
Prepared by Synack, Inc.
We’re pleased to share with you our latest report: The Complete Guide to Crowdsourced Security Testing. “Crowdsourcing” is today’s security trend that CISOs seem ever-more ready to adopt. This report is intended for the decision-makers who want to break through the noise and the confusion in order to choose the best way to harness ethical hackers for their organization’s needs.

The old way of doing security has failed, and more organizations are starting to trust crowdsourced ethical hackers to help with the growing demands of cybersecurity in a world that is technologically complex and increasingly threatened. As Crowdsourced Testing Solutions, including bug bounty programs, vulnerability discovery and hacker-powered penetration testing solutions have become viable options for a growing number of security leaders in recent years, defining the landscape and describing the differences and evolution of different offerings is overdue.

At Synack, we have earned our position as experts in the field of crowdsourced security testing. With an established base of loyal, security-conscious enterprise customers, Synack protects billions of dollars of Fortune 500 revenue, trillions of dollars in financial assets, and the reputation of top global brands. We have based the analysis in this report on the data we have gathered through thousands of tests over the last few years; including hacker demographics, hacker activity, vulnerabilities found, vulnerabilities not found (but searched for), customer demographics, customer asset data and security of those assets over time. To avoid bias to Synack’s enterprise and government customers, we also decided to include published data from other companies that offer Crowdsourced Security Testing solutions. These include Bugcrowd, Cobalt, and HackerOne alongside Synack. Thank you for taking the time to learn more about crowdsourced security testing. Enjoy!

–Team Synack
Companies are Taking Big Hits from Cyber Attacks

Recent corporate breaches like Equifax, Uber, and Yahoo have proven that cyber attackers are easily out-performing our defenses, and the consequences are devastating. According to Verizon’s 2017 Data Breach Investigations Report, over 98% of organizations take only minutes to compromise.

Traditional security testing has failed...

- Organizations haven’t been able to verify people lurking in networks asking for sensitive information.
- Development and security teams haven’t been able to pinpoint the places where credentials are vulnerable.
- Even if security teams do find and try to fix vulnerabilities, they often have difficulty verifying that their patches are effective.

Why Are Companies Getting Breached?

<table>
<thead>
<tr>
<th>Company</th>
<th>Breach Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equifax</td>
<td>Failure to Patch: Lack of a patching system and patch verification system led to exploitation of a known vulnerability.</td>
</tr>
<tr>
<td>Yahoo!</td>
<td>Misplaced Trust: An unknown Russian-sponsored hacker used spear phishing to gain access to the Yahoo network.</td>
</tr>
<tr>
<td>Uber</td>
<td>Unsecured Credentials: Attackers were the first to find login credentials to gain access to Uber’s AWS, since no one looked earlier.</td>
</tr>
</tbody>
</table>

What Are Breaches Costing Companies?

<table>
<thead>
<tr>
<th>Category</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue</td>
<td>-42%</td>
</tr>
<tr>
<td>Bottom Line</td>
<td>$1B</td>
</tr>
<tr>
<td>Market Performance</td>
<td>-40%</td>
</tr>
</tbody>
</table>

- **Drop in Equifax quarterly revenues following breach**
  Source: Equifax financial statements

- **Estimated cost of Sony breach**
  Source: Kowsik Guruswamy, CTO of Menlo Security

- **Breached companies’ underperformance of the NASDAQ three years after breach**
  Source: Analysis, How data breaches affect stock market share prices by Comparitech
It’s not as if companies aren’t trying to secure their systems and their data...

**Cyber budgets are up:**

More than **89 billion dollars** were spent on cybersecurity software and services in **2017**.

More than **96 billion dollars** will be spent on cybersecurity software and services in **2018**.

Clearly, more of the same simply isn’t working for today’s enterprise CISOs. Security teams have been trying to solve dynamic problems with static approaches. A traditional pen test typically offers 80 hours of testing by two consultants, but this limited scale is grossly outmatched by expanding digital attack surfaces and a dynamic, diverse set of adversaries.

