bugcrowd

HOW MOTOROLA MOBILITY REDUCES RISK WITH BUGCROWD'S PRIVATE BUG BOUNTY & VDP

The Elite Crowd + VDP provide Motorola with maximum security coverage

Security at Motorola Mobility

Motorola Mobility is one of the world's largest consumer electronics and telecommunications companies. It has a robust security program across many departments and applications. After recognizing the need for a channel to connect with the security researcher community to find critical vulnerabilities quicker and more efficiently, the company launched its first private bug bounty program with Bugcrowd in 2015.

After the success of its private bug bounty program, Motorola needed to:

- Affirm its security commitment to its customer base
- Provide an operationally efficient framework for accepting and processing external security feedback.

Since the launch of its vulnerability disclosure program in March 2018, the number of submissions has doubled, without increasing the time to triage and validate. The continuous testing from Bugcrowd's community of thousands of security researchers provides the Motorola team with valuable vulnerability findings at scale.

Seizing the Opportunity

Before Bugcrowd, Motorola was running an internal bug bounty program, but it was a painful process. The small security team had to do all the vulnerability triage and validation, coordinate and communicate with thousands of security researchers around the world - provide notifications and reporting, and deal with the logistics of sending out bounty payouts in different currencies. What started out as a part-time project, turned into something that the two-person team in charge spent almost all their time working on.

While Motorola believed in the power of crowdsourcing security vulnerability findings, trying to do it internally with no structure around it become a drain on resources. Motorola launched a private bug bounty program with Bugcrowd in March 2015 to incentivize an Elite Crowd of security researchers without having to use precious internal resources, for things like recruiting, triage, validation, coordination, and logistics of bounty payouts. The bug bounty program includes websites from both Lenovo and Motorola.

Private bug bounty programs allow organizations to harness the power of the crowd – diversity of skill and perspective at scale – in a more controlled environment. At Bugcrowd, only those researchers who have a proven track record, those who have proven their skill and trustworthiness receive invitations to private programs – The Elite Crowd. Private programs can be scoped or built around a customer's testing needs and parameters. A private program can also meet requirements around background checking, ID verification or even location.

MOTOROLA

About the Motorola Program

Launched: March 2015

Type: Private and VDP

Scope: Websites and mobile from Lenovo and Motorola Mobility

Rewards: $100 – $1,500 per vulnerability

Vulnerabilities Rewarded: 391

Average Payout: $344.44

Average Priority: 2.78

Paid Out: $140,400

"With all these breaches happening around us, it becomes very easy for us to say to our executive staff, 'Isn't it better to know vulnerabilities exist before we get exploited by the bad guys?' Having a bug bounty program gives us not only actionable insights to stay ahead of the adversaries, but also peace-of-mind."

"From the mobile device manufacturing side, you always run into applications on the devices as one area of focus, but you also have the backend of those applications to worry about. Almost all applications that exist today transmit data and talk to web servers in the backend, so having a Crowd of people that can both look at the applications, look at the code itself, and look at the infrastructure support becomes very critical."

Richard Rushing
CISO, Motorola Mobility

After the success of its private bug bounty program, Motorola needed to open a channel to showcase security maturity and communicate the wider researcher community that they could submit bugs that were outside of the private bounty scope.

Motorola then launched a vulnerability disclosure program in March 2018 to expand security coverage. The continuous testing from Bugcrowd's community of thousands of security researchers provides the Motorola team with valuable vulnerability findings at scale.

> “What is amazing about Bugcrowd — With all the security technology and process that we have in place at Motorola we always find bugs when product goes live. Bugcrowd has saved us close to $60 million, simply because we've avoided major data breaches in the eyes of our customers.”
>
> **Richard Rushing, CISO of Motorola Mobility**

The Value of Vulnerability Disclosure Program

Vulnerability disclosure programs (VDP) provide a coordinated channel and framework for security feedback from the global community. Much like a “neighborhood watch” for an organization's internet assets, the program encourages security researchers to report something if they see something. VDPs do not offer monetary rewards and are ideal for continuous testing of internet web properties, self-sign up apps, or anything publicly accessible.

Bugcrowd's vulnerability disclosure program mixed with a private bug bounty has equipped Motorola with the largest possible talent pool of researchers available, all with collective talents that would be otherwise difficult to assemble, as well a maximum security coverage for its Internet assets. With Bugcrowd, Motorola has been able to operationalize its vulnerability disclosure process, delivering an all-in-one platform for centralized discovery and management.

Bug Bounty Program Results

Over the course of the Bugcrowd bug bounty program, Motorola has experienced ongoing success and has adopted the Bugcrowd platform as an essential — if not primary — part of its security strategy. The Motorola team is able to reallocate resources to what matters most to the business.

Working together with Bugcrowd, Motorola Mobility was able to incorporate the Crowdcontrol platform into an ongoing and holistic security program using the most innovative technology available. It was able to automate a managed process from discovery, validation, reproduction, review/triage, submitter payment, ticket creation and on to a final successful outcome.

As evidenced by its ongoing relationship, Motorola Mobility has acknowledged the ROI the Bugcrowd solution provides.

391 vulnerabilities rewarded

2.78 average priority

$140,400 total paid out

> “Bugcrowd actually scales our application security program. I know the vulnerabilities are legit, the reporting is legit, and that my team has to take action. All I have to do is approve the bounty payout and start working with the developers to fix the bug.”
>
> **Richard Rushing**
> **CISO, Motorola Mobility**

Benefits of Choosing Bugcrowd

As an enterprise company, Motorola Mobility needed to affirm its commitment to its customer base with a meaningful, actionable way to uncover and repair security issues.

Bugcrowd provides the perfect vehicle for managed vulnerability disclosure and remediation. Bugcrowd has the largest, most experienced team for managed crowdsourced security programs - 4x more experience managing bug bounty programs than the competitor. Motorola enjoys:

- Comprehensive onboarding for each program — The resulting program briefs, with scope, rewards and rules/regulations drive great accurate, actionable submissions with less noise
- Expert triaging with no clean-up work for the internal security (before they can forward to development — this means both less work and faster risk reduction)
- Researcher engagement and awareness — removes complexity with dealing with logistics of coordinating reports with thousands of researchers and getting the word out about your program.

Learn why hundreds of companies have turned to Bugcrowd:
www.bugcrowd.com/get-started