bugcrowd

USING THE CROWD TO RAISE THE BAR ON SECURITY FOR THE WORLD'S CONNECTED DEVICES

wink

WHY CROWDSOURCED SECURITY?

Consumers of Internet-connected devices expect them to operate securely within secure environments; Wink is actively using the power of the Bugcrowd security researcher community to meet these expectations in ways not possible with traditional internal and commercial firm assessments.

"Bugcrowd is a no brainer; you're getting a much larger pool of researchers with the different backgrounds, skills and expertise that matter."

BRIAN KNOPF
Principal Security Architect & Security Researcher at Wink

ABOUT WINK

Wink is helping the world build a smarter home by delivering single-app control for connected products representing some of the top Internet of Things brands. As these devices open up the consumer to privacy and safety issues, Wink is focused on becoming the brand consumers know and trust, the one that works securely with every Internet-connected device, no matter who built it or what technology it uses to communicate.

Targeted expertise for your security assessment program

As with any successful security assessment program, you really need to understand what you're looking for. If you've done nothing in security, it's really hard to run an assessment—let alone a bug bounty program—that provides value. Before you begin, you have to understand what your program interfaces are: Are they wireless or Ethernet? Are there applications or Web Services involved? And, most importantly, you need a view into how someone or something could break into your program interfaces. Essentially, it's about identifying the threat landscape and mapping out the highest risks. Then, the next critical component is finding the right people with the right skills and expertise to help with the security assessments in those specific areas while being prepared to address what they find.

In order to identify these experts, you must have visibility into the skill set and quality of the researchers. Even if a commercial assessment company has a good reputation for providing solid security audits, it all comes down to the individual(s) conducting the particular audit and their expertise related to the technologies being assessed in your program. Why invest crucial project time and pay top dollar for security research to only have a junior researcher assigned to your program?

With Bugcrowd, you gain visibility into the expertise and quality of the researchers, thus giving you the confidence that the right researchers with the right skill sets and expertise are invited to participate in your assessments at the right times. Because Bugcrowd brings in a large number of vetted and trusted researchers to the program, a much larger set of eyes looks at your products compared to your own internal testers or that of a dedicated commercial security assessment firm.

Challenges

- External assessments by dedicated security firms are expensive and often limited in the results achieved
- Security expert "guns for hire" are great but cost-prohibitive as full-time direct hires
- Internal assessments are narrowly focused on finding the expected in-your-face bugs

Solution Highlights

- Real-time access to extremely smart people with different perspectives on how to break things
- The right technical experts at the right times in the project lifecycle
- Product quality is significantly enhanced, without breaking the bank

BUSINESS BENEFITS

Value: Wink paid $5400 out of a $10K bounty, and one of the vulnerabilities identified was worth far more than that.

Control: Allows you to focus investments and control costs associated with managing risks connected with end-to-end product security.

Resources: Bugcrowd fills the knowledge and/or time gap that your internal teams may not have.

Credibility: Brings products to market faster with a higher level of security, thereby building trust with the consumer.

Brand: Reduces the likelihood of a security breach, thereby avoiding unnecessary damage to the brand and potential impact to product sales.

ABOUT BUGCROWD

Bugcrowd has combined the power of a curated crowd of 16,000 researchers with a sophisticated management platform to safely, efficiently and quickly identify and solve your security issues. Cost-effective and lightning fast compared to standard vulnerability programs, we're bringing the next generation of bug bounty to the enterprise.

Completely Flexible Assessment Program

Wink's initial Bugcrowd Flex program includes two phases. The first phase is a two-week invite-only effort consisting of 26 researchers focused on specific areas of specific Wink products. This is followed by a long-term phase where an extended set of researchers continue to submit vulnerabilities for the products available in the first phase, but also other products and features opened up to the program. This flexibility remains a key feature of the Bugcrowd solution as Wink is able to control the cost while adjusting the program based on how and when new technologies are released.

"The value of a single bug found in our initial program paid for the entire program—I would have paid ten times as much for that one vulnerability," said Knopf.

Unmatched Return on Investment

Organizations can spend upwards of $10K-$20K for a traditional external audit. But even an $80K audit on a product won't find everything. You can get much more effort and far better results out of that money by using the top researchers available in the Bugcrowd community than you can from three dedicated researchers or penetration testers conducting a security audit through a commercial firm. Selected researchers from Bugcrowd specialize in particular techniques that identify the big-time vulnerabilities you are really looking for; you're going to uncover things you wouldn't find otherwise.

"We weren't just adding testers for numbers sake, we were also adding the right people—we wanted proven success in hardware, the cloud, and the Internet of things," said Knopf.

Establishing Trust in a Five-Star Security Rating System

Consumers are concerned about security; they just don't know what to do about it. "Our job as security professionals is to make the controls invisible so consumers never have to think about security," said Knopf.—but not at the expense of hiding the fact that things are secure. In response to this need, Wink is driving an industry-wide five-star rating system, similar to that already found in the automotive and medical device industries.

"Bugcrowd is a critical piece of our five-star security rating strategy as the industry works to drive down vulnerabilities in our connected devices," said Knopf.