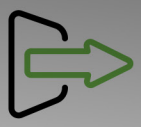
hackerone

The Beginners' Guide to HACKER-POWERED SECURITY

Pre-Seed Hacker Invites

Phase 2 - Launch

(H1) Deliver Challenge Report
Meet with H1 to Discuss Results
Provide Feedback + Q&A
Discuss Future Engagement



Phase 3 - Debriefing

Launch Program
Update Security Page
(H1) Triage Incoming Reports
(H1) Manage Bounty Payments
(H1) Provides Updates on Progress

Introduction

It only takes a casual glance at the latest news to see yet another organization having an unknown (or, all too often, known) vulnerability exploited by criminals.

These days, no matter what type of organization you are, or what size, it's clear that the security of your data, systems, and products is top of mind for you and those you serve. Your job is to reduce the risk of a security incident, protecting your brand and assets, and ensuring the security of your customers and their valuable data.

But keeping those assets secure is a non-stop endeavor that requires highly-technical and specialized skills, and adding those skills to your organization can be prohibitively expensive. It also requires a new and novel approach, one that's been proven by some of the most respected organizations from across the globe.

According to Gartner's *Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing* report, published in June 2018, crowdsourced security testing is "rapidly approaching critical mass". And, according to The Hacker-Powered Security Report 2018, customers of HackerOne resolved more than 27,000 hacker-discovered vulnerabilities in the past year alone.

THE BIGGEST ORGS TRUST HACKER-POWERED SECURITY

When organizations as diverse as Starbucks, Lufthansa, General Motors, the U.S. Department of Defense, Twitter, Goldman Sachs, American Express, and Nintendo are using crowdsourced security tactics, and seeing this level of success, it's clear your toolset is incomplete without it.

Leveraging the wisdom and power of the vast white-hat hacker community is a new security expectation from your customers, partners, and even government agencies and industry groups. It improves and scales your security capabilities, helps protect your assets and strengthen your brand, and demonstrates innovation. The best part is that it's pretty easy to get started and to scale your efforts, as long as you plan your path.

Read on to learn the best practices for starting and running effective disclosure and bug bounty programs, and how to integrate hacker-powered security into your organization.

What is 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 (such as HackerOne Bounty), time-bound bug bounty programs (HackerOne Challenge), and vulnerability disclosure policies (HackerOne Response). With hacker-powered security testing, organizations get the skills, experience, and nonstop coverage of white-hat hackers and researchers to help 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. The first known "bug" bounty program that paved the way for today's industry was launched by operating system company Hunter & Ready in 1983. In the past 35 years, hacker-powered security has moved from being a tactic used only by pioneering tech organizations to a must-have for any organization in every sector. The hackers themselves have even emerged from the shadows and are no longer operating in legal gray areas. In fact, lawmakers and global government agencies as varied as the European Commission to the U.S. Food and Drug Administration are recommending and promoting the implementation of hacker-powered security.

With HackerOne, our expert services team is by your side every step of the way, all with the goal of improving your security. And it's easier than ever to get started using proven, online platforms and turnkey solutions that can bolster your team's security resources significantly. The alternative is attempting to build a hacker-powered security program on your own, relying on cobbled together solutions and trying to piece together tools that were never designed for crowdsourced security.

Hacker-Powered Terminology

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

Hacker-Powered Security: Any 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 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.

Hacktivity: Hacker activity published on the HackerOne platform.

Public Bug Bounty Program: An open program any hackers 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 program with a pre-determined limited time frame. In most cases hackers will register or be invited.

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. 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.

A Security Imperative

Adding hacker-powered security to your security playbook is critical. With criminals, nation states, and nefarious groups getting more aggressive and more clever by the second, organizations cannot afford to ignore any security technique, especially proven ones. In the recent past, organizations used to have just one option for staying ahead of criminals: hire more engineers. But that is unsustainable, expensive, and doesn't even solve the problem.

With hacker-powered security entering the mainstream, the prevailing wisdom has flipped from fearing it to embracing it. It is now viewed as a liability to not include it in your security efforts. Some even argue that, when laws and regulations like GDPR implore you to do everything possible to protect systems and data, ignoring hacker-powered security is irresponsible.

But where hacker-powered security used to be a complex and risky proposition, packaged solutions now make it easy and flexible, especially if you start small and let your program grow alongside your own needs and bandwidth. What you need is a platform that offers flexible yet comprehensive features and expert delivery, tight engagement with a large and diverse hacker community, and demonstrable results from a wide range of satisfied customers.

