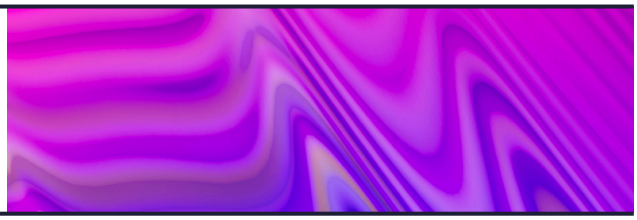
hackerone

The 15% Advantage:

How High-Performing CISOs Leverage Crowdsourced Security

Table of Contents



Offensive security is a broad category of proactive tactics including penetration testing, red teaming, and vulnerability assessments.

Crowdsourced security is a specialized branch of offensive security that engages a global community of ID-verified security researchers to continuously identify, validate, and help mitigate vulnerabilities.

Increased cross-functional collaboration is required with:

- **CLOs** (Chief Legal Officers)
- **CTOs** (Chief Technology Officers)
- **CIOs** (Chief Information Officers)

A New Reality for CISOs

Security leaders are juggling more than ever, and the evolving threat landscape continues to throw more responsibility into their hands.

On top of their duty to manage enterprise-wide cybersecurity risk, **CISOs now have two new mandates**: maintain an airtight environment to prevent data privacy issues, and simultaneously secure the multitude of ways AI can be used throughout their organization. With these responsibilities come new collaborators, as Chief Legal Officers, CTOs, and CIOs are now key stakeholders.

84% are now responsible for AI security

82% now oversee data privacy

But even the best CISOs have blind spots. To expand their field of view, more than three-quarters of security leaders are leveraging the power of crowdsourced security, a specific approach within offensive security. And of those who don't, 86% plan to adopt it soon.

The problem? Nearly half of CISOs use only some crowdsourced security elements, and are not yet experiencing the full benefits, according to our latest research of 400 professionals' perceptions, barriers, and use of crowdsourced security methods.

Only 56% of CISOs  use all key elements of crowdsourced security

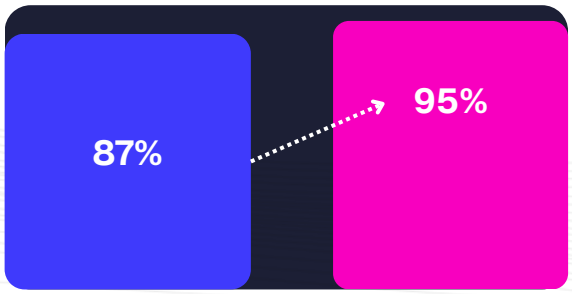
Luckily, the data also reveals a solution to bridging this effectiveness gap—there is a growing 15% of CISOs forging a clear path, employing a layered set of crowdsourced security elements that double the effectiveness for spotting and eliminating vulnerabilities throughout their potential attack surface compared to those with a partial implementation.

We find that CISOs, across industries and sizes, share common barriers to begin using crowdsourced security or to integrate it more comprehensively. To overcome these challenges is to join a rising wave of crowdsourced security leaders.

Current State of Crowdsourced Security

Crowdsourced security methods—bug bounty programs, vulnerability disclosure programs (VDPs), and third-party penetration testing—tap into the expertise of global, independent security researchers to reveal vulnerabilities that may go undetected by internal teams.

