HACKERONE CONGRATULATES THE DEPARTMENT OF DEFENSE ON 11K VULNERABILITY REPORTS

Oct 22 2019 HackerOne SHARE

HackerOne and the U.S. Department of Defense began working together in 2016 with the launch of Hack the Pentagon. Announced at the third annual Security@ San Francisco, in three short years, hackers discovered 11,000 valid vulnerabilities exclusively through the organization's Vulnerability Disclosure Program (VDP). Congratulations to the Department of Defense and all the hackers that made the internet safer one bug at a time.

We sat down with Kris Johnson, Director of the VDP, U.S. Department of Defense, to learn more about trailblazing hacker-powered security, what it’s like working with hackers, the impact on company culture, notable moments over the years, lessons learned, and more. Here’s a glimpse into our conversation.

Q. The Department of Defense was the first branch of the U.S. government to use white hat hackers back in 2016. What drove that trailblazing decision?

A. I think that the decision really boiled down to the Department recognizing the awesome capability and collective power of the white hat researcher community. The innovative minds within the Department, including Defense Digital Service (DDS), Office of the Under Secretary of Defense for Policy, DoD Chief Information Officer (CIO), and DoD Cyber Crime Center (DC3), to name a few, saw first-hand how successful vulnerability disclosure programs were in the private sector and wanted to replicate that on one of the largest networks in the world.

Q. Why was the VDP an important part of the “Hack the Pentagon” initiative from the beginning?

A. "Hack the Pentagon", as well as all of the subsequent Bug Bounty events, have been phenomenally successful and expertly run by our partners at the DDS and HackerOne. The Department understood up front that they are inherently limited in length (1-4 weeks), one-off events, and have a narrowly defined scope. The DoD VDP was planned from the beginning because it has a different objective than Bug Bounty events. They knew that we needed to have a door open to the researcher community 24/7/365, and allow the submission of vulnerabilities found on ANY DoD website to VDP. With the immense scale of the DoD's attack surface it is critical to keep the lines of communication open and a remediation process to address vulnerabilities to researchers on a permanent basis.

A. We have seen a paradigm shift in the Department's acceptance of crowdsourcing cybersecurity work in order to more effectively secure our networks. Most of us grew up in a time when "hacker = only bad guys/gals". However, that is no longer the case. Initiatives like Bug Bounties, VDP, and hacking events like the F-15 at DEFCON this past year, continually demonstrate a world-class capability of the researcher community to discover vulnerabilities that our internal DoD Components haven't. The amazing results cannot be ignored, and we must continue to find ways to partner with the researcher community to illuminate critical DoD information technology system and network vulnerabilities.

Q. Have there been any notable vulnerabilities reported that have especially impressed the team that we can highlight? (We've done this for past bug bounty announcements)

A. The list is extensive, but the two best vulnerability reports to highlight are with the U.S. Army Aviation and Missile Research Development and Engineering Center's Safe Access File Exchange (AMRDEC SAFE) and the Defense Finance and Accounting Services (DFAS) myPay sites. The VDP superstar researcher, Jack Cable, discovered and disclosed them to the DoD VDP within the past 12 months. AMRDEC SAFE allowed two-factor authentication bypass due to an insecure download cookie generation vulnerability; giving an unauthorized user full file access across the entire site. It took several months for the vulnerability to get mitigated, and led to the development of the more modern DoD SAFE enterprise service. In May 2019 the newly redesigned myPay site was launched with several critical and high-severity vulnerabilities. Jack Cable discovered an improper authentication vulnerability which allowed for a full account takeover as well as the plaintext storage of passwords. To date, the DoD VDP program has yielded over 10,000 cases, left unaddressed, the damage to DoD Warfighters, if exploited by our adversaries, would be catastrophic.

Q. What has the DoD's experience been working with the hacker community?

A. Our experience with the hacker community has been nothing short of remarkable. November 2019 will be the three-year anniversary of DoD VDP, and the partnerships and relationships that we have built over this time are amazing. We communicate with the researchers daily through the HackerOne platform, Twitter, and email. We know many by name, and have watched some part time researchers hone their hacking skills to the point of making it their full-time job. At the end of the day our door is always open to them, and we continually strive to find innovative ways to keep the program fresh and beneficial for the researchers.

Q.What has most impressed or surprised the DoD team about the hacker or security researcher community?

A. Easily the most impressive aspect of the security researcher community is its growing diversity. We are seeing more females entering what was a predominately male-dominated field. Women like Alyssa Herrera, Katie Moussouris, Kimber Diaz, Amit Elazari, Chloé Messdaghi, and Reina Staley (to name a few) are making real-world impacts in the cybersecurity field. The DoD VDP team has been fortunate to have them as trusted partners, and we look forward to continuing our work together to secure the DoD.

Q. More than two years into the program, what have been the biggest lessons learned?

A. The two biggest lessons learned for the DoD VDP are things that occur behind the scene; implementing a mature remediation process and developing a unified vulnerability management platform.

