TAG CYBER

TAG Cyber Advisory Report: Crowdsourced Security Testing with Synack

The Synack Crowdsourced Security Testing platform is proven to reduce enterprise security risk through a continuous crowdsourced testing methodology enhanced by machine learning and artificial intelligence. The platform allows enterprises to scale to the dynamic and distributed needs of today's dynamic enterprise.

Prepared by
Katie Teitler
Senior Analyst, TAG Cyber
katie@tag-cyber.com

Version 0.0
September 10, 2020

Introduction

Best practices in cyber security include a requirement for organizations to continuously test and assess systems and software for vulnerabilities that may lead to compromise. Traditional methods of testing and assessment include vulnerability scanning, penetration testing, and red teaming. Best-in-class organizations avail themselves of all three methods, but each of the traditional methods have its pros and cons.

Traditional vulnerability scanning can provide broad-based coverage and can be relatively continuous, but it only accounts for known, easy-to-find, vulnerabilities, which can create results with false positives and/or false negatives. Penetration testing introduces the attacker's point of view but is limited to that particular tester's knowledge base and, usually, to a defined set of parameters set by the hiring enterprise. Red teaming is the most life-like but requires testers to possess a very high skill set, which is normally hard to recruit, and often accompanied by a very high cost to enterprises. Traditional penetration testing and red teaming are challenging to scale and maintain at a continuous cadence so they often only provide a point-in-time assessment of organizations' assets and risk posture.

More recently, bug bounties have become popular with enterprises. They provide a refreshing, modern approach, but have limitations; exposing the customer to additional risk of unknown hackers and putting a heavy burden on the internal security team. In an open bug bounty model, there is limited control over who participates in the program. In addition, opponents of bug bounty programs argue that the pay-per-vulnerability model incentivizes researchers to prioritize volume over quality of submissions.

Although all of these models offer critical features recently it has become clear that security testing has had to evolve beyond these separate traditional tools used by enterprises in years past. The dynamic nature of organizations' assets, expanding attack surfaces (including cloud, containers, IoT, and remote work), and adversaries' use of automation and machine learning have made it more difficult for enterprises to maintain a proactive security posture and limit their potential risks. Today's security conscious company needs a platform that combines the ability to scale to continuous testing without sacrificing quality or burdening the internal security organization.

In this analyst note, we provide an overview of the testing market, with a focus on the Synack Crowdsourced Security Testing platform as a best-of-breed testing option. We will pay particular attention to the needs of today's dynamic, remote workforces and how a crowdsourced model provides both breadth and depth of coverage, as well as the functionality for ongoing assessment without an exorbitant cost.

Security Testing Requirements: Let's Review What has Changed

The functional requirements to support continuous testing have evolved based on three factors. First, the growth and maturity of cyber adversaries has made it eminently clear that enterprises—defenders—need ongoing and continuous testing and assessment of their systems, networks, applications, and security controls. As cyber criminals will use all available resources, enterprises must also use every tool in the proverbial toolbox to take a more proactive approach to finding vulnerabilities in organizational assets and hardening security controls.

Second, enterprises' attack surfaces are expanding exponentially as digital transformation continues. In conjunction with corporate-managed digital asset expansion, enterprises are connected to a greater number of 2nd, 3rd, and Nth party systems over which they have no direct control but which directly affect the potential for compromise. This problem has become no more readily apparent than during the recent shift to large-scale work-from-home requirements, accompanied by the explosion of personal and unmanaged devices hitting corporate resources. Enterprises cannot afford to take a wait-and-see approach to testing.

Third, the cyber security workforce talent shortage continues to plague companies looking for highly skilled individuals. Workforce dynamics have driven up the cost of hiring the most experienced and skilled cyber security practitioners—either as full-time employees or part-time /limited-engagement contractors—making it challenging for smaller and medium-sized businesses to implement the continuous testing needed to protect the organization.

The Emergence of a Platform Approach to Security Testing

Among the cyber security community, some confusion exists as it pertains to the definition of "security testing." Between scanning, pen testing (for which humans can manually test or use automated tools), and red teaming, there is quite a bit of variability and inconsistency in the commercial market. However, many organizations seek a cohesive approach that provides comprehensive results. And that's difficult to accomplish with a varied set of tools of tools and processes.

