Synack

WHITE PAPER

SOLVING THE CYBER TALENT GAP WITH DIVERSE EXPERTISE

By Kim Crawley

Executive Summary

The cyber talent gap is making it hard to find individuals with the right skills to protect your attack surface. And there are more technologies, skills and certifications than ever before, presenting challenges to both candidates and hiring managers.

The best security teams not only have the right skills, but a *diversity* of skills, certifications, backgrounds and even life experiences. To solve for the talent shortage and skills gap, on-demand security talent must be available to augment your internal teams.

The Power of Collective Intelligence

Criminal hackers are creative and persistent, so pentesters and security professionals must be, too. However, no matter how experienced a practitioner is, how many certifications they have, or how many tools they know how to use, there will always be exploits they haven't considered.

That's why getting researchers with a diversity of skills and perspectives to defend your attack surface is critical to finding every vulnerability that matters.

Naturally, the more eyes on target, the more variety there will be in skills, certifications and tactics.

In the midst of the cyber talent gap, however, hiring a multitude of skilled professionals with just the right combination of qualifications to truly protect your organization's attack surface is a pipe dream.

Top security practitioners are in short supply and salaries are highly competitive. For hiring managers, it's also dizzying to sift through the myriad of skills, backgrounds and technical knowledge to ensure a job seeker is really the right fit. Finding that perfect candidate with just the right skills is hard enough, let alone a team of professionals with a diversity of skills, certifications and experiences. In one 2022 report, 60% of organizations struggled to hire talent, and 78% found it hard to find the right certifications. Furthermore, 70% agreed that diversifying their teams was important, and a challenge.

Organizations must also reconcile the variety of skills with actual priorities. Hiring a full-time professional to perform specific, infrequent tasks isn't necessarily a good use of your department's budget. At the same time, the tasks that require those skills are still essential.

That's why Synack provides on-demand, global security talent — the Synack Red Team (SRT) — to protect your attack surface. The SRT members' breadth of skills and qualifications is exceptional, ensuring highly creative engagements that outmatch the most creative adversaries.

Bridging the Talent Gap Today with On-Demand Talent

The SRT is a crowdsourced community of over 1,500 elite ethical hackers from all over the world. Their diversity is evident not only in technical skills, but in their professional titles, certifications, languages and cultural backgrounds.

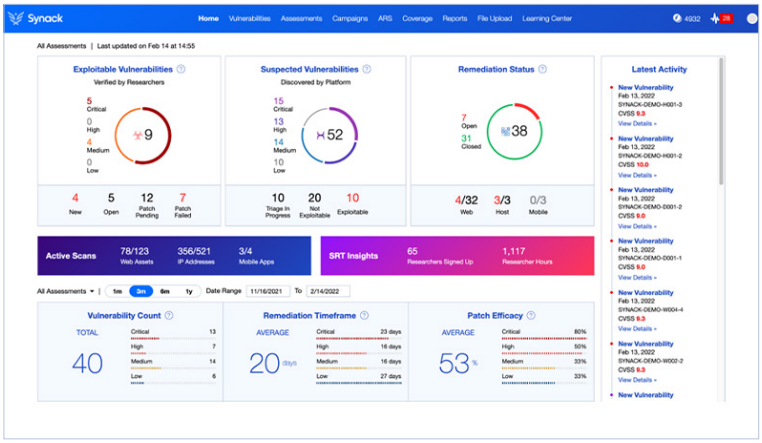
With the SRT, you can stop the search for full-time candidates and reap the benefits of on-demand talent augmentation.

The following table lists only a subset of the diversity found within the Synack Red Team:

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 Profes- sional (OSCP)	eMAPT	OSWE
LANGUAGES	English	Spanish	Italian	Portuguese	German	Hindi

With such a variety of backgrounds, the SRT community is the ideal force to power high-performance pentesting, in addition to executing on-demand security tasks for your organization, such as cloud testing, OWASP Top 10 checks, threat modeling and more.

