Synack

The Value of a Trusted Crowd of Ethical Hackers for Election Security

A closer look at the critical role that managed crowdsourced security testing can play in securing the technologies that underpin American democracy

In the summer of 2020, soon after red team researchers from a managed network of ethical hackers began examining the State of Colorado's voter registration website for potential vulnerabilities, they spotted something alarming. Problems with the website's CAPTCHA challenge, a common first line of defense online, could have opened up the site to a distributed denial of service (DDOS) attack or created a gateway for further malicious activity during an already challenging year for election officials nationwide.

"They found bugs in how we implemented CAPTCHA that no other testers had ever discovered," said Trevor Timmons, CIO for the Secretary of State of Colorado. The state had previously worked with traditional pen testing firms to evaluate online election systems and related websites. "That was jarring to say the least, but we wouldn't have found it if we didn't have the best ethical hackers working with us to ensure we've done everything possible—and haven't overlooked any part of our system—to keep the election process safe and secure."

The state worked with the red team network through a pro-bono Secure the Election Initiative designed so states could take advantage of a managed network of ethical hackers and gain critical security insights ahead of the election. Researchers who approach security with an adversarial mindset have become incredibly powerful resources for Global 2000 corporations, the Department of Defense, international financial institutions and the biggest healthcare organizations.

In total, the red team network discovered seven vulnerabilities in Colorado's election-related systems as well as the Secretary of State's official website. Colorado patched all of them well ahead of Election Day using the detailed reports they received in real time from the provider's Crowdsourced Security Platform.

Crowdsourced security testing provides a rigorous, adversarial perspective on the security of assets. It differs from Vulnerability Disclosure Programs (VDP) in the level of testing quality and controls that it provides. A managed crowdsourced testing platform will recruit the top security researchers, vet them based on their technical abilities and background, and incentivize them to find vulnerabilities in systems using their offensive skill sets. The adversarial testing activity is carried out through a smart platform designed to accelerate the time it takes researchers to find flaws, all while providing customers with control, visibility, and advanced analytics.

On the other hand, VDPs offer a "see something, say something" approach by allowing anyone on the internet to report a vulnerability. Still, VDP is a critical ingredient of a robust security testing strategy for providing a mechanism through which people can report potential security issues and for getting additional eyes on a digital asset. However, if not managed carefully, a VDP can also burden an organization if they are not prepared. Reports submitted through VDPs are often false positives and numerous, requiring a lot of time to sift through and find any valid vulnerabilities.

Figure 1: Differences in Crowdsourced Security Models

	Vulnerability Disclosure Program	Crowdsourced Security Testing Platform Used by Colorado
People	• Open to anyone on the internet	• Vetted crowd, monitored through the platform
Process	• Submit a report through a portal	• Incentive-driven testing and compliance • User has power to stop/start testing • Legal protection
Technology	• N/A	• Smart scanning technology enables researchers and accelerates findings
Results	• High volume of submissions with varying quality	• High-quality, triaged vulnerability and assessment reports • Real-time analytics for rapid response

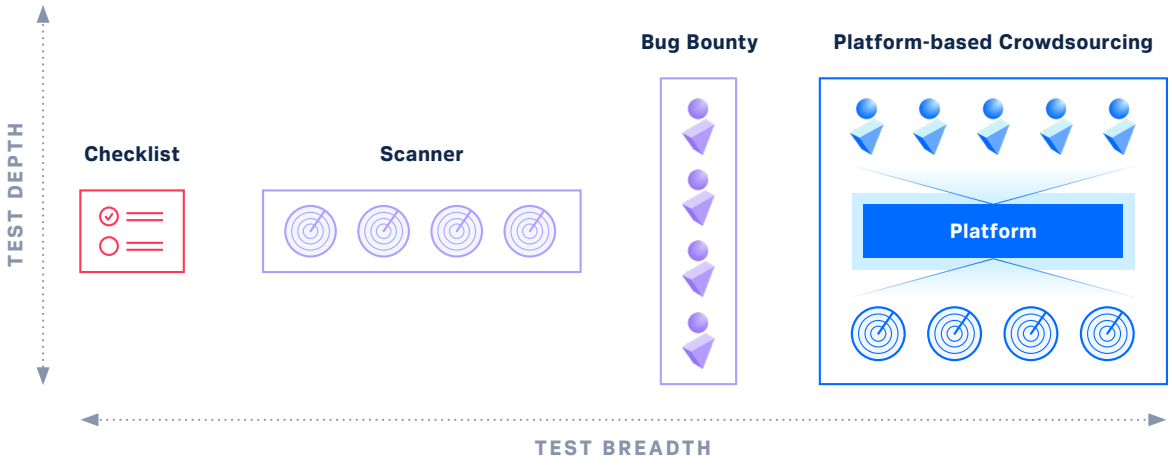
Before starting a VDP, states should consider:

- Are resources available to triage all submissions and remediate valid vulnerabilities? Triage and remediation resources are critical for prioritizing key issues.
- Are integrations with development and automation tools available to help save time and stay on track?
- Their willingness to include all internet-connected assets in the VDP to maximize coverage.

For anyone looking to start a crowdsourced security program, Dr. Mark Kuhr, a former U.S. National Security Agency technical director and CTO of a leading crowdsourced security platform, recommends starting with a managed crowdsourced penetration test. “Starting with a controlled, targeted test by a select group of security researchers that we know are highly skilled and highly trustworthy can help identify and patch the critical vulnerabilities before the public sees them,” Kuhr explains. “Once an attack surface has been hardened through crowdsourced penetration testing, we then recommend layering in a vulnerability disclosure program and continuous testing and scanning through the platform.”

Crowdsourced security testing has been recommended by the DoD, the White House, and the U.S. Senate as a best practice. Traditional penetration testing can fall short in modern digital environments. The static testing team, point-in-time testing cadence, and checklist-driven approach cannot scale to the magnitude of today’s pervasive and persistent threat.

Figure 2: Differences in Security Testing Models



Voting equipment vendors have also adopted crowdsourced testing to test election-related hardware. In August 2020, during the Black Hat USA cybersecurity conference, one of the largest U.S. election vendors announced a partnership with the same crowdsourced platform with which Colorado partnered to test its newest electronic poll book. That development was hailed as a breakthrough in the relationship between election vendors and independent election security researchers. At the time, Wired Magazine wrote that the collaboration showed the beginning of a new partnership between security researchers and election vendors.

The crowdsourced security testing platform allowed the election equipment vendor to utilize top security researchers through a managed and private engagement. The research also helped the vendor prioritize any vulnerabilities the red team discovered through rigorous testing. The election equipment provider chose not to publicly reveal vulnerabilities discovered during testing. The process allowed them to "learn about and fix potential security issues before malicious hackers find them," wrote Wired, which also noted "the company plans to run additional crowdsourced penetration tests with [the crowdsourced security platform] on other products as well."

The recent SolarWinds Orion hack calls for a more adversarial mindset when it comes to security testing. In that assault on thousands of organizations, nation-state hackers were not only able to enter victims' systems through a software update, they successfully expanded across networks to access incredibly sensitive government and industry data. Testing such as the kind performed by a crowdsourced security platform can help harden internal assets against these types of "lateral movement" attacks.

"The crowd needs to be a critical part of any good cybersecurity strategy," said Kuhr. "An adversarial model of crowdsourced penetration testing is about as close as an organization can get to testing systems against a real adversary. This approach is designed to harness the collective brainpower of the world's best ethical hackers when it comes to finding and fixing the most critical vulnerabilities and other weaknesses that can leave organizations dangerously vulnerable."

About the Author

Synack, the most trusted crowdsourced security testing platform, delivers smarter penetration testing to security teams. The platform provides continuous testing and actionable results to today's organizations that need a scalable, efficient way to test their attack surfaces. Synack's crowdsourced penetration testing is powered by the world's most skilled and trusted ethical hackers and augmented by AI-enabled technology to give customers the best of human intelligence and machine intelligence. Headquartered in Silicon Valley with regional offices around the world, Synack protects leading global banks, federal agencies, DoD classified assets, and more than $1 trillion in Global 2000 revenue. A 4-time CNBC Disruptor 50 company, Synack was founded in 2013 by former NSA security experts Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.

For more information, please visit www.synack.com.