TROLLEYE SECURITY

# Crowdsourced Cybersecurity **vs Penetration Testing as a Service (PTaaS)**

## What's the Most Reliable Approach to Secure Your Enterprise?


**PHONE:**
(833) 901-0971

**CONTACT:**
trolleyesecurity.com/contact

# Table of **Contents**

TROLLEYE SECURITY

# Executive **Overview**

**Organizations face an expanding attack surface, tighter regulatory requirements, and mounting expectations from customers and stakeholders to safeguard sensitive information.**

**Against this backdrop, new approaches to security testing continue to emerge, with the goal of making it continuous and scalable at an efficient cost.**

Two of the newer approaches to vulnerability discovery and validation that have gained prominence are: Crowdsourced Cybersecurity and Penetration Testing as a Service (PTaaS).

Both aim to identify weaknesses before adversaries do, yet they differ substantially in their structure, delivery models, and outcomes.

This white paper examines the differences between these approaches, drawing on executive insights and real-world experiences. The intent is to provide clarity on how each model operates, what risks and benefits they carry, and where they may align with an organization's security objectives.

*The global crowdsourced security market size is projected to grow to nearly $59 billion by 2035 with a compounded annual growth rate (CAGR) of 16.71%.* ***But is this common testing methodology the best way to scale your security testing?***

# Structural Differences **Between Crowdsourced Cybersecurity & PTaaS**

Crowdsourced cybersecurity and PTaaS both seek to uncover vulnerabilities before attackers exploit them, but they differ in areas such as quality of findings, trust and accountability, and incentive alignment.

| | Crowdsourced | PTaaS |
|---|---|---|
| **Quality of Findings** | **Crowdsourced cybersecurity engages a distributed group of testers, each bringing different backgrounds, experiences, and testing approaches.** | **Penetration Testing as a Service (PTaaS) involves a defined team of specialists who use standardized methodologies.** |
| **Trust and Accountability** | **Crowdsourced cybersecurity often includes contributors who may participate under pseudonyms or without direct identification.** | **Penetration Testing as a Service (PTaaS) is carried out by identified professionals within a defined engagement.** |
| **Incentive Alignment** | **Crowdsourced cybersecurity programs typically compensate participants on a per-finding basis, emphasizing higher risk vulnerabilities.** | **Penetration Testing as a Service (PTaaS) is organized as a defined engagement, with testing aligned to broader objectives.** |

TROLLEYE SECURITY

## 1st Risk with Crowdsourced Cybersecurity

# Quality **of Findings**

The first risk with crowdsourced cybersecurity is that while it can offer a wide range of perspectives and insights, it may also introduce notable variability in the quality of both vulnerability reports and the testing process.

It is worth considering whether this broad-based approach truly aligns with your organization's need for consistent, actionable findings.

*"The rapid democratization of AI tools could overwhelm security teams with low-quality noise, making high-fidelity validation critical.*

*Relying on inconsistent skill sets risks distracting security operations in false positives while sophisticated, structural threats could slip through the cracks."*

**Aby Rao**
**CISO at Paylocity**

**Crowdsourced**

### Skill Disparity

**Participants range from highly skilled professionals to amateurs, resulting in a wide variability in the quality of vulnerability reports.**

### Standardization Problems

**Lack of standard protocols for reporting vulnerabilities means the quality and comprehensiveness of reports can vary widely.**

### False Positives and Negatives

**Low-quality reports can lead to false positives that waste resources and false negatives that leave critical vulnerabilities unaddressed.**

**PTaaS**

### Professional Expertise

**PTaaS employs experienced professionals who adhere to industry best practices and standards, ensuring consistent and high-quality vulnerability assessments.**

### Standardized Methodologies

**PTaaS uses a platform to both generate PDF reports and display vulnerabilities as they're found.**

### Ongoing Support

**PTaaS offers ongoing support, including retesting and validation of remediation efforts, ensuring vulnerabilities are effectively addressed.**

TROLLEYE SECURITY

## 2nd Risk with Crowdsourced Cybersecurity

# Trust & **Accountability**

Secondly, trust and accountability sit at the core of any security testing program. While crowdsourced approaches can bring in diverse skill sets, they often rely on participants whose identities and motivations are difficult to verify.