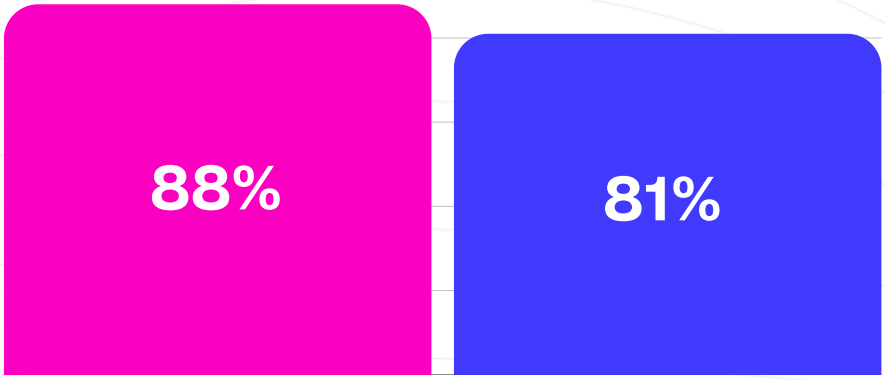
And it's a well-known form of cybersecurity: **94% of CISOs are familiar with crowdsourced security**, and **more than three quarters already use it with success** in some form, including in their new responsibilities in AI security and data privacy.



87% find offensive security important, but this jumps to 95% for those who leverage crowdsourced security

Of the CISOs who don't yet use crowdsourced security, 86% plan to within a year. More than half of those plan to leverage it for **AI security**, and nearly a third plan to include **data privacy** challenges.

Effectiveness of Crowdsourced Testing in Eliminating Vulnerabilities



of CISOs using crowdsourced security find it effective for discovering and eliminating **data privacy vulnerabilities**

of CISOs using crowdsourced security find it effective for discovering and eliminating **AI vulnerabilities**

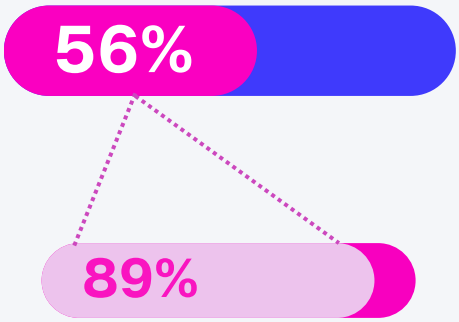
The Gap Between Partial and Powerful Offensive Testing

As CISOs increasingly adopt crowdsourced security, and use multiple methods, they continue to see value.

More than half of current users leverage all core elements: bug bounties, VDPs, and third-party pentesting. But fewer include AI systems and data privacy components in their offensive testing programs.

Partial implementation delivers partial success.

CISOs with lower maturity in building trust with security researchers, parsing the accuracy of their reported vulnerabilities and acting on their feedback, tend to experience reduced effectiveness of crowdsourced security.



of CISOs use all three elements: bug bounty programs, VDPs, and pentesting

of CISOs using all three say crowdsourced testing is effective at discovering and eliminating vulnerabilities

Just over half of CISOs include **data privacy** in offensive testing scope now

32% intend to include it within a year

1 in 3 CISOs include **AI systems** in offensive testing scope now

52% intend to include it within a year

Meet the 15%—Leaders Driving Impact with Crowdsourced Security

Four actions define the CISOs who maximize the impact of offensive security:

- **Use a crowdsourced approach** in their offensive security strategy
- **Include testing for data privacy**-related vulnerabilities
- **Leverage all three key elements** of crowdsourced security (bug bounty, VDP, pentesting)
- **Include testing for AI security** vulnerabilities

With these four elements in place, crowdsourced security leaders are:

2x as likely to find crowdsourced testing models **very effective** in finding and eliminating **security vulnerabilities**

59% more likely to consider crowdsourcing models **effective** at eliminating **data-privacy vulnerabilities**

38% more likely to say offensive security is **very important** to their organization's strategy

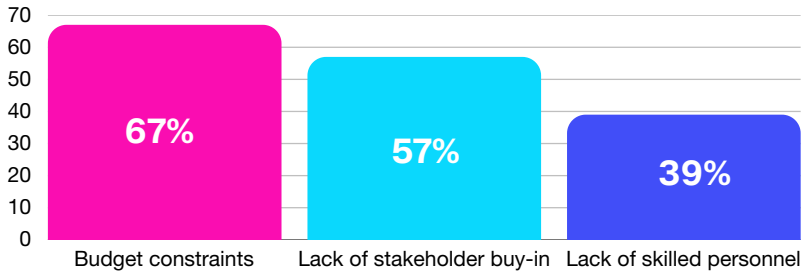
26% more likely to **continuously monitor security risks**

