hackerone

The Beginners' Guide to Bug Bounty Programs

Hackers can provide continuous security at the speed of innovation.

The last several years have seen the most destructive data breaches of our time. 2019 was another year of numerous and highly damaging data breaches that put hundreds of millions of consumers at risk. But it could have been worse. Tens of thousands of security vulnerabilities were eliminated with the help of hackers.

Hackers are no longer anonymous guns-for-hire. Everyone from the financial services industry, to e-commerce giants, to government agencies has embraced hackers as part of a mature, proactive security strategy.

It's not hard to see why. Businesses process more data—and more personal data—than ever before. As companies work overtime to push code, criminals work overtime to find vulnerabilities.

Your job is to reduce the risk of a security incident, protect your brand and assets, and ensure the security of your customers and their valuable data. Keeping those assets secure is a non-stop endeavor that requires highly-technical and specialized skills—but equipping your organization with this toolbox be prohibitively expensive. It's almost impossible to scale security with internal resources alone.

According to Gartner's "Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing" report, crowdsourced security testing is "rapidly approaching critical mass."

Over $74 million in bounties have been awarded to hackers for identifying more than 140,000 security vulnerabilities. Each one of these vulnerabilities posed real-world risk to an organization. Combined, they represent a clear picture of the real-world risks we face today.

In The Beginners' Guide to Bug Bounty Programs we will look at how organizations include Starbucks, LendingClub, Airbnb, GitHub, Hyatt, Verizon Media, Priceline, Nintendo and Google Play are working with hackers to protect their customers and brands.

Introduction to Hacker-Powered Security

Before we dive into bug bounty programs, let's define hacker-powered security. Hacker-powered security is any technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include bug bounty programs, hacker-powered pentests, and vulnerability disclosure policies.

Hacker-powered security arms organizations with the skills, experience, and nonstop coverage of creative and experienced hackers and researchers. These finders work to identify vulnerabilities before they can be exploited by criminals. It's a fast, structured, and proven model for crowdsourcing the right expertise, applying it when and where you need it, and paying only for results. Think of hacker-powered security as an extension of your in-house security team, but with nearly limitless capabilities and an elastic, on-demand usage model.

Bug bounty programs offer continuous testing to secure applications that power your organization.

KEEP OUR PEOPLE SAFE

We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks. We know that. What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference, who want to help keep our people and our nation safer.

ASH CARTER,
DEPARTMENT OF DEFENSE

READ THE CASE STUDY

FANDUEL

In this customer story, Security Specialist Liam Somerville tells HackerOne why their 7-person strong security team relies on hackers to be a key force multiplier.

Important Terms

Hacker: One who enjoys the intellectual challenge of creatively overcoming limitations.

Hacker-Powered Security: Any goal-oriented hacking technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include private bug bounty programs, public bug bounty programs, time-bound bug bounty programs, hacker-powered penetration testing for compliance, and vulnerability disclosure policies. With hacker-powered security testing, organizations can identify high-value bugs faster with help from the results-driven ethical hacker community.

Hacker-Powered Pentest: A limited access program where select hackers apply a structured testing methodology and may be rewarded for completing security checks.

Hacktivity: Hacker activity published on the HackerOne platform.

Public Bug Bounty Program: An open program any hacker can participate in for a chance at a bounty reward.

Private Bug Bounty Program: A limited access program that select hackers are invited to participate in for a chance at a bounty reward.

Time-Bound Bug Bounty Challenge: A limited access program with a pre-determined time frame where select hackers have a chance at earning a bounty award.

Vulnerability: Weakness of software, hardware or online service that can be exploited.

Vulnerability Disclosure Policy (VDP): An organization's formalized method for receiving vulnerability submissions from the outside world, sometimes referred to as "Responsible Disclosure." This often takes the form of a "security@" email address. The practice is outlined in the Department of Justice (DoJ) Framework for a Vulnerability Disclosure Program for Online Systems and defined in ISO standard 29147.

What is a Bug Bounty Program?

