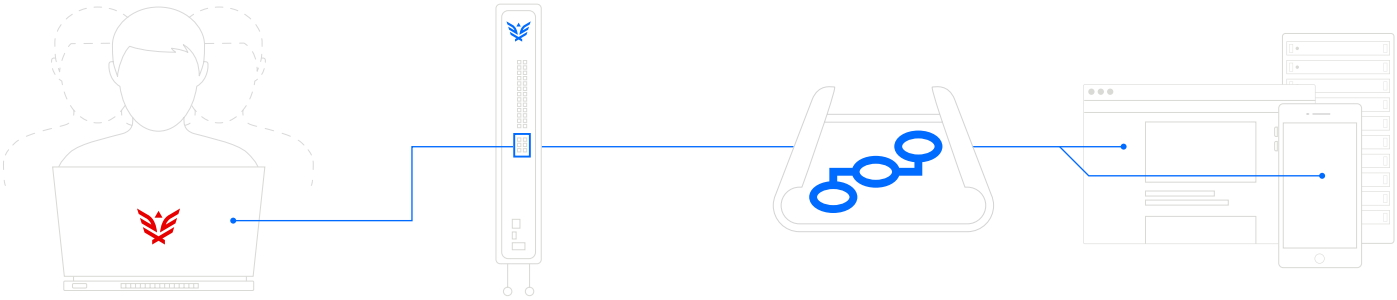
# Synack Crowdsourced Penetration Testing

## Crowdsourced Penetration Testing from the World's Best Ethical Hackers

For customers that need to meet specific compliance standards by a regulating body, a Synack Crowdsourced Penetration Test (CPT) offers checklist-style task completion in addition to Crowdsourced Vulnerability Discovery. This solution adds documented proof that specific security checks were completed at a point in time. Synack Red Team researchers, complemented by Synack's intelligent scanning technology, are incentivized by a bounty model to find vulnerabilities and to complete compliance checklists. Completing regular Crowdsourced Penetration Testing ensures that an entire organization's security practices are working correctly and improving over time.

Crowdsourced Penetration Testing adds **Missions**—a checklist-driven approach to security compliance—to the creative vulnerability discovery of Synack CVD. Each Mission addresses an item from individual requirements such as those from OWASP or PCI.

## The Synack Process



### SRT + Hydra Technology

Hydra technology enables the Synack Red Team to complete security test (via Missions) and discover vulnerabilities efficiently and effectively.

### LaunchPoint®

All SRT testing activity is routed through our secure gateway technology, providing our clients with full transparency and control.

### Mission Ops

Mission Ops triages and validates all vulnerability submissions and Missions documentation before passing them to the client.

### Customer Assets

Synack tests each customer asset on a continuous basis and provides real-time testing coverage results and analytics.

The result of Missions is a documented report of security testing that was performed, regardless of whether a vulnerability was found. CPT with Missions helps establish that any lack of breach is due to following good security practices and not just luck.

During a two week engagement, customers receive a fully managed service that includes compliance verification, a dedicated program manager, scoping services, intelligent scanning, researcher management and bounty payouts, platform access, vulnerability notifications, patch verification, and detailed data analytics and reporting.

## 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). Hybrid target environments (such as the infrastructure and applications in a PCI Cardholder Data Environment) are eligible for testing. **Don't see what you're looking for? Ask a Synack representative.**



Web Apps



Infrastructure



Mobile



Cloud



API

## Crowdsourced Penetration Testing Missions

The following are 25 Missions that are accomplished with CPT - Basic (list subject to change). Clients receive documentation that checks were performed. Mission documentation is in addition to any vulnerabilities found.

- Account Enumeration and Guessable User Accounts
- Anonymous Accounts (Anonymous FTP)
- ARIN Information Gathering
- Default Credentials
- Dictionary Attacks (Bruteforcing)
- DNS Amplification DDoS Attack
- DNS Subdomain Bruteforcing
- DNS Subdomain Takeover
- DNS Zone Transfer
- DoS via SSH, SMTP, FTP, HTTP, and SIP
- Forward/Reverse DNS
- Host Fingerprint
- Host-Based Multi-Factor Authentication Schema Bypass
- Host-Based Privilege Escalation
- Information Leakage
- Information Leakage via Search Engine Discovery and Reconnaissance
- Insecure Direct Object Reference (IDOR)
- Password Cracking
- Remote Code Execution
- SMTP Relay
- SSL Vulnerabilities
- SSL/TLS Certificate Anomalies
- Virtual Host Detection and Enumeration
- Weak or Deprecated Ciphers
- Whois Information Gathering

**Synack, Inc.**

855.796.2251 | www.synack.com | info@synack.com