Barriers to Realizing Full Benefits

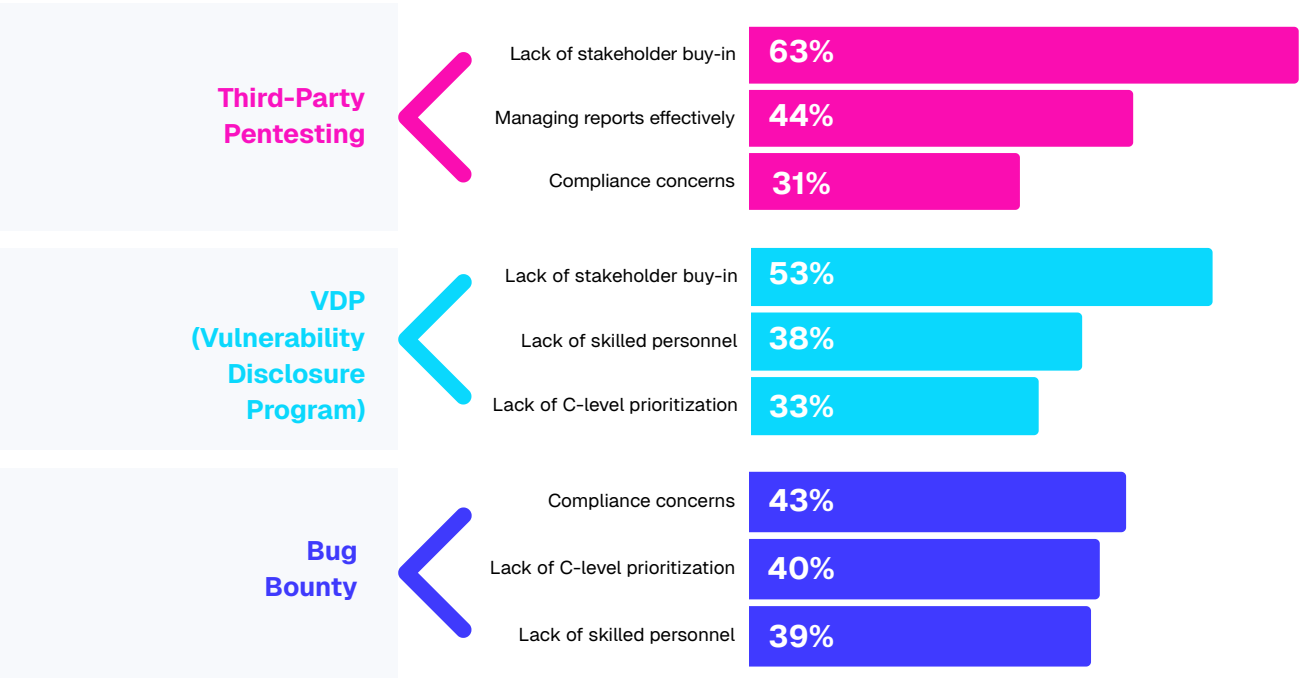
How can a CISO become a crowdsourced security leader?

Those who are new to crowdsourced security, or are just dipping their toes in, may face some common barriers and challenges. But these limiting perceptions don't have to hold you back from diving in to see the biggest impact.

