Synack

The Complete Guide to Crowdsourced Security Testing

GOVERNMENT EDITION

Prepared by Synack, Inc.

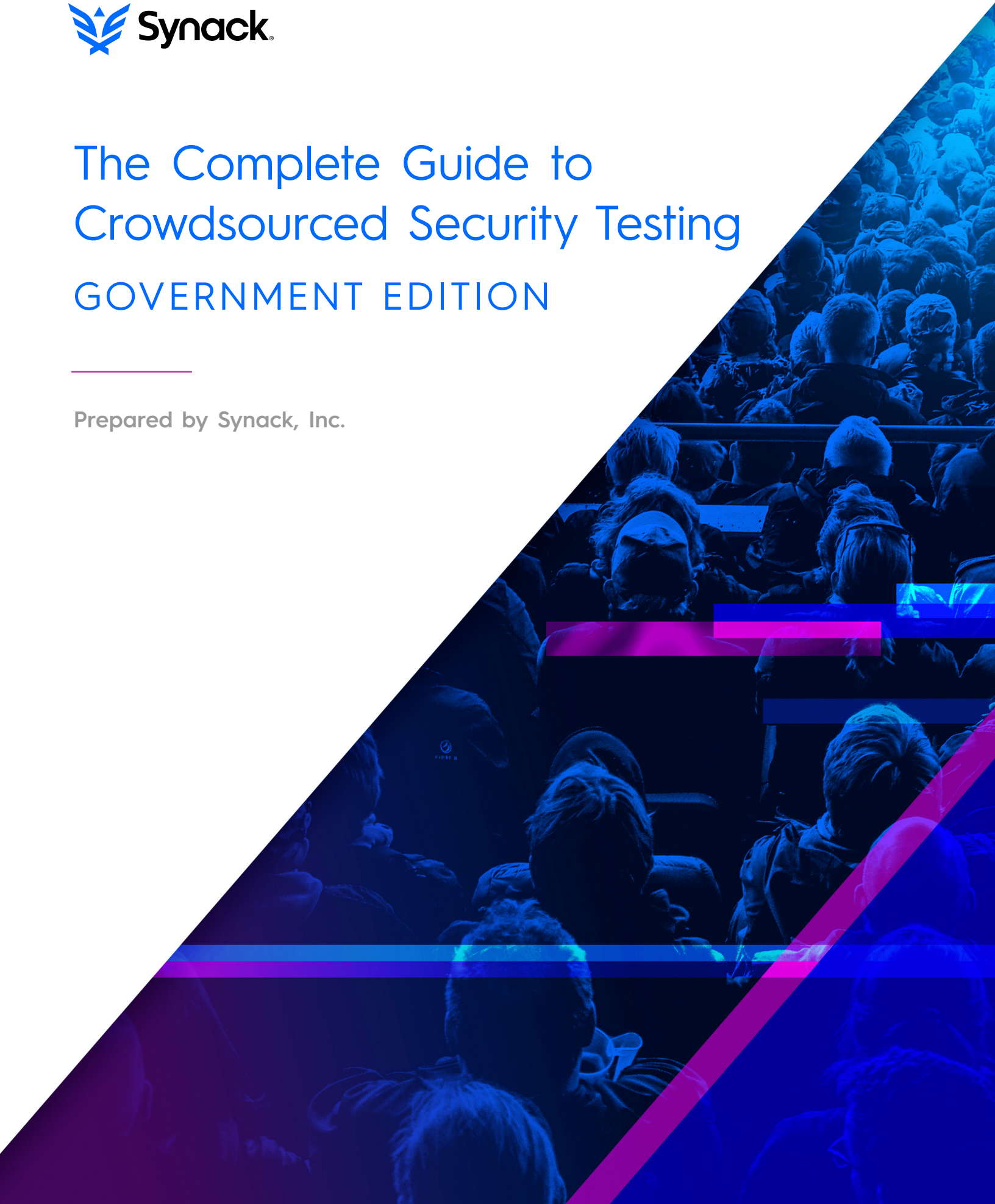


Table of Contents

Synack A Note from Team Synack

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 outperforming 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?

EQUIFAX®

Failure to Patch: Lack of a patching system and patch verification system led to exploitation of a known vulnerability.

YAHOO!

Misplaced Trust: An unknown Russian-sponsored hacker used spear phishing to gain access to the Yahoo network.

UBER

Unsecured Credentials: Attackers were the first to find login credentials to gain access to Uber's AWS, since no one looked earlier.

What Are Breaches Costing Companies?

REVENUE **-42%**

Drop in Equifax quarterly revenues following breach

Source: Equifax financial statements

BOTTOM LINE **$1B**

Estimated cost of Sony breach

Source: Kowsik Guruswamy, CTO of Menlo Security

MARKET PERFORMANCE **-40%**

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.**[1]

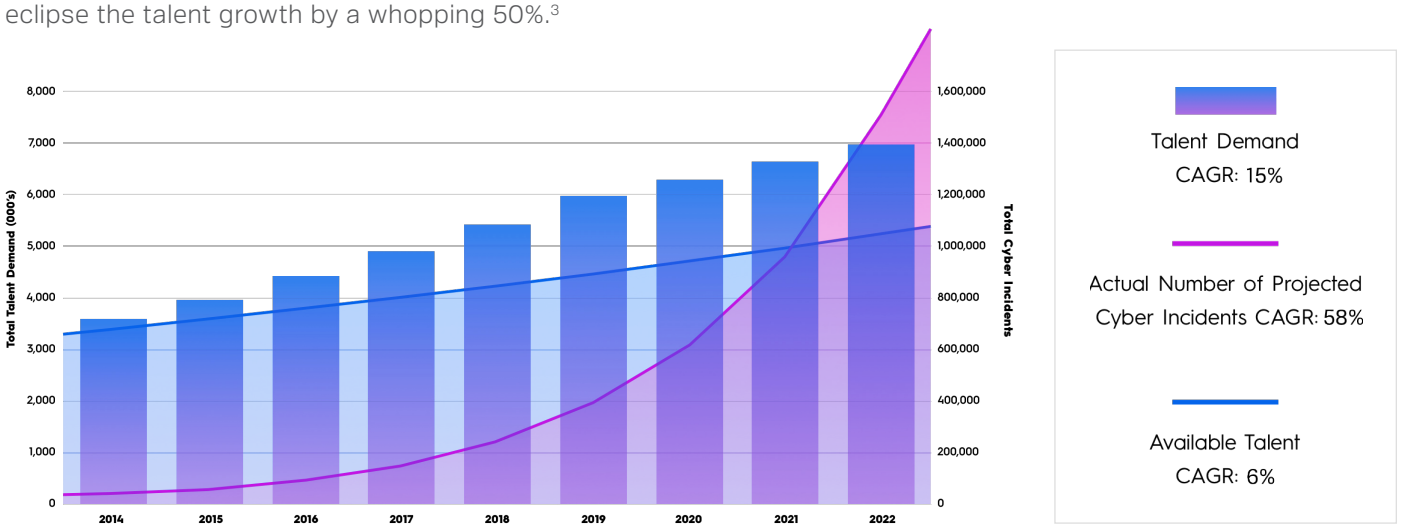
And according to a recent survey conducted:[2]

