Defending the Federal Government from Cyber Attacks

A Model Every Organization Can Learn From

hackerone

Introduction

The U.S. Department of Defense (DoD), in a first for the U.S. Federal Government, invited white hat hackers to find security flaws in systems run by the Pentagon, Air Force, and Army. What they learned helped the DoD bolster their cyber defenses and prove the benefits of hacker-powered security to a wide range of government agencies — and organizations like yours!

Hack Us!

In April 2016, the DoD took a bold step: they launched the first bug bounty program in the history of the Federal Government. It was just a month-long program, but it was the start of a flurry of activity from other government agencies who not only launched more hacker-powered security programs, but published guidance on how to leverage this powerful tool in the fight against cyber attacks.

Today, agencies as diverse as the Federal Trade Commission, the Food and Drug Administration, and the U.S. Air Force are recommending hacker-powered security or using it internally to improve their own security. And, they're all serving as models for how any organization, public or private, can use hackers to make their systems, networks, hardware, and software more secure.

"We need to understand where our weaknesses are in order to fix them, and there is no better way than to open it up to the global hacker community."

CHRIS LYNCH

Director of Defense Digital Service

Photo by Stephanie Dreyer

It Began with Hack the Pentagon

ASH CARTER
Former U.S. Secretary of Defense

Hack the Pentagon was a security initiative taken by the DoD's Defense Digital Service (DDS) team. Launched as a bug bounty pilot program, it gained support from then Secretary of Defense Ash Carter, and, according to DDS, exceeded all expectations.

Hack the Pentagon was designed to identify and resolve security vulnerabilities within the Defense Department's public-facing websites. The first report was submitted 13 minutes after launch, and within 6 hours, that number grew to nearly 200.

Over the course of the 24-day program, more than 1,400 hackers registered to participate, with 250 working to submit a new report every 30 minutes on average. As part of the HackerOne program, DDS leveraged HackerOne's triage services, which allowed the DDS security team to focus on resolving valid reports.

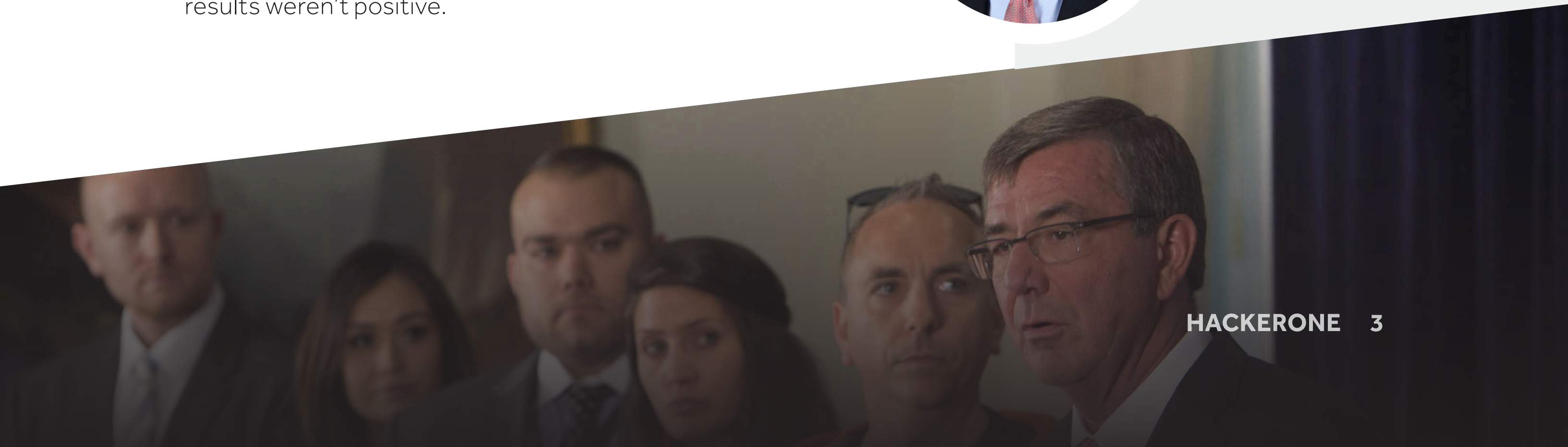
SUPPORT FROM ABOVE

Such a rapid commitment to hacker-powered security would not have been possible without an unwavering belief in the power of HackerOne's platform and talented community of hackers.