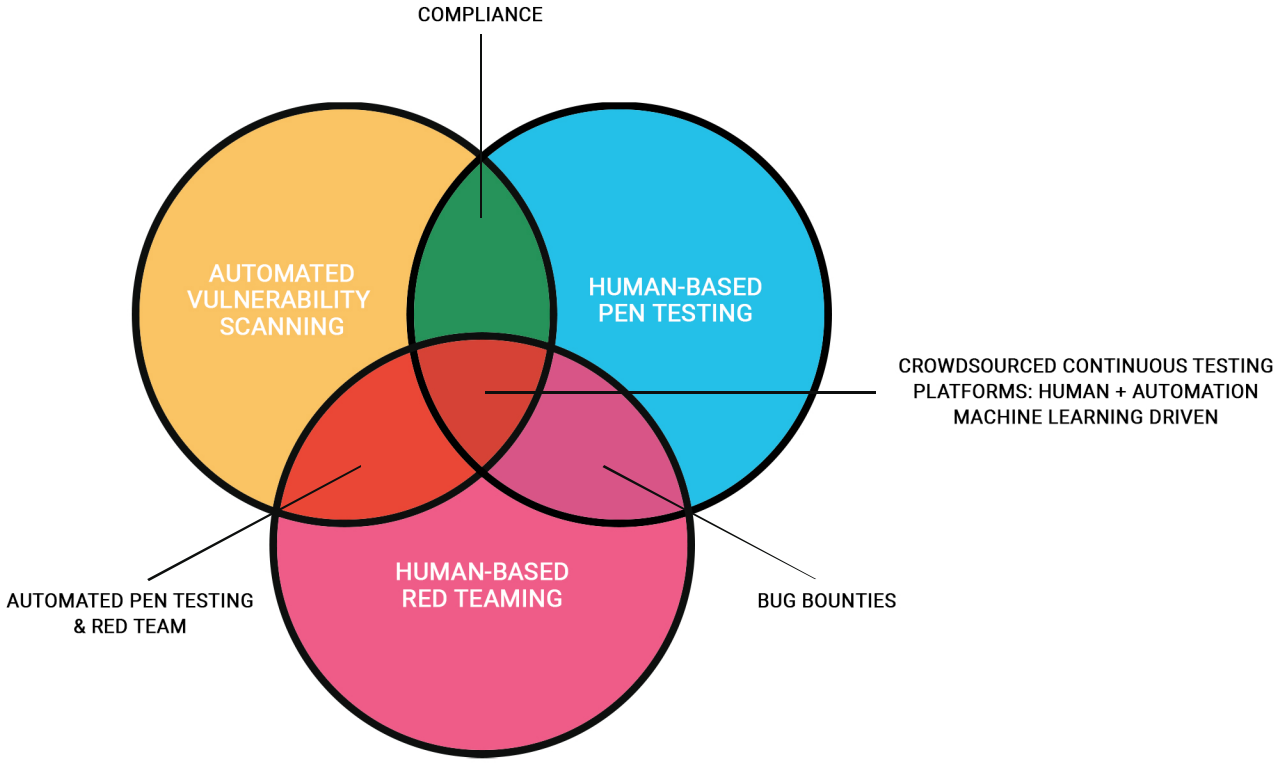

Figure 1. Emergence of a Platform Approach to Security Testing

With current capabilities in automation and the scramble to offer lightweight, affordable testing solutions to enterprises, the vendor market for automated testing has considerably grown in size. This is a win for organizations; however, vendor marketing messaging can be confusing, infusing buzzwords, and muddling any differentiation among toolsets. In a vendor-to-vendor bake-off, security practitioners have a hard time deciphering functionality based purely on how sales and marketing teams are presenting the solution.

Finally, despite the potential benefits of adding new testing tools or resources, internal teams worry about how to handle "noise," i.e., the additional data and alerts that accompany any type of assessment. End user practitioners are constantly looking for ways to raise signal from noise and focus internal efforts on the most potentially impactful activities.

Analyzing the Synack Crowdsourced Security Testing Platform

The Synack Crowdsourced Security Testing platform is an industry-leading platform that combines the necessary but varied testing methods mentioned above. In this section, we outline the more salient aspects of the Synack platform and show how its functionality combined with a crowdsourced approach allows enterprise security teams to optimize asset testing (people, processes, and technology), consistent with industry-recommended practices for making enterprise systems more resilient to cyber compromise. Synack is the premier crowdsourced security platform within the industry today. Below are the main features of the platform:

Crowdsourced ethical hackers

As organizations adopt continuous integration/continuous development (CI/CD) cycles, traditional methods of security have become hard to scale. Synack saw an opportunity in the security market to combine the best attributes of automation with human-based efforts and build a platform that meets the security needs of today's businesses.