The bug bounty program is the most advanced form of hacker-powered security. It provides continuous security testing and vulnerability reports from the hacker community.

When a new bug bounty program is launched, in 77% of the cases, hackers find the first valid vulnerability in the first 24 hours. That is how fast security can improve when hackers are invited to contribute.

Bug bounty programs can be either public or private. Public bug bounty programs, like Starbucks, GitHub, and Airbnb, are open to everyone, while private programs require organizations to invite hackers to participate. Public programs are open to the widest range of hacker diversity and therefore produce superior results. On average, **public bug bounty programs have engaged six times the number of hackers reporting valid vulnerabilities.** That number nearly doubled in 2019.

Private programs make up 79% of all bug bounty programs on HackerOne, whereas public programs make up the remaining 21%. By starting with a private program, security teams can then work with a smaller group of hackers to identify unknown and easily found vulnerabilities as they optimize internal security processes. This allows them to become comfortable with the volume and types of vulnerability reports they might expect to receive before advancing to a public bug bounty program.

Bug bounty programs are very similar to **vulnerability disclosure policy** (VDP). VDPs are referred to as the "see something, say something of the internet" and provide clear guidance for external parties to report security weaknesses to an organization so they can be resolved. The principal difference is that VDPs simply create a framework for interacting with and accepting help from the security community, while bug bounty programs actively incentivize that work by offering rewards for vulnerabilities that the community discovers.

Bug bounty programs include incentive structures and processes designed to encourage individuals with a range of experience and talent to identify and report potential security vulnerabilities so they can be safely resolved before they're exploited. No money changes hands until after the vulnerability is reported, validated, and determined to be in line with the program terms, as defined in the policy or security page. Done properly, a bug bounty program can be an enormous boost to your organization's security.

STARTING WITH SECURITY@

A Vulnerability Disclosure Policy (VDP) will help you create your process for monitoring, managing, vetting, responding to, and fixing reported vulnerabilities. It's a great first step to dealing with incoming bug reports and building a team and a process for handling those reports. To learn more about this security best practice check out, the 5 critical elements to a VDP.

Public? Private? Either Way, It's Yours

No matter how you choose to structure your bug bounty program, it can be entirely private, blatantly public, or anywhere in between. Here's how they differ.

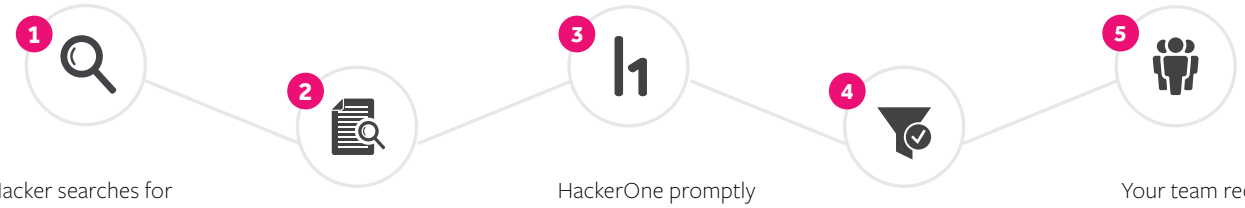
Private programs are known only to those hackers you choose to invite based on skills, experience, location, or other attributes. But every report, participant, bounty, and other aspect of the program is totally private.

Public programs are open to all hackers and can maximize both your program's visibility and the volume of participants and their varying skills.

They give you better coverage and exposure to hackers, and can also be publicized to show your customers how much effort you're putting into security. But even public programs are customizable: bug reports can remain private and redacted, disclosure timeframes are up to you, bounty values are yours to set, and many other elements can be controlled as you wish. Private bug bounty programs currently make up 79% of all bug bounty programs on HackerOne. You can see more statistics and analysis in The 2019 Hacker-Powered Security Report.

