The HackerOne Community Difference

Get to know the HackerOne community of hackers and see details of the HackerOne platform and approach.

hackerone

In today's world of cybersecurity talent shortage, hacker-powered security is the answer for reducing your risk by tapping into the collective intelligence of the broader security community.

More and more, the community of ethical hackers are collaborating with industry leaders to search for and report critical vulnerabilities before they can be exploited by criminals. Only when a vulnerability is reported can it be fixed, and those security gaps quickly closed.

HackerOne's community of hackers has grown 10-fold in just the past 2 years, currently at more than 200,000 members. Today more than 1,200 organizations trust HackerOne's community to find and report critical security vulnerabilities including: General Motors, The U.S. Department of Defense, Starbucks, Intel and Google.

This paper will address questions like: Who are the hackers? What metrics does HackerOne track? What does HackerOne do to ensure quality of submissions? What are the rules of engagement and how does HackerOne approach community management?

Who are the Hackers?

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

Hackers are generally curious, tenacious, communal and charitable. Many hackers share knowledge freely with other hackers, and they have, for example, helped the U.S. Department of Defense resolve more than 5,000 vulnerabilities because it's the right thing to do.

Hackers are vital members of our modern digital society. They're real people with in-demand skills who want to help make the internet a safer place for everyone. Some treat hacking as their full-time career, while others do it to earn extra cash or just for the learning experience. Whatever their motivation, they're ready to help your organization, too.

To learn more about hackers and what motivates them to make the internet safer, read The 2018 Hacker Report.

HackerOne has interviewed dozens of hackers at our live hacking events around the world. See the full playlist on our YouTube channel and get to know more about our community!

Frans

SWEDEN

"Personally I hack because I really love to build stuff and I also love to break stuff...the best way to know how to build stuff is to know how you can break it."

REPUTATION

6.55	Signal
95th	Percentile
24.38	Impact
96th	Percentile
20313	Reputation
7th	Rank

CREDITS

622	Bugs found
143	Thanks

Sandeep

INDIA

"Whatever I learned, it's from the community.

REPUTATION		CREDITS
5.12 Signal	90th Percentile	1014 Bugs found
16.70 Impact	86th Percentile	143 Thanks
22476 Reputation	4th Rank	

Johnny

UNITED STATES

"I choose to hack on HackerOne because I enjoy doing it. I like learning more techniques. So it's an opportunity to try things on on systems that maybe I wouldn't normally have access to try things on."

REPUTATION		CREDITS
6.41 Signal	95th Percentile	189 Bugs found
20.96 Impact	93rd Percentile	75 Thanks
4305 Reputation	87th Rank	

Pete

CANADA

"The thrill I get when I find a big bug is kind of indescribable. It's a massive rush."

REPUTATION		CREDITS
5.79 Signal	93rd Percentile	247 Bugs found
17.84 Impact	88th Percentile	49 Thanks
5655 Reputation	65th Rank	

What Metrics Does HackerOne Track?

Hacker activity and quality of submissions is tracked in three main ways: Reputation, Signal, and Impact. Signal measures average report validity, Impact measures average report severity, and Reputation is a cumulative measure of Signal and Impact. These scores can be used as a filter for determining which hackers are invited to your program or to serve as an initial method for evaluating incoming reports.

SAMPLE HACKER PROFILE

Sean Melia (meals)

SENIOR SECURITY ENGINEER, GOTHAM DIGITAL SCIENCE
@seanmeals | Member since September 24th, 2014

REPUTATION		CREDIT
5.48 Signal	93RD Percentile	876 Bugs Found
17.36 Impact	88TH Percentile	80 Thanks Received
20033 Reputation	5TH Rank	

***Signal**: the average Reputation per report. Reputation is gained or lost each time a report is closed, making Signal an aggregate representation of report validity. Ranges from -10 to 7.*

***Impact**: the average Reputation per bounty. Reputation is gained based on the relative size of the awarded bounty, making Impact an aggregate representation of report severity. Ranges from 0 to 50.*

***Reputation**: Points gained or lost based on report validity, and is weighted based on the size of the bounty (and, therefore, the criticality of the reported vulnerability).*

***Credit**: the number of bugs found and thanks received by this hacker from organizations using the HackerOne platform.*

***Percentile**: the percentage of HackerOne community members with a Signal or Impact below this hacker's value.*

***Rank**: the hackers stacked rank compared with the entire HackerOne community based on their Reputation score.*

How Does HackerOne Determine if a Report From a Hacker is Valid?