This lack of transparency can create uncertainty around the credibility of findings and the safety of sensitive data.

*"I recommend PTaaS over crowdsourced security because trust must come first. Crowdsourced models rely on anonymous testers with unverifiable motives, which creates too much uncertainty about who has access to sensitive data and whether results are reliable.*

*PTaaS provides the assurance of vetted professionals, clear accountability, and consistent findings which make it the more secure and dependable choice."*

**Chris Spohr**
**CISO at Republic Finance**

**Crowdsourced**

### Anonymity of Participants

**Many crowdsourcing platforms allow for anonymous participation, making it difficult to verify the identity and credibility of contributors.**

### Lack of Accountability

**Without clear mechanisms for accountability, participants may not feel responsible for the accuracy or quality of their findings.**

### Potential for Malicious Activity

**There is a risk that some participants could exploit their access for malicious purposes, such as launching further attacks or selling discovered vulnerabilities.**

**PTaaS**

### Verified Professionals

**PTaaS providers ensure that all security experts are thoroughly vetted, eliminating the risks associated with anonymous participation.**

### Clear Accountability

**PTaaS engagements are governed by contracts that outline the responsibilities of both parties, ensuring accountability.**

### Trust and Reliability

**PTaaS providers often have established reputations and proven success in the industry, offering a higher level of trust compared to unknown participants.**

TROLLEYE SECURITY

## 3rd Risk with Crowdsourced Cybersecurity

# Incentive **Alignment**

Finally, crowdsourced security researchers' motivations may not always align with their broader security priorities, sometimes resulting in an emphasis on high-profile vulnerabilities at the expense of equally critical but less visible issues.

As a result, best practices are leaning toward more strategic and comprehensive approaches to cybersecurity.

*"PTaaS provides a reliable, collaborative framework emphasizing long-term security. Unlike crowdsourcing's focus on quick wins, PTaaS ensures comprehensive, expert-guided assessments.*

*By prioritizing continuous improvement over fleeting rewards, PTaaS enables sustainable cybersecurity strategies that effectively address vulnerabilities and ensure lasting protection."*

**Hiral Shah CISO at Elecon Engineering Company**

**Crowdsourced**

### Focus on Rewards

**Participants may prioritize vulnerabilities that offer the highest rewards or recognition, neglecting less lucrative but important issues.**

### Competition Over Collaboration

**The competitive nature of crowdsourced platforms can discourage collaboration, leading to fragmented efforts and missed opportunities.**

### Short-Term Engagement

**Researchers may only be interested in short-term gains, resulting in a lack of ongoing commitment to the organization's long-term security goals.**

**PTaaS**

### Alignment With Your Priorities

**PTaaS engagements are tailored to the needs and priorities of the organization, ensuring that all critical areas are thoroughly assessed.**

### Collaborative Approach

**PTaaS fosters an environment where professionals collaborate to provide comprehensive testing, leveraging each other's expertise.**

### Long-Term Partnership

**PTaaS providers are committed to building relationships with clients, focusing on continuous improvement and security posture enhancement.**