A FULLY-MANAGED HACKERONE BUG BOUNTY PROGRAM

Our experts will design, manage, and support your bug bounty program from end to end. Here's how it works:



1. Hacker searches for vulnerabilities
2. Hacker submits it to your organization
3. HackerOne promptly communicates with the Hacker
4. HackerOne triages all submissions
5. Your team receives only valid, well-documented vulnerability reports

More than 140,000 security vulnerabilities (and counting!) have been eliminated with help from hackers on HackerOne. Combined, these vulnerabilities represent a clear picture of the real-world risks we face today. Want to learn what the most common threats are? The HackerOne Top 10 Most Impactful and Rewarded Vulnerability Types is an interactive site allowing you to explore bounty award levels, severity scores, total report volumes, and more.

HackerOne Bounty provides a managed, turnkey bug bounty program with all the flexibility, expertise, and resources needed to integrate bug bounties into your security apparatus with little effort and little disruption. Our experts work with you to design, manage, and support your program from end-to-end, ensuring a smooth launch and seamless integration into your security efforts. For those new to bug bounty, this is a great entry point. For those experienced, it's a fast way to support the training, payments, hacker vetting, report tracking, compliance, and other considerations that are outside your core mission.

APPLICATION TESTING

When the same internal teams are testing an application for a long time, they lose that 'fresh-eye' perspective that often helps in finding interesting bugs.

VLADYSLAV CHEREDNYCHENKO,
INFORMATION SECURITY ENGINEER, **ABOUT YOU**

Why Work with Hackers

Organizations as diverse as Starbucks, Airbnb, GitHub, Verizon Media, Lending Club, PayPal, Google and Intel and Twitter are using bug bounty programs to reduce risk and protect customers and their brands. Your customers, partners, and even government agencies and industry groups now expect you to leverage the wisdom and power of the vast hacker community. It improves and scales your security capabilities, helps protect your assets and strengthen your brand, and demonstrates innovation.

Security flaws aren't shameful; they're a fact of software development. No matter how many processes or security measures you put into place, it's impossible to prevent all vulnerabilities. But with a bug bounty program, you can extend your processes to handle these bugs safely and efficiently by inviting hackers to assist you. The best part is that it's pretty easy to get started and to scale your efforts, as long as you plan your path.

CRITICAL IMPORTANCE

Cybersecurity is of critical importance to Priceline. This is why we are enhancing this essential layer of protection with our expanded bug bounty program.

MATT SOUTHWORTH,
CHIEF INFORMATION SECURITY OFFICER, PRICELINE

Overcoming Resistance to Working with Hackers

Hacking is here for good—for the good of all of us.

We cannot prevent data breaches, reduce cyber crime, protect privacy or restore trust in society without pooling our defenses and asking for external help. Cybersecurity has rightfully become a company-wide responsibility that goes beyond just security and IT teams.

A public-facing security solution, such as your bug bounty program, could involve buy-in from legal, finance, and even the Board of Directors. However, people outside security and IT, such as legal, finance, and public relations teams, don't necessarily know that it's possible to improve your security posture by safely leveraging the external research community—and by implementing a formal policy that spells out what can be tested and what cannot.

Some points to keep in mind when discussing bug bounty programs and hackers with legal, finance and PR teams:

- **Current security measures can't catch every vulnerability. Bug bounty programs can catch business logic issues that a scanner will miss.**
- **Bug bounty programs offer ongoing testing unlike point-in-time testing.**
- **Bug bounty programs enlist the help of experienced hackers to find vulnerabilities before attackers do.**
- **Bug bounty programs have become a best practice in the industry and are used by companies and governments around the world including Goldman Sachs, the U.S. Department of Defense, and Hyatt Hotels.**

The following entities can be cited as support for working with ethical hackers:

Department of Justice (DoJ) published a Framework for a Vulnerability Disclosure Program for Online Systems. https://www.justice.gov/criminal-ccips/page/file/983996/download

ENISA: Economic Union Agency for Network and Security: recommends VDPs for the government and private organizations.

Hack DHS: requires the Department of Homeland Security to implement a VDP and Bug Bounty Program.