The Synack Platform facilitates access to on-demand SRT talent. Through our platform, you can communicate about vulnerability findings directly with researchers, request patch guidance and verification, activate additional testing and more. Synack organizes researchers so they work efficiently, minimizing duplication of each others' findings and without unnecessary traffic on your systems.



Streamline and automate your red team pentesting engagements with the click of a button. It's simple, yet dynamic, when you deploy Synack's Platform with the power of our Synack Red Team human intelligence. We interviewed several SRT members to demonstrate how they're able to take on whatever testing or security task is thrown their way.

Ryan Rutan, SRT Community Manager

No one has the luxury of choosing where cyber threats will emerge, who will attack them or when they will get attacked. Security through diversity is the best way to cover as many threats with the limited resources and time you have available. This is why we've implemented two programs to promote collaboration and open the pool of possible SRT members.

The Artemis Red Team, a sub-community inside the SRT, is designed as a space for skilled women working in offensive security to flourish and network with peers while gaining invaluable industry experience. We also leveraged our industry-leading platform and strong community roots to cultivate a one-of-a-kind paid mentorship program. Ethical hackers from around the world flock to the SRT for a chance to get paid teaching or learn from expert hackers in a tight-knit cyber community.

Meet Some SRT Members

After talking with several SRT members, we found that each member has a unique combination of skills and advanced expertise to contribute. These researchers are the best in the business, and they were proud to discuss the accomplishments they've achieved with the SRT. Here are excerpts from our interviews with five SRT members.

Malcolm Stagg

Synack handle: malcolmst

Skills

General source code review, Windows Server exploitation, bug hunting, Linux vulnerabilities, hardware-specific vulnerabilities, the R programming language.

How he engages

He uses his reverse engineering experience to review source code from the fundamental levels of applications and services. His hardware and advanced programming expertise empowers Stagg to dig deep into applications to find vulnerabilities that network and application vulnerability scanning tools miss.

Stagg's specific skill set has helped him in a variety of ways. From engagements with a government agency, to uncovering Internet of Things (IoT) vulns, he has proven the value of his unique background.

"I think the most interesting things I've done with Synack were with a couple targets in particular." Stagg says. *"One was [related to DARPA FETT, a bug bounty program by the U.S. Defense Advanced Research Projects Agency]. In that case it was Linux and custom hardware targets, and I found the bugs mainly from source review.*

Another I think was pretty interesting recently was [health care provider]. That's where I found a bunch of R [a statistical computing and graphics programming language] vulnerabilities on some of their data analysis apps, with some new techniques like a R deserialization RCE [remote code execution to rebuild structured data into an object]."

He describes how his knack for source code review gives him an edge:

"I'm pretty familiar with several languages, but even if it's something I'm not really familiar with, like R, I find it helps me a lot to find bugs whenever I see some source code for an app."

Stagg also described a favorite Internet of Things experience relative to his talent for reverse engineering, where he extracted an app from a Samsung Smart TV.

"That was kind of fun. Samsung wasn't the target though, just happened to need that app."

Stagg's experience shows how his penchant for source code review and reverse engineering have found vulnerabilities where others might not have.

Ian Beers

Synack handle: n0c4ptch4

Skills

OSINT, threat modelling, cyber attacker psychology, authentication attacks.

How he engages

His unique grasp of cyber attacker psychology finds the ways that threat actors exploit human nature through social engineering. Social engineering is a key component in the majority of cyber threats which is often overlooked and requires a personal touch in order to grasp.

Beers is also a master in using OSINT to find information that organizations leave all over the Internet which can be used to compromise their security postures. Beers takes a philosophical approach to his pentesting with the SRT.

"Take a painter for instance," he starts. "If you were to ask them what the most important phase of their project is, you'll almost always get the same answer: preparation."

He makes a point about how a lack of preparation is what makes script kiddies, novices who use scripts or programs developed by others to attack an organization, often ineffective against an organization's defenses.