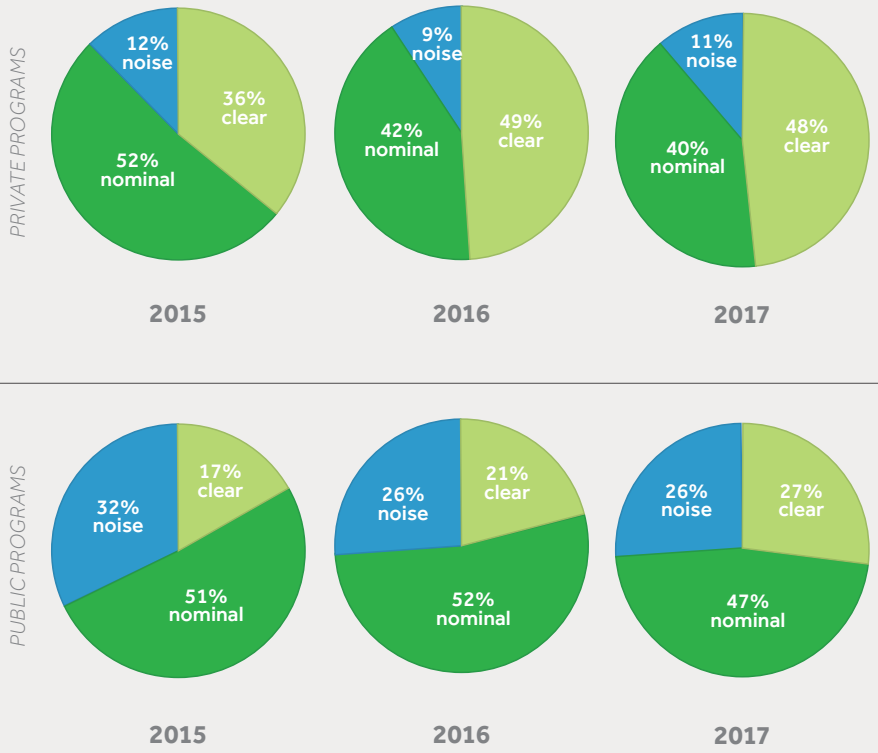
With historical behavior and bug activity tracked for every hacker, the guessing game of "who this hacker is" and "are they good" is completely mitigated.

Signal-to-noise is a quantitative measure of a program's submission quality based on the validity of incoming reports. Signal indicates the number of valid reports received, while noise is the share of non-valid reports received. A higher signal-to-noise ratio means more valid reports are received and less time and resources are spent on invalid reports.

In the early days of hacker-powered programs, signal-to-noise was often an obstacle to overcome in order for organizations to be successful. Do-it-yourself bug bounty programs that don't benefit from noise reducing platform features can experience signal-to-noise ratios as low as 4%, which means just 4 reports are valid out of 100 total reports received. Today, with platform automation, smart algorithms, hacker signal data, and trained professionals on-demand, that number is brought closer to 100% signal.

Delivering the best signal-to-noise ratio in the bug bounty industry means customers save a lot of time, freeing up valuable team resources to focus on more impactful tasks. False positives are a reality for many security products, but they are no longer a significant concern with Hacker-Powered Security.

SIGNAL TO NOISE RATIO DESCRIBED



Historical signal-to-noise ratios on the HackerOne platform

CLEAR, NOMINAL, NOISE

4% DIY programs can see SNRs in the single digits.

18% Other platforms publish data that reveals SNR ratios as low as 18%.

HackerOne has shown a steady year-over-year improvement in our signal-to-noise ratios (see chart above), and are very proud to be #1. Here's how it helps:

Platform Automation and Smart Algorithms: HackerOne's set of crowdsourced vulnerability data results in unrivaled machine learning algorithms. In January 2018, we announced Human-Augmented Signal, which improves the signal of programs significantly and automatically. How does it work? Our system utilizes various criteria to automatically classify all incoming reports and reports with potential noise are forwarded to HackerOne security analysts for review. This human-in-the-loop review guards against false positives and further trains our machine learning classifiers over time.

> *"With the addition of HackerOne's Human-Augmented Signal, we have a higher degree of confidence in the reports we evaluate, reproduce, and triage." - Ian Melven, Director of Product Security New Relic*

> *"The Human-Augmented Signal program at HackerOne has helped us to respect those volunteers' valuable time by reducing the noise on our program by over thirty percent! For us that means more time focusing on helping to keep WordPress users secure and less time responding to invalid reports. Thank you HackerOne!" - Aaron D. Campbell, WordPress Security Team Lead*

Expert Triage and Service: Since 2016, HackerOne has been offering managed services, which include full triage and bug bounty program management to serve as the most convenient option for resource constrained organizations. Managed programs on HackerOne consistently garner higher signal (40%) than unmanaged programs on HackerOne. HackerOne Triage is the practice that takes Signal up to 100%.

