Distributed Defense: How Governments Deploy Hacker-Powered Security

Government agencies around the globe trust HackerOne to manage their hacker-powered security programs

hackerone

Government voices are supporting hacker-powered security for their agencies and related organizations.

The U.S. Department of Justice recommends vulnerability disclosure policies, both the European Union and the Ministry of Justice and Security in the Netherlands encourage responsible disclosure, and U.S. Senators have introduced legislation to support hacker-powered security.

Increased Adoption by Government Agencies Implementing Bug Bounty and Vulnerability Disclosure Programs.

The European Commission recently selected HackerOne as the platform for their first ever bug bounty program. The U.S. General Service Administration's Technology Transformation Service (TTS, aka 18F) launched the first bug bounty program run by a civilian federal agency. And even traditionally secretive and high-security organizations are leveraging HackerOne to identify and mitigate bugs before they can be exploited. From the U.S. Department of Defense (DoD) to Singapore's Ministry of Defence (MINDEF), defense departments are using a global community of white-hat hackers to help them make their data and systems more secure.

THE PENTAGON USES HACKERONE

The U.S. Department of Defense, arguably the most security-aware organization on the planet, has used the HackerOne platform to resolve more than 3,000 vulnerabilities in less than two years. Programs like Hack the Pentagon, Hack the Army, and Hack the Air Force have helped the DoD secure and protect sensitive data and systems with the help of HackerOne's community of diverse, creative, and expert hackers.

> "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**

GOVERNMENTS ACROSS THE WORLD EMBRACE HACKER-POWERED SECURITY

HACK THE PENTAGON

HACKERONE CHALLENGE | APRIL–MAY 2016

The U.S. Department of Defense made the move into hacker-powered security with the first bug bounty program for the federal government. Read more

1,400+	13 MINUTES	$75,000	138
Hackers Registered	First Report	Bounties Paid	Valid Reports

U.S. DEPARTMENT OF DEFENSE

HACKERONE RESPONSE | LAUNCHED NOVEMBER 2016

After Hack the Pentagon, DoD had noticed that bugs were still being submitted. So the feds announced an open-ended Vulnerabilities Disclosure Policy that didn't offer rewards, but would legally allow people to submit bugs any time related to public-facing websites and web applications owned by DoD.

650+	3,000+
Hackers Participating	Vulnerabilities Resolved

HACK THE ARMY

HACKERONE CHALLENGE | NOVEMBER–DECEMBER 2016

Building on the Pentagon's success, this program targeted operationally significant websites including those mission critical to recruiting. Read more

371	5 MINUTES	$100,000	118
Hackers Participating	First Report	Bounties Paid	Valid Reports

HACK THE AIR FORCE

HACKERONE CHALLENGE | MAY–JUNE 2017 & DECEMBER 2017–JANUARY 2018

Expanded the Pentagon's hacker-powered initiatives to include non-U.S. participants and an increased bounty budget. Read more

275+	1 MINUTE	$233,883	313
Hackers Participating	First Report	Bounties Paid	Valid Reports
with 30 from outside U.S.		*($130,000 + $103,883)*	*(207 + 106)*

EU-FREE AND OPEN SOURCE SOFTWARE AUDITING (EU-FOSSA) PROJECT

HACKERONE CHALLENGE | DECEMBER 2017

The European Commission's first ever bounty program, designed to protect critical EU software in the aftermath of the Heartbleed incident. Read more

SINGAPORE MINISTRY OF DEFENCE (MINDEF)

HACKERONE CHALLENGE | DECEMBER 2017–JANUARY 2018

Singapore's first crowd-sourced security initiative and the first program of its kind by a government agency in Asia. Read more

GENERAL SERVICE ADMINISTRATION'S TECHNOLOGY TRANSFORMATION SERVICE

HACKERONE BOUNTY | LAUNCHED AUGUST 2017

The first-ever bug bounty program for a civilian federal agency in the U.S. Read more

Hacker-Powered Security Delivers Quick Results.