"By allowing outside researchers to find holes and vulnerabilities on several sites and subdomains, we freed up our own cyber specialists to spend more time fixing them than finding them," said former Secretary of Defense, Ash Carter. "The (program) showed us one way to streamline what we do to defend our networks and correct vulnerabilities more quickly."

The DoD is trailblazing a path to make society safer, and has taken the opportunity to be a leader in working with security researchers. And with Hack the Pentagon, the DoD created a model for others to follow, including other government agencies. But it wouldn't have been deemed a success if the results weren't positive.

> ***"What Hack the Pentagon validated is that there are large numbers of technologists and innovators who want to make contribution to our nation's security, but lack a legal avenue to do so."***
>
> *ERIC FANNING*
> Former Secretary of the Army



STRONGER RESULTS

Of the valid reports submitted during Hack the Pentagon, 138 were found to be "legitimate, unique and eligible for a bounty," earning hackers a combined $75,000 in total bounty rewards.

TIME TO FIRST VULNERABILITY REPORT

13 MINUTES

HACKERS REGISTERED TO PARTICIPATE

1,410

REPORTS SUBMITTED IN FIRST 6 HOURS

200

BOUNTIES PAID

$75,000

The power of a bug bounty program lies in the large number of diverse and highly skilled hackers looking at the code, and for Hack the Pentagon, reports poured in from 44 states and from US expert participants based as far away as Japan, Germany, and England. There was even a wide range of ages participating, with the youngest hacker to receive a bounty aged 14 and the oldest aged 53.

Over 138 unique software vulnerabilities were resolved. An SQL Injection issue was the most severe and earned $3,500 as the highest individual bounty. The average bounty was $588 with the top earning hacker making a total of $15,000 from this program.

But Hack the Pentagon was just the beginning.

Then Hack the Army ...and More

Within months of the successful Hack the Pentagon program, the DoD expanded their relationship with HackerOne to extend 3 years and provide hacker-powered security to multiple departments. Their next program, Hack the Army, was driven by Secretary of the Army Eric Fanning.

As the most ambitious federal bug bounty program to date, Hack the Army targeted operationally significant websites, including those mission critical to recruiting. The program aimed to engage with the diverse talent of the hacker community and supplement the existing security efforts of the Army red teams and the DDS.

Running little more than 3 weeks, the program's results were nothing less than spectacular.

Read more on our blog

TIME TO FIRST VULNERABILITY REPORT

5 MINUTES

ELIGIBLE HACKERS PARTICIPATING

371

TOTAL REPORTS RECEIVED

416

BOUNTIES PAID

$100,000

HACK THE ARMY
BY THE NUMBERS
Registered eligible participants 371
Total reports received 416
Total valid reports 118
Total time it took to receive first vulnerability report 5 minutes

HACKER CREATIVITY BEATS AUTOMATION

Beyond the overall success of Hack the Army, an extremely critical vulnerability was discovered by a hacker who creatively chained together a series of bugs. Exploiting the combination of vulnerabilities provided access to an internal DoD website that should have required special credentials. An open proxy enabled access to the network, but only a highly skilled hacker could recognize the several independent flaws underlying the vulnerability. Automation alone is rarely capable of such leaps of logic, and likely would not have highlighted this complex issue.

The Army remediation team, as well as the Army Cyber Protection Brigade, acted fast to block any further attacks and ensure there was no way to exploit the chain of vulnerabilities.

"I'm done with being afraid to know what our vulnerabilities are. That's not okay."

CHRIS LYNCH

Director of Defense Digital Service

VULNERABILITY DISCLOSURE: MODERN APPLICATION SECURITY 101

Shortly after Hack the Army was announced, and in a first for the U.S. government, the DoD introduced a Vulnerability Disclosure Policy (VDP) on HackerOne. The VDP gives hackers clear guidance on how to legally test for and disclose vulnerabilities in DoD's public-facing websites, including those outside of the other time-bound challenges.

In the past year, the DoD has thanked over 360 hackers for disclosing potential vulnerabilities, and has maintained an average time to first response of just 2 days.

You can learn more and read their full vulnerability disclosure policy here.

"The return on investment is incredible, both in terms of cost and in terms of making government assets more secure."