**Cyber Incidents vs Cyber Talent**

While cyber incidents are expected to grow by more than 50% by 2019, the available talent in the cybersecurity industry is expected to stay fairly constant at a 6% growth rate. The growth in cyber threats is expected to eclipse the talent growth by a whopping 50%.

Leading enterprises are coming to terms with the fact that their current security processes must change. To protect valuable business and consumer data from the relentless modern adversary, CISOs are racing to move beyond traditional solutions to more realistic and effective means of uncovering and patching unknown vulnerabilities before they can be exploited.

---

1 Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017, Gartner
2 2018 CISO Investment Blueprint, Bugcrowd
Why We Need the Crowd

Crowdsourced testing sets creative hackers on an unstructured hunt through a company’s digital assets. Hackers are incentivized through a bug bounty model with fast-paying rewards to find vulnerabilities and submit reports on their findings for verification and remediation. This unstructured testing methodology mimics actual attack attempts that adversaries use to exploit vulnerabilities, providing a level of scale, speed, pragmatism and intelligence that traditional testing models lack.

Hackers: The Ideal Security Partner

• Offensively minded
• Diverse, dynamic and creative
• Persistent
• Privy to tons of data and the latest technology

“Develop and recruit people who are ‘T-shaped’—Flexible, curious, ‘eclectic specialists.’”
—“CIO Futures: The IT Organization in 2030”, Gartner, May 2017

Since 2015, the number of organizations using bug bounty platforms for bug bounty or responsible disclosure has increased from just under 700 to over 1,500 today.⁴ According to The State of Bug Bounty Report, the number of enterprise bug bounty programs had nearly tripled from 2016 to 2017;⁵ Microsoft reported that the number of submitted vulnerabilities had risen 111% from 2012 to 2017;⁶ and Google reported that they had rewarded nearly $12 million in hacker rewards since they founded their program in 2010.⁷ To date, more than 155,000 valid vulnerabilities have been processed through a crowdsourced program.⁸

As a CISO, I want to get the sense of how our organization really looks from the outside, not how we look from a consulting firm’s perspective. If an adversary is trying to break in, then I want to know what they are going to find.
—Synack Customer

---

⁴ Aggregated data from Bugcrowd, HackerOne, Synack internal
⁵ The State of Bug Bounty Report, Bugcrowd
⁶ Microsoft Vulnerabilities Report 2017, Avecto
⁷ Vulnerability Reward Program: 2017 Year in Review, Google
⁸ Aggregated data from Bugcrowd, Google, HackerOne, Microsoft, Synack internal
The Numbers Behind Crowdsourcing

The Power of Scale
A crowdsourced approach adds scale to your organization, providing more eyes on a target and more hours of testing than a basic pen test.

- Hundreds of available, skilled, and trusted hackers
- Over 200 hours spent on target

Basic Pen Test:

<table>
<thead>
<tr>
<th>Testers</th>
<th>Hours</th>
<th>Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>40</td>
<td>80</td>
</tr>
</tbody>
</table>

Synack Crowdsourced Test:

<table>
<thead>
<tr>
<th>Testers</th>
<th>Hours</th>
<th>Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>50–80</td>
<td>5–10</td>
<td>200+</td>
</tr>
</tbody>
</table>

The Power of On-Demand Software
A basic pen test takes weeks to schedule and begin testing, and you won’t see any results until the 2-week testing is completed. An on-demand and SaaS-based crowdsourced test like Synack’s can save a company a lot of time.

- 24 hours to onboard
- 24 hours to first vuln notification
- Real-time analytics during the entire test

Basic Pen Test vs. Synack Crowdsourced Test

- Synack: Onboard in 24 hours, Real-time Analytics in 2 weeks, Final Report
- Pen Test: Onboard in 3 weeks, Final Report in 2 weeks
What Will You Find With a Crowdsourced Test?

