Synack Red Team researcher requirements

Bridging the talent gap with trusted and skilled researchers

Synack Red Team (SRT) researchers must pass through a rigorous, five-stage vetting process before being onboarded. This ensures that researchers are both technically qualified and trustworthy.

Synack's unique approach provides additional assurances and enables a customizable researcher talent pool. SRT Grouping provides the ability for resource customization on a per assessment basis through tailored grouping features and a specialized researcher requirements intake process.

Synack Red Team vetting process

FRONT-END SCREENING: APPLICATION, RESUME REVIEW AND INTERVIEW

Following an initial triage of applications, qualified candidates undergo a behavioral interview. Behavioral interviews are performed in-person or via video by trained and designated members of Synack's Researcher Onboarding Team (ROT) to assess the candidate's integrity and suitability for membership.

During the interview, the ROT will establish a score for the candidate's threshold for ethics, learn about candidate motivations and goals, and communicate Synack's stringent requirements and expectations.

SKILLS: SKILLS TEST AND ASSESSMENT

Synack's assurance that only qualified researchers will engage with client assets is enabled by our cybersecurity skill assessment program. Consisting of a written and practical application component, each skill assessment is specific to a technical domain, such as web or mobile application or host-based testing.

To ensure fidelity, skill assessments are internally created, maintained and administered. Written and practical components may be taken only once, and must be completed in a single session.

TRUST ASSESSMENT: BACKGROUND & ID CHECKS, ACCEPTANCE & MONITORING

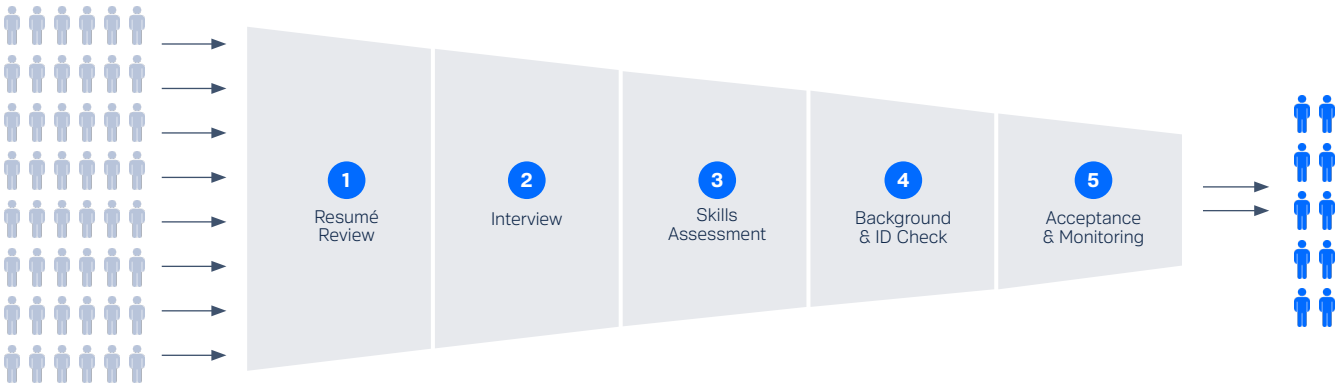
Prior to onboarding, all researchers undergo a mandatory trust assessment consisting of background and identity verification, and the following mandatory criminal background checks:

- Global terrorism and sanctions list search
- County criminal record history search (7-year)
- Department of Justice sex offender records search
- Federal Excluded Parties Listing System search

A Social Security Number trace, including address history cross-referencing[1]. Once the researcher is admitted to the platform, they undergo a 45-day monitored qualifying period before being fully accepted into our program.

1 A DoJ sex offender records search and Social Security Number trace are conducted for domestic candidates only.

The 5-stage vetting process



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

Vetting stages	Success	Elimination
1. FRONT-END SCREENING: APPLICATION REVIEW • Applications are received, tracked and evaluated within Synack's human resource management system. All process workflows are maintained and tracked within this system to ensure a consistent and auditable process • The candidate's claims surrounding work experience, certifications and education are evaluated and cross-referenced with Open Source Intelligence (OSINT) sources	• Bachelor's degree or relevant experience and 3 years of penetration testing experience or • Demonstrable history of exceptional capabilities or accomplishments	• Less than 18 years of age • Restricted geography (ex: OFAC nations) • Suspicious social media activities or connections • Presence on watch list(s)
2. FRONT-END SCREENING: BEHAVIORAL INTERVIEW • Create a rapport with the candidate through an interactive, live video interview • Establish an initial assessment of the candidate's character, motivations and goals • Gather secondary information relevant to vetting process and uncover 'red flags' • Determine the candidate's primary technical competency	• Active understanding of requirements and expectations • Responses to questions surrounding employment and activities are candid and forthright • Alignment of the candidate's stated motivations and goals	• Attempts to disguise location or identity • Answers conflicting with application, public profile(s) or previous answers • Exhibition of 'red flag' behaviors
3. SKILL ASSESSMENT: WRITTEN EXAM & APPLICATION • The written skill assessment consists of multiple choice and open-ended questions, designed to evaluate the candidate's fundamental understanding of a specific technical domain • Practical skill assessments are predominantly black box in nature to reflect the nature of Synack engagements	• Consistent, accurate answers • A passing score as defined by Synack's grading rubric	• Poor quality or inconsistent answers • Suspicious answers or exam activity • Failure to meet time requirements

4. TRUST ASSESSMENT: BACKGROUND & ID CHECKS • Identity verification and criminal background checks are completed by designated and qualified third-party assessors. • Waivers for non-material misdemeanor activity may only be granted after a designated individual case review	• Verified identity • Thorough and clear record	• Failure to meet Synack requirements
5. TRUST ASSESSMENT: ACCEPTANCE & MONITORING • The active monitoring period is a required 45-day qualifying period. The researcher is required to submit a valid vulnerability report before fully being on-boarded • Zero tolerance policy: Researcher traffic is actively monitored and tracked ongoing; use of high-velocity scanners and similar automated tools that could bring down a target environment result in termination of SRT membership	• Adherence to Rules of Engagement (RoE) • Submission of valid vulnerability report within qualifying period • A passing score as defined by Synack's grading rubric	• Failure to adhere to RoE or qualifying period requirements • Poor written report quality • Suspicious session or engagement activity surrounding the assessment • Failure to meet time requirement

Additional Researcher Controls

TAILORED RESEARCHER GROUPING	Synack maintains detailed demographic information and profiles on each researcher on the Synack Red Team. This information can be used to limit researcher engagement based on demographic criteria including geographic location, nationality and employment background.
SPECIALIZED RESEARCHER REQUIREMENTS INTAKE	In the most sensitive and restricted environments, client-specific onboarding, background checks and other assessments are required. Synack's researcher requirements intake process uses a modular integration approach to incorporate client-specific requirements into Synack's vetting process.