With the evolution of open source harnessing talent and creativity otherwise unavailable to one company through their own employee base, Synack capitalized on the trend of crowdsourced, but in a way that had never been seen before in the security market; the company's platform uses a crowdsourced approach to recruit elite ethical hackers. Drawing from candidates across the globe, all applicants are required to undergo a rigorous, multistage vetting process before they're invited to participate in testing. This process produces a large pool of experts with diverse skill sets, backgrounds, and perspectives more reflective of the attacker community—an obvious benefit to Synack customers. The group of carefully selected testers compromises the Synack Red Team (SRT), more than 1,500 ethical hackers from 80+ countries who conduct ongoing testing for Synack's customers. This approach is significantly different from traditional red teaming or penetration testing, for which a small group of experts is generally hired for a limited, point-in-time engagement.

Machine learning- and AI-optimized data

The SmartScan component of the Synack platform is powered by Hydra, an automated continuous vulnerability scanning tool which uses machine learning (ML) to find and contextualize vulnerabilities, incorporating new insights as they're discovered. Hydra scans web assets using fuzzing, crawling, etc.; host infrastructure for open port detection, plugin detection, automated screenshot capture, etc.; and cloud instances for enumerations, authorizations, and more. Hydra automatically forwards identified vulnerability intelligence to the SRT for further investigation and enables their work in pen testing or red teaming. In addition to hunting for vulnerabilities, the Synack Red Team verifies all suspected vulnerabilities discovered by Hydra. The technology allows for scaling not possible by human means alone. Though AI and machine learning are components in other scanning tools on the market, none combines AI/ML with active human powered investigation—a clear advantage for Synack customers.

Secure virtual collaboration

The collaborative nature of Synack's platform enables a workspace where customers can view the results of testing against their assets and where testers can input and track progress on their work and the work of fellow testers who are servicing the same account. Unquestionably, this workspace must be highly secure and maintain the privacy of both tester and customer data.

LaunchPoint™ is Synack's secure VPN gateway through which SRT testing traffic is routed and through which customers can access testing data, including hours logged, attack analysis, and coverage maps. LaunchPoint+ is an optional enhancement included with the company's year-round service that provides a secure, hosted virtual workspace where testers conduct their testing and which layers on additional security, privacy, and regulatory controls.

The importance of LaunchPoint and LaunchPoint+ cannot be underscored enough. Were a malicious hacker to target a platform like Synack, it would be a goldmine of vulnerability data, including the status of found vulnerabilities in customer systems. Synack's founders and executive team know the criticality of placing the highest level of controls around this system and data, as their roots are in the U.S Intelligence community. This attention to secure transmission, storage, and access is important for enterprise teams as they're considering the privacy, assurance, and vetting aspects of managing a crowdsourced or collaborative technology. The platform includes a very high level of security control, including least privilege access, multi-factor authentication requirements, and segmentation.

Enhanced reporting & high quality insights

Today's security platforms require an easy-to-use dashboard and customer interface that encompass real-time, always up-to-date data, and Synack is no exception. As explained in the previous section, testers submit all testing data via LaunchPoint. From there, all findings and analytics are automatically sent through to the customer's dashboard where they can view real-time results, including vulnerability status: exploitable vulnerabilities (discovered by the SRT OR identified by SmartScan and verified by the SRT), including impact, steps to reproduce, and recommended fix; informational findings; remediation status; and analytics on security progress.

Testers are required to submit sufficiently detailed reports—including remediation recommendations upon which customers can act—before they receive a bounty. The premise is that vulnerability information without action does nothing to reduce customer risk—and the goal of testing should always be to identify, then mitigate risk.