With a crowdsourced approach, you can combine the varied skill sets and experience levels of hundreds to thousands of hackers to ensure that you find just about any security vulnerability that may be lurking in your digital systems.

Synack’s Vulnerability Breakdown by Percentage of Accepted Vulnerabilities:

```
Cross Site                     | Authorization
Information                  | Business Logic
Content                       | Authentication
SQL Injection                 | CSRF
Remote Code                   | DoS
Brute Force                   | Other
```

10%  | 20%  | 30%

**Not-So-Fun Fact:** We saw over 100% growth in Information Disclosure, Functional Abuse/Business Logic, Authentication Flaws, Remote Code Execution, and Brute Force vulnerabilities during 2017.

If you had these vulnerabilities lurking in your systems but you never found them, what would happen? We polled our crowd of hackers for some of the most famous attacks conducted against organizations that either left these vulnerabilities unpatched or had no idea that they were even there...

**Cross Site Scripting:** Samy is an XSS worm that spread across MySpace in 2005. The worm carried a payload that displayed the string “but most of all, samy is my hero” on a victim’s MySpace profile page then also sent Samy a friend request. When another user viewed an infected profile page, the payload was replicated and planted on their own profile page continuing the distribution. Within 20 hours of it being released, over one million users had run the payload.

**Authorization/ Permissions** The US Office of Personnel Management Committee was breached in 2015 by attackers who probably used social engineering to obtain valid user credentials to the systems. Then by using custom-crafted malware, the attackers escalated privileges to gain access to a wide range of OPM’s systems.

**SQL Injection:** A SQL injection vulnerability was discovered in June 2017 that affected one of the most popular Wordpress plugins, WP Statistics, and was installed on over 300,000 websites. The vulnerable function didn’t check for privileges and the SQL queries weren’t being sanitized properly, which allowed the attacker to steal databases and possibly hijack the site remotely through SQL injection.

**Cross Site Request Forgery:** A CSRF was found on PayPal.me in 2016 that allowed an attacker to change any PayPal user’s profile without their permission. The request contained a CSRF token but the user was able to remove/edit the token to perform the attack.

**Remote Code Execution:** The Drupalgeddon2 vulnerability allows an attacker to perform unauthenticated remote attacks to execute malicious commands. This was due to insufficient sanitation of inputs passed. The vulnerability exists within multiple subsystems of Drupal 7.x and 8.x.
Types of Crowdsourced Security Programs

Different forms of crowdsourced testing via a bug bounty payout model can be divided into the following segments:

**Responsible Disclosure**

A Vulnerability Disclosure policy is recognized as a basic layer of security infrastructure, allowing organizations to receive vulnerability submissions from the general public. A company can set up a policy on any of their public-facing websites or applications. Once the program is established, anyone can report a vulnerability or issue found on the site. A company will often issue a formal recognition (or “give kudos”) to the researcher who submitted a valid vulnerability. It is expected by the researcher who discloses a vulnerability that there will be a timely and thoughtful response from the company. Without one, the researcher could feel justified in releasing vulnerability details to the public. About 6% of the Forbes Global 2000 currently have a disclosure policy in place.³

**Managed Responsible Disclosure**

A Managed Responsible Disclosure program utilizes a third party to help review and triage vulnerability submissions that come in from the public. Like Vulnerability Disclosure, any researcher who submits a valid vulnerability can receive public recognition.

**Open Bug Bounty/Paid Responsible Disclosure**

Open Bug Bounty programs allow for vulnerabilities to be submitted from the public and offer swag or cash payouts to researchers who find valid vulnerabilities. The bug bounty model seeks to motivate hackers with incentives to find exploitable vulnerabilities in public assets.