"They might be using great tools or well written PoCs (proof of concepts) written specifically for a particular piece of technology. However, without the awareness and preparation reconnaissance phase, as most skids often skip over, their attacks become toothpicks thrown at a giant, barely causing any harm."

He describes reconnaissance as an essential preparatory phase to complete on a target. Specifically, open source intelligence (OSINT) tactics can enhance the effectiveness of an engagement by providing items like publicly listed company domains, sub-domains, information on key personnel and more.

"With this data, it's very easy to cross reference this against public breach lists that may reveal several employees' plaintext usernames and passwords within. This makes a great starting point for creating a password list, as we know many people unfortunately use the same password on multiple sites."

Beers went on to discuss common ways business materials can leak from an organization, such as through social media photos of company badges, computer screens and sticky notes.

"That just barely touches the surface on the vast actionable intel gathered from OSINT reconnaissance engagements."

Beers displays how his commitment to reconnaissance helps organizations discover more about their security posture than vulnerabilities alone, while also enhancing the vulnerability findings themselves.

Nicolas Krassas

Synack handle: krasn

Skills

System and network security, reverse engineering, penetration testing, security auditing, system administration, virtualization, high availability solutions, Dockers and Kubernetes, SS7, SIGTRAN, PCI-DSS, ISO 27001, ETSI TS 101/102 456, EJBCA, HSM, PGP, EPP, OSPF, BGP, IGRP, TCP/IP, DNS, VOIP, DHCP, HTTP, PCAP, ASA, CHECKPOINT, CISCO, XEN, VMWARE, QEMU, SSL, FTP, IDA, DBG, EIP, EAX.

How he engages

Krassas has incredible mastery of a wide range of networking protocols, data privacy regulations and application development technologies, from the most common to the most esoteric. Even computer science professors may be stumped by some of the protocols and APIs that are intuitive to him. He's especially in his element when he tests sophisticated cloud service deployments through various platforms and SaaS providers.

Krassas is a master pentester and a valuable asset to the SRT. In one engagement, his persistent analysis of a web server eventually revealed several vulnerabilities that might not have been obvious to another researcher.

"On the initial scan, everything appeared to be locked and password protected on the website. By gathering information and gaining a better understanding of the environment, it started to make sense that there are additional endpoints on top of the web server."

He got creative and found unprotected virtual hosts that had evidence of several SQL injections. As he continued to detail the engagement, he revealed a finding that is a testament to his deep expertise:

"On the same target, there was an old Java based web server running on a high port. The server, despite its age, appeared to lack known vulnerabilities. On that target, I was able to identify a case which was not known or disclosed before [a zero day vulnerability], which allowed file inclusion to be performed."

Krassas isn't the only SRT member to find a zero day during an engagement. While pentesting engagements with the SRT naturally bring breadth in skill, members like Krassas help to bring the depth of expertise that uncovers vulnerabilities that matter.

Mustafa Can İPEKÇİ

Synack handle: nukedx

Skills

Critical server side vulnerabilities, SQL injection, Remote Code Execution, cloud exploitation, all kinds of web server and web application exploitation.

How they engage

Remote Code Execution is an exploitation technique that's beloved by the most dangerous advanced persistent threats (APT) out there. Nukedx finds where the worst threat actors could attempt code injection and execution in your applications. They also have unique web application hacking skills, going back to the '90s. These are primary ways that organized cybercriminals harm enterprises, and that's what Nukedx excels in detecting.

We asked Nukedx how long they've been exploiting web applications.

"Since 1999, I have been part of the milw0rm (a hacktivist group), if you remember it. I was co-admin there, which meant I was in charge of forums and IRC channels."

Nukedx released some exploits on the Exploit Database website during that time.

Given their decades-long experience in hacking and red teaming, we knew Nukedx would have some good stories of digging up exploits with ingenuity and resilience. They described one SRT engagement where they leveraged multiple skills for a multinational conglomerate holding company focused on transportation.

