

## The Synack Customer Journey

When it comes to security, you shouldn't have to compromise. Our hacker-powered security platform offers top quality testing results and expert insights on priorities and remediation routes, packaged in an efficient solution that doesn't burden your team or usurp your control. Your journey with Synack will ensure you gain efficient, effective results with zero compromise.



### What the Customer Gets:

- Synack will assess your unique requirements and deploy a custom approach to meet your needs
- Control of the engagement—you can start and pause testing as needed
- Receive real-time notifications of triaged vulnerabilities
- Real-time analytics on testing coverage, vulnerabilities discovered, researcher activity, and impact via the Client Portal
- Detailed vulnerability reports with suggested risk mitigation steps
- Unparalleled communication: Control when, where and how you share our on-demand, human-readable, customizable and downloadable reports



### What Synack Does:

- Meet with the customer to identify the technical objectives, specify success criteria, set rules of engagement, and define engagement timeline.
- Deploy the Synack Red Team, with Hydra scan data in hand, on the target(s) to look for vulnerabilities.
- Triage all vulnerabilities immediately and thoroughly to deliver ONLY valid, exploitable vulnerabilities back to the customer.
- Manage all researcher activity, communication, and payouts for valid submissions.
- Verify patch integrity to ensure that the vulnerability has been fixed and is no longer accessible.
- Summarize testing performance and impact.
- Review comprehensive results and performance benchmarking
- Conduct security training for your organization on lessons learned to aid your DevOps journey
- Create an Attacker Resistance Score based on the ease at which vulnerabilities were found Available with select Synack offerings.
- Deliver checklist-style report including exactly which weaknesses were probed and NOT found. Available with select Synack offerings.

Our Crowdsourced Security Testing model integrates seamlessly with your existing security operations to keep you one step ahead of the adversary. You can count on 24/7 support from Synack, zero hidden operational burden, and a relentless effort to help you achieve your security goals.

## The Synack Vulnerability Journey

Vulnerabilities are introduced into software quietly, remain until discovery, and end with a patch. Synack's goal is to shorten the life of a vulnerability by finding it, helping remediate it, and providing valuable intelligence so it doesn't come back.



### Introduction

A vulnerability can be introduced in many ways. The most common bugs are due to insecure coding practices, misconfigurations, recycling open source code for a different application, and/or using programming languages that are more susceptible to specific attack types.



### Automated Scanning and Recon

**Finding suspected vulnerabilities:** Synack Hydra® technology scans the testing environment for up to 3 days to find suspected vulnerabilities. For maximum efficiency, already known and easily detectable vulnerabilities are detected by Hydra, then passed on to the Synack Red Team for further investigation. The hunt can begin.



### Human (Synack Red Team) Testing

**Finding Hidden Vulnerabilities:** The Synack Red Team is securely unleashed on the previously scanned asset to find exploitable vulnerabilities that scanners missed. SRT members bring creativity, persistence, and deep expertise in vulnerability hunting, just as an adversary would.

Human testing occurs via Synack's LaunchPoint gateway, which captures all traffic and attack attempts, making testing auditable and repeatable. When a researcher finds a vulnerability, they submit a report to Synack's Vulnerability Ops team for triage and validation.



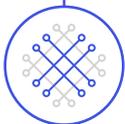
### Triage

The Synack Mission Ops team reviews all vulnerability reports to check for duplicates and exploitability. Vulnerability submission noise gets cut to near zero by Synack Mission Ops. Only real, exploitable vulnerabilities are passed on to the client (in real-time) to protect the security team's valuable time.



### Remediation Intelligence

All vulnerabilities are passed to the client with a suggested fix.



### Patch Verification

Anytime a customer deploys a patch, they can request Patch Verification. A request is sent directly to the researcher who found the vulnerability to confirm that the vulnerability has been effectively patched.



### Analysis and Reporting

Synack reports include a human-written summary of trends and observations, giving the customer vulnerability information that is more digestible, meaningful and actionable than scan reports or alert logs. Pass security reviews and shine a light on your security programs.

*Note: All intellectual property resulting from the testing and/or the vulnerability find is owned by the customer NOT the researcher. This helps protect the customer and the researcher and gives full control on action and communication to the customer. This is unique in the hacker-powered security industry.*

## The Synack Researcher Journey

The Synack Red Team (SRT) is a diverse group of highly skilled and vetted security researchers who represent over 55 different countries around the world. These researchers have reported over 20,000 vulnerabilities for Synack clients across every major industry. The SRT typically finds their first vulnerability within hours of launch.

### What Synack Researchers Do:



#### Becoming Part of the World's Most Esteemed Red Team

Trusted and experienced security researchers from around the world and across academia, government, and the private sector are sought out by Synack to apply for the Synack Red Team. Applicants must undergo an intensive 5-stage vetting process for trust and skill in order to join our crowd. About 10% of applicants successfully complete all vetting stages and onboard to the Synack platform for a probation period, during which they must submit their first valid report.



#### Platform Onboarding

Once a member of the SRT, researchers get access to Synack's platform. Synack's platform is built by hackers for hackers, helping SRT researchers work as safely, efficiently and effectively as possible. There they get information about earning opportunities, new targets, levels, messages, and payment status.



#### Getting Ready to Test

Once the researcher chooses from the list of targets available, s/he embarks on a hunt. There are two types. One is free-form as part of a creative vulnerability discovery process. The other is structured, seeking a specific weakness, by selecting Missions from a list. Both lead to skills development, challenge, recognition, and income.



#### Security Testing

A research logs into Synack's LaunchPoint™ to get started. For SRT, it protects researchers by capturing all testing traffic for auditability, to demonstrate all research activity was authorized and within program rules.

Hydra provides insightful analytics to researchers through automated scanning and reconnaissance, yielding ideas on where to efficiently hunt for vulnerabilities..

Synack Mission Ops provides support If any problems or questions arise. It's all one team - acting consistently - preventing any need to scout an individual company's bug bounty program and its operators before investing time in research



#### Level-Up

Researchers accrue and retain "status" through successful completion of vulnerability discovery challenges, competitions and community contributions made through the Synack platform.



#### Getting Paid

The SRT researcher will submit reports to Synack. The Synack Mission Operations team helps hone the researchers' skill so that all reports meet the Synack standard for high quality. Vulnerability reports are reviewed by Missions Ops for validity, exploitability, and duplication. Missions work is checked for completeness and accuracy. When valid, all reports are paid out in <24 hours.

The Synack platform enables you to utilize your unique hacking skills to help keep our clients secure. Being a part of the Synack Red Team rewards you fairly for your work without drama, enables you to learn new techniques and skills, and exposes you to enterprise companies with a variety of interesting targets.