Penetration Testing

Gartner defines penetration testing as a method that goes beyond vulnerability scanning, instead using multistep and multi-vector attack scenarios in an attempt to further infiltrate applications and infrastructure—providing visibility into aggregations of misconfigurations or vulnerabilities that could lead to an attack. But what attack vectors are most relevant?

Traditional pen testing engagements just don’t measure up to the levels of testing depth and diversity that an enterprise organization actually needs in gaining a true security risk analysis from an adversarial perspective.

*To beat a hacker, you have to think like a hacker... but to protect an enterprise against constant, complex threats, you can’t just think like one or two pen testers; you have to ignite hundreds of the world’s best ethical hackers into rapid action. Synack’s crowdsourced penetration testing and application security that incentivizes hackers with a bounty model to do just that. Here’s how it compares:*

<table>
<thead>
<tr>
<th>Traditional Penetration Testing</th>
<th>Synack Crowdsourced Penetration Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Days to Weeks</strong> (Variable due to delays in finding available resources with appropriate skillsets)</td>
<td><strong>Onboarding</strong></td>
</tr>
<tr>
<td><strong>Point-in-time test includes a few days of active testing</strong></td>
<td><strong>Time Frame</strong></td>
</tr>
<tr>
<td><strong>1–2 pen testers with variable skillsets</strong></td>
<td><strong>Personnel</strong></td>
</tr>
<tr>
<td><strong>Pen testers paid hourly, regardless of results</strong></td>
<td><strong>Payment Model</strong></td>
</tr>
<tr>
<td><strong>20–60 man hours of active testing in a 1 week period</strong></td>
<td><strong>Testing Hours</strong></td>
</tr>
<tr>
<td><strong>Testing period followed by one cumulative report hand-off</strong></td>
<td><strong>Vulnerability Reporting &amp; Management</strong></td>
</tr>
<tr>
<td><strong>Little-to-no support following final engagement report</strong></td>
<td><strong>Vulnerability Management</strong></td>
</tr>
<tr>
<td><strong>Cloud-based solution, diverse testing community can be activated within 24 hours</strong></td>
<td><strong>Ethical hackers paid only for valid vulnerabilities through an incentive-driven model</strong></td>
</tr>
<tr>
<td><strong>Extreme flexibility—Engagements range from week-long to continuous/year-long testing windows</strong></td>
<td><strong>Hundreds of hours of active testing in a 1 week period</strong></td>
</tr>
<tr>
<td><strong>Continuous vulnerability triaging and reporting in real-time and highly prioritized final report</strong></td>
<td><strong>Synack Operations provides end-to-end vulnerability lifecycle management beyond initial reporting</strong></td>
</tr>
</tbody>
</table>
Why Synack Crowdsourced Penetration Testing?

Synack Crowd Security Intelligence Core Components

Synack’s crowdsourced penetration testing and application security solution is a full-service model that encompasses the trusted, controlled aspect of a high touch penetration testing service with the diversity, continuity, and incentive-driven nature of bug bounty programs, plus the scalability and analytical capabilities of automated vulnerability technologies.

**Diverse, Hacker-Powered Penetration Testing Team**

The Synack Red Team attracts the most sought-after ethical hackers from across the globe to join the SRT. Our community offers unparalleled diversity in perspectives and insights and utilizes the latest attacker tools, techniques, and procedures to mimic the activity of real world malicious hackers and detect exploitable vulnerabilities in a safe and controlled manner. We provide customers with a truly adversarial approach to information security, web and mobile application security testing, network and infrastructure security, connected IoT device and embedded device hacking, or physical security/special project activities.

**Penetration Testing at Scale**

Don’t fret over finding the right pen test team or wait until they’re available. Synack’s team of expert ethical hackers is always “on call”. The solution is cloud-based and can be rapidly activated to discover vulnerabilities across your business-critical assets within 24 hours, with no delivery or installation of on-site devices or need for on-premise teams. Synack remains actively engaged with our client’s security teams throughout the entirety of the vulnerability lifecycle—from discovery, to validation and prioritization, to remediation, and even patch verification. Additionally, Synack’s testing engagements can be paused at any time through the click of a “switch” on the Synack client dashboard (as necessary).

**Reduce the False Negatives**

With traditional pen testing there is a rising cause for concern over vulnerabilities that remain undetected, or “false negatives”. Synack’s elite crowd of ethical hackers paired with advanced proprietary technology provides superior vulnerability detection capabilities in surfacing even the most challenging and complex vulnerabilities. And, unlike pen testing firms/consultants who are paid regardless of results, being paid by bounty rewards only motivates and drives all Synack Red Team (SRT) researcher testing activity. If SRT members don’t report valid vulnerabilities, they don’t get paid. The more impactful/severe the potential exploitation, the greater the rewards, incentivizing the SRT to constantly test for critical vulnerabilities and report them in a prompt fashion.

**Reduce the False Positives**

Before reporting vulnerabilities, the Synack Mission Ops team checks all findings through a rigorous triage process that includes vulnerability reproduction, verification of exploitability and cross-checking with the engagement scope and existing known vulnerabilities to eliminate duplicate reports. This allows Synack to deliver a >95% signal-to-noise ratio to customers—when you hear from Synack, it matters. Synack provides intelligence that allows the customer to understand just how exploitable something is and how to attack the remediation helping the security team build a productive relationship with the development team. Synack also provides customers with a way to confirm the efficacy of a patch through Synack’s patch verification process. In our experience, 15% of patches fail the first time. You don’t want to learn this the hard way.

**Continuous**

**Scalable**

**Hacker-Powered**

**Fully-Managed**

**Enterprise-Trusted**

Crowdsourced Application Security & Penetration Testing

**WHY SYNACK?**

- Continuous
- Scalable
- Hacker-Powered
- Fully-Managed
- Enterprise-Trusted

**Synack, Inc.**

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

© 2016 Synack, Inc. All rights reserved. Synack is a registered trademark of Synack, Inc.