"I found a CORS [cross-origin resource sharing] misconfiguration on a target's main app. It allowed me to take over any user's account. But for exploiting it, I needed to abuse subdomain hijacking on their www2 subdomain. That's because they had leftover DNS records on their cloud provider. The records were available for anyone to claim. That subdomain hijack allowed me to access cookies, as they were scoped to the root domain. Meanwhile the cookies weren't available via any XSS [cross site scripting].

To abuse the vulnerability, I wrote a specially crafted page and served it under that subdomain. I do so by simply sending a request to the target. I was able to generate a valid token on the API that hosted on it. Thanks to cookies, I was able to take over any account."

Not all SRT members have decades of experience like Nukedx, but because of the nature of the community, sharing strategies and advice is common. Younger members with less experience have the opportunity to find mentorship within the SRT.

Clark Voss

Synack handle: x11

Skills

Mobile applications, exploiting cameras, smoke detectors, SCADA equipment, and other IoT devices, web and API testing, medical devices, cloud platform testing, Amazon, and Google, Kubernetes testing, Citrix breakout testing.

How he engages

Voss is a master when it comes to industrial cybersecurity and IoT. If your enterprise wants to learn how your SCADA systems could succumb to advanced cyberwarfare, Voss is your guy. IoT hacking is another highly specialized area where Voss has unique skills. He can test your Internet-connected embedded computers in everything from point-of-sale systems to CCTV security cameras.

Voss told us about an engagement where he leaned on his ability to sleuth around mobile apps and found hardcoded credentials in the app.

"I used them to get access to data that I shouldn't have been able to access. In that engagement, I had to understand how to unpackage the application, then understand where credentials might be hardcoded. I had to understand how those credentials may be used in the application, and then understand how to use them outside the application to interact with the APIs the application uses to get at the data."

Voss' mobile expertise gives him a valuable perspective that any company with a mobile app will want to have on their attack surface. Such expertise isn't something you normally find in every candidate, as he describes it as a specialty not easy to obtain:

"Mobile testing can require binary analysis, web testing experience and API testing experience in all one engagement, which is why I have always felt it's an uphill climb to get started in. But if you like a challenge, then it's perfect."

BattleAngel

Skills

Web application pentesting, network vulnerabilities, exploiting misconfigurations, access control vulnerabilities.

How she engages

BattleAngel is an expert when it comes to exploiting web applications in a network or facing the public Internet. She also has specific expertise in Linux network device implementations. She can trace a potential exploit from the Internet, to a network's perimeter, and then break through web servers and other network-connected data assets.

BattleAngel is an expert in all things web and network with a flair for chaining vulnerabilities for maximum impact. Her ability to sniff out misconfigurations and access control errors has given her an advantage in SRT engagements. She described a recent engagement where her skills pushed other vendors out of the equation.

"There was a particular engagement wherein selective SRT were allowed to participate. The client wanted to test the skills of our SRT members on that engagement so that they could compare us with other vendors. This target was pretty hardened and there were no submissions on this target at that time, but because of my expertise in looking for web app misconfigurations, I found an issue where I got complete access to the internal administrative interface.

Due to this, I had complete access to user data, PII info, admin data, payment settings of every user, etc. This was a CVSS 9.8 and the VO called it an excellent find and they really liked my reporting as well."

The Future of Security is Diversity

This report features just a handful of the bright minds that comprise the Synack Red Team. While each member has unique strengths, expertise and combinations of skills, the advanced skill applications featured here are typical of what Synack Red Team is capable of. These are advanced pentesting techniques that our team uses every day in client engagements of all kinds.

Our SRT members know how to maneuver through different operating systems, applications, types of hardware, programming languages, APIs, you name it. When the Synack Red Team is on your side, your organization can leverage the upper hand against the most advanced cyber attackers, cybercrime groups and cyber threats. If you've got it, we can pentest it.

2022-726