bugcrowd

SPOTLIGHT: Government & Defense Cybersecurity

How the U.S. government uses crowdsourced security to keep data safe

Since the launch of the United States Digital Service (USDS) in 2014, the federal government has been entrenched in digital transformation efforts designed to keep pace with the shift to cloud-first architecture, increasing adoption of IoT, and always-on expectations of the American people. But as evidenced by **electoral breaches, sensitive data exfiltration, foreign state attacks, and disruption to critical infrastructure,** a shift in data delivery without equal attention to data security creates opportunity for exploitation. To help mitigate these risks, the Defense Digital Service (an agency of the USDS), took a bold step in 2016 by launching the federal government's first crowdsourced bug bounty program.

This spotlight highlights drivers behind an increased adoption of crowdsourced security, at the federal level, and provides an overview of how Bugcrowd is supporting the evolution of these programs across agencies and initiatives.

Case study: **U.S. Air Force**

What: The Common Computing Environment (CCE) provides enterprise-wide cloud environments to support current and future cloud-hosted applications for the U.S. Air Force.

Why: The migration (100+ applications) necessitated a crowdsourced approach to ensure continuous, consistent security testing

How: A three month Bug Bounty challenge consisting of six distinct testing phases

Results: From **March 18 - June 21, 2019** the CCE saw:

54
vulnerabilities

$123,000
paid out

$20,000
for most critical

"Bugcrowd's ability to dedicate resources on focused areas that we know are critical, was invaluable. The feedback loops, including retesting to make sure each vulnerability was fixed, were integral to our success."

- Lt. Stephen Cunningham, U.S. Air Force

Key testing initiatives for government customers:

- External assessment
- Source code analysis
- Cloud configuration and environment testing
- Internal network testing
- Application testing
- Social engineering

What's driving federal adoption?

1. In 2019, the White House released **$15 billion in cybersecurity funding** — a **$583.4 million increase (4.1%) over 2018.**
2. In the public sector, **79% of all breaches are executed by nation-state actors,** indicating a high level of sophistication and coordination.
3. Public sector breaches are more than **2.5 times more likely** to **remain undiscovered** for years due to lack of coordinated detection efforts across legacy systems
4. Across Bugcrowd hosted government and defense targets, more than **33% of all submissions** are classified as **P1 or P2 vulnerabilities -- the most critical.**

With increased adoption of crowdsourced security in the federal sector, a steady shift toward a **"defend forward"** mindset is becoming more and more evident; and it's not just for the benefit of public entities. Thanks to several regulatory requirements stipulating the publication of such initiatives, private enterprises are becoming increasingly exposed to best practices driven by their public counterparts.

Government systems, both internal and external, hold some of the most precious data available. Bugcrowd enables government agencies to test and proactively assure the security, scale, and performance of their networks and communications on a continuous basis.

"Expanding our crowdsourced security allows us to build a deeper bench of tech talent and bring more diverse perspectives to protect and defend our assets."

Chris Lynch, Director of the Defense Digital Service

"The DoD's strategy mandates that we defend forward...We must be active because inaction on our part cedes advantage to capable adversarries willing to flout international law and impose their own norms of cyber conduct."

General Paul Nakasone, Commander, US Cyber Command @Senate Committee Feb 14, 2019

Trusted by Leading Companies Around the World

mastercard. ATLASSIAN TESLA FCA FIAT CHRYSLER AUTOMOBILES NETGEAR Square cisco Meraki SAP Concur

Learn why government entities are turning to Bugcrowd:
https://www.bugcrowd.com/solutions/government/