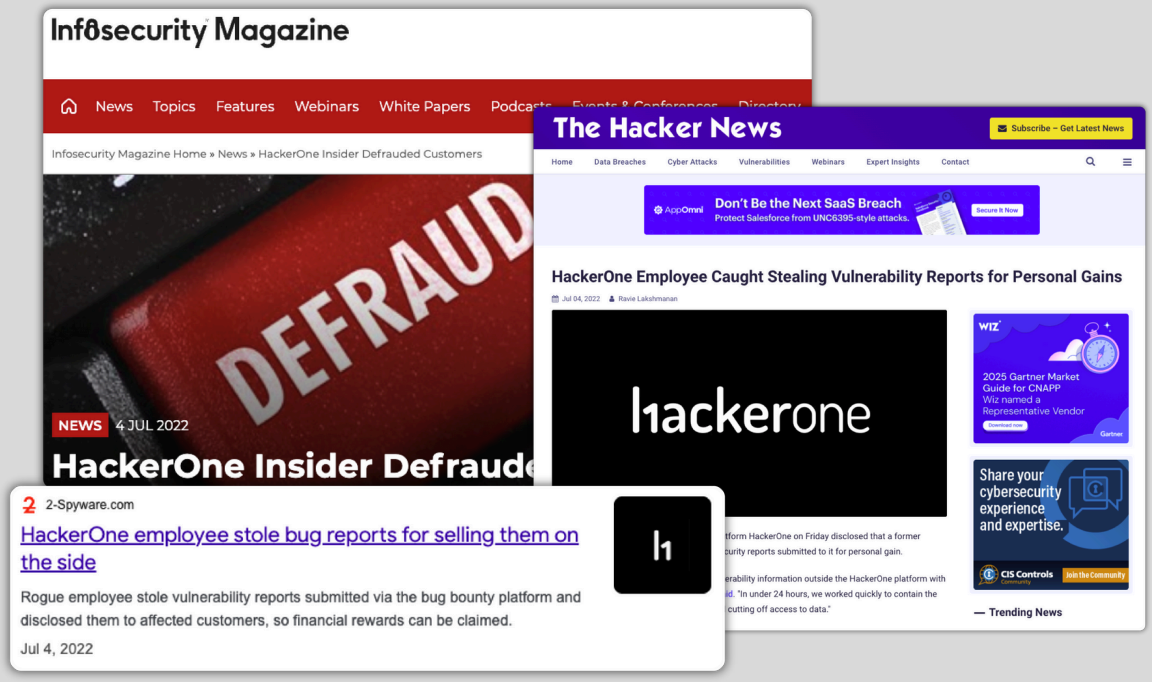
# Real World Example
# **Insider Misuse at HackerOne (June 2022)**

One of the most notable incidents in crowdsourced cybersecurity occurred when a HackerOne employee misused privileged access to vulnerability reports. Operating under a pseudonym, the insider attempted to resubmit findings directly to affected organizations in order to collect bounties.

This incident showed how insider threat risk can extend even to vetted staff and trusted researchers. Crowdsourced platforms rely heavily on distributed trust, yet privileged access can be misused in ways that bypass normal oversight.

At the same time, the sensitivity of vulnerability reports, essentially blueprints of organizational weaknesses, means that mishandling or premature disclosure can create an opportunity for extortion or direct attack.

Without clear visibility into who is handling data or how it is being protected, organizations face uncertainty over whether findings are safeguarded or at risk of being repurposed.



# Real World Risk
# North Korean Infiltration of U.S. Companies

Nation-state infiltration has become one of the most pressing threats facing organizations today. North Korea, in particular, has built a track record of disguising operatives as legitimate professionals who, once embedded, install malware, exfiltrate data, and gain a foothold for broader espionage.

On crowdsourced security platforms, where participant pools are global and decentralized, this risk compounds: adversaries could masquerade as researchers, access sensitive vulnerability data, and weaponize it for state-sponsored campaigns.

## 1 KnowBe4 Hiring Incident (2023)

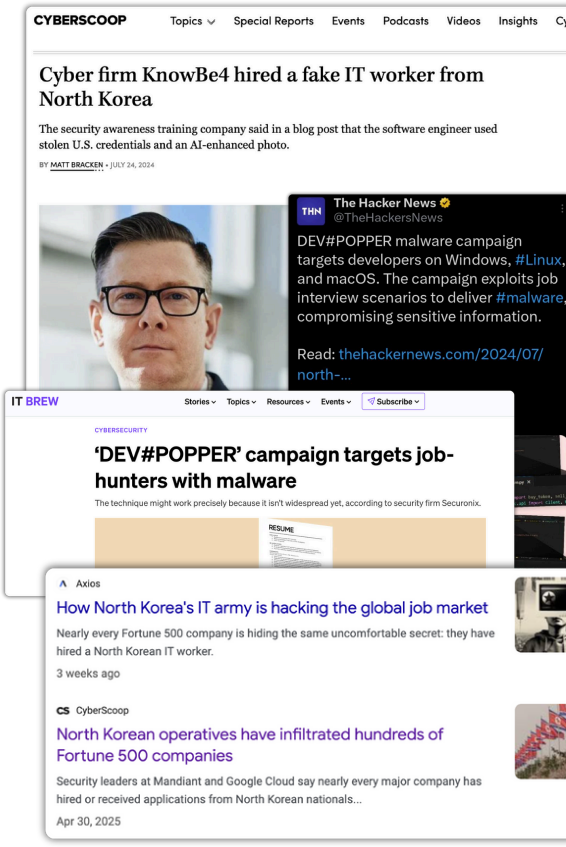
A North Korean operative successfully passed interviews and background checks at KnowBe4, using AI-generated video masking and stolen identities. The individual attempted to deploy malware internally before being discovered.