The remediation process starts with a formalized Concept of Operations (CONOPS). The DoD VDP CONOPS is a document that describes the intent of the program, measures of success, and defines the roles and responsibilities of each organization. This provides the foundation for each organizational Standard Operating Procedure (SOP) to be built from. The VDP SOP describes a step-by-step methodology for how each function will be performed. This creates a consistent, repeatable, and accurate process for which all team members can easily follow. Additionally, DoD views it is as a living document that is constantly updated to reflect the changes necessary to better perform the mission. For example, DoD is currently considering expanding authorities (and scope) to increase the applicability and adoption of VDP across the Department.

The unified vulnerability management platform is another huge lesson learned for the DoD VDP. The DoD Cyber Crime Center (DC3) has some tremendously capable software developers that created the Vulnerability Report Management Network (VRMN). Prior to VRMN we had a slow and archaic method of tracking vulnerabilities through SharePoint, spreadsheets, and emails. This became an absolute nightmare to manage when our submission volume increased. The beauty of VRMN is the malleability of the commercial Jira platform. It is able to be highly customized to meet DoD’s requirements, scalable for future growth, and logs every single action and comment within each report. It also gives us the ability to create executive-level dashboards, automatically produce reports, or get in the weeds and pull data-driven metrics. The implementation of VRMN has resulted in an 86% decrease in the amount of time VDP takes to perform the initial triage of each report. DoD is committed to pushing VRMN access further downstream to reduce the time between when a vulnerability is discovered to when it is mitigated by the system owner.

Q.What best practices would you like to share with those launching new crowdsourced security programs?

A. There are three best practices for those thinking about launching new crowdsourced security programs. The first is to establish a clear, easy to understand disclosure policy. Many of the researchers that participate in the DoD VDP are English as a Second Language (ESL) or don't speak English at all. Keep it simple! Second, is a standard best practice but will help with your crowdsourced security programs, and that is IT asset management. It is critical that you understand your network topology, IP space, public facing systems, hardware/software list, and system administrator contact information. The faster you can mitigate and award the researcher the better, and this will reduce the time to hunt down system specific information. Finally, you must always have an open communication channel with the researcher community. This will build trust, ensure that questions/issues are resolved quickly, and facilitate an increase in the overall effectiveness of the program. .

Q. How has the DoD changed its approach to security since the initial “Hack the Pentagon” program?

A. One change that we have seen is the inclusion of crowdsourced, hacker-fueled programs included alongside the more traditional security tools within the DoD's defense-in-depth strategy. The department fully embraces the fact that the security of our critical technologies, infrastructure, and data has been improved by the white hat community. I believe that you will continue to see more crowdsourced security programs and events being hosted by the DoD based upon all of the tremendous successes to date. Take for example the F-15 hacking efforts at this year’s DEFCON. The fact that a small group of hackers were able to uncover so many vulnerabilities in a critical aviation system speaks volumes to the need of including hackers into the DoD's cyberspace security strategy. The VDP researchers have uncovered almost 500 critical and high severity vulnerabilities on just DoD websites; a remarkable and noteworthy statistic! I do not believe that there is a better return on investment than these programs.

Q. How has the DoD’s conceptualization of the word “hacker” changed over the years? Why do you think that change occurred?

A. "Hacker" is no longer a four letter word in the DoD. The DoD's conception of a hacker today has been modernized from being just wayward kids in their mother's basement. We have hackers roaming the halls of the Pentagon, sitting in meetings, making decisions and presenting innovative ideas to improve the cybersecurity of the DoD. We train many of our Cyber warfighters in the ‘ways of the force’, and continually seek to employ hackers that want to protect our nation. The department also fully recognizes the capability of our adversary's hackers, and are investing resources to remain ahead of them in order to fight and win on the 21st century battlefield. The more successes that hackers demonstrate in programs like VDP and Bug Bounties the more the culture will continue to change.

Q.What are some future updates to VDP that we can expect to see in the next year?

A. VDP has several very interesting initiatives that we are looking to roll out in the next 12 months. We actually just published our inaugural version of the VDP Bug Bytes report. This is going to be a monthly and annual rollup of statistics, updates, and tips to benefit both the private and public sectors. As mentioned previously, DoD is pursuing the expansion of its scope from DoD websites to all DoD Information Systems. Since the program started in 2016 we have had hackers continually submit amazing but out of scope vulnerabilities on systems not covered within the existing policy.

Moving to a "see something, say something" approach will allow the researcher community to disclose anything that they find in the wild while being afforded the legal safe harbor to do so. VDP is also exploring ways to support the Defense Industrial Base (DIB) in order to better protect the DoD's supply chain. Finally, we are developing some monthly contests for the researcher community to foment more interest and competition in making DoD’s cyberspace more secure, with the winners receiving formal recognition, bragging rights, swag. The best place to stay up to date on these initiatives is our Twitter page @DC3VDP.

FOR BUSINESS