EASY TO GET STARTED, NO MATTER WHERE YOU BEGIN

A simple vulnerability disclosure policy (VDP) is a logical place to start for many organizations, while others jump right to incentivizing the community in a time-bound bug bounty challenge or with a continuous bug bounty program. It all depends upon your experience, the resources you have available, and your ability to handle incoming reports.

No matter where you choose to begin, our team of hacker-powered security experts can help you with any questions or concerns. Ask us anything and everything that comes to mind. Even if you're considering launching a program on your own, you'll quickly see why over 1,000 organizations trust us to be their hacker-powered security partner.

HackerOne streamlines the process of finding and attracting top hacker talent, providing data and guidance on bounty values, integrating reports into your existing bug tracking workflow, and facilitating bounty payments across countries and currencies. Few companies choose to manage all of those foundational aspects alone, and HackerOne does it better than anyone.

A Methodical Path to Better Security

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

Nearly every organization or agency promoting hacker-powered security recommends starting with a VDP. Providing a mechanism for anyone to report a potential vulnerability is table stakes for security in today's digital world. It can be as simple as a monitored email address, but even a detailed VDP need not be more than a page or two of rules, scope, and expectations. The intent is to give discoverers a clear and concise path to follow when they find a potential bug, and also let them know what you expect from them (report details, disclosure limits, etc.) and what they should expect from you (response time, disclosure timing, communication frequency, etc.).

Internally, a VDP will also 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.

Next, short-term hacker-powered programs can be used to replace or augment your existing penetration tests by having hackers focus on a specific attack surface for a limited time. It's a great way to evaluate the benefits and impact of a broader bug bounty program and get more from your pen test budget. How you set bounty values can also help you manage report volumes or aim attention at specific areas of concern.

TRANSITIONING TO CONTINUOUS SECURITY

Moving to 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 Hacker-Powered Security Report 2018, public bug bounty programs represent the highest hacker diversity and therefore produce superior results. On average, public programs engage 3.5 times the number of hackers reporting valid vulnerabilities.

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

Let's take a deeper dive into each of these areas of hacker-powered security and how HackerOne can help you on your journey.

Control What Used to Be Chaotic:
Launch a Vulnerability Disclosure Policy

A vulnerability disclosure policy (VDP), commonly referred to as the "see something, say something" of the internet, is an organization's formalized method for receiving vulnerability submissions from the outside world without offering rewards. The practice has been defined by the U.S. Department of Justice (DoJ) and in ISO 29147. In a nutshell, a VDP instructs hackers on how to submit vulnerability reports, and defines the organization's commitment to the hacker on how reports will be handled.

There are 5 critical elements to a VDP, one of which is creating a safe harbor for hackers. In March 2018, Dropbox added a legal safe harbor pledge to its VDP, promising "to not initiate legal action for security research conducted pursuant to the policy, including good faith, accidental violations." Dropbox then made its VDP "a freely copyable template" for others to follow their lead. HackerOne also introduced legal safe harbor language as a default for new policy pages, further solidifying it as industry standard.

HackerOne Response lets you work directly with third-party researchers and white-hat hackers to safely receive, validate, and track reported vulnerabilities with minimal impact on your internal team. Incoming reports are secure and they can be integrated with existing workflows and bug tracking systems. We even offer experienced triage services to supplement your internal resources.

Organizations like General Motors, the U.S. Department of Defense, AlienVault, and others are already using HackerOne Response to manage their own VDPs.

Featured case studies:

- General Motors: Learn why hackers have become an essential part of their security apparatus.
- AlienVault: Read how they moved from an email-driven VDP to a holistic program that helps them realize response times of 48 hours or less.

5 Critical Elements for Every VDP

1. **Promise**: Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.

2. **Scope**: Indicate what properties, products, and vulnerability types are covered.

3. **"Safe Harbor"**: Assures that reporters of good faith will not be unduly penalized.

4. **Process**: The process finders use to report vulnerabilities.

5. **Preferences**: A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Get the Power of More with Time-Bound Bug Bounty Challenges via Hacker-Powered Pen Tests

A focused, time-bound penetration test is a great way to dip your toes into hacker-powered security. HackerOne Challenge offers a compliant, results-driven program that vastly outperforms traditional pen tests by creating performance-based incentives for hackers to focus on what matters most to you.

HackerOne Challenge starts by letting you invite hackers based on skills and experience so your test aims the right talent at the right targets. You then set the test's start and end dates to fit your annual or quarterly testing regimen, and structure the bounties to focus the effort where you want it while also motivating the appropriate talent.