HUNTER PRICE

Director of Air Force Digital Service

Now Hack the Air Force

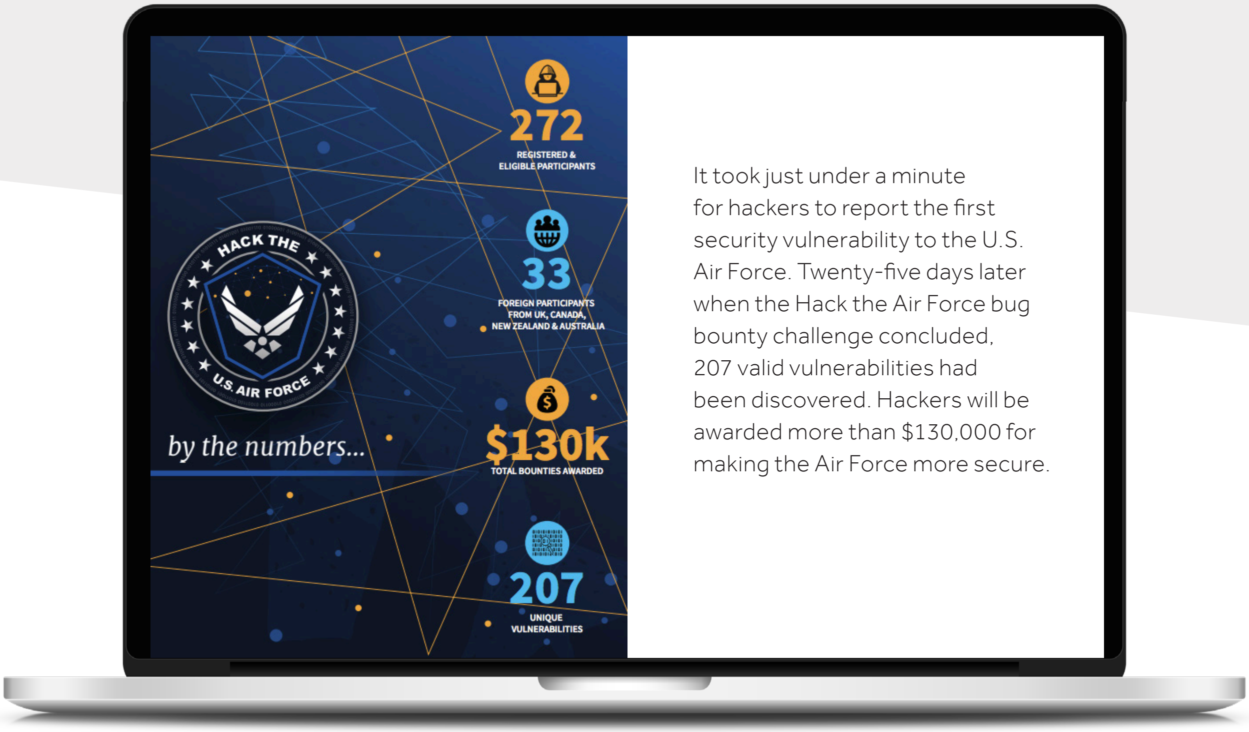
Next on the docket for the DoD was Hack the Air Force, which was their largest program of the time and which expanded to include participants from partner nations Australia, Canada, New Zealand, and the United Kingdom. As the biggest federal bug bounty program to date, Hack the Air Force targeted operationally significant websites and online services. The goal was to explore new approaches to security and to adopt the best practices used by the most successful and secure software companies in the world.

Again, support from the top netted both awareness and validity to their hacker-powered security efforts. The program was announced by Air Force Chief Information Security Officer Peter Kim at HackerOne headquarters, with Kim disclosing that "this was the first time the Air Force opened its networks to such broad scrutiny."

"We have malicious hackers trying to get into our systems every day," Kim added. "It will be nice to have friendly hackers taking a shot and, most importantly, showing us how to improve our cybersecurity and defense posture. The additional participation from our partner nations greatly widens the variety of experience available to find additional unique vulnerabilities."

With programs like Hack the Air Force, the DoD is redefining American defenses in the digital era. But, as with every new initiative, success relies on results.

Read more on our blog



It took just under a minute for hackers to report the first security vulnerability to the U.S. Air Force. Twenty-five days later when the Hack the Air Force bug bounty challenge concluded, 207 valid vulnerabilities had been discovered. Hackers will be awarded more than $130,000 for making the Air Force more secure.

