around the world.

2. Why do companies hire ethical hackers?

There are a few reasons why companies hire ethical hackers. Primarily, employing the help of ethical hackers enables businesses to execute a defensive strategy with an offensive approach.

Ethical hackers are highly skilled individuals and can safely replicate the behaviours of black hat hackers to highlight weak links in a company's cybersecurity posture. By working with ethical hackers, companies become aware of and fix their vulnerabilities. Not only does this improve the strength of their cybersecurity defences, but it empowers them to stay one step ahead of cybercriminals.

Another reason companies employ ethical hackers is because it helps limit their liability. In case of a real cyberattack, businesses can demonstrate the steps they've taken to avoid it.

Hiring ethical hackers also enables businesses to:

- Dedicate a commitment to continuous security testing

- Reduce the risk of losses from a cyberattack
- Increase their reputation and trustworthiness as data protectors
- Better keep up with ever-evolving cyberthreats
- Develop their internal team based on key learnings and insights.

There are a few types of ethical hackers that businesses can employ.

Types of ethical hackers

1. Red team/blue team

The red team vs blue team exercise aims to strengthen the organisation's preventative, detection, and response controls. This model comes from the navy where a Red Team attacks and a Blue Team defends. These cybersecurity professionals collaborate closely to improve security through continuous feedback and bi-directional knowledge transfer.

2. Bug bounty hunters

Bug bounty hunters are crowdsourced cybersecurity enthusiasts and professionals that perform continuous security testing. They are extremely creative individuals who are well versed in finding flaws and vulnerabilities without following a predefined methodology. Rather than being remunerated for their time, an organisation will reward them if they successfully report a new, unique and in-scope vulnerability.

Bug bounty platforms allow security-driven organisations to publish a program and invite bug bounty hunters to research and submit cybersecurity issues. Programs can be published publicly (where anyone can contribute) or privately (where specific researchers are invited to participate.) They can also be time-bound or have no end date. However, most companies opt for the latter to ensure they have continuous security testing in place.

3. Penetration testers

A penetration tester evaluates the security of a computer system or network by simulating an attack from malicious outsiders, typically within a given timeframe and/or target scope as set out by the client. Their purpose is to identify attack vectors and vulnerabilities, and control weaknesses. It involves the use of a variety of manual techniques supported by automated tools and looks to exploit known vulnerabilities.

Within Intigriti's community of bug bounty hunters, 43% also deliver penetration test services as part of their day job.

3. Are ethical hackers in demand?

Yes, ethical hackers are in demand due to the widely reported reputation of cybercriminals. They still have some work to do to convince businesses that they're here for the right reasons — but perceptions are shifting, and today, ethical hackers are seen by many to be the backbone of IT security testing.

> "*"We need the support of ethical hackers to reinforce our IT-Security before non-ethical hackers find a possible vulnerability that they will of course not report to us!"*
>
> *Jean-François Simons, CISO at Brussels Airlines"*

Ethical hackers, such as bug bounty hunters, are also in demand because they help fill the cybersecurity skills gap. According to a 2020 study by Robert Walters and Vacancysoft, 70% of European companies say they do not have the appropriate cybersecurity talent available. A network of security experts means organisations can tap into a larger network of skills, experiences, and expertise. They're empowering security teams everywhere to scale up without the additional headcount.

Finally, according to a 2021 survey by Intel, 73% of IT security professionals say they prefer to buy technology and services from vendors who are proactive about security, including leveraging ethical hacking and having transparent communications about vulnerabilities.

4. What kind of personality traits must an ethical hacker have?

Ethical hackers are highly inquisitive, curious and investigative people. They're eager to develop their knowledge of the fast-moving and ever-changing security landscape. The Ethical Hacker Insights Report 2021 found that 70% of our hackers are on our platform to learn and develop their skills, and 40% are driven by the challenge.

To be a successful vulnerability researcher, you need to be able to approach the task of hacking with a fresh perspective, apply unharnessed creativity, and be unafraid to go against the grain.

Ethical hackers must also be patient, persistent and detail orientated. Security researcher, Pieter, explains how he works:

> "*"I'll work at a target and find four or five bugs, lose inspiration, move on, but return to it again only six months later. I'm interested to see how they fixed the previous bugs I reported and whether any new ones have appeared when they made updates."*
>
> *@Pieter*, security researcher"

There are obvious benefits to taking the legal route to disclose vulnerabilities: The money, the recognition and the free swag. But ultimately, ethical hacking is about being part of a community of people with a strong desire to help.

