Bridging the talent gap with on-demand, skilled researchers

Diverse perspectives and creativity that outmatch the adversary

When hiring a security professional, there is an excess of skills and qualifications that you might consider including in the job description. For example, in 2021, 32% of hiring managers sought out individuals with certifications, 25% sought out advanced cybersecurity skills and 65% sought out previous relevant IT or cybersecurity work experience[1]. You need someone with the right experience to match your company's specific suite of security tools and initiatives. In one report, organizations were found to be using on average over 75 security tools[2].

To achieve that level of breadth, cybersecurity professionals are educating themselves on a variety of specialities. In 2021, 40% sought to develop their cloud security expertise, while 22% focused on DevSecOps and 22% trained on social engineering, among other specializations[1].

With all of these requirements on the hiring end and the endless combination of specializations from security professionals, finding the best-fitting team member to solve your security objectives is challenging.

75+
security tools in an organization[2]

32%
hiring managers seek candidates with cyber certifications[1]

50%
of candidates lack cloud expertise[1]

A candidate today has more tools and technologies to learn than ever before. There is an overwhelming number of possibilities both for candidates in terms of what they want to learn, and for hiring managers in terms of what they seek in a candidate.

[1] (ISC)2 2021 Workforce Study
[2] Panaseer Security leaders peer report

Stop the search — your next candidate is already here

With continuous and on-demand access to a diverse community of ethical hackers, you can augment the capabilities of your existing security team and stop searching for that "unicorn" candidate.

With talent from around the globe and over 1500 researchers on-platform, the diversity of skills and backgrounds provide for effective penetration testing and a variety of on-demand security tasks to help you achieve your overall security objectives.

Technical and skill diversity in the Synack Red Team

The following table represents data from SRT researchers on their title, certifications and other characteristics. This is just a sample of the diverse skills and perspectives found in the community.

PROFESSIONAL TITLES	Software Developer	Penetration Tester/ Red Teamer	Security Analyst	Cryptanalysis	Network Administrator	Cyber Incident Responder
RECON SKILLS	Software Kill Chain	OSINT	Change Detection	Digital Footprinting	Dark Web Recon	Social Media Analysis
TECHNOLOGIES	Cloud — Azure, GCP, AWS	Docker and Containers	Kubernetes	OSINT Tools	Linux Environments	PHP Environments
ASSET TYPES	Web App	Host/Infrastructure	Mobile	Cloud	API	IoT
VULNERABILITY EXPERTISE	Business Logic	SQL injection	Remote Code Execution (RCE)	Cross Site Request Forgery (XSRF)	Session Authentication	Information Disclosure
OFFENSIVE SECURITY SKILLS	Reverse Engineering	Fuzzing	Tool Development	Remediation Guidance	Cryptography and Cryptanalysis	Web Application Testing
CERTIFICATIONS	CISSP	Certified Ethical Hacker (CEH)	PNPT	Offensive Security Certified Professional (OSCP)	eMAPT	OSWE
LANGUAGES	English	Spanish	Italian	Portuguese	German	Hindi

The value that our SRT members add to our premier security testing goes beyond their impressive technical backgrounds. Members, spanning generations, represent over 80 countries, hundreds of educational institutions and diverse life experiences which brought them to hacking.

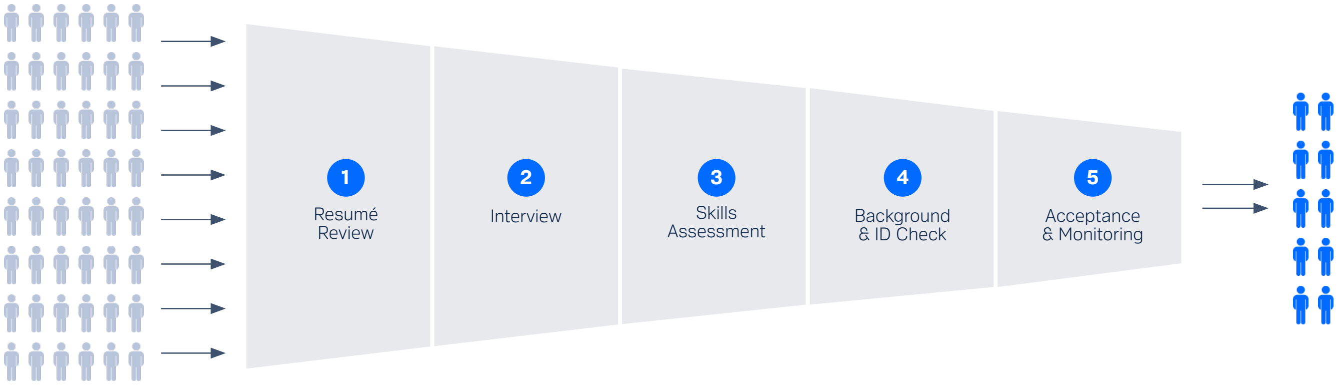
The community works across multiple industries, business cultures and disciplines within cybersecurity. Just as millions of different antibody types fend off disease in humans, the SRT community finds security holes with the same expansive, exploratory breadth for an organization's attack surface.

