Synack Secure the Election

Why Secure the Election

The right to a fair election has become a primary target of our adversaries. Secretary of State Mike Pompeo has "every expectation" that election meddling is an ongoing issue and that Russia will attempt to meddle in future elections, as soon as the midterms in November 2018[1]. The Secure the Election initiative is a bipartisan effort led by Synack, the leader in crowdsourced security testing, to bring together the best American security talent and tools to help our states build their attacker resistance. We believe that the best security comes from a united effort.

Together, we are offering states a pro bono crowdsourced security testing solution that augments security teams' efforts to find and fix security vulnerabilities in election systems before they can be exploited by the adversary. The majority of states have under 15 FTEs on their enterprise security teams, with <7% of states able to conduct third party penetration testing more than annually[2]. Synack's crowdsourced security testing solution augments internal security teams with scale and provides on-demand testing and an assessment of security risk from an adversarial perspective.

What We Test

Voter registration databases are a prime target for attackers. If exploited, an attacker could add, alter, or delete voter records, fundamentally affecting the outcome of the election. In 41 states, these systems are over ten years old, making them especially vulnerable to attack[3]. The National Association of Secretaries of State have flagged voter registration systems as a priority for upgrade[4].

This crowdsourced security testing solution looks for vulnerabilities in remotely-accessible voter registration databases and online voter registration websites from a hacker's perspective. We discover vulnerabilities left undetected by other solutions and help to remediate them before the election and before exploitation by the adversary.

We look for:

- Which servers are connected to the internet?
- Does online voter registration connect to the voter registration database (VRDB)?
- Can admin access be gained? Can accounts be edited?
- Can VRDB be accessed through a 3rd party system (e.g., HHS, DMV)?

What you can expect from a Synack crowdsourced security test:

- **Trust:** Full control & visibility
- **Efficiency** 24 hours to deploy, 24 hours to find severe vulnerabilities, 24 hours to triage
- **Quality:** >95% signal-to-noise ratio
- **Coverage:** >200 testing hours & 100s of security researchers in a 2-week test
- **Results:** Real-time analytics on results and asset hardness relative to peers
- **Partnership:** Force multiplier for your security teams

[1] "Russia 'will target US mid-term elections' says CIA chief," BBC, http://www.bbc.com/news/world-us-canada-42864372.

[2] 2016 Deloitte-NASCIO Cybersecurity Study.

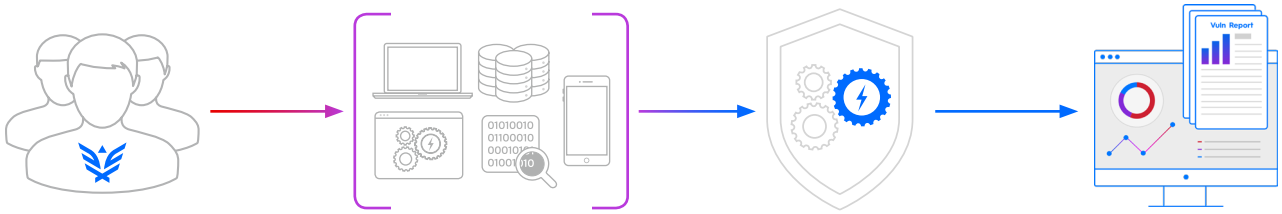
[3] Final Report, Congressional Task Force on Election Security, January 2018.

[4] Final Report, Congressional Task Force on Election Security, January 2018.

Synack

How Crowdsourced Security Testing Works

Synack, government's most trusted Crowdsourced Security Testing provider, uses a secure platform, vetted crowd of the top security researchers in the world and technical controls to provide the most effective and efficient testing solution with the least amount of risk. This approach was born out of our founders' offensive cyber experience at the NSA and has been engineered by top Silicon Valley talent.



