bugcrowd

CASE STUDY

U.S. federal agency chooses Bugcrowd for critical system security

The best solution to autonomously test their critical weapon systems applications for vulnerabilities, formulate patches, and deploy them in real time on network

The situation

A U.S. federal agency (listed anonymously in this case study) is responsible for billions of dollars in safety-critical equipment and missions. A single flaw in a system not only costs money, but puts their mission and lives at risk.

In 2018, the U.S. Government Accountability Office (GOA) reported that there were mounting challenges in protecting weapon systems from increasingly sophisticated attacks:

> **"This state is due to the computerized nature of weapon systems, the agency's late start in prioritizing weapon systems cybersecurity, and the agency's nascent understanding of how to develop more secure weapon systems. Weapon systems are more software dependent and more networked than ever before."**

The agency has moved to embrace cyber as a new domain of warfare, with that comes the requirement to check weapon systems' applications dynamically.

> **An expansion of a comprehensive software security solution into some of the most critical systems was needed across multiple branches of the agency.**

The agency's organizations buy separately and have different missions. Between multiple organizations and missions, there was an aligned need to create automatic defensive systems capable of reasoning about flaws, formulating patches, and deploying them on the network in real time with an accelerated time to value.

The challenge

- As weapon systems became increasingly software dependent and networked, the challenges in protecting the associated applications from increasingly sophisticated attacks grew.
- Once the need for additional software security testing was identified, it was difficult to find automatic defense systems capable of identifying vulnerabilities, formulating patches, and deploying them in real time on network.
- The delayed prioritization of weapon system security created a critical need to recognize cyber warfare as a new domain of conflict.
- The agency was left with a pressing need to find an autonomous software security solution with an accelerated time-to-value to address emerging weapon system security issues within select critical missions.

The Bugcrowd solution

The agency recognized a potential solution to the weapons system security problem in the original version of Mayhem Security, which was later acquired by Bugcrowd, featured in the Cyber Grand Challenge in 2016. They moved to apply Mayhem to select critical missions within the agency.

Mayhem's performance in the DARPA Cyber Grand Challenge showed fully autonomous security was possible. The key components that formulated its winning approach included:

- **Discovery/vulnerability identification:** Mayhem automatically found new vulnerabilities in commercial-off-the-shelf (COTS) software, even without developer participation.
- **Patching:** Mayhem automatically hardens programs.
- **Strategy:** The goal of cyber is to beat the attacker while still meeting mission and business objectives. Mayhem delivers by focusing on usability and integration into the development pipeline.

Bugcrowd "tests like a hacker" to find exploits. Bugcrowd is faster, more accurate, and less expensive than manual approaches and is truly automated, because it is not necessary for humans to double check the results.

The outcome

Mayhem Security, now Bugcrowd, was awarded a contract of up to $45 million with the agency. The partnership was leveraged to design the product after the agency's needs, allowing it to be rapidly and meaningfully iterated and improved upon using direct feedback from critical users, leading to a much accelerated time to value.

The agency has expanded Bugcrowd's software solution into some of their most critical systems. Over a dozen agency organizations leverage Bugcrowd for either operational cybersecurity programs or to accelerate DevSecOps and comply with MDA or NIST guidelines. Bugcrowd has helped the agency achieve its mission to test critical software, including weapon systems, both with and without developer participation.