ISO 29147: recommends vulnerability disclosure as a best practice and offers guidelines on how to include in their processes when receiving information about potential vulnerabilities from external individuals or organizations.

NIST Cybersecurity Framework: Provisionally added RS.AN-5 which recommends that processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

The earliest recorded bug bounty program dates back to 1983. The practice was first scaled in the enterprise by Google, Facebook and Microsoft over the past half-dozen years. As of 2019, more than 1,600 active hacker-powered security programs are run by organizations today including The U.S. Department of Defense, General Motors, Google, Goldman Sachs, PayPal, Hyatt, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, and Intel. These organizations have awarded hackers over $70M in bug bounties to hackers for safely reporting over 140,000 vulnerabilities and to a growing community of 500,000 hackers.

Do you require strict finder verification capabilities? Download this datasheet to learn about HackerOne's Advanced Vetting for organizations that require strict finder verification and enhanced program controls.

Who are the Hackers?

Another common question is, who are these hackers? Or, aren't they criminals? No. Security experts may be described using a variety of titles including *hacker, ethical hacker, white hat, security researcher, bug hunter,* and *finder.* One title is conspicuously absent: criminal. Hackers are not criminals. Specifically, bug bounty platforms offer no benefit to someone with criminal intent. On the contrary, reputable bug bounty platforms will record data about every hacker on the platform and only reward actions that follow the rules. For these reasons, criminals go elsewhere.

What if hackers do something bad? This is where it is essential for vendors to clearly define the scope of the bug bounty program. To set hackers up for success, the program scope should be detailed and regularly updated. The bug bounty vendors should, among other things, be able to background check hackers, know what their reputation is, what their skillset is, and have personal relationships with their hacking community. Some platforms require agreement to disclosure guidelines and codes of conduct. Extortion and blackmail are strictly forbidden. Criminals will attempt extortion tactics whether or not you have a bug bounty program.

But what if someone demonstrates explicit disregard for the rules? They have a name: criminals.

If you are operating a bug bounty program, it is critical that you employ a vocabulary that distinguishes between vulnerability and breach. A bug bounty program is not an invitation to be breached—these programs encourage the discovery of vulnerabilities that could lead to a breach (if left undiscovered). Of course, the likelihood of a breach in the first place is reduced for those running a bug bounty program.

A properly structured bug bounty program will authorize participants to search for vulnerabilities so long as a specific set of rules are adhered to. All participants in HackerOne programs are under instruction to Respect Privacy and Do No Harm. Just as with any authorized security test, an inadvertent access of data by an authorized participant does not trigger statutory breach notification requirements.

Why do Hackers Hack?

Youthful, hungry for knowledge, and creative. Nine out of 10 hackers are under 35, while 8 out of 10 are self-taught. More and more are coming from diverse industries outside of technology, allowing them to bring myriad skillsets and perspectives to bear on their bug hunts. They're also hacking more than ever, with more than 40% spending 20-plus hours per week searching for vulnerabilities and making the internet safer for everyone. Hackers' motivation to join is not solely centered around bounties. Nearly three times as many hackers (41%) begin hacking to learn and to contribute to their career and personal growth, and nearly as many hack to have fun (13%) as those who do it for the money (14%). With each new company and government agency joining HackerOne every day—such as the Hyatt Hotels, Airbnb, GitHub, Starbucks, HBO, U.S. Department of Defense, General Motors, Alibaba, Goldman Sachs, Toyota and more—comes curiosity and a genuine desire to help the internet become more secure (9%).

Every 5 minutes, a hacker reports a vulnerability. Every 60 seconds, a hacker partners with an organization on HackerOne. That's more than 1,000 interactions per day towards improved security.

For a deep dive into the hacker community, checkout the 2019 Hacker Report.

555K+

TOTAL REGISTERED HACKERS

140K+

TOTAL VALID VULNERABILITIES SUBMITTED

$74M+

TOTAL BOUNTIES PAID

**As of November 2019*

What Are The Most Common Vulnerabilities Hackers Report?