A typical HackerOne Challenge lasts just 4 weeks. In week one, the project's scope is defined and hackers are invited. Hackers then test the target properties and applications in weeks two and three while internal security teams and/or HackerOne experts triage incoming reports. Finally, in week four, the results are reviewed and a final, formal report is delivered.

Challenges typically last 4-weeks, but one particular flavor of this product is a one-day live hacking event. Picture the world's largest and most exciting one-day live penetration test where hackers collaborate and mingle with world-class security teams.

ONE DAY, BIG BENEFITS

A live hacking event increases engagement, builds relationships with top hackers, provides an opportunity to test new scope, and helps security teams and hackers work better together. For hackers, live events help them better understand what security teams value most, build relationships with security teams and other hackers, and provide unique opportunities to hack new scope and earn more cash.

Organizations like Okta, Yext, Salesforce and others are already using HackerOne Challenge to redefine or augment their current pen test requirements. Learn more about time-bound bug bounty challenges in this on-demand webinar.

Featured case studies:

- U.S. Department of Defense: Read why they became the first U.S. government agency to challenge white hat hackers to find security flaws in their systems.
- Oath: Learn how their bug bounty challenge resulted in bounty awards of over $400,000 in a single day.

HackerOne Challenge: Timeline

Sign Up with HackerOne

Phase 1 - Preparation

Process Recap/Overview
Test Plan
Policy Guidance
Bounty Payment Guidance
Establish Testing Window
Pre-Seed Hacker Invites

Phase 2 - Launch

(H1) Deliver Challenge Report
Meet with H1 to Discuss Results
Provide Feedback + Q&A
Discuss Future Engagement

Phase 3 - Debriefing

Launch Program
Update Security Page
(H1) Triage Incoming Reports
(H1) Manage Bounty Payments
(H1) Provide Updates on Progress

Build a Nonstop Security Army with a Continuous Bug Bounty Program

HackerOne Bounty gives you access to more than 200,000 hackers, and together we've already helped our customers resolve more than 72,000 security vulnerabilities. We also offer the experience and best practices we've gained from launching more than 1,000 bug bounty programs—that's more than any other platform!

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 hacker-powered security, this is a great entry point. For those experienced, it's a fast way to offload the training, payments, hacker vetting, report tracking, compliance, and other issues that are outside your core mission.

Alternatively, you can manage your own program yet still take advantage of the HackerOne Platform's community of hackers, our tracking, management, and integration tools, and our bounty payment features. Or, you can mix and match products and services to build a custom program on our platform.

Build a Nonstop Security Army with a Continuous Bug Bounty Program

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 specifically 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. It gives 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 with a public program, 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, down from 88% in 2017 and 92% in 2016 calendar years. You can see more statistics and analysis in The Hacker-Powered Security Report 2018.

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:

- GitHub: Learn how they reduced blind spots and supplemented their internal teams with hacker-powered security.

- Shopify: Read how one response to an incoming vulnerability led to a model bug bounty program that others continue to emulate.

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 unearthed 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

The benefits of hacker-powered security are many, from improving on traditional pen 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.

Conversely, consider the benefits 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%.

"Coordinated Vulnerability Disclosure can greatly reduce the possibility of a massive data breach."

- Atlantic Council

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 526 of them considered valid. That's a 4% signal-to-noise ratio.

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

HACKERONE DELIVERS

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. Download our resource on working with vetted, trusted hackers to learn more.

HackerOne has helped all types of organizations manage thousands of programs since 2012, resolving more than 75,000 vulnerabilities and paying out more than $35 million in bug bounties. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security partner. That means we're trusted by some of the most demanding and visible organizations across the globe, including the U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel and the CERT Coordination Center.

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

References

For more information on hacker-powered security, check out the resources below or view all of our guides, case studies, infographics, and more at hackerone.com/resources.

- Vulnerability Disclosure Policy Basics: 5 Critical Components
- 7-Step Roadmap To Hacker-Powered Security Success by 451 Research
- The Bug Bounty Field Manual
- Hacker-Powered Pen Tests and the Power of More
- HackerOne Challenge Customer Testimonials
- The Hacker-Powered Security Report 2018
- Hacker Vetting: Trusted Security Talent for the Enterprise

hackerone

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. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,000 other organizations have partnered with HackerOne to resolve over 80,000 vulnerabilities and award over $35M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, and the Netherlands.

Contact us **to get started.**