Synack Crowdsourced Penetration Testing

Crowdsourced Penetration Testing from the World's Best Ethical Hackers

Synack Crowdsourced Penetration Testing (CPT) takes Synack's core vulnerability discovery and adds Attacker Resistance Scoring and compliance checks. The result is a broader test that can serve demanding security needs that come from a broad range of teams and goals. CPT delivers both true positives (vulnerabilities) that can be used by product and security teams and true negatives (security checklist results) that can be used by audit and security teams.

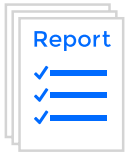
What You Get

CPT provides results for security improvement and the capability to report compliance to third parties such as auditors. CPT customers receive a comprehensive report at the conclusion of every test that includes a human-written analysis, and PCI DSS 11.3 certification (see Coalfire paper on the same topic) in addition to vulnerabilities found. Customers also gain access to Synack's unique Attacker Resistance Score - which uses SRT performance data to measure the hardness of customer assets against attack. The Attacker Resistance Score can be used to benchmark against competitors in your industry or against the Synack platform average.

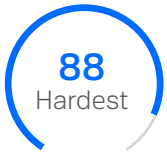
Vulnerabilities

Diverse, Skilled Crowd of Researchers

Testing Data



Professional Report



Attacker Resistance Score

PCI-Ready Report

The Synack Process

During a two-week engagement, customers participate in a simple launch process with Synack, then receive validated vulnerability reports, verified compliance checks, and their unique Synack Attacker Resistance Score. Unlike pen testing or bug bounty platforms, customers have complete control over testing traffic. During the testing, customers can view real-time results and work with their dedicated program manager for specific insights. All effort to produce the results is handled by Synack, including scoping, scanning, prioritizing, testing, triage, validation, motivating, paying and notifying. Data is collected throughout to understand not just what was found, but how it was found—an essential question to answer for better future security.

What Synack Tests

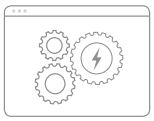
Synack handles a wide range of target types. They can be tested individually or in combination (such as a Mobile App using a REST API). **Don't see what you're looking for? Ask a Synack representative.**


Web Apps


Infrastructure


Mobile


Cloud


API

Features and Benefits

Top, Trusted Talent	Tested, interviewed and holistically evaluated. Not just ID checks.
Compliance Ready Reports	Reports suitable for PCI DSS 11.3 and other compliance needs.
Attacker Resistance Score	A realistic assessment of assets' actual hardness against attack based on penetration test performance data.
Own your Vulnerability Intellectual Property	Vulnerabilities Reports belong to Synack customers, not Synack and not the researchers.
Control of Research Traffic	Research traffic can be paused instantly for any reason.
Full Service and Support	All work except turning valid reports into internal remediation plans is handled.
Scalable Recon and Scanning	Synack's hybrid software-human scales better than bug bounty hunters.
Divert Research from Public Internet	Research traffic is diverted to Synack's LaunchPoint VPN gateway for security and reliability, minimizing the strain on your production systems.
Measure Testing in Progress	Unlike Standard Penetration Testing, Synack measures the aggregate time and volume of activity researchers spend performing work.
Classified Attack Traffic	Synack provides classifications of most attack traffic to see alarming trends before they set off alarms.
Analytics	Spot trends through testing coverage analytics that could result in unfound vulnerabilities living longer than necessary.
Dashboards	See program status at a glance, including research hours logged, researchers engaged, patch statuses, vulnerability status, burndown chart, and much, much more.
Detailed Report	Reports on demand with results found to date, including methodology, targets, human-written summary analysis, and results.
Time-Bound	Bundled in two-week bursts of research activity to fit with your development and security cadence.
Fair Liability Terms	Synack takes responsibility for the work of the Synack Red Team. It's not a contract directly between you and bug bounty hackers.

Synack, Inc.
855.796.2251 | www.synack.com | info@synack.com