hackerone

HOW GM WORKS WITH HACKERS TO ENHANCE THEIR SECURITY

GM produces some of the most technologically advanced vehicles in the world, so keeping them secure has pushed this 110-year-old company to take a decidedly modern approach to security.

CUSTOMER STORY

GM

Customer Data

PRODUCT TYPE

HackerOne Response

Public Vulnerability Disclosure Policy

LAUNCH DATE

January 2016

VULNERABILITIES RESOLVED

700+

COMPANY SIZE

180,000+

INDUSTRY

Transportation/ Automotive

PARTICIPATING HACKERS

500+

In 2017, General Motors **delivered nine million vehicles globally**, each containing a host of mechanical, electronic, and communications systems.

Alone, they accounted for over 17% of the total number of cars and trucks sold in the U.S. in 2017. What's more, their cars and trucks carry some of the most advanced technology on the road. GM has already sold more than 8.6 million vehicles with 4G LTE connectivity built in. They've also released Super Cruise in their 2018 Cadillac CT6, which is currently the only semi-autonomous driving system where drivers are permitted to completely remove their hands from the steering wheel.

Yeah, that's some awesome tech! If you add in GM's push to have 20 electric models on the road by 2023, the amount and sophistication of technology they produce will only increase. And that means a traditionally non-tech company has some huge tech security issues to consider.

> Leveraging HackerOne's relationship with the research community, and seeing firsthand the results they provide, has been extremely encouraging.
>
> **JEFF MASSIMILLA, VICE PRESIDENT GLOBAL CYBERSECURITY, GM**

Reducing Risk with Industry-First Security Innovations

GM's security team recognized long ago the need to get in front of potential security issues. The company recently created the role of Vice President of Global Cybersecurity, and merged all cybersecurity activity—both product and corporate—into one central organization. This organizational shift reflects the progressive mindset within GM, as does their move into the world of hacker-powered security.

"We've always approached security with a diverse set of tools in our toolbox," said Jeff Massimilla, Vice President Global Cybersecurity at GM. "In today's connected world, it's critically important that product and corporate cybersecurity functions are aligned across all areas of the business."

HackerOne recommends every organization, regardless of industry, begin with a vulnerability disclosure policy (VDP). The automaker took that advice in early 2016. Two years later, hackers working through GM's VDP program have helped them identify and resolve more than 700 bugs.

"Leveraging HackerOne's relationship with the research community, and seeing firsthand the results they provide, has been extremely encouraging," added Massimilla. "Hackers have become an essential part of our security ecosystem."

Scaling Hacker-Powered Security Across Suppliers and Partners

Gizmodo highlighted a security researcher who notified GM of a way to bypass data limits on their car's OnStar wi-fi hotspot system. That hotspot is on the road in more than 4 million GM vehicles, so the potential fallout of that vulnerability could have been enormous.

Once a report like that comes in, GM responds to bugs with impressive speed and agility, putting their broad and experienced internal security team to work on fixes. And even with a mature security team structure already in place, GM has recognized the value of tapping into the ethical hacker community to help find bugs they might have missed.

"Researchers are engaged, and the quality of information we're receiving is extremely valuable and is helping us improve security across all areas of GM," said Massimilla.

Those security improvements don't just stop at GM's doors, but extend to key suppliers and other external partners, making it one of the most comprehensive VDPs in any industry.

And it's not just the tech within vehicles GM is concerned with. As Gizmodo mentions, they're also keeping an eye on potential vulnerabilities across thousands of dealerships, and even in car museums which feature GM brands.

It truly is a minivan approach to cybersecurity!

“

Hackers have become an essential part of our security ecosystem.

JEFF MASSIMILLA, VICE PRESIDENT GLOBAL CYBERSECURITY, GM

Eliminating Barriers for Security Researchers

After two years and great results with their HackerOne VDP, GM is expanding their hacker-powered security efforts to include a private bug bounty program and a special program to give hackers more access to their vehicles and systems.

Initially, GM's bounty program will focus on infotainment systems, since they're connected platforms and have been an entry point for hackers. But asking hackers for help on vehicle systems isn't as easy as asking for their help on websites. The biggest challenge: you need a car to hack.

> “We are employing strategies and programs, like our VDP with HackerOne, with the sole purpose of protecting our customers, their vehicles and their data.
>
> **JEFF MASSIMILLA, VICE PRESIDENT GLOBAL CYBERSECURITY, GM**

To help eliminate this lofty and expensive hurdle, GM is giving select hackers access to their Red Team lab. The program is intended to put the hands of those with the most expertise on more of GM's connected systems.

“This is really, really cool because, if you think about it, there's a lot of barriers to entry in our environment,” said Massimilla in the Gizmodo article. “You have to have a car, you have to have the infotainment system, things like that.”

GM is Committed to Hacker-Powered Security

GM is leading the automotive industry into the 21st century with a close eye on cybersecurity. According to HackerOne research, just seven of the top 50 automotive brands have a way for external researchers to report vulnerabilities. However, four of those seven are GM brands, cementing GM's leadership in automotive cybersecurity.

Along with their upcoming hacker-powered initiatives, GM is setting a new standard of collaborative cybersecurity in the name of public safety. And, they're one of the few automotive companies who understand they are also a technology company.

"We're taking cybersecurity very seriously at General Motors," said Massimilla. "It's a top priority for our company, and our most senior executives, including the CEO, fully support our organization."

It's a priority GM is driving with the help of the hacker community.

"We value the expertise of the security research community, and have been very pleased with the program's performance to date," Massimilla concluded.

Because for the largest auto manufacturer in the U.S., **#TogetherWeHitHarder**!

Learn more about HackerOne Response or reach out to start a conversation today.

About HackerOne

HackerOne is the #1 hacker-powered security platform, helping organizations receive and resolve critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security partner. Organizations, including the U.S. Department of Defense, U.S. General Service Administration, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel and the CERT Coordination Center trust HackerOne to find critical software vulnerabilities. HackerOne customers have resolved over 65,000 vulnerabilities and awarded over $26M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York and the Netherlands.