HackerOne customers have received more than 140,000 (and counting!) valid security vulnerabilities across more than 1,600 programs of all sizes. Combined, they represent a clear picture of the real-world risks we face today.

The HackerOne Top 10 Most Impactful and Rewarded Vulnerability Types is an interactive site allowing you to explore bounty award levels, severity scores, total report volumes, and more.

Here are the highlights:

- The technology world's mass migration to the cloud has resulted in increased risks from vulnerabilities like Server Side Request Forgery.
- Despite the ever-growing attention on protecting user privacy and data, Information Disclosure vulnerabilities are still common.
- Less than half of this edition of the HackerOne Top 10 overlap with the OWASP Top 10.
- Highly impactful vulnerabilities, like SSRF, IDOR, and Privilege Escalation, are harder to come by but continue to be the most valuable vulnerabilities based on bounties awarded.

Risk is a fact of life. Today, technology unicorns, governments, startups, financial institutions, and open source projects are embracing collaboration with hackers to identify their unknown vulnerabilities. What are the most impactful vulnerabilities that may not be in the OWASP Top 10?

You can view the data on the The HackerOne Top 10 Most Impactful and Rewarded Vulnerability Types today and share your newfound knowledge with your colleagues and friends.

Transitioning to Continuous Security

As with anything new, it's prudent to take a methodical approach to hacker-powered security. As you learn from each step, you'll be better able to understand resource constraints and needs.

Once you've established a VDP, a private, targeted bug bounty program is the next step in the hacker-powered security journey. A private program allows you to further hone and test your internal processes while limiting the number of hackers involved, the volume of incoming reports, and public awareness of the program. A private program also lets you view the potential size and cost of a broader bounty program, giving you time to scale your internal teams and processes to match.

After running a private or time-bound bounty program, you're ready to open your technology up to a continuous public bug bounty program. As we showcased in the 2019 Hacker-Powered Security Report, Public bug bounty programs represent the highest hacker diversity and therefore produce superior results.

That's the best part of hacker-powered security: you're always in control!

Let's take a deeper dive into the different types of bug bounty programs and how HackerOne can help you on your journey.

The Power of More: Time-Bound Bug Bounty via Hacker-Powered Pentests

Today's applications and sites rely on data from more sources, leverage more packages, deploy on a greater variety of cloud infrastructure, and serve users on a larger diversity of devices. For all these reasons, it is vital to keep an eye on the annual OWASP top ten application security risks and comparing it to your current and planned tech stack.

Injection flaws, improper authentication, and exposing sensitive data top the most recent OWASP list. Security teams are wise to also watch for emerging threats like dangling DNS names and leaked API credentials.

Traditional "point-in-time" penetration testing by a small team of researchers is expensive and simply can't keep pace with today's continuous delivery (CD) software model. Instead, companies are tapping into the global community of white hat hackers to stay secure while they continuously innovate. With HackerOne's global hacker community, you benefit from the diversity of skills, "on-tap" availability, and cost-effectiveness you need. In fact, HackerOne pentesting customers see up to 600 percent ROI compared to traditional penetration tests.

For the first time, Forrester breaks down the benefits using the proven Total Economic Impact methodology. Based on interviews with multiple HackerOne customers, Forrester calculates composite savings compared to traditional penetration testing of more than $500,000 over three years.

SAVE TIME, AVOID TROUBLE

Our developers are frequently blown away by the ingenuity of the researchers. Using HackerOne saves our security team a large amount of time, but more importantly it also saves our finance team a lot of trouble.

NEIL MATATALL,
SECURITY ENGINEER, **GITHUB**

Want to learn more? Download the free report from Forrester.

Crowdsourced Security with Absolute Confidence, Visibility and Control

Security and control are essential for highly-regulated industries, businesses that handle sensitive or personal data, and government sectors.