## 2 DEV#POPPER Campaign (2023–2024)

North Korean actors posed as recruiters offering fake developer jobs. Victims were given malicious “coding tests” that installed malware capable of stealing browser cookies, credit card details, and system credentials.

## 3 Broader Infiltration Tactics

Beyond individual companies, U.S. agencies have documented North Korea’s use of fake freelancing profiles and overseas job applications to infiltrate organizations worldwide. These schemes allow operatives to collect intelligence, move laterally into larger partners, and fund state operations through cybercrime.



# Where Crowdsourced Cybersecurity **Can Add Value to Your Program**

While some risks are associated with it, crowdsourced cybersecurity can be an important tool for some organizations, particularly those with large attack surfaces and consumer-facing platforms.

| | |
|---|---|
| **Consumer & IoT Device Testing** | **Crowdsourced testing helps uncover vulnerabilities in smart home and IoT devices across environments that can't be replicated in a lab.** |
| **Niche Hardware & Peripherals** | **Crowdsourced programs are effective at testing specialized devices like printers or gaming accessories.** |
| **New App & Feature Rollouts** | **Large researcher pools can quickly expose logic flaws and abuse scenarios in new consumer app features before they scale.** |
| **Public-Facing APIs** | **Crowdsourced programs are effective at stress-testing APIs, revealing weaknesses that surface under unpredictable use.** |
| **Regional & Localization Gaps** | **Global rollouts gain protection from region-specific issues, like localization bugs, identified by researchers in those markets.** |

Crowdsourced security works best when applied to broad, exploratory testing challenges where diversity of thought and scale are the greatest assets. It is not a complete solution, but it can be an effective way to complement internal security efforts and increase visibility.

***"Meridian Cooperative leverages both Crowdsourcing through our Managed Bug Bounty program and Penetration-Testing-as-Service (PTaaS). To combat some of the concerns noted in the article regarding Crowdsourcing, Meridian Cooperative selected a private Bug Bounty program so only the top-performing, U.S.-based, background-checked security researchers participate in our Managed Bug Bounty program.***

***Meridian Cooperative also partners with an industry-leading vendor for its AI-based PTaaS platform that we offer our utilities and leverage in-house. The PTaaS platform helps reduce security risk by autonomously finding exploitable weaknesses and providing detailed remediation guidance. It also allows you to perform internal, external, IAM, AD Password Audits, and Cloud-based penetration testing. Ultimately, the value of the PTaaS platform is in better understanding weaknesses that lead to critical impacts, so you know exactly what to fix in order to disrupt the kill chain."***

**Greg Gray**
**CIO at Meridian Cooperative**

# Why Crowdsourced **Security Isn't the Best Way to Scale Testing**

Crowdsourced security is often promoted as a cost-effective way to expand testing, drawing on a wide pool of external researchers. But at scale, the model introduces risks that go beyond vulnerability discovery.

Anonymous participants raise concerns about trust and accountability, competitive incentives can skew focus toward flashy issues, and inconsistent methods produce uneven results.

For organizations aiming to make penetration testing continuous and scalable, these gaps create real exposure. A more secure path relies on vetted professionals and repeatable processes, delivering ongoing testing without the uncertainty of open participation.

**That's the role PTaaS is built to fill.**