- **77%** of CISOs are utilizing regular penetration testing
- **66%** of CISOs have an incident response process
- **62%** are using application vulnerability scanners
- **57%** have application security training in place

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%.[3]



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

[3] Global State of Information Security Survey 2016, PWC and Cybersecurity Jobs Report 2018-2021, Cybersecurity Ventures, 2017

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:

2 Testers

X

40 Hours

=

80

80 Hours of Work

Synack Crowdsourced Test:

50–80 Testers

X

5–10 Hours

=

200+

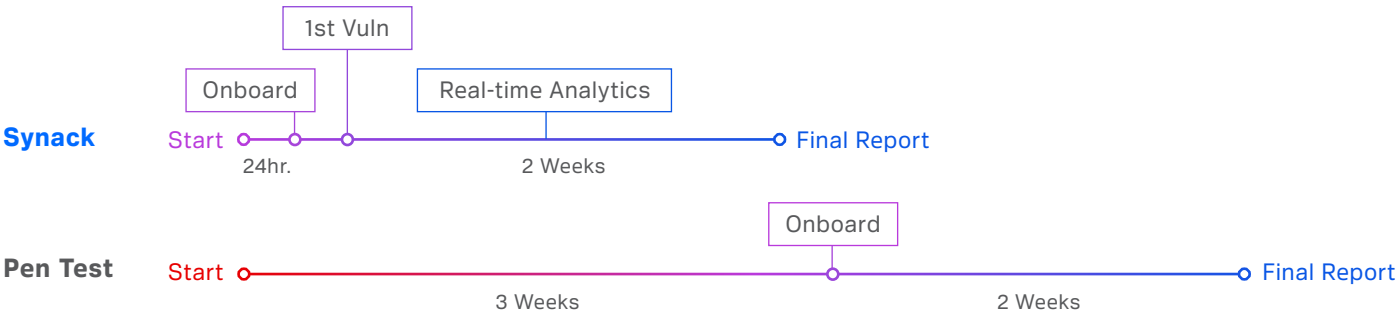
200+ Hours of Work

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

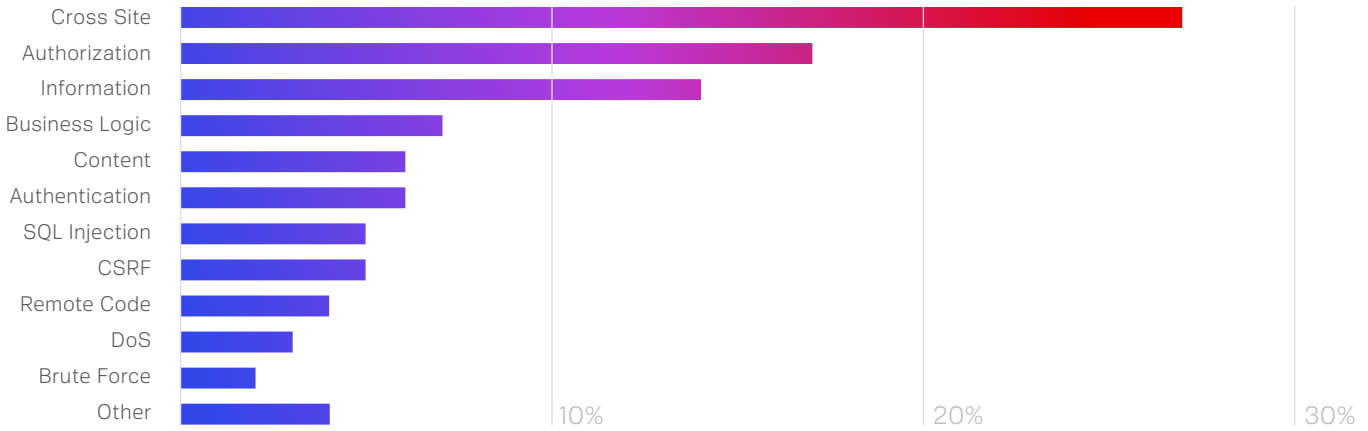
Basic Pen Test vs. Synack Crowdsourced Test



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:



> ***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 U.S. 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.[9]

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.[10]

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.[11]

[9] The Hacker-Powered Security Report, HackerOne

[10] Aggregated Bugcrowd, HackerOne data

[11] 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

Scanners

- Basic Coverage for Unknown Vulns

Penetration Tests

- Compliance

Responsible Disclosure / Open Bug Bounty

- **Basic Coverage for Unknown Vulns**

Invite-Only Bug Bounty

- Adversarial Testing Coverage
- **Selected Crowd**

Managed Vulnerability Discovery

- Adversarial Testing Coverage
- Highly Vetted Crowd
- **Vuln Triage & Full Program Management**
- **Auditable Testing Traffic**
- **Testing Coverage Analytics**

Managed Crowdsourced Penetration Testing

- Compliance
- Adversarial Testing Coverage
- Vuln Triage & Full Program Management
- Highly Vetted Crowd
- Auditable Testing Traffic
- Testing Coverage Analytics
- **Security Scoring**
- **Ongoing Risk Reduction**