*Between open and invite-only bug bounty programs, about 15% are open programs.*⁴

**Invite-Only Bug Bounty**

Invite-only bug bounty programs go an extra step in minimizing customer engagement risk related to engaging with public, unvetted hackers. These programs operate on an invite-only basis, selecting from the larger subset of hackers. Rules and payments vary widely across invite-only programs, so hackers are forced to research each program to get a sense of the rules of engagement and payment speed. The criteria for admitting researchers into these programs vary as well, but are usually based on past performance and submissions, as judged by and in comparison to other hackers on the platform.

*Between open and invite-only bug bounty programs, about 85% are invite-only.*⁵

³ The Hacker-Powered Security Report, HackerOne
⁴ Aggregated Bugcrowd, HackerOne data
⁵ Aggregated Bugcrowd, HackerOne data
**Managed Crowdsourced Vulnerability Discovery**

Managed Crowdsourced Vulnerability Discovery sets creative hackers on the same unstructured vulnerability hunt as a bug bounty program, but adds consistency. Every researcher undergoes a stringent, consistent vetting process to confirm trustworthiness and skill. They are paid consistently (and well) across all managed programs, which attracts the most professional hackers. In return, they are held to a higher standard of conduct, including secrecy, when required.

The vendor guides customer scoping, manages bounty pricing structures, triages vulnerabilities submitted, and helps verify fixes. Pricing is based off of a flat subscription fee as opposed to variable bounty payouts over time.

Managed programs utilize technology in their testing platform. Automated scanners can alert hackers for any change detected in the environment, guiding human testing to places with expected vulnerabilities. Testing activity can be tracked and controlled through a secure gateway, giving the customer the ability to start and stop testing. Testing activity data collected from the gateway contributes to higher customer visibility and auditability through testing coverage maps and reporting.

**Managed Crowdsourced Penetration Testing**

Security teams can add compliance-based testing checklists to the Managed Vulnerability Discovery process. This solution provides a customer with documented proof that specific security checks (OWASP Top 10, PCI, etc) were completed at a point in time.

**Continuous Testing**

Continuous testing provides constant attention to a constantly-changing digital footprint, helping organizations to harden their attack surface. The most dynamic security will offer a combination of change detection tools, continual automated scanning, ongoing human testing, and meaningful metrics.
The Evolution of Crowdsourced Testing

**Basic**
Achieve compliance through completing checklists that have been created from common past vulnerabilities.

**Hacker-Powered**
Activate adversarial-based testing in order to uncover and fix vulnerabilities before present-day criminal hackers can exploit you.

**Hacker-Powered with Intelligence**
Utilize metrics and insights from your adversarial testing to stay a step ahead of criminal hackers by continuously hardening assets to attack and reducing your risk.
What’s the Best Crowdsourced Test For Your Organization?

It’s critical to think about your objectives and the resources and capabilities you have internally so that you can choose the best crowdsourced program to meet your needs. Bug bounties should be used as a tool to enhance your security team; they shouldn’t be burdening your team with work that you can’t handle.

- Is your objective to find vulns or is it to reduce your risk?
- How many internal resources do you have to manage a crowd on your own?
- Do you value control of the crowd or diversity of the crowd?
- Do you value efficiency over quantity or vice versa?
- How much insight and intelligence do you hope to capture from your program?
Do You Just Need a Platform? Or Do You Need a Partner?

A Deeper Dive into the Unmanaged or Managed Decision

Going with a platform-centric approach vs. a partner-centric approach can lead to a very different crowdsourced security testing experience. The unmanaged experience is a bare-bones, do-it-yourself model; the managed experience provides built-in structure, processes, and protection. Consider what’s best for your team, with a careful eye out for hidden time, costs, and risks.