Barriers to Expand Offensive Security



Challenges to Implement Crowdsourced Security Elements



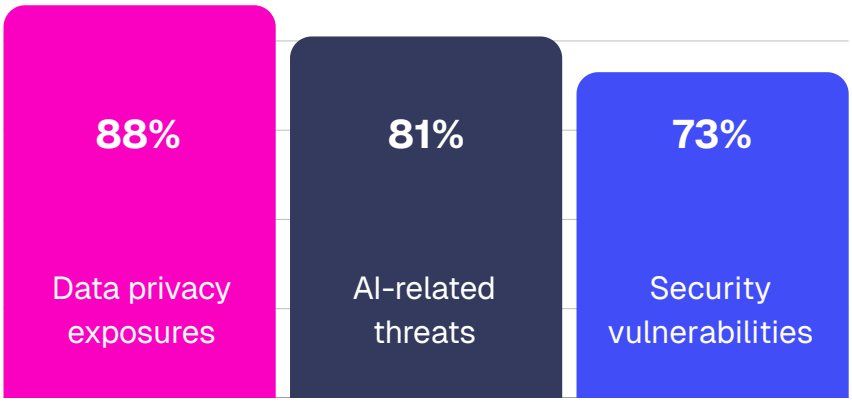
Overcome Barriers to Start or Expand Offensive Security

Insights from the 400 surveyed CISOs provide valuable proof points to overcome barriers. For the most common challenges, data from successful offensive and crowdsourced security practitioners can sway your stakeholders to see the value and impact.

Lack of stakeholder buy-in is the top challenge for those looking to implement third-party pentesting and VDPs, and the most frequently cited challenge overall.

Proof point: 73% of CISOs using some form of crowdsourced security say it's effective in discovering and eliminating security vulnerabilities, with even higher detection rates for data privacy and AI-related threats. This effectiveness jumps to 89% when CISOs leverage all three crowdsourced security elements.

Crowdsourced Security Effectiveness for Data Privacy, AI, and Security Threats



Perception improves with familiarity: *The unfamiliar view crowdsourced security as difficult to manage and scale, while the familiar see it as an effective method to spot vulnerabilities.*

"Having a VDP is a core component to a robust vulnerability management program. Cultivating a positive relationship with the researcher community is incredibly valuable to your overall security program."

James Johnson
CISO at John Deere

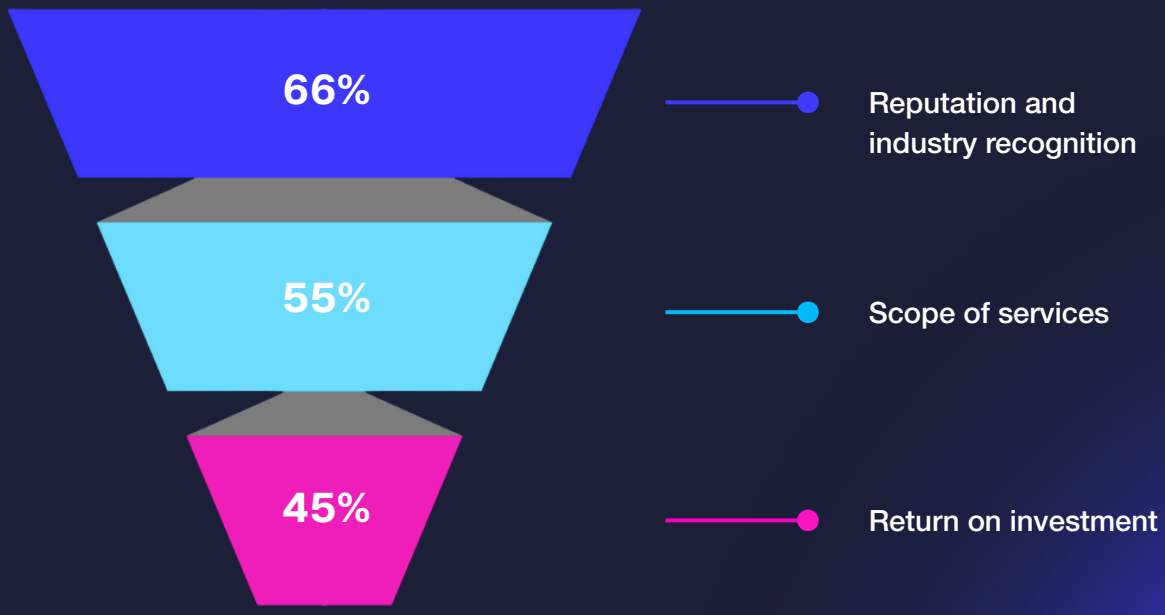
A lack of skilled personnel is a challenge cited for expanding offensive security programs, and for implementing a VDP or bug bounty program.