Our product development efforts in this arena continue as we seek to eliminate noise for all programs. As we continue to build out and beta test features, more improvements in signal and breakthroughs are inevitable. While eliminating all noise is improbable we've set ourselves a target to reach 90% signal—a standard that hasn't been seen on any other platform in our industry.

What are the Rules of Engagement and Community Management Best Practices on the HackerOne Platform?

At HackerOne, every hacker on our platform is a part of our community. It's part of our DNA to encourage collaboration, camaraderie, and creativity. Many platforms force conversations to go through an intermediary. We take the opposite approach, facilitating a community and platform that is built to have meaningful interactions between security teams and hackers.

Just like any online community, there are rules of engagement and best practices to ensure the community maintains its integrity and value. Here's a glimpse into how HackerOne approaches the success of our community and comfort of our customers.

TERMS OF SERVICE AND CODE OF CONDUCT

By participating in any HackerOne program, hackers and security teams agree to follow our Terms of Service and Code of Conduct, which detail how both sides are expected to act, communicate, and work with each other.

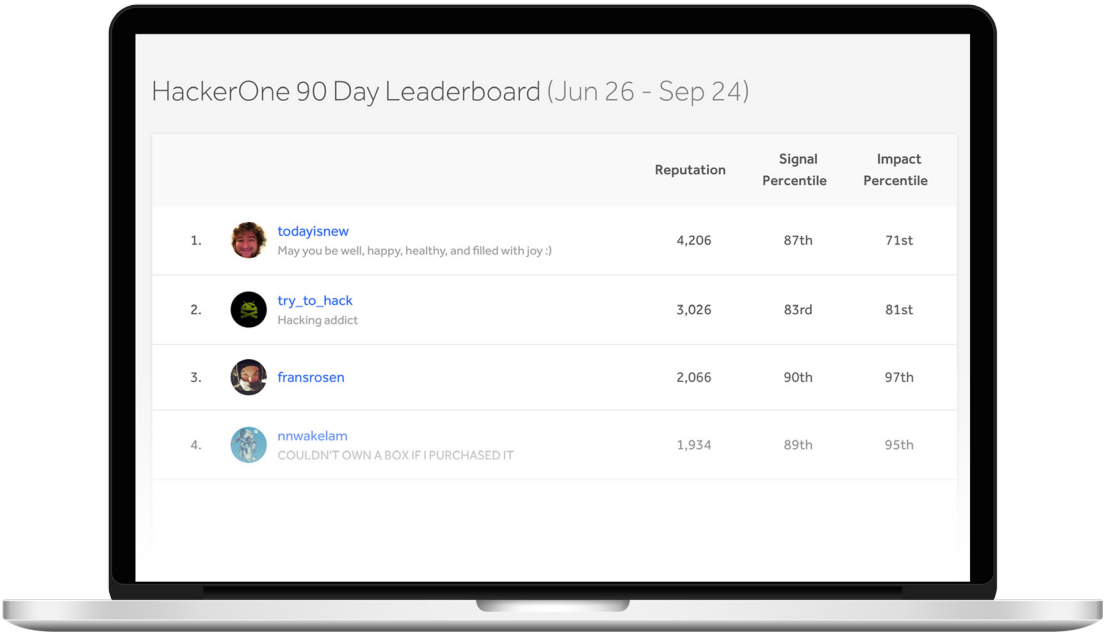
For those who find vulnerabilities, the Code of Conduct guides them to respect and operate within the rules set forth by security teams, or to speak up when they are in strong disagreement with said rules. They should also make a good faith effort not to access or destroy another user's data, to clarify and support their reports upon request, and to act for the common good through the prompt reporting of all found vulnerabilities.

For security teams, the Code of Conduct implores them to make a good faith effort to resolve reported security issues in a prompt and transparent manner. It also guides them to respect finders and give them public recognition for their contributions. Obviously, rewarding research to financially incentivize finders should occur when appropriate. And, security teams should not take unreasonable punitive actions against finders, like making legal threats or referring matters to law enforcement.

