bugcrowd

CASE STUDY

VULNERABILITY DISCLOSURE

National Australia Bank Strengthens Security with Bugcrowd Vulnerability Disclosure Program

nab

Industry

Bank / Financial Services Institution

Challenge

No formal or uniform way for security researchers to disclose potential vulnerabilities to NAB

Solution

Vulnerability Disclosure Program (VDP)

Outcomes

- Crowdsourced security testing provided greater depth to NAB's security controls
- It uncovered more vulnerabilities, strengthened remediation processes, and reduced risk while providing more secure products and services for customers

About the National Australia Bank

National Australia Bank (NAB) is one of the four largest financial institutions in Australia in terms of market capitalization, earnings and customers. NAB was ranked 21st-largest bank in the world measured by market capitalisation and 52nd-largest bank in the world as measured by total assets in 2019.

> The NAB was seeking new solutions to reduce its security risks, accelerate digital transformation, and make better decisions through contextual visibility.

NAB's Standpoint on Security

The partnership with Bugcrowd marked NAB's first venture into crowdsourced security testing. It provided a complementary layer of assurance alongside a suite of existing assurance and testing controls. In addition, NAB has since expanded its penetration testing services with Bugcrowd, having previously worked with several other service providers.

Other Important Policies in Action

After seeing success with the VDP, NAB implemented a bug bounty program to solicit potential vulnerabilities from the security community. As the attack surface expanded, NAB needed more eyes on its assets to help keep them safe for customers, colleagues, and shareholders. While NAB saw value in the VDP, it is by nature a passive program. So, in order to seek active testing and increase the coverage of assurance across all services, NAB created a bounty program and engaged an army of broadly skilled researchers on an ongoing basis. Going forward, NAB plans to expand its bounty programs to cover the software development lifecycle as well.

The NAB was seeking new solutions to reduce its security risks, accelerate digital transformation, and make better decisions through contextual visibility.

A New Policy

Vulnerability Disclosure Program with Bugcrowd

The NAB achieved a wide range of benefits to strengthen its security posture by engaging with Bugcrowd for the VDP and Bug Bounty program. These benefits included:

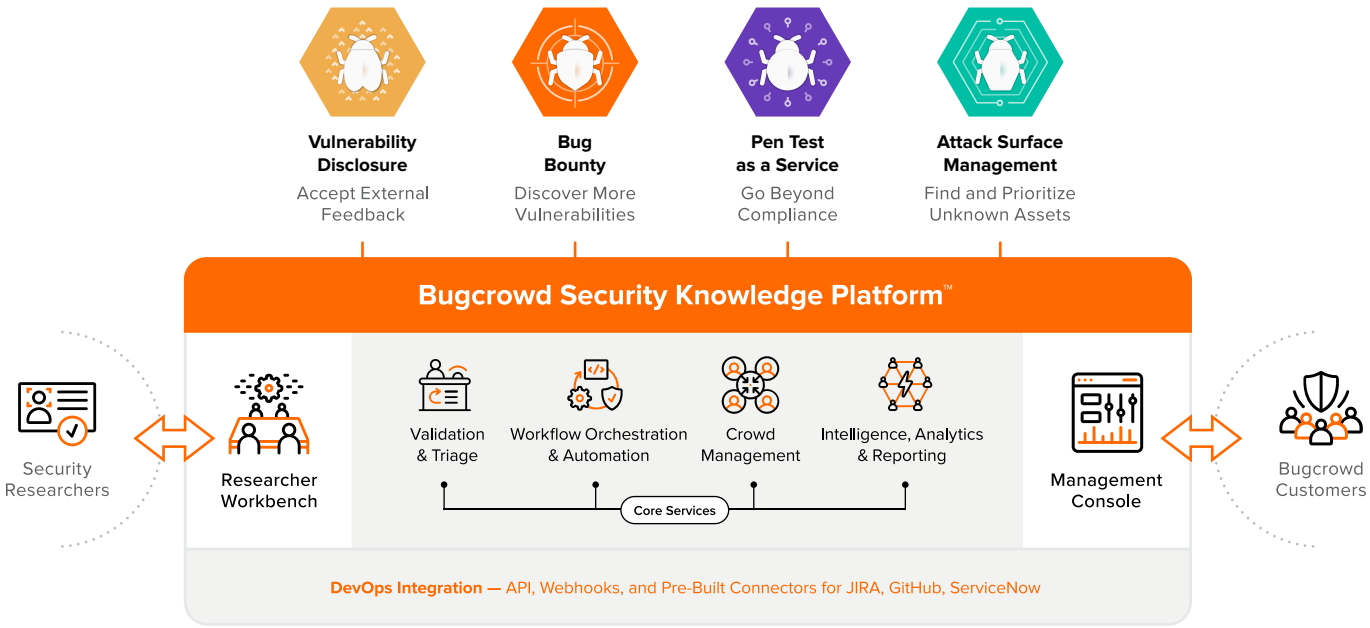
- Using the crowd with a wider range of skills to find gaps that may have been missed by traditional security assessments.
- Gaining access to a large, global crowd of 160 security researchers with broadly diverse skills, resulting in shorter lead times to add targets to scope.
- Having access to a controlled risk environment through Bugcrowd's Crowdcontrol platform, with Bugcrowd acting as the intermediary.
- In addition, having an independent party to triage submissions helped NAB to save on internal resources and staff efforts.
- Potential vulnerabilities were reported quickly, reinforcing the fact that speed is an advantage.
- Testing was not time bound, which allowed security researchers enough flexibility to test whenever, and for however long, they chose.
- NAB was able to demonstrate the maturity of its security practice through the VDP and Bug Bounty program, reinforcing its commitment to robust security practices to customers, partners, and the security community.
- The VDP platform established a positive relationship between NAB and the Whitehat security community, encouraging greater transparency and responsibility.
- The program also created a new talent pipeline, as the VDP provided a good platform to recruit standout researchers for its bounty program.
- The effort returned a relatively low false positive rate, with no additional cost to retest.
- Overall, the program has enabled NAB to discover numerous critical findings of severe security shortcomings.

So, why Bugcrowd?

NAB found that Bugcrowd offered a comprehensive service which allowed room for growth and complemented its existing security controls. The option to start with a VDP helped NAB understand the workflow and develop its internal processes. The management overlay that Bugcrowd provided across the VDP and bug bounty program, with a team of engineers to triage submissions, helped alleviate any potential pressure on internal processes. In addition, Bugcrowd was commercially competitive and NAB was encouraged by the company's responsiveness to suggestions for ideas and enhancements to drive product development.

Bugcrowd Security Knowledge Platform™

Organizations of all kinds need to do everything proactively possible to protect themselves, their reputation, and their customers from being blindsided by cyber attacks. The Bugcrowd Security Knowledge Platform™ finds hidden vulnerabilities before attackers do by uniquely orchestrating data, technology, and human intelligence—including tapping into the global security researcher community ("the Crowd")—for solutions that span Pen Testing as a Service, Vulnerability Disclosure, Bug Bounty, and Attack Surface Management.



Best Security ROI from The Crowd

We match you with the right trusted security researchers for your needs and environment across hundreds of dimensions using ML

Instant Focus on Critical Issues

Working as an extension of the platform, our global security engineer team rapidly validates and triages submissions, with P1s often handled within hours

Contextual Intelligence for Best Results

We apply accumulated knowledge from over a decade of experience across 1000s of customer solutions to your goals for better outcomes

Continuous, Resilient Security for DevOps

The platform integrates workflows with your existing tools and processes to ensure that applications and APIs are continuously tested before they ship