<table>
<thead>
<tr>
<th>CHALLENGES AND BENEFITS</th>
<th>UNMANAGED (Basic Platform)</th>
<th>MANAGED (PLATFORM AND PARTNER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker Trust and Ethics</td>
<td>Unknown</td>
<td>Known</td>
</tr>
<tr>
<td>Hacker backgrounds, skill level, trust</td>
<td>Unknown</td>
<td>Known</td>
</tr>
<tr>
<td>Extortion Threats</td>
<td>Unprotected</td>
<td>Fully Protected</td>
</tr>
<tr>
<td>Vulnerability Leaks to Public</td>
<td>Unprotected</td>
<td>Fully Protected</td>
</tr>
<tr>
<td>Program Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing Coverage</td>
<td>Unknown testing coverage reach</td>
<td>Fully tested attack surface within scope</td>
</tr>
<tr>
<td>Triaging Submitted Vulnerability Reports</td>
<td>Handled by security team</td>
<td>Handled by vendor</td>
</tr>
<tr>
<td>Responding to hacker payments and demands</td>
<td>Handled by security team</td>
<td>Handled by vendor</td>
</tr>
<tr>
<td>Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated Scanning</td>
<td>None</td>
<td>Provided</td>
</tr>
<tr>
<td>Hacker Traffic Tracking</td>
<td>None</td>
<td>Monitored</td>
</tr>
<tr>
<td>Coverage Data and Analytics</td>
<td>None</td>
<td>Provided</td>
</tr>
</tbody>
</table>

“If organizations want to find the most critical problems, they’ll have to be thoughtful about how they set up their bounty programs—the hackers they include, the incentives they offer, and the targets they invite them to probe.”

—John Ombelets, CXO Magazine
Crowdsourcing has taken the security industry from a standard of compliance to a standard of finding vulnerabilities. By inviting and incentivizing hundreds of outside researchers to hunt for bugs in organizations’ digital assets, crowdsourced programs have proven their ability to find a large volume of vulnerabilities. However, does finding vulnerabilities necessarily prove that your security team is reducing your business risk? Not really.

Here’s what you should be asking of your crowdsourced testing:

- Are my high-value assets being prioritized in the testing scope?
- Is the crowd of researchers incentivized to find high severity and vulnerabilities that have measurable impact on my organization?
- Is my security team able to process and validate all of the vulnerabilities submitted?
- Is my security team able to prioritize high-impact vulnerabilities and patch them effectively?
- Do I see a reduction in vulnerabilities introduced into my digital environment?

If your answer is ‘no’ to any of these questions, your crowdsourced program could be incentivizing researchers to submit a lot of low-quality, low-risk vulnerabilities that ultimately don’t impact your organization’s security and leave you overburdened in the end.

You shouldn’t be finding more vulnerabilities. You should have fewer vulnerabilities to find over time...

Your primary goal of engaging crowdsourced security testing should be to build increasing resistance to cyber threats over time. With that in mind, what’s a better way to measure the success of your program? Instead of just metrics around vulnerability volume, you need to consider metrics around the quality of testing, vulnerability impact, effectiveness of remediation, and testing efficiency. To do this, you need trackable and measurable testing procedures every step of the way. Each phase of engagement should be measured and evaluated, from scoping, onboarding, testing execution, vulnerability reporting, vulnerability triaging, to remediation. If you can prioritize high-value assets, map security vulnerabilities to potential impact to the organization, remediate impactful vulnerabilities, and decrease vulnerabilities introduced in the future, you are well on your way to mitigating your cybersecurity risk.
Vulnerability Criticality

We use the Common Vulnerability Scoring System (CVSS) to describe and categorize vulnerabilities in a way that reflects their relative severity. Ranging from 0-9, the score is translated into low, medium, high, and critical to help security teams assess and prioritize their vulnerabilities in terms of impact and risk. Based on a combination of factors such as exploitability, complexity, and impact, the CVSS score helps security teams prioritize and focus on high and critical vulnerabilities.

What is a Low Severity Vulnerability?
- Vulnerabilities in the low range typically have very little impact on an organization’s business. Exploitation usually requires local or physical system access.

