3 ways ethical hackers can help reduce cybersecurity skills gaps

BY ANNA HAMMOND · FEBRUARY 11, 2022 · LAST UPDATED ON MARCH 6, 2025

How often do you read in the news about the great job a cybersecurity team just did? The inevitable response is just one of many reasons for today's acute cybersecurity skills gap. Information security hiring managers are struggling to attract enough talent, and most pundits consider understaffed security teams as bad news for cybersecurity. A recent study from the Information Systems Security Association (ISSA) indicates that 38% of cybersecurity jobs remain open.

But here's some good news: The cybersecurity skills gap is, in part, narrowing through crowd-sourced ethical hacking communities. And often, these security experts have skills levels that aren't teachable through the traditional classroom environment .

Let's take a look at three ways ethical hackers and bug bounty platforms are reducing the cybersecurity skills shortage for both organizations and professionals.

1. Lean on a crowd, to fill your organizational skills gaps

Today, there is already a large ethical hacker community using their skills for good worldwide. Intigriti's annual ethical hacker report outlines how, by engaging in bug bounty programs, these crowdsourced experts help to create safer digital environments by researching, identifying, and alerting companies to weak links in their security systems.

Advantages of working with crowdsourced security experts include:

- Access to always available talent through trusted bug bounty programs
- A diversity of highly specialized skills
- Rapid scalability of security testing
- High motivation from researchers working for bounties
- Ability to expand without adding to your internal headcount
- Affordability, as you only pay for results, unlike pentests.

2. Get free access to educational resources

Traditional educational establishments are struggling to offer comprehensive and up-to-date training in the rapidly evolving world of cyber threats.

"Hackademies", like Intigriti's Hackademy, have stepped in to help fill this educational gap. As their name suggests, they are online locations where wannabe white hat hackers can come and learn about

categories of security vulnerabilities, see real world examples, and learn how to identify and protect against such weaknesses. There is a lot to learn and, thankfully, a huge and growing number of resources are available.

Interested to learn how to hack? *After enrolling to our* ***Hackademy*** *, why not also check out our* ***YouTube channel*** *and* ***knowledge base*** *. If you're truly dedicated to binge-learning, you might also enjoy our pick of* ***top 20 bug bounty YouTube channels to follow*** *.*

3. Empower your team to learn from incoming vulnerability reports

Bug bounty programs aren't just good for crowdsourcing and educating ethical hackers. They can also provide a valuable source of learning for cybersecurity employees through well written vulnerability reports and dedicated support.

A good vulnerability report will clearly document where a security issue lies. It will also document the potential exploitation opportunity, the level of risk it represents, and—where necessary—useful suggestions on how to mitigate the risk.

Reports delivered by a bug bounty provider can help educate cybersecurity staff in the following ways:

1. They help staff stay up-to-date on unknown and evolving threats. A lot of cybersecurity teams are spread thin, and so they haven't got time or resources to dedicate towards official training. A good report means they can learn on the job.

2. Reports are comprehensive and can offer a recommended (optional) solution so staff can learn about how bugs were discovered, and how they can be fixed.

3. Triage provided by a bug bounty program provider, like Intigriti, also means only valid reports come through, so cybersecurity staff can focus their time on learning about important bugs only.

4. Dedicated triage teams can also advise internal teams on finding fixes for found bugs.

> "*I cannot understate the importance and the value that the triage team offers to us. Our developers know that any vulnerability that makes it through the triaging steps is important and in need of remediation. The value is immense for us.*
>
> *Cyber Resilience Manager & CISO of Port of Antwerp, Yannick Herrebaut*"

Bug bounty programs are changing cybersecurity

The cybersecurity skills gap amongst employees is set to continue. But the good news is that bug bounty programs have created an agile, rapidly scalable and affordable way of getting expert human security experts to assist in testing and improving cybersecurity for all types of organization.

These ethical hackers are highly motivated and ready to work. Couple this with a strong bug bounty platform and expert triage team, and suddenly cybersecurity isn't just about the bad news after all.

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