Trusted Crowd of Security Researchers

5 step vetting process accepts only 10% of security researcher applicants:

1. Application Review
2. Behavioral Interview
3. Skill Assessment
4. Trust Assessment (Background & ID checks)
5. Continuous Monitoring

FVEY & SF-85P cleared researcher groups are available for government projects

Secure Platform

- Researchers must connect through Synack's secure gateway
- Synack tracks researcher activity & movement

Managed Testing

- Client scopes digital assets for testing and sets rules of engagement
- Synack's proprietary scanner conducts reconnaissance on the attack surface to increase researcher efficiency
- Researchers test through the secure platform
- Researchers report vulnerabilities through the platform

Real-time Results

- Synack triages and prioritizes all vulnerabilities and shares findings in real time via the Client Portal
- Findings are shared with clients in real time via the Client Portal
- Synack researchers work with security teams to remediate rapidly

TRUSTED BY:

DoD & Civilian Agencies

F500 Banks & Credit Card Companies

Technology

Healthcare

eCommerce

> "Synack's professionalism and our partnership during this program have provided immense value."
>
> —Synack Government Customer

Terms & Conditions of the Secure the Election Pro Bono Offer:

This offer is available to U.S. state governments only (including Synack's existing state and local government customers). Each eligible recipient will be limited to one (1) free 14-day Synack Crowdsourced Vulnerability Discovery Test of an online voter registration website or remotely-accessible database that is expected to be used in the November 2018 mid-term election. Any website or database submitted for testing must be approved by Synack, such approval may be withheld at Synack's sole discretion. Each test must be concluded by or before November 6, 2018 and will be subject to Synack's standard terms and conditions. Synack reserves the right to cease or change this offer at any time.

Frequently Asked Questions

Who is Synack?

Synack was founded in 2013 by Jay Kaplan and Mark Kuhr, two former NSA operators. They saw firsthand the ease with which defenses could be bypassed to gain access to assets. From lessons learned, they developed a methodology to attract, vet, and retain the world's best researchers and built a patented testing platform for them to connect to government and enterprise environments and securely discover and help fix vulnerabilities before adversaries can exploit them.

What's the typical profile of a Synack researcher?

The average security experience of a Synack researcher is 9 years. Common job titles are Senior Security Engineer, Application Security Specialist, Security Architect. Common certifications are CEH, OSCP, GIAC, OSCE, and CISSP. Synack has established a highly selective 5-step vetting process which includes multiple skill assessments, interviews, identity verification, background checks, and social media monitoring. Typically, <10% of applicants to the Synack Red Team are accepted based on Synack's skill and trust standards.

What does Synack test?

Synack tests web apps, mobile apps, host infrastructure, and cloud-based apps and infrastructure.

What's involved from our security team?

The Synack Mission Operations Team fully manages every crowdsourced security test that it conducts. This includes 24/7 program management and support, noise removal and risk reduction through 24-hour triage of all findings, performance tracking and benchmarking, and managing the crowd of Synack researchers (the Synack Red Team), including communications, payouts, and maintaining high levels of engagement. We are a force multiplier - we do what your teams should not have to.

How long does it take to start a program?

Synack offerings are cloud-based and can be activated within 24 hours. It takes 24 hours to deploy a program, 24 hours to find severe vulnerabilities on average, and 24 hours to triage findings. We also verify all patches within 72-hours to accelerate the remediation process.

How do I receive my results?

The Synack Platform provides one place for security teams to access information and analytics about their security testing in real time. Vulnerabilities flow through a logical, easy-to-use workflow from discovery to patch. Detailed coverage analytics, performance tracking and benchmarking, reporting and statuses are all available at a glance to understand your engagements. Reports from Synack are tailored to the client and can be customized and downloaded on demand. Reports include testing methodology, details, high-level summaries, and custom-written assessments from Synack's security experts.

Who are your clients?

Synack is the trusted provider of crowdsourced security testing to F500 companies and government agencies. Over 100 organizations have used Synack across the government (federal, state, and local), technology, financial services, e-commerce, and healthcare industries. To maintain the confidentiality and privacy of all of our customers, we do not disclose their names unless given written consent. However, we are happy to provide references upon request.

In October 2016, the Pentagon and Synack launched the Defense Department's first private bug bounty program. It took only four hours to find critical vulnerabilities in what was thought to be a hardened system, and Synack helped DoD security teams prioritize and remediate those vulnerabilities in real time. The value of Synack was expressed by the customer: "The professionalism of Synack and the partnership we have built during this program have provided immense value."

Synack, Inc.

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