Since 2016, our Advanced Vetting capabilities have helped HackerOne bring crowdsourced security to some of the most risk-averse organizations around, including the U.S. Department of Defense. Whether the organization seeks to protect sensitive national security data, regulated health or financial data, or simply wish to satisfy a wary legal department, HackerOne Advanced Vetting ensures all finders undergo the most intense vetting possible.

To qualify for Advanced Vetting, finders must undergo an annual background check and ID verification, maintain a threshold Reputation score on the HackerOne platform, and be free of any code of conduct violations. Advanced Vetting, part of HackerOne Clear, goes beyond ID verification and criminal background checks to include real-world validation of finders' skills based on their performance in HackerOne programs.

Clear's Advanced Vetting feature is designed for organizations that require strict finder verification capabilities consisting of ID verification, criminal background checks, and skill validation based on the finder's historical performance.

SPECIALIZED AND UNIQUE

The carefully selected, diverse population of HackerOne Clear researchers applied their specialized and unique skills to give us a controlled approach to the crowdsourced security testing model.

BRIAN NEELY,
CIO AND CSO,
AMERICAN SYSTEMS

Want to learn more? Contact us today or visit us online.

Do it Live: One Day, Big Benefits

Though this community thrives on the internet, HackerOne also brings hackers together through live hacking events around the world. Live hacking is a unique type of bug bounty engagement in which hackers from all over the globe fly in to participate in an in-person, timeboxed testing period focusing on a targeted set of assets.

This traditionally includes two weeks leading up to the event, culminating in 2-3 days in a particular city. During those several days, we bring the programs' security teams and hackers together for social activities, sightseeing, knowledge-sharing, and of course, lots of hacking. Special scopes are released for more compelling testing, companies are encouraged to provide metadata or unique feature access for additional research, cash bonuses and bounties are offered, and there's a leaderboard for the event with awards for the top hackers for best bug, best signal, highest reputation gain, and the best hacker of the event (Most Valuable Hacker).

This gives customers the opportunity to build relationships with the hacker community in person. These events increase hacker engagement on mature programs, support customer recruiting efforts, and result in thousands of resolved security vulnerabilities for the likes of Uber, Dropbox, GitHub, Shopify, Verizon Media, U.S. Air Force and the U.S. Marine Corps. With highly skilled hackers collaborating on the same attack surface, critical vulnerabilities that could have existed for years are instead uncovered in days. Recent live hacking events have taken place in San Francisco, London, Amsterdam, Singapore, Las Vegas, and other cities around the world.

We also host hacking workshops for student groups, structured hacking mentorship sessions and job recruiting workshops. HackerOne's first live hacking event, h1-702, was in Las Vegas in August 2016 during DEF CON and spanned three days, paying out over $150K to a group of about 30 hackers. Live hacking events have come a long way since then, improving the structure and experience for top hackers and customers alike and paying hackers nearly $1M during a one day event.

Build a Nonstop Security Army: Continuous Bug Bounty Program

Bug bounty programs can be continuous, global, and comes with nearly limitless skills and experience. A bug bounty program puts all of these elements to work improving and hardening your security, all day, everyday. HackerOne Bounty gives you a flexible platform to manage, coordinate, and analyze a bug bounty program designed to fit your unique needs.

WHERE AND HOW BUG BOUNTIES FIT INTO THE SDLC

1. TRAINING & RISK ASSESSMENT

Revelations of missing best practices and the subsequent gaps and security risks that are uneaxrthed through bug bounties present a leading indicator for your next training session for engineering.

2. REQUIREMENTS

Bug bounties identify issues that were never found prior and provide valuable input to guide the development requirements to maintain strong application security.

3. DESIGN

Bug bounties reveal insecure coding practices, and the unknown risks associated with a certain architecture, design, or code implementation. This informs your design and application architecture approach.

4. DEVELOPMENT

Bug bounties reveal critical vulnerabilities in your software. This is the ultimate goal, to make the unknown issues known and a fix prioritized before criminals can exploit them.

5. TESTING

Dynamic testing (bug bounties can be deployed in sandbox development environments as well as live in production) results in faster and more effective feedback loops.