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

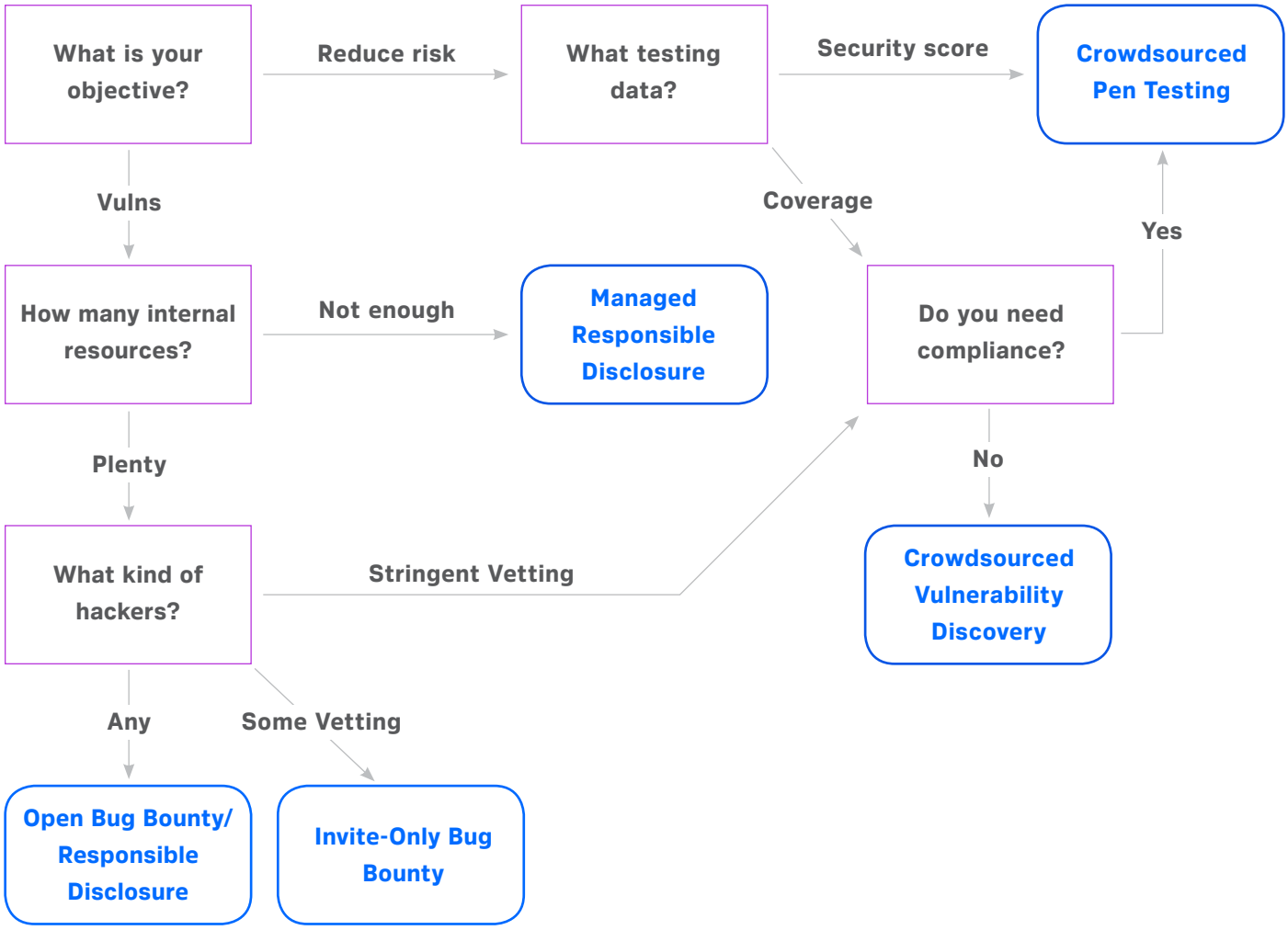
Hacker-Powered
Activate adversarial-based testing in order to uncover and fix vulnerabilities before present-day criminal hackers can exploit you.

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.

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

> "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

Better Success Metrics for Crowdsourced Programs

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.

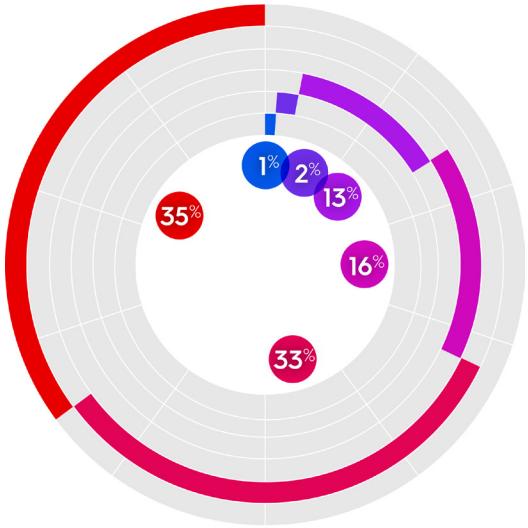
What is a High Severity Vulnerability?

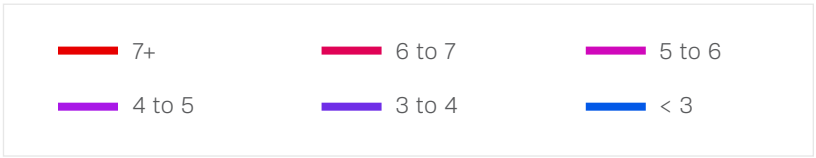
Exploitation could result in elevated privileges, significant data loss, and/or downtime.

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 starting 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

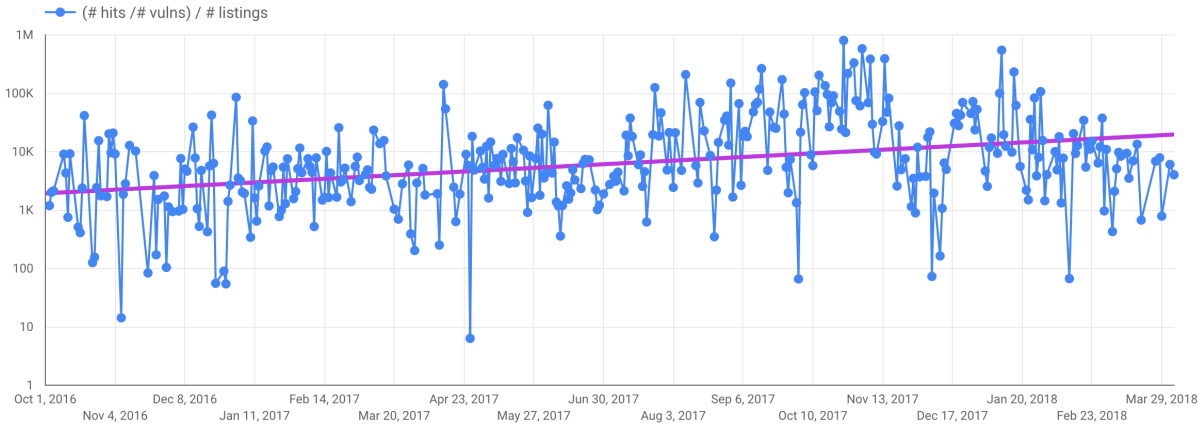
Hits/Vulns

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 to 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:

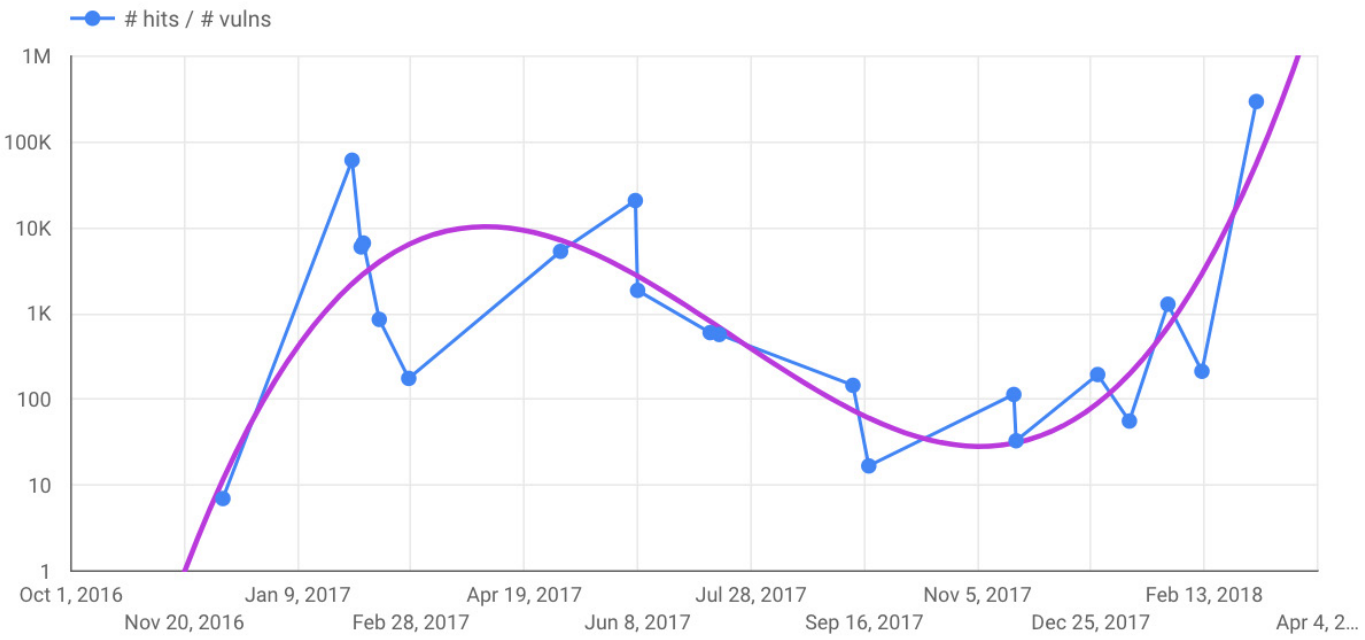


In January of 2017, the client assets of Synack continuous or renewing customers took an average of 8,565 hits to produce a vulnerability.

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.

Customer Snapshot

Industry: Technology **Application Type:** Web



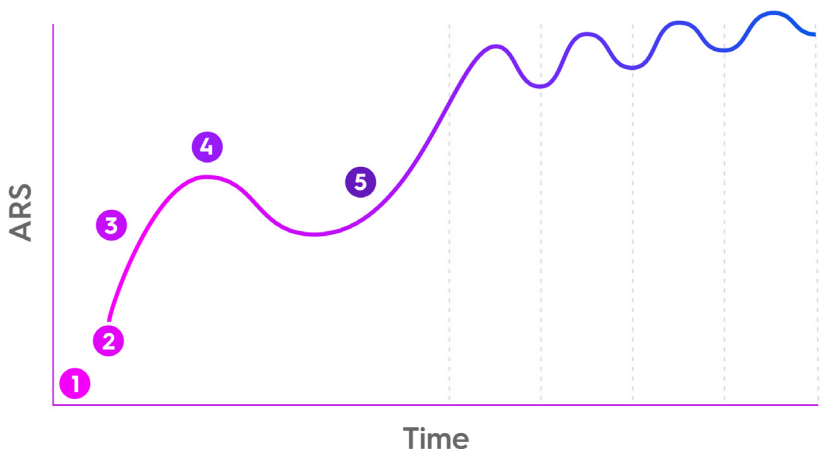
- The customer started testing with Synack in November of 2016 and Synack Red Team researchers began probing the assets in scope to discover previously unknown vulnerabilities. At the beginning of the project, just a few hits by a researcher would turn into a valid vulnerability.
- Over the course of 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

Attacker Resistance Score = **Attacker Cost** + **Severity of Findings** + **Hacker Skill** + **Remediation Efficiency**



Conceptual sample of ARS over time

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?

Basic

Penetration Tests

- **Compliance**

Hacker-Powered

Responsible Disclosure / Open Bug Bounty

- **Basic Coverage for Unknown Vulns**

Invite-Only Bug Bounty

- Adversarial Testing Coverage
- **Selected Crowd**

Hacker-Powered with Intelligence

Managed Vulnerability Discovery

- Adversarial Testing Coverage
- Highly Vetted Crowd
- **Vuln Triage & Full Program Management**
- **Auditable Testing Traffic**
- **Testing Coverage Analytics**

Managed Crowdsourced Penetration Testing

- Compliance
- Adversarial Testing Coverage
- Vuln Triage & Full Program Management
- Highly Vetted Crowd
- Auditable Testing Traffic
- Testing Coverage Analytics
- **Security Scoring**
- **Ongoing Risk Reduction**