Proof point: Beyond identifying unknown vulnerabilities, CISOs most often say the primary goal of crowdsourced security is to supplement their internal security efforts. And the scope of services is a key factor CISOs use when evaluating crowdsourced security providers who offer scalable and traceable access to a global pool of vetted security researchers.

"Every organization has blind spots. Having the hacker community on the other side of the screen looking at those things you've missed means you can close those holes."

Matthew Southworth
Vice President, Security Engineering at Priceline

Top Factors That Influence a CISO's Crowdsourced Security Provider Choice



Budget constraints are the most common challenge for CISOs looking to expand offensive security.

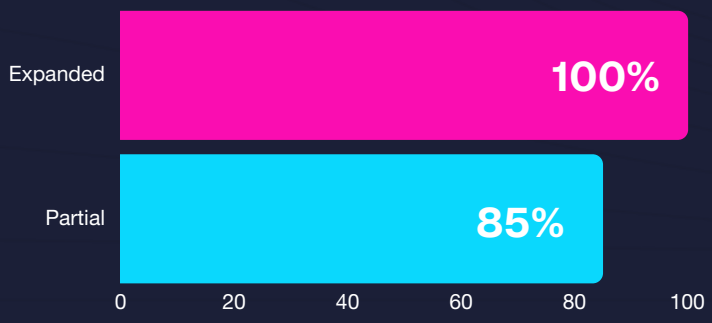
Proof point: The more CISOs invest in offensive security, the more convinced they are. A full 100% of leaders—those who harness all three elements of crowdsourced security, with data-privacy and AI included—say it's important to their overall cybersecurity strategy. This importance also rises with an organization's revenue, showing that early investment compounds over time.

"Since 2019, Zoom has worked with 900 hackers, of which 300 have submitted vulnerabilities that we have had to quickly move on. We've paid out over $7 million. It's a substantial investment but the returns are worth it: we find world-class talent to find real-world solutions before it's a real-world problem."

Michael Adams
CISO at Docusign (formerly CISO at Zoom Video Communications)

Offensive Security Importance Correlates with Larger Revenues

Importance Increases as Offensive Security Strategy Expands



5 Recommendations to Become a Crowdsourced Security Leader

Demonstrating the value of crowdsourced security can help you leverage methods that more than 90% of leaders find effective to truly optimize and future-proof your security posture.

Five recommendations outline the key steps to joining the growing group experiencing the full value of crowdsourced security.

1. Leverage the Full Spectrum of Offensive Security Tools

CISOs who deploy VDPs, bug bounty programs, and pentesting working in concert report higher effectiveness. Mature programs aren't siloed—they integrate continuous testing approaches to maximize coverage and response time.

Take Action: Adopt a layered offensive security strategy that combines transparency (VDPs), continuous testing (BBPs), and targeted assessments (pentests) to strengthen real-world resilience.

2. Prepare for the Offensive Side of AI Security

84% of CISOs now report responsibility for AI security and safety, yet many lack clear strategies or frameworks.

Take Action: Treat AI systems as part of your offensive testing surface, not a separate challenge. Use red teaming and external expertise to uncover vulnerabilities unique to GenAI and LLMs. Prioritize early, frequent testing to stay ahead of emerging threats and regulatory expectations.