The DoD's first-ever hacker-powered security challenge, Hack the Pentagon, was designed to identify and resolve security vulnerabilities in public-facing websites. Over the course of the 24-day program, more than 250 vetted hackers found 138 validated bugs and earned more than $75,000 in bounties. The results of these early DoD programs were so successful, the DoD quickly expanded their relationship with HackerOne to extend 3 years and provide hacker-powered security to multiple departments.

> "We need to move to a world...where all companies providing internet services and devices adhere to a vulnerability disclosure policy."
>
> **JULIAN KING**
> **SECURITY UNION COMMISSIONER, EUROPEAN COMMISSION**

During Hack the Army, more than 370 hackers combined to submit over 400 bug reports and earned more than $100,000 in bounties. For Hack the Air Force, nearly 300 hackers discovered more than 200 vulnerabilities, earning $130,000. And for the second iteration of Hack the Air Force, the DoD paid $103,883 in bounties to white-hat hackers for 106 vulnerabilities found in just 20 days.

In Singapore, the results were similarly fast and impactful. In just 3 weeks, MINDEF received 35 unique vulnerability reports and awarded $14,750 in bounties to 17 trusted hackers. MINDEF also leveraged the global community, with Singaporean hackers joined by others from India, Romania, Canada, Russia, Sweden, Ireland, Egypt, Pakistan, and the U.S.

"The success of the program helped us boost our cybersecurity in a matter of weeks," said Mr David Koh, Deputy Secretary (Special Projects) and Defence Cyber Chief at Singapore's Ministry of Defence.

Hacker-Powered Security Helps Save Millions of Dollars While Improving Cybersecurity.

In a single, month-long HackerOne Challenge, the U.S. Department of Defense paid roughly $150,000 in bounties, yet saved nearly a million dollars in the process. "If we had gone through the normal process of hiring an outside firm to do a security audit and vulnerability assessment, which is what we usually do, it would have cost us more than $1 million," said Ash Carter, U.S. Secretary of Defense at the time of the program.

"The return on investment is incredible, both in terms of cost and in terms of making government assets more secure," said Hunter Price, Director of Air Force Digital Service

> "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**

Hacker-powered security enables governments to utilize modern and cost effective security efforts. It's a proven approach to improving the security posture of any agency or organization.

"We have malicious hackers trying to get into our systems every day," said Air Force Chief Information Security Officer Peter Kim before Hack the Air Force began. "It will be nice to have friendly hackers taking a shot and, most importantly, showing us how to improve our cybersecurity and defense posture."

Start With Disclosure, Then Move to Bounties.

Getting started with hacker-powered security is simple, methodical, and can fit any needs or any pace. Putting a vulnerability disclosure policy (VDP) in place is the first step in leveraging hacker-powered security for any organization, public or private. 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.