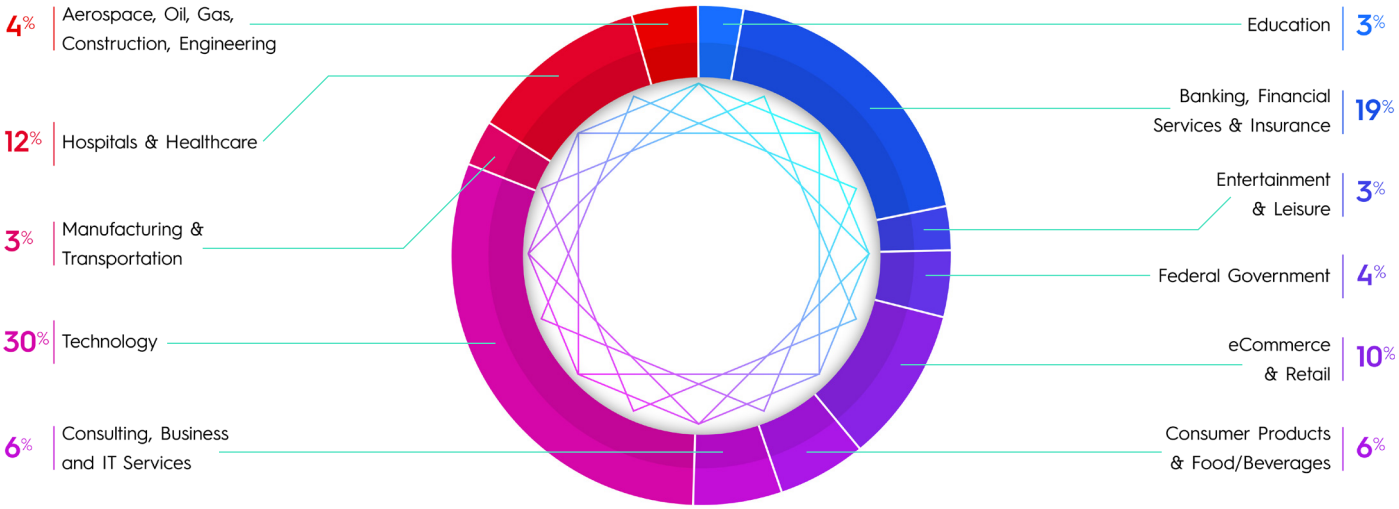
Is Your Crowdsourced Security Testing Successful?

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

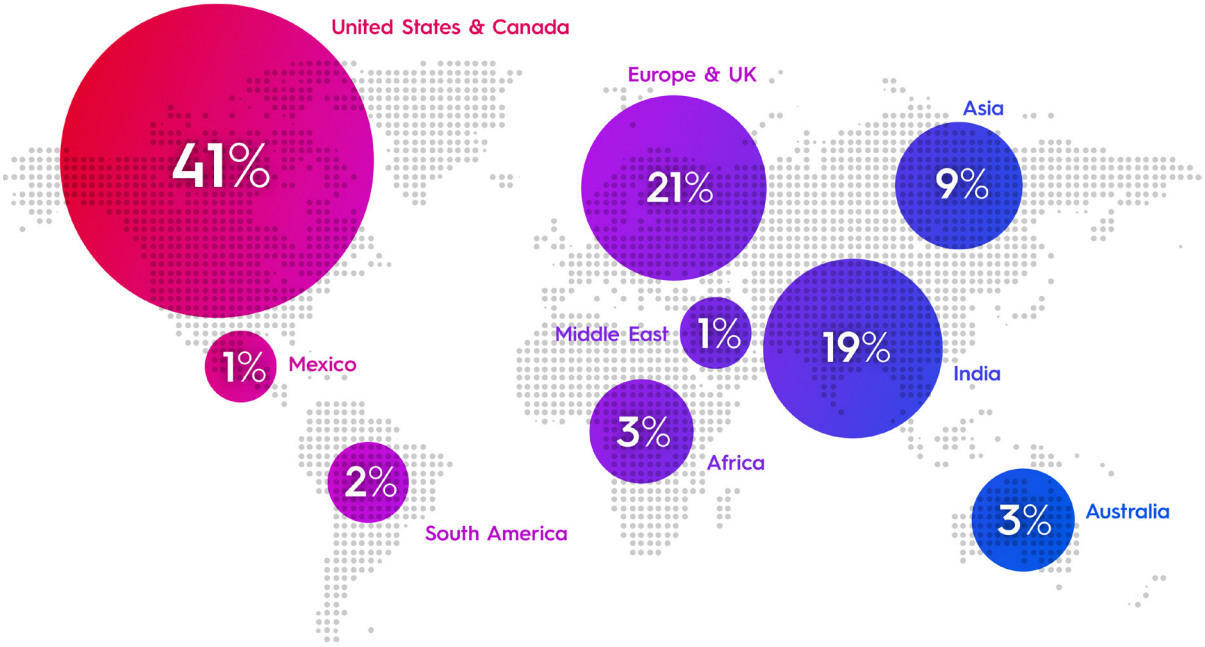
What does Synack Protect?

- **>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 U.S. Taxpayer** via the IRS
- **U.S. DoD** Classified Assets

Who Trusts Synack?



Where in the World are the Synack Hackers?



Crowdsourced Security Testing Is the New Testing Standard in Government

From the Hill to 1600 Pennsylvania to state and local governments around the country, government organizations are buzzing about crowdsourced security. As traditional methods of security testing fall short in identifying critical vulnerabilities that cause debilitating damage, agencies, legislators, and executives have been looking for a more aggressive approach to their defenses.

Crowdsourced security testing increased 9x in 2017, received seven mentions in legislation in just six months, and has captivated the attention of the White House. So what does the buzz around "crowdsourced security," "bug bounty," and "Hack the X" acts mean for you?

In general, this means more security testing talent and skill available to you to find vulnerabilities before the adversary can. It could also mean more efficiency for your team and mitigated risk of a breach - but not all crowdsourced security programs are created equal. To maximize the efficiency and effectiveness from your crowdsourced security program, you need to conduct your due diligence on what you're signing up for. Below is a primer on crowdsourced security for government and the key questions you should be asking to make sure you are getting the most value for your money.

Timeline: Key Events in Crowdsourced Security's Path to Establishment

Government innovators have disrupted how the government thinks about penetration testing and have paved the way for crowdsourced security testing to become the new standard.