What is a Medium Severity Vulnerability?
- A vulnerability that requires user privileges for successful exploitation. Exploitation would require the attacker to manipulate individual victims via social engineering tactics, to reside on the same local network as the victim, or set up denial of service attacks. Often provides only very limited access.

What is a High Severity Vulnerability?
- Exploitation could result in elevated privileges, significant data loss, and/or downtime.

What is a Critical Vulnerability?
- A vulnerability whose exploitation could allow code execution without user interaction. Exploitation likely results in root-level compromise of servers or infrastructure devices.

Distribution of Vulnerabilities by Criticality: Synack Customers

- Average severity of vulns according to CVSS 2.0 was 6.2 (2017)
- Average of 12 high severity vulns (>7.0 CVSS 2.0) per asset
- 30% of vulns found by Synack Researchers had >7.0 CVSS (2017)
- Less than 9% of valid vulnerabilities reported to Synack are below CVSS 4.0
Asset Hardening

What if security teams started thinking about the success of their security strategies in terms of increased resistance to attack? In order to harden their assets to present and future attack attempts, security teams should be taking a closer look at testing metrics like number of attack attempts, attack types, number of vulnerabilities, hours of testing, etc. By enforcing continual work and continual testing, measuring results, and then prioritizing improvements, security teams will ensure that their security testing performance improves over time.

“Security teams moved from pen testing to hacker-powered bug bounty programs when they realized compliance alone was ineffective at defending against the modern cyber adversary. However, while hacker-powered programs hand off a lot of vulnerabilities to security teams, there hasn’t been a clear idea of the amount of coverage or the level of risk reduction that comes with the testing.”

—Jay Kaplan, CEO and Co-Founder of Synack

Hits/Vulns

We decided to take a look at researcher attack attempts on customer assets over time and compare them to the number of vulnerabilities found on those assets during the same time period. We call this the “hits/vuln” ratio, and it can give security teams an idea of how strong or weak their listing is at any given time of testing.

**Hit:** Any researcher attack attempt on a customer application or host captured through the Synack Launchpoint gateway; for example, a SQL injection attempt on a given URL.

**Vuln:** An accepted valid vulnerability. A vulnerability submitted by a researcher, then triaged and accepted by Synack Mission Ops team.

An average of all Synack customer listings over time:

In January of 2017, the client assets of Synack continuous or renewing customers took an average of 8,565 hits to produce a vulnerability.

In January of 2018, those same Synack clients had increased their overall hits/vuln ratio by over 600% from the previous January. Synack client assets took an average of 56,693 hits to produce one vulnerability.
The customer started testing with Synack in November of 2016 and Synack Red Team researchers began probing the assets in scope to discover previously unknown vulnerabilities. At the beginning of the project, just a few hits by a researcher would turn into a valid vulnerability.

Over the course of a few months, it took significantly more attempts by a researcher to find a single valid vulnerability, meaning their assets were significantly building up a resistance to attack.

In January of 2017, and again in June 2017, the customer released new code and/or broadened their initial scope of testing. This gave Synack Red Team researchers another chance to test assets that had never been tested before, making it a little easier again to find vulnerabilities.

Over time, it took significantly more attempts to find a single valid vulnerability, and overall, the organization's assets continue to build up resistance to attack.
The Journey to Attacker Resistance

Hits to vuln ratio over time is just one way (and a simplistic way) to track and measure the performance of a digital asset’s security over time. What goes into a holistic and comprehensive Attacker Resistance Score?

- **Attacker Cost**: How much time/effort was required to discover vulnerabilities in an environment
- **Severity of findings**: The impact and quantity of vulnerabilities discovered in an assessment
- **Hacker Skill**: A measure of the level of complexity of the vulnerability based on the researcher skill level required to discover it
- **Remediation Efficiency**: How efficiently an organization is able to resolve identified issues in their environment

$$\text{Attacker Resistance Score} = \text{Attacker Cost} + \text{Severity of Findings} + \text{Hacker Skill} + \text{Remediation Efficiency}$$

Modern attack surfaces change constantly. Continuous change requires continuous testing:

1. Release Software
2. Test & Find Vulnerabilities
3. RemEDIATE & Verify
4. Release Hardened Software
5. Repeat

“Attacker Resistance is a metric that is really important to me. Knowing how hardened my assets are against attack lets me set the priorities of my security operations accordingly.”