> "*"I like targeting medical companies because it helps a lot of people. I did some pen tests for a hospital recently that didn't have any reward to give. However, I only needed fifteen minutes to look into their site to report many vulnerabilities. I helped them secure their digital assets for almost nothing of my time."*
>
> *@Kuromatae666, Security researcher*"

For 21% of our community, their primary goal on the platform is to do good and 21% want to help defend against cybercrime.

5. How do ethical hackers find jobs?

Ethical hackers can seek out penetration testing jobs through traditional job-seeking methods. However, many also choose to look for opportunities via bug bounty platforms. As previously mentioned, the researcher only receives a reward or compensation if they successfully identify a previously unexposed bug. Therefore, there is a big financial incentive to seek out in-scope security flaws and submit quality reports.

When security researchers participate in a program and find a bug, the report goes through a process of quality control, known as triage, before the report reaches the organisation. The additional step gives researchers the best opportunity to be successful and ensures businesses only receive valid reports.

There's a great deal of clarity around what is 'safe' to hack on a bug bounty platform, which removes their fear of being threatened with legal action — despite reports being made in good faith. They also know that the companies operating on bug bounty platforms are likely to be progressive in the arena of cybersecurity.

Like ethical hacker communities, companies find bug bounty platforms to be one of the most reliable and stable ways to set up programs. When you sign up to Intigriti as a client, for example, a customer success manager will help you define a clear scope for your program and advise on aspects like what you'll compensate researchers and how you'll manage budget flow.

6. What are the requirements to become an ethical hacker?

When it comes to qualifications, there aren't any official requirements for ethical hackers. Most hackers use a combination of self-teaching, online blogs and articles, and online courses to learn how to hack.

However, amongst Intigriti's community or researchers, most have taken the steps to build upon their highest level of education, which once again, demonstrates their inherent need to develop. Whilst useful, certification isn't always accessible to everyone, and learning outside of the traditional classroom can offer a truer reflection of cybercrime activity and techniques.

7. How much do ethical hackers make in a year?

According to PayScale, US penetration testers earn between $58,000 – $144,000 per annum. In the UK, the average salary is around £39,000 per annum. In France, the average annual base salary is €40,000. However, ethical hackers can boost their yearly income with additional work, such as bug bounty hunting.

When we asked our community what motivates them to hack, 63% said they hunt for vulnerabilities to earn more money. For 10% of our community, bounty earnings make up their sole income. However, more than half (52%) say their bug bounty earnings contribute less than 10% to their total income — they hunt for vulnerabilities so they can afford extra luxuries in life.

In August 2020, Intigriti hacker,@MattiBijnens, reached a very exciting milestone. Having set himself a challenge to earn enough bug bounties to be able to afford a Tesla, he finally reached his goal.

Other members of our community invest in their existing skills. Intigriti's hacker, @__D3LT4__ took to Twitter in November 2020 to showcase his newly purchased laptop, monitor, and keyboard, which he bought entirely through bug bounty rewards. He explained that the purchase was a case of spending money to earn more money.

8. Where do hackers work?

As the work-from-anywhere culture grows in businesses, so too has the world of ethical hackers. Remote working has made it possible for companies and researchers to collaborate from all corners of the world. In 2020, Intigriti's security researchers submitted vulnerability reports from more than 140 countries.

Given that home-working trends are growing, it's expected this number will grow significantly over the next few years. In a FlexJobs survey, 65% of respondents reported wanting to transition to remote

work full-time post-pandemic, and 31% desire a hybrid remote work environment.

Bug bounty platforms allow security professionals to work from anywhere — which makes it an attractive option to candidates who can't get this level of flexibility elsewhere.

Want to learn more about ethical hackers?

Download your free copy of The Ethical Hackers Insights Report 2021 to discover:

- Key ethical hacker demographics & statistics
- Hacking motivations & ambitions
- How ethical hackers operate
- What to expect within 48 hours of launching a bug bounty program
- How businesses can establish successful relationships with ethical hacking communities.

DOwnload here

Interested in inviting ethical hackers to contribute towards your security testing? Speak to a member of the Intigriti team today to request a demo.

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