6. DEPLOYMENT

Going beyond testing, bug bounties can have a significant impact on process improvement as the "always on" feedback from hackers blends perfectly with rapid deployments

7. RESPOND

The basis for a good bug bounty program, your Vulnerability Disclosure Policy will drive the conversations with hackers, improving your overall security posture.

Reduce Risk, Launch Products Faster, and Strengthen Your Brand with Hacker-Powered Security

No matter how you choose to structure your bug bounty program, it can be entirely private, blatantly public, or anywhere in between.

Private bug bounty programs currently make up 79% of all bug bounty programs on HackerOne, down from 88% in 2017 and 92% in 2016 calendar years. You can see more statistics and analysis in the 2019 Hacker-Powered Security Report.

No matter how you structure your bug bounty program, you are in good company with organizations like Starbucks, GitHub, Airbnb and many others who trust HackerOne to be their bug bounty platform.

Featured case studies:

- Yelp: **Read how Yelp transitioned from a private bug bounty program to a public bug bounty program and their learnings and statistics.**
- GitHub: **Learn how they reduced blind spots and supplemented their internal teams with hacker-powered security.**
- European Union: **In the aftermath of the Heartbleed incident, The European Union launched EU-FOSSA to take a proactive stance to strengthen the security of the key open source infrastructure it uses. They recently expanded the program with EU-FOSSA 2.**

The benefits of hacker-powered security are many, from improving on traditional penetration tests by identifying 10-times the number of critical vulnerabilities, to identifying dozens or hundreds of vulnerabilities in a few days, to spending just a fraction of a security engineer's salary while paying only for validated results. Even government regulators and industry groups are imploring organizations to use hacker-powered security, publish VDPs, and consider bug bounty programs.

AUGMENT SECURITY

One of the best ways for us to augment our internal security team is to work with the white hat community. This was a pain before HackerOne but now is significantly easier.

TOBIAS LUTKE,
SHOPIFY

READ THE BUG BOUNTY CASE STUDY

You may consider launching a program on your own, but you'll quickly run into challenges with finding and attracting top hacker talent, integrating reports into your existing workflow, and paying bounties in various currencies and across international borders. Even the largest companies that operate do-it-yourself bug bounty programs experience very low signal-to-noise ratios. In a 2016 blog post, Facebook noted that they received 13,233 vulnerabilities, with just 526 of them considered valid. That's a 4% signal-to-noise ratio.

Conversely, consider the benefits of working with a proven platform that's built a stellar reputation with the hacker community, and has experience tracking, categorizing, and triaging tens of thousands of reports. The resulting knowledge built into the platform benefits all users with faster and more accurate triage and a signal-to-noise ratio of 80% or higher. Triage is the process which brings signal up to 100%.

HackerOne Delivers

From implementing the basics of a vulnerability disclosure process to supercharging your existing security programs via a bug bounty program, HackerOne has you covered. No matter which program or hacker-powered security choice is right for you, working with HackerOne means you work with vetted, trusted hackers. HackerOne provides several layers of control for selecting, inviting, and approving hackers based on their Reputation metrics, past program participation, specific skills, and more.

HackerOne is the #1 hacker-powered pentest & bug bounty platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. With over 1,600 customer programs, including The U.S. Department of Defense, General Motors, Google, Goldman Sachs, PayPal, Hyatt, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, HackerOne has helped to find over 140,000 vulnerabilities and award over $74M in bug bounties to a growing community of over 550,000 hackers. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, France and Singapore.

Do you require strict finder verification capabilities? Download the datasheet to learn about HackerOne's Advanced Vetting.

And we can help you, too! Learn more by visiting our website or contacting us today.

About Us

HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. With over 1,600 customer programs, including The U.S. Department of Defense, General Motors, Google, Goldman Sachs, PayPal, Hyatt, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, HackerOne has helped to find over 140,000 vulnerabilities and award over $74M in bug bounties to a growing community of over 570,000 hackers. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, France and Singapore.

hackerone

Contact us to get started.