APR 18, 2016	**Hack the Pentagon** pilot kicks off
JUN 02, 2016	**Internal Revenue Service** launches their continuous crowdsourced security program to protect U.S. taxpayers
OCT 20, 2016	**Hack the Pentagon** program launches, engaging the **U.S. Army, U.S. Air Force, Defense Information Systems Agency**, and other private DoD agencies.
MAY 25, 2017	**Hack DHS Act** calls for a crowdsourced security program to protect DHS assets
JUNE 07, 2017	**National Defense Authorization Act** proposes scaling crowdsourcing security across the DoD
AUG 01, 2017	**IoT Cybersecurity Improvement Act of 2017** suggests a vulnerability disclosure program for IoT contractors
AUG 18, 2017	**Intelligence Authorization Act for FY2018** requests a plan for crowdsourced security across the intelligence community
AUG 30, 2017	**Report to the President on Federal IT Modernization** recommends use of crowdsourced security for more rigorous security testing
SEP 28, 2017	**Treasury Innovation Act** proposes adopting crowdsourcing security at the Department of Treasury
OCT 31, 2017	**Securing America's Voting Equipment Act** suggests crowdsourced security to help secure election systems
APR 5, 2018	**Hack Your State Department Act** calls for a crowdsourced security program to protect State Department assets

Early crowdsourced security programs at the Department of Defense (DoD) and Internal Revenue Service (IRS) have been followed by a wave of programs at other agencies, including the General Services Administration, Centers for Disease Control and Prevention, and other private agencies.

Why Crowdsourced Security Testing?

1. The U.S. Government's growing attack surface means traditional security testing solutions simply can't scale.

The U.S. government is charged with a paramount task: protecting our nation's critical infrastructure. These are the physical and virtual assets that are vital to our country's security[1].

A couple of decades back, this definition was limited to eight traditional infrastructures, including telecommunications, electrical power systems, and transportation[2].

But as technology has advanced, and the adversary has become more sophisticated, our attack surface has grown, and the threat has evolved. More and more physical assets are coming online, and digital assets are multiplying. By 2020, we expect to see over 20 billion devices connected to the internet[3].

Today, the government's list of critical infrastructure sectors has surged from eight to sixteen. New additions include nuclear reactors, healthcare, critical manufacturing, and government facilities, under which election systems were most recently designated[4].

Our security teams are strapped for the time, resources, and talent to scale to the magnitude of our attack surface and threat.

> "Cleaning up all the code in the weapons systems being produced for DOD would cost hundreds of billions of dollars alone."
>
> —Richard Stiennon, Chief Research Analyst, IT-Harvest

2. Spending more money on the same solutions isn't helping agencies successfully defend against attacks.

The FY19 President's Budget includes $14.98B for cyber activities[5], a four percent increase above FY18 estimated levels (not including classified budget lines). However, historically speaking, increasing the cyber budget hasn't resulted in fewer breaches—in fact, it's been the opposite[6]. While federal cyber investments increased 162% from 2006 to 2018, the number of federal cyber incidents were increasing at a rate of 1512% from 2006 to 2016. Traditional models of cyber defense are failing to defend against modern cyber threats, which is driving lawmakers and government agencies to explore innovative solutions.

[1] Department of Homeland Security website, https://www.dhs.gov/critical-infrastructure-sectors

[2] Executive Order EO 13010 Critical Infrastructure Protection, July 15, 1996

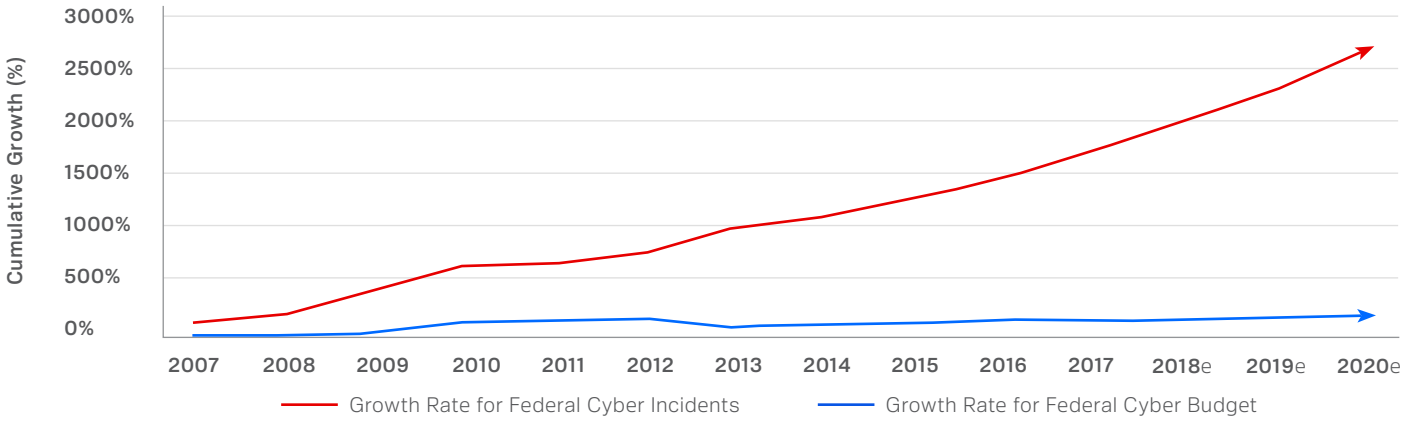
[3] Gartner, https://www.gartner.com/newsroom/id/3598917

[4] Presidential Policy Directive - Critical Infrastructure Security and Resilience, February 12, 2013

[5] Fifth Doman, How much does federal government spend on cybersecurity? https://www.fifthdomain.com/civilian/2017/09/01/how-much-does-federal-government-spend-on-cybersecurity/

[6] Synack, Dear President Trump: We ran the numbers, you've inherited a cyber problem, https://www.synack.com/2017/01/20/trump-inheriting-cyber-problem/