HIGH-FLYING RESULTS

Hack the Air Force instantly became the most successful government-run, hacker-powered security program in history, nearly doubling the results of the first Hack the Pentagon program from a year prior. Running for most of June 2017, the program resulted in 207 discovered vulnerabilities, the first of which was reported in less than a minute. Within the first 24 hours, 70 reports were submitted, 23 of which were valid.

Kim and his team were more than prepared, with some reports getting responses in less than a minute. Over the 25-day program, the average response time was 8 hours and the average time to resolution during the challenge was just 4 days.

On the hacker side, 33 participants came from outside the U.S., and a 17-year-old from Chicago earned the largest total sum for 30 discoveries.

"Adversaries are constantly attempting to attack our websites, so we welcome a second opinion — and in this case, hundreds of second opinions — on the health and security of our online infrastructure," said Kim. "By engaging a global army of security researchers, we're better able to assess our vulnerabilities and protect the Air Force's efforts in the skies, on the ground and online."

With the unprecedented success of the Air Force bug bounty pilot program, coupled with the success of Hack the Pentagon and Hack the Army, the DoD has plans for at least 17 more hacker-powered security events.

Beyond the DoD, the success of these and other programs has not only legitimized hacker-powered security, it's created a flood of support for bug bounty and vulnerability disclosure programs.

TIME TO FIRST VULNERABILITY REPORT

1 MINUTE

ELIGIBLE HACKERS PARTICIPATING

272

TOTAL VULNERABILITIES DISCOVERED

207

BOUNTIES PAID

$130,000

"The ideal end-state is that bug bounties become a regular, common tool in securing all IT assets across the Department of Defense. We will always have security vulnerabilities. We can approach that reality of one of two ways: we can deny it, or we can be proactive, open to it and use every tool in our toolbox to remediate or mitigate them. "

HUNTER PRICE

Director of Air Force Digital Service

Expanding Across the Federal Government

As hacker-powered security takes hold in the private sector, government entities are following the DoD's lead in expanding the use of these valuable programs. The entry point for most organizations are vulnerability disclosure policies and programs designed to help improve security and reduces risk.

In keeping with the government angle, VDPs are often compared to the U.S. Department of Homeland Security's "If You See Something, Say Something" program, which implores citizens to alert authorities when they "see something you know shouldn't be there." VDPs serve the same purpose by giving people a way to report the "something" that seems amiss.

Since software, hardware, and other cyber security issues generally require a high level of technical expertise to even notice, let alone understand, those who see the issues often have the skills to also exploit them, if they so choose. While some see VDPs as a fast-track to finding and fixing vulnerabilities, others — especially many in conservative government agencies — see it as inviting unknown actors with unknown motivations to snoop around websites and products.

But more and more federal entities are beginning to embrace ethical hackers, and are even pushing public- and private-sector organizations to actively consider and implement VDPs. The National Telecommunications and Information Association (NTIA) organized a multi-stakeholder process for Coordinated Vulnerability Disclosures. The Federal Trade Commission (FTC) released a "Start with Security" guide, which recommends implementation of a VDP. And the Cybersecurity Unit of the Department of Justice developed a framework for VDPs.

> *"Automotive industry members should consider creating their own vulnerability report/disclosure polities, or adopting polities used in other sectors or in technical standards. Such polities would provide any external cybersecurity researcher with guidance on how to disclose vulnerabilities to organizations that manufacture and design vehicle systems."*
>
> *NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION (NHTSA)*
>
> "Cybersecurity Best Practices for Modern Vehicles"

> *"(Medical device) Manufacturers should adopt a coordinated vulnerability disclosure policy."*
>
> *FOOD AND DRUG ADMINISTRATION (FDA)*
>
> "Management of Cybersecurity in Medical Devices"

> *"The lesson for other business? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security(@) your company.com) for receiving reports and flagging them for your security staff."*
>
> *FEDERAL TRADE COMMISSION (FTC)*
>
> "Start with Security"

PUBLIC OR PRIVATE, VDPS ARE TABLE STAKES

The expectation of implementing a VDP has grown to include ISO/IEC 29147, which specifically covers vulnerability disclosures. The standard provides guidelines for vendors on how to receive information about potential vulnerabilities, how to disseminate resolution information, and provides examples of content that should be included in a policy.

All of this and more has led private-sector companies like Adobe, General Motors, and New Relic to leverage VDPs to improve their security posture. Some of these programs collect hundreds of bug reports per quarter, with up to two-thirds of those reports being confirmed as valid and previously-unknown, which are subsequently fixed.