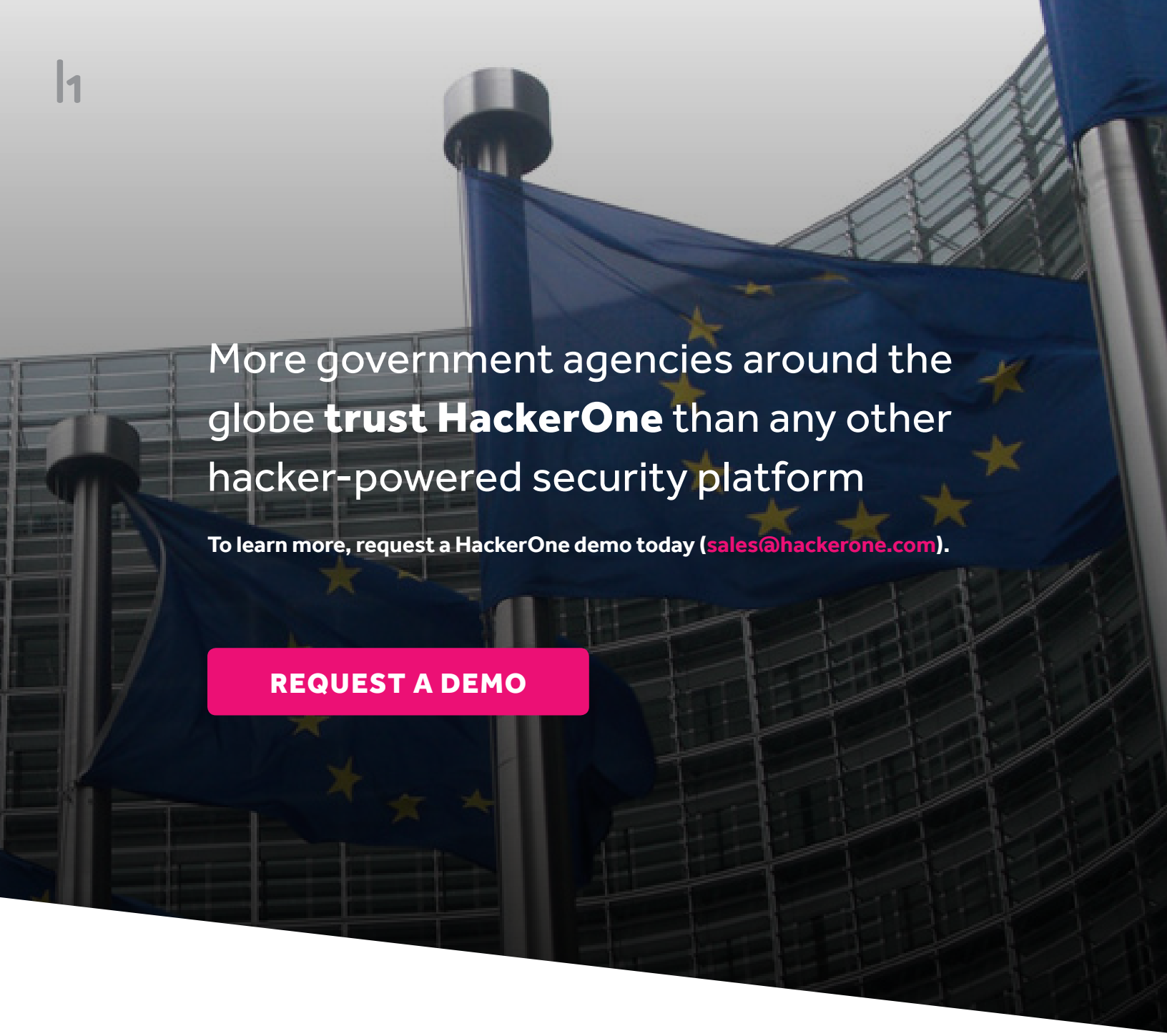
> "Companies should communicate and coordinate with the security research community as part of a continuous process of detecting and remediating software vulnerabilities."
>
> **U.S. FEDERAL TRADE COMMISSION**

A continuous bug bounty program, like 18F, brings a proactive approach to finding vulnerabilities across every critical surface. HackerOne Bounty enables agencies and organizations to leverage the power of the global hacker community along with the expert services of HackerOne. Using internal resources, HackerOne's professional services team, or a combination of both, a continuous bug bounty program quickly scales and expands the reach of every security team.

Conclusion

The global community of white-hat hackers exists to make the internet safer. An oft-used hashtag for the community is #TogetherWeHitHarder, which speaks to both the benefits of hacker-powered security and the nature of their intent. The more than 160,000 hackers in the HackerOne community contribute to an overall safer internet, and they do it faster, less expensively, and more effectively than alternative means.

Government entities, agencies, and departments of all sizes can benefit from hacker-powered security, whether it's to attack a pinpoint challenge, instill a broad and persistent security apparatus, or anything in between.



More government agencies around the globe **trust HackerOne** than any other hacker-powered security platform

To learn more, request a HackerOne demo today (sales@hackerone.com).

REQUEST A DEMO

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

European Commission

YANG PERTAMA DAN UTAMA
MINDEF
SINGAPORE

HACK THE PENTAGON

HACK THE ARMY

HACK THE AIR FORCE

TTS BUG BOUNTY