HACKTIVITY

HackerOne's Hacktivity feed is one of the most-trafficked pages on HackerOne.com and is a resource for hackers to learn from their peers by reading and reviewing published vulnerability reports and related communications. In total, over 6,200 reports have been disclosed on HackerOne's hacktivity stream. These disclosed vulnerability reports are an invaluable learning tool for hackers, and a simple disclosure mechanism for HackerOne customers.

LEADERBOARDS AND GAMIFICATION



Every hacker on the HackerOne platform is ranked against each other on the HackerOne Leaderboard. This ranking includes all activity in the past 90 days, and covers reputation, signal, and impact.

Beyond bounties, hackers can achieve non-monetary recognition from organizations for various activities. These badges and thank-yous provide additional information on the reputation and credibility of individual hackers.

> *For those looking to instill an additional level of trust, HackerOne Clear provides advanced program monitoring capabilities on top of the world's most trusted network of hackers. HackerOne Clear ensures hackers meet the strictest background and identity standards of the most demanding global organizations, such as the U.S. Department of Defense, and adds powerful access control and monitoring capabilities to increase your confidence, compliance, and control. Contact us to learn more.*

MEDIATION

Misunderstandings can happen. Sometimes it's helpful to have a guide on the side that can help mediate through questions and concerns.

With hacker mediation, programs and hackers can both request assistance from HackerOne. It is usually reserved for extreme cases when all normal discussions have been unfruitful.

When a hacker requests mediation, the following actions are taken:

- An email is sent to the program's security team, requesting that they make their best effort to resolve the issue with the hacker within 3 business days.
- If the security team doesn't respond to the hacker or if the situation isn't resolved, HackerOne will evaluate all available information about the vulnerability report, the hacker who requested mediation, and the organization to determine the appropriate level of escalation.
- If, in HackerOne's judgment, the hacker's case warrants bringing to the company's attention out of band, HackerOne's Customer Success team will do so.

Hacker mediation has been used to successfully bridge understanding between security teams and hackers, resulting in a more favorable outcome for everyone involved. Read more about hacker mediation on our documentation site.

THE DIFFERENCE BETWEEN A COMMUNITY AND A CROWD

We work with hackers to uphold the essence of being a community. We treat them with respect, but we also hold them to the high expectations that our customers demand.

We use the word community to describe our hackers because they are just that: a group of people with a common focus. We work hard to recognize and celebrate our community and the individuals who make it work so well. We also strive to give them support and provide opportunities for them to learn and grow, which is evident in several initiatives:

- **Live Hacking Events**: HackerOne hosts live hacking events around the world to put some of our most innovative customers in the same room with top hackers for a couple of days. It's a fantastic venue for energizing an ongoing bounty program or to run a one-time security test on a specific attack surface. The value of face-to-face interactions helps hackers add skills, build relationships, and find more bugs faster, which benefits our customers as well.

- **Hacker101**: HackerOne curated a collection of educational content to help hackers learn how to work within the bug bounty format. It's a free program, and is taught by a HackerOne security specialist. New content is added monthly including a live twitter chat with James Kettle the Head of Research at PortSwigger (makers of the popular Burp Suite offensive hacking tool), and just recently launched a full 18-flag, 6-level capture the flag challenge available 24x7.

- **Internet Bug Bounty**: Making the community safer for everyone, by working together. HackerOne has partnered with GitHub, Facebook, The Ford Foundation, and Microsoft to create the IBB program, offering rewards for core internet infrastructure and free open source software.

- **Disclosure Assistance**: For organizations that do not have well-defined methods of receiving vulnerability reports from external finders HackerOne will work with friendly hackers on a best effort basis to verify the legitimacy of a vulnerability, reach out to and verify the identity of an individual at the affected organization, then share the vulnerability with the organization so it can be resolved.

All technology contains bugs, and we believe that security is enhanced with visibility and partnership.

Hacker-Powered Security is Accessible to All

Without HackerOne, security teams are pressured to do more, find more, and learn more. It's an untenable position, yet bigger budgets and more engineers is not the solution. Products will always contain bugs, new technologies will appear and require more knowledge, and criminal will always find new ways to exploit whatever you release. But you do continue to ask for more budget, yet your risk profile stays nearly static.

With HackerOne, however, you're adding an elastic, continuous, and nearly limitless resource of talent, experience, creativity, and coverage. HackerOne provides you expertise that no single team can afford to assemble, neither in time nor in budget.

HackerOne offers everything from simple access to a community of hackers to a broad, effective, and proven platform from which to expand, augment, and deepen your security efforts. In the end, your goal is to reduce risk and improve security. That's our goal, too.

AND TOGETHER WE HIT HARDER!

Contact Us Today!