3. Expand Internal Capacity Through Community Collaboration

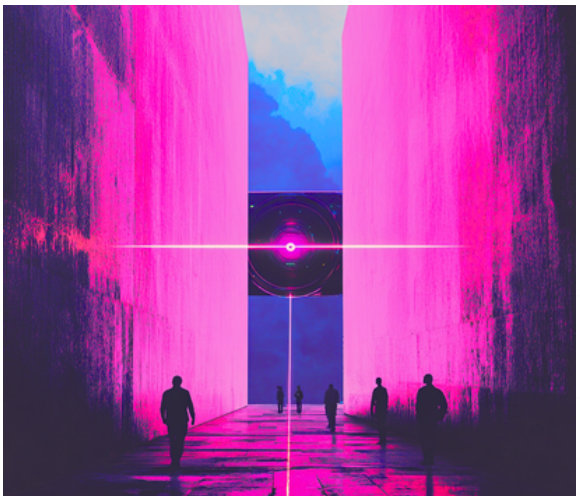
Skills gaps remain a concern for nearly 40% of organizations, and a global shortage of cybersecurity professionals continues. Yet crowdsourced approaches provide access to external expertise to complement internal teams.

Take Action: Invest in models that scale security talent through external collaboration, especially when internal resources are stretched or specialized skills (like AI testing) are needed.

4. Address Stakeholder Alignment Early and Often

Lack of internal buy-in remains a key blocker, even among adopters. CISOs need compelling, organization-wide narratives that link offensive security directly to business outcomes.

Take Action: Frame offensive security as a strategic enabler. Use Return on Mitigation (RoM), compliance coverage, and risk reduction as anchors when building support across the C-suite and board.



5. Define and Measure Maturity —Then Evolve It

Many CISOs express interest in expanding their programs but lack clarity on what "good" looks like. Without benchmarks or maturity models, progress stalls.

Take Action: Use a structured maturity model to assess current state and chart a path forward with benchmarks—one that includes asset coverage, cadence, stakeholder alignment, and researcher engagement.

Final Takeaway: Trust the Numbers

Insights from 400+ CISOs across industries reveal clear correlations between the implementation of crowdsourced security and the confidence in its effectiveness, with nearly 90% of CISOs finding it effective at spotting and eliminating **security**, **AI**, and **data privacy** vulnerabilities. Comprehensive programs include three key methods: bug bounties, VDPs, and pentesting—with clear increases in efficacy when **all three** work together.

Whether you're ready to dive in or start small, choosing the right crowdsourced security partner can help strengthen and scale your security posture. **HackerOne** is a trusted partner and global leader in offensive security solutions. Our HackerOne Platform combines AI with the ingenuity of the largest community of security researchers to find and fix security, privacy, and AI vulnerabilities across the software development lifecycle.

*"HackerOne's community is **second to none**. Over the past decade, they've built an ecosystem that values customer and researcher feedback. Their pace of innovation, particularly in AI features, has been impressive."*

Jim Higgins
CISO at Snap Inc.

Consult with experts on a tailored crowdsourced security strategy. Contact us today.

Survey methodology:

Oxford Economics surveyed 400 CISOs from April to May of 2025. Respondents represented four countries (US, UK, Australia and Singapore) and 13 industries (Telecommunications, Real Estate/Construction, Utilities, Government/Public Sector, Consumer Goods, Education, Retail, Banking/Financial Services/Insurance, Retail/Ecommerce, Manufacturing, Healthcare, Transport/Logistics, and Not-for-profit/Non-profit).

70.5% of respondents worked at publicly-held organizations, while the other 29.5% worked for private organizations. Roughly 2 out of 5 respondents work at smaller organizations (between 1,000 and 2,500 employees); respondents from organizations with at least 10,000 FTEs make up 27% of the sample. Finally, revenue breakdowns are evenly split across 5 revenue buckets: Less than $500m; $501m to $999m; $1b to $4.9b; $5b to $9.9b; and $10b and more.