A Widening Gap: Federal Cyber Incidents vs. Federal Cyber Budget



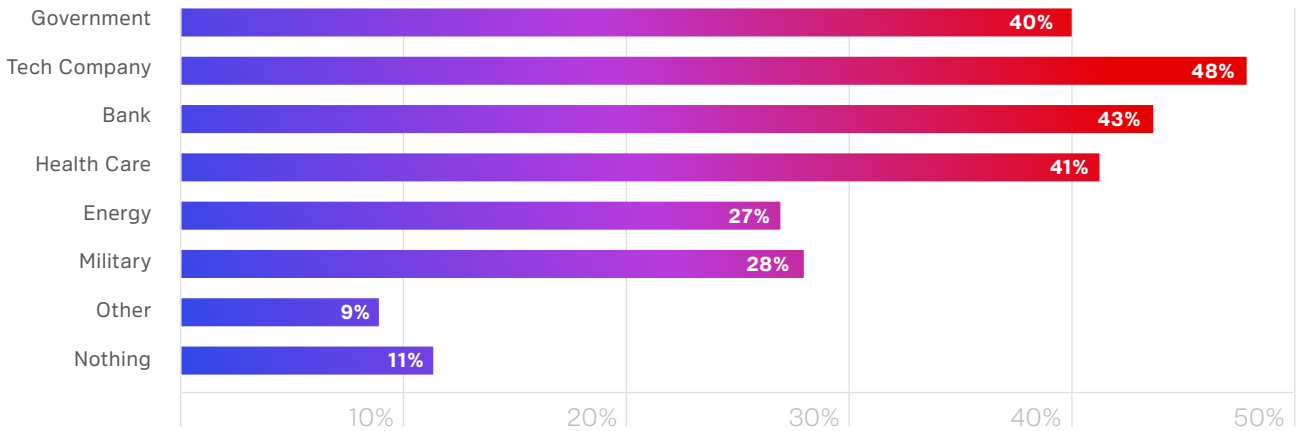
Sources: GAO Report on Information Security, FISMA Annual Report to Congress, Morgan Stanley Blue Paper on Cybersecurity, Synack Analysis.

3) There isn't enough cyber talent in the U.S. government to combat growing threats.

The 2016 report by the Commission on Enhancing National Cybersecurity identified the need to train 100,000 cyber specialists by 2020[7]. However, government agencies are struggling to attract, retain and develop talent: several hundred NSA employees have left over the last three years[8]; none of the original 127 Air Force cyber officers returned to the cyber mission after their first tour in 2017[9], and up to 10,000 cybersecurity positions currently remain unfilled across government[10].

The talent gap isn't just felt in government; it affects the public and private sector alike. According to Cybersecurity Ventures, the talent gap will reach 3.5 million by 2021[11]. As organizations across industries are trying to attract cyber talent from a small pool, competition for talent intensifies.

If you were a cyber pro, what type of organization would you want to protect?



Raytheon, Securing Our Future: Closing the Cybersecurity Talent Gap, 2016

[7] Report on Securing and Growing the Digital Economy, Commission on Enhancing National Cybersecurity, https://www.nist.gov/cybercommission

[8] NSA's top talent is leaving because of low pay, slumping morale and unpopular reorganization, Washington Post, https://www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html

[9] Air Force 'chronically undermanned' in cyber, Fifth Domain, https://www.fifthdomain.com/home/2017/07/05/air-force-chronically-undermanned-in-cyber/

[10] DHS cybersecurity mission facing real challenges, Cyberscoop, https://www.cyberscoop.com/dhs-cybersecurity-hearing-chris-krebs-jeanette-manfre/

[11] Cybersecurity Jobs Report 2018-2021, Cybersecurity Ventures, https://cybersecurityventures.com/jobs/

Industries like technology, banking, and healthcare are more popular than government among young cyber talent, according to a recent Raytheon report. While an entry-level civilian professional in the government earns around $50,000 per year, recruiting websites suggest entry level cyber security salaries average over $67,000 in the private sector. And as millennials in the workforce increasingly want to believe in the mission of their employer, sometimes government isn't favored in their own personal career mission.

Crowdsourcing has become the go-to solution of federal agencies to augment their teams with top talent that is motivated to serve their country AND is paid competitively by independent crowdsourced security platforms.

Government Crowdsourced Security Snapshot: Hack the Pentagon Pilot

Early pioneers within the DoD piloted crowdsourced security testing with the Hack the Pentagon program. They wanted to test and demonstrate that crowdsourced security testing was a more effective, efficient approach to security testing. The first target? The DoD's externally-facing webpage. The program began with an invite-only bug bounty model to probe the site. Initially, the program received some skepticism:

> "When we started [the DoD bug bounty], we weren't that inclined."
>
> —Essye Miller, Principal Deputy, DoD CIO[13]

The concept of actually inviting external security researchers to "hack" the Pentagon was new to the Defense Department. Nevertheless, the pilot turned out to be a success and exceeded the Pentagon's expectations of engaging a large number of security researchers (>1,400 registered to participate) to find as many vulnerabilities as possible (>1,180 submitted)[14].

Government Crowdsourced Security Snapshot: Hack the Pentagon - A Higher-Stakes Program

The Defense Department then pushed the model a step further to see if crowdsourced security could be used to test its most sensitive systems. Now the stakes were higher. This time, the DoD used Synack's private, managed crowdsourced vulnerability discovery approach to test their sensitive internal assets. Rather than aiming to find large volumes of vulnerabilities with a wide open crowd, the DoD opted to utilize only an elite, controlled crowd of the world's top security researchers and a secure crowdsourced penetration testing platform to augment internal security teams, find critical vulnerabilities, and learn from the intelligence gathered by these security researchers. This was the first time that the DoD had employed a crowdsourced model to engage ethical hackers to protect critical systems.

The Goal: Mimic realistic cyber threats in order to assess how hardened their critical systems were to attack from nation states, using a safe, easily controlled model.

[13] Essye Miller, Security Fireside Chat, San Francisco CyberTalks, April 2018

[14] Carter Announces 'Hack the Pentagon' Program Results, U.S. Department of Defense, https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/

What We Achieved:

- 100 highly vetted security researchers engaged
- >7,000 hours of active testing time on target
- 5 sensitive systems over the course of 4 projects
  - Sensitive systems included a file transfer mechanism (used for sending sensitive information across networks).

When crowdsourced security testing of the file transfer mechanism began, the DoD expected to find nothing and told remediation teams to stand down for one week. In fact, it took only four hours to find a critical vulnerability and less than 24 hours to triage it. Synack worked with DoD teams to provide remediation guidance, and after the vulnerability was fixed, the same researcher who discovered it verified that the patch was effective within 72 hours.