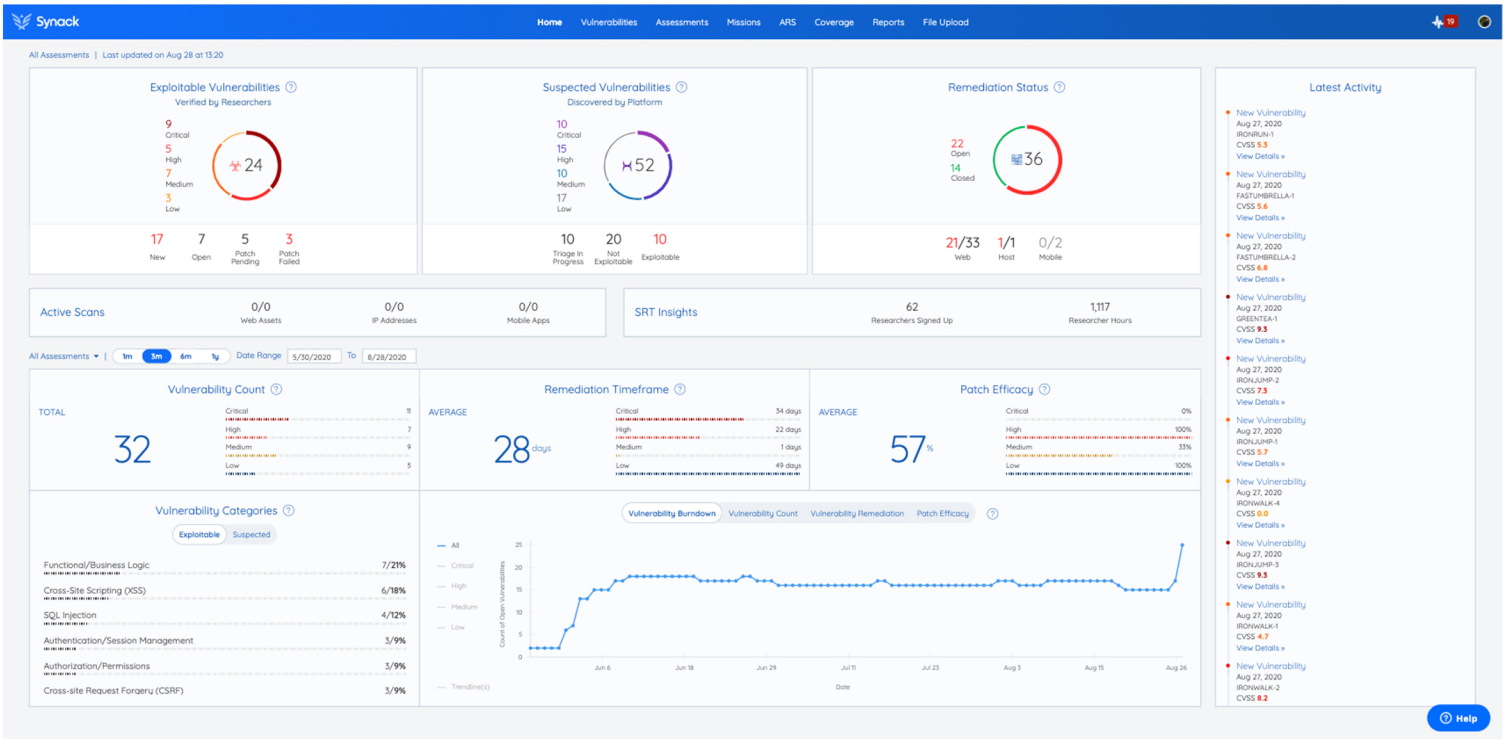

Figure 2. Dashboard snapshot

One useful and exclusive aspect of Synack's reporting is their Attacker Resistance Score™ (ARS) metric—an assessment of the exploitability of a vulnerability from a hacker's perspective, in this case, a member of the Synack Red Team (SRT). The ARS shows the customer how difficult it was for the tester to find the vulnerability and penetrate the system, the severity of the vulnerability (the potential impact of a real-life exploit), and which assets in the customer's environment are the weakest and most likely to be attacked.

All reporting is customizable per customer requirements/preferences and incorporates detailed, human-written analyses about all findings by the SRT, including remediation recommendations, severity ratings, and peer-to-peer benchmarking.

Action Plan

The Synack Crowdsourced Security Testing platform provides government agencies, large enterprise, the mid market, and start-ups, a comprehensive continuous testing capability that will help reduce unnecessary exposure. The crowdsourced approach combined in a SaaS platform solves the problems of talent acquisition, technology integration, and scalability, while reducing the amount of noise customers would normally handle by managing disparate systems and processes concurrently.

Further, the Synack platform allows for economy of scale in terms of depth and breadth of coverage as well as cost, resulting in greater ROI. From previous assessments of the platform, we have found Synack's platform to impress enterprise clients with the speed at which vulnerability data is delivered, the expertise and diversity of the SRT, and the enhanced reporting features that allow for rapid and prioritized remediation on the part of the customer.

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

About Synack

Synack, the most trusted crowdsourced security platform, delivers continuous and scalable penetration testing with actionable results. The company combines the world's most skilled and trusted ethical hackers with AI-enabled technology to create an efficient and effective security solution. Synack protects leading global banks, federal agencies, DoD classified assets, and close to $1 trillion in Fortune 500 revenue. Synack was founded in 2013 by former US Department of Defense hackers Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.

Learn More