—Ethan Steiger, VP & CISO, Domino’s
Summary

Why Crowdsource?

The Power of Scale
- Hundreds of available, skilled, and trusted hackers
- Over 200 hours spent on target

The Power of On-Demand Software
- 24 hours to onboard
- 24 hours to first vuln notification
- Real-time analytics during the entire test

The Power of Incentives
- 150,000 valid vulnerabilities and counting
- At least 12 high and critical severity vulns discovered in a 2-week test

What Does Crowdsourced Security Look Like?

<table>
<thead>
<tr>
<th>Basic Penetration Tests</th>
<th>Hacker-Powered Responsible Disclosure / Open Bug Bounty</th>
<th>Hacker-Powered Invite-Only Bug Bounty</th>
<th>Hacker-Powered with Intelligence Managed Vulnerability Discovery</th>
<th>Managed Crowdsourced Penetration Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compliance</td>
<td>• Basic Coverage for Unknown Vulns</td>
<td>• Adversarial Testing Coverage</td>
<td>• Adversarial Testing Coverage</td>
<td>• Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Selected Crowd</td>
<td>• Highly Vetted Crowd</td>
<td>• Adversarial Testing Coverage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Vuln Triage &amp; Full Program Management</td>
<td>• Vuln Triage &amp; Full Program Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditable Testing Traffic</td>
<td>• Highly Vetted Crowd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Testing Coverage Analytics</td>
<td>• Auditable Testing Traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Testing Coverage Analytics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Security Scoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Ongoing Risk Reduction</td>
</tr>
</tbody>
</table>

Is Your Crowdsourced Security Testing Successful?

- High-Impact Vulnerabilities are Found and Patched
- Continual testing and measurement shows performance improvements
- Hardened Assets Over Time
- Organizational Risk Reduced Over Time

About Synack

Synack, the leader in crowdsourced security testing, provides real security to the modern enterprise. We leverage the world’s most trusted ethical hackers and an industry-leading platform to find critical security issues before criminals can exploit them. Companies no longer have to choose between working with the best security talent and a lack of time, resources, or trust. Headquartered in Silicon Valley with regional offices around the world, Synack has protected over 100 global organizations by reducing companies’ security risk and increasing their resistance to cyber attack.

Questions about the crowdsourced security testing options and what’s best for your team?

Contact us at www.synack.com and a Synack team member would love to help.
More About Synack

What does Synack Protect?

- >830M credit card & payment accounts
- Banks with >$5 trillion in assets
- Close to $1 trillion in Fortune 500 Revenue
- 268 Food & Beverage Brands
- Top 10 Consulting Firm
- Top 10 Retailer
- Every US Taxpayer via the IRS
- US DoD Classified Assets

Who Trusts Synack?

- 4% Aerospace, Oil, Gas, Construction, Engineering
- 12% Hospitals & Healthcare
- 3% Manufacturing & Transportation
- 30% Technology
- 6% Consulting, Business and IT Services

- Education 3%
- Banking, Financial Services & Insurance 19%
- Entertainment & Leisure 3%
- Federal Government 4%
- eCommerce & Retail 10%
- Consumer Products & Food/Beverages 6%

Where in the World are the Synack Hackers?

- United States & Canada 41%
- Europe & UK 21%
- Asia 9%
- India 19%
- Africa 3%
- South America 2%
- Middle East 1%
- Mexico 1%
- Australia 3%

Synack, Inc.
855.796.2251 | www.synack.com | info@synack.com
© Copyright 2018 Synack, Inc. All rights reserved.