The ROI: In the words of the Department of Defense:

> **"Our private vulnerability assessment programs have a proven track record of eliciting quick, impactful results by harnessing the depth and breadth of security talent across the globe. Their skill-sets and contributions have been critical in our ability to secure the assets responsible for daily operations across the Department, whether that be military logistics systems or applications that handle sensitive data for millions of people. The unique insights the hacker community brings are so invaluable and necessary to maintain a technical edge and avoid disastrous consequences."**
> ***—Reina Staley, Co-Founder & Hack the Pentagon Lead, Defense Digital Service***

Broader Benefits: Beyond the ROI of securing sensitive assets, the program had broader benefits for the Pentagon:

1. **Force Augmentation:** DoD is home to an incredible population of technical talent, but the magnitude of digital assets owned by the DoD vastly out-numbers them. Rather than crippling from the weight within, the Hack the Pentagon program allows the Department to augment internal teams with external expertise from hundreds of security experts across the country and the globe.
2. **Avenue to Talent:** The Hack the Pentagon program provided a pathway for security researchers with a desire to serve to help secure their nation's critical assets. It also provided the Defense Department an opportunity to build relationships with this talented "cyber militia."
3. **Strengthening Relationships with Allies:** DoD security is not just a U.S. interest - a shared responsibility for common defense among our international partners is key. Expanding upon U.S. alliances and leveraging the talent of U.S. foreign counterparts, particularly within our FVEY and NATO community, has proven to be a continued success of this program and in building/strengthening relationships with the international security community.

DoD Lessons Learned:

1. Bring in third party security to ensure a fresh perspective and new ideas that uncover previously unknown or unconsidered opportunities that could be exploited. Teams or organizations inevitably become desensitized to flaws in systems they have daily interactions with.
2. Test earlier in the development cycle to catch vulnerabilities before they are fielded. DoD is forging ahead and incorporating crowdsourced hacking for systems still in development.
3. Train defensive teams by bringing them onto the crowdsourced security platform. Hacking does not follow a structured playbook; running offensive hacking challenges in a controlled environment keeps our defensive capabilities sharp.
4. Simulate environments to create testing opportunities. The ability to simulate classified systems in simulated, unclassified environments allows for greater opportunity for trusted researchers to contribute their skillset to secure the nation's more mission critical systems.
5. Increase attacker resistance by working with ethical hackers to harden against attack and reduce the number of vulnerabilities found over time.
6. Gain efficiency through crowdsourcing when you choose a solution that provides stringent vetting, tracking, triage and analytics.

Through the success of the Hack the Pentagon program, skeptics saw the potential for the model:

> "I've become a big fan. It tells us real-time where we have issues. It also drives us to what's most important, what we need to address, and to engage industry... Helps us see ourselves better."
>
> —Essye Miller, Principal Deputy, DoD CIO[15]

[15] Essye Miller, Security Fireside Chat, San Francisco CyberTalks, April 2018

Hacker-Powered vs Hacker-Powered with Intelligence

Hack the Pentagon has highlighted key differences in crowdsourced security models and the associated differences in potential applications:

	Hacker-Powered: INVITE-ONLY BUG BOUNTY	Hacker-Powered with Intelligence: MANAGED VULNERABILITY DISCOVERY
Security Researchers		
Vetting	Invitation Only	Rigorous 5-step vetting process including background checks, <10% acceptance rate.
Researcher backgrounds, skill level, trust	Unknown	Known—vetting aligned with federal background investigation criteria.
Vendor liability for researchers	None	100% vendor responsibility
Extortion Threats	Unprotected	Fully Protected
Vulnerability Leaks to Public	Unprotected	Fully Protected
Process		
Testing Coverage	Unknown testing coverage reach	As scoped—attack surface will be fully tested.
Triaging Submitted Vulnerability Reports	Handled by internal security team or an addendum to the contract.	Included. Handled by vendor.
Responding to hacker payments and demands	Handled by security team	Included. Handled by vendor.
Technology		
Automated Scanning	None	Provided
Researcher Traffic Tracking	None—researchers can remain in networks for weeks after test.	Monitored; stopping possible at any time. Testing gateway torn down immediately after test conclusion
Coverage Data and Analytics	None	Included
Performance Score	None	Included
Applications		
	Certain public-facing assets. Non-critical assets.	External websites, e.g., taxpayer systems Internal assets, e.g., pre-production systems, enterprise information systems, logistics systems

More Agencies are Going Crowdsourced

Invite-Only Bug Bounty Approach:

U.S. Army

U.S. Air Force

General Services Administration

Managed Vulnerability Discovery Approach:

U.S. Army

U.S. Air Force

Internal Revenue Service

Defense Information Systems Agency

Centers for Disease Control and Prevention

Other Private Agencies

Agency adoption of the Managed Vulnerability Discovery Approach grew 9x in 2017!

> "The efficiency, insights, and visibility that we gained through managed vulnerability discovery would not have been possible through a bug bounty program."
>
> —Government Crowdsourced Security User

What Does Success Look Like for Your Agency?

A crowdsourced security program should increase Attacker Resistance. This means:

Increased efficiency

- Do you have more testing coverage across your attack surface?
- Are you able to deploy tests rapidly?
- Is your testing solution unburdening your security team and accelerating their activities?
- Are insights making remediation easier than it was before?

Increased effectiveness

- Are you finding issues earlier?
- Are you finding vulnerabilities you didn't find before?
- Are you better equipped to prioritize your vulnerabilities for remediation?

Increased insight

- Do you have a full audit trail of testing activity?
- Are you seeing your results in real-time?
- Are you identifying which of your assets are more vulnerable to attack, from a researcher's perspective?
- Do you have metrics with which you can benchmark across assets or against other organizations?

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.

Synack's ROI for Taxpayers

Synack Crowdsourced Security Testing has the potential to save at least $229M in taxpayer value annually:

- **Federal Cyber Budget FY18:** $14.4B
- **Synack Estimate of Federal Security Testing Budget:** .03 * $14.4B = $432M
  **Industry reports from Gartner and IDC estimate that 3-5% of an organization's security budget is allocated to security testing.*
- **ROI Estimate of Synack Pen Test:** 1.53 * $432M = $661M value
  *A comparison of value delivered through a Synack crowdsourced security test versus a traditional two-week, 80-hour penetration test estimates 53% more ROI from Synack[16].
- **Potential Taxpayer Dollars Saved Using Synack Crowdsourced Security Testing:** $661M - $432M = $229M saved

Questions about the crowdsourced security testing options and what's best for your team? Contact us and a Synack team member would love to help.

[16] The Synack Value, Synack, https://www.synack.com/2017/08/02/synack-pen-test-means-higher-roi/

Synack, Inc.

855.796.2251 | www.synack.com | government@synack.com