You need researchers you can trust

Often, organizations take pause at the thought of an anonymous cohort of crowdsourced researchers and ethical hackers being introduced into their environment. The reality is that any organization who has public-facing assets *already* has hackers poking away at their environment. For that reason, having someone trustworthy test your security from an adversarial perspective is essential.

Building a trustworthy community with rigorous vetting

At Synack, we take great care to ensure that our crowdsourced community of ethical hackers is made up of the most elite global talent that you can trust. The selected SRT members become better vulnerability hunters as they grow and understand how organizations want to be tested, how to most clearly present findings and how to communicate on remediation. Additionally, the culture of the SRT is one of mentorship; members are happy to help each other learn, which translates to better performance for an organization's pentesting and security tasks.

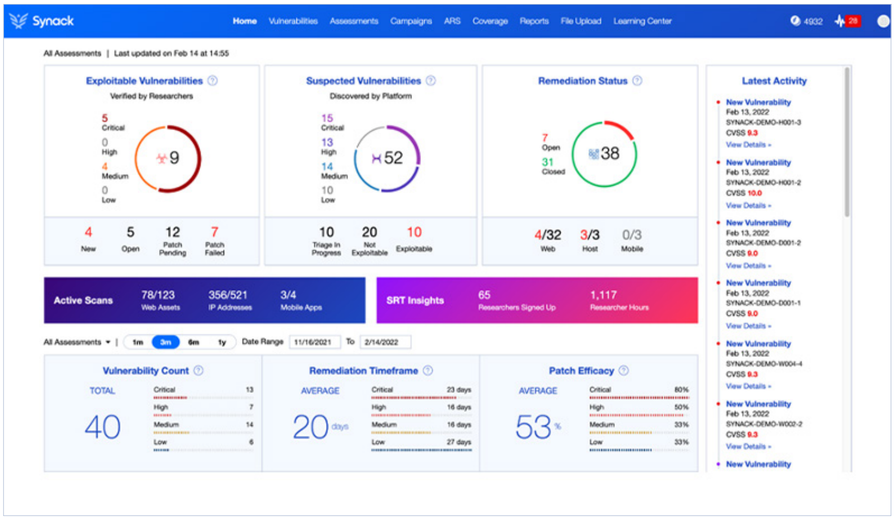


Applicants go through a series of rigorous steps when applying to be a part of the Synack Red Team community.

Bridge the gap today through the Synack Platform

The Synack Platform provides access to the Synack Red Team (SRT), a community of elite ethical hacking talent from around the world. Each researcher is vetted through a rigorous, five-step process and brings a valuable adversarial perspective to your attack surface.

Request a demo today or reach out to your Synack representative to get started with Synack testing today, and bridge the cyber talent gap with on-demand access to Synack Red Team researchers.


Synack
Home
Vulnerabilities
Assessments
Campaigns
ARS
Coverage
Reports
File Upload
Learning Center
4932
28
All Assessments | Last updated on Feb 14 at 14:55
Exploitable Vulnerabilities
Verified by Researchers
5 Critical
0 High
4 Medium
0 Low
9
4 New
5 Open
12 Patch Pending
7 Patch Failed
Suspected Vulnerabilities
Discovered by Platform
15 Critical
13 High
14 Medium
10 Low
52
10 Triage In Progress
20 Not Exploitable
10 Exploitable
Remediation Status
7 Open
31 Closed
38
4/32 Web
3/3 Host
0/3 Mobile
Latest Activity
New Vulnerability
Feb 13, 2022
SYNACK-DEMO-H001-3
CVSS 9.3
View Details »
New Vulnerability
Feb 13, 2022
SYNACK-DEMO-H001-2
CVSS 10.0
View Details »
New Vulnerability
Feb 13, 2022
SYNACK-DEMO-D001-2
CVSS 9.0
View Details »
New Vulnerability
Feb 13, 2022
SYNACK-DEMO-D001-1
CVSS 9.0
View Details »
New Vulnerability
Feb 13, 2022
SYNACK-DEMO-W004-4
CVSS 9.3
View Details »
New Vulnerability
Feb 13, 2022
SYNACK-DEMO-W002-2
CVSS 9.3
View Details »
New Vulnerability
Active Scans
78/123 Web Assets
356/521 IP Addresses
3/4 Mobile Apps
SRT Insights
65 Researchers Signed Up
1,117 Researcher Hours
All Assessments
1m
3m
6m
1y
Date Range 11/16/2021 To 2/14/2022
Vulnerability Count
TOTAL 40
Critical 13
High 7
Medium 14
Low 6
Remediation Timeframe
AVERAGE 20 days
Critical 23 days
High 16 days
Medium 16 days
Low 27 days
Patch Efficacy
AVERAGE 53 %
Critical 80%
High 50%
Medium 33%
Low 33%