But not everyone is working to close their security gaps. According to the Hacker-Powered Security Report 2017, 94 percent of the Forbes Global 2000 do not have known vulnerability disclosure policies, even with prodding from government agencies.

STRIKE BACK WITH BUG BOUNTIES

After implementing a VDP, the next step in utilizing hacker-powered security is a bug bounty program. These programs are exploding across nearly every private-sector industry, with close to 50,000 security vulnerabilities being resolved by customers on HackerOne since 2014, and over 20,000 in 2016 alone. In total, customers on HackerOne have paid out more than $20 million in bug bounties.

Growth in the public sector is slower, but growing. The General Service Administration's Technology Transformation Service (TTS) recently launched the first bug bounty program administered by a civilian federal agency. By taking the learnings of the DoD's time-bound programs, TTS created an ongoing bounty program more typical of non-governmental organizations.

In their first month, TTS paid out nearly $7,000 in bounties for 19 resolved reports. They thanked 15 hackers in that same time, with individual bounties ranging from $150 to $2,000.

Getting Your Organization Started

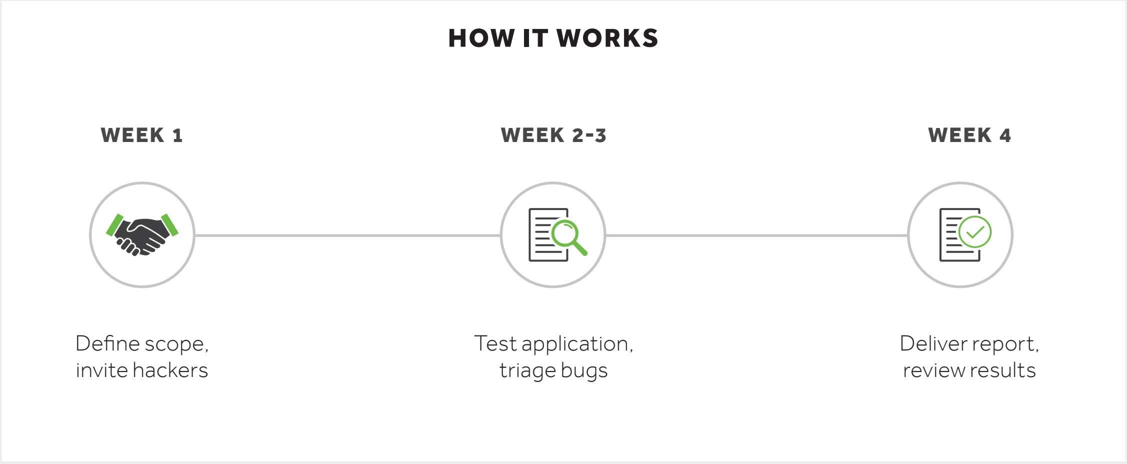
Putting a VDP in place is the first step in leveraging hacker-powered security for any organization, regardless if it's a small private company, a large global enterprise, or a government entity. Then, move on to time-bound bounties, hacker-powered alternatives to penetration tests, or a continuous bounty program.

FIRST, PUBLISH A VDP

To get started, check out HackerOne's "VDP Basics", a complete guide for crafting an effective vulnerability disclosure policy. Or, learn more about HackerOne Response, a turnkey solution to help organizations receive, respond to, and resolve security vulnerabilities discovered by third-parties.

NEXT, DIP INTO BOUNTIES

Time-bound programs, like Hack the Pentagon, offer an alternative to traditional penetration testing. HackerOne Challenge provides a private, turnkey program with a focused scope and a finite length. It's an easy way to dip a toe into hacker-powered security, and it's cost-effective: hackers are paid for valid results, not man-hours. That means hackers are incentivized to find the issues with the biggest bounties, which directly correlates to the most value to you and to them.



HOW IT WORKS

WEEK 1

Define scope, invite hackers

WEEK 2-3

Test application, triage bugs

WEEK 4

Deliver report, review results

The typical HackerOne Challenge is a discreet, one month engagement with HackerOne's best hackers, and comes with a detailed summary report with complete results.

Start Your Hacker-Powered Security Journey Today

REQUEST A HACKERONE DEMO

Peter E. Kim, CISO U.S. Air Force

Photo taken at HackerOne's San Francisco Headquarters