bugcrowd

MONASH UNIVERSITY LEVERAGES BUGCROWD FOR IMPROVED SECURITY VISIBILITY AND CONTINUOUS ASSURANCE

HOW ONE OF AUSTRALIA'S LEADING UNIVERSITIES LOWERED OPERATIONAL OVERHEAD, ACHIEVED BETTER VALUE FOR MONEY, AND IMPROVED ITS CYBERSECURITY POSTURE WITH BUGCROWD'S VULNERABILITY DISCLOSURE AND BUG BOUNTY PROGRAMS

The Challenge of Cybersecurity in Higher Education and Research

Monash University, in Melbourne, Australia, ranks among the world's top 100 universities. This global university fosters a culture of collaboration, research and continuous learning. Monash prioritises embracing technology. In fact, they were one of the first universities in Australia to access the internet.

Amidst increased focus on cybersecurity from the federal government in Australia, Monash has continued its legacy of leading with technology. It is the first university in Australia and beyond to implement a Vulnerability Disclosure Program and Bug Bounty Program, leading the way in higher education cybersecurity.

It has traditionally been a challenge to provide appropriate and proportionate protection for the University's systems, information and reputation while promoting a culture of digital innovation, agility and openness. The university's Cyber Risk & Resilience team, composed of 21 members and led by Dan Maslin, Chief Information Security Officer, work daily to achieve and maintain that balance.

One of the unique challenges of cybersecurity in the higher education and research industry is the scale and complexity of the constantly changing environment. Monash has a large digital footprint, with over half a million external IP addresses and a significant variety of technologies managed by different groups. It's difficult to have visibility into such a large environment that changes regularly.

Continuous Coverage vs. Point-In-Time Testing

When Dan Maslin started at Monash in November 2019, one of his top priorities was to implement a Vulnerability Disclosure Program (VDP). "There was a deliberate intention to move to a state where we are aggressively proactive in identifying any critical cybersecurity weaknesses—a crowd-sourced testing regime has allowed us to do this at scale," said Maslin.

Previously relying on traditional vulnerability scanners and infrequent, point-in-time, limited-scope penetration tests, the team found these methods to be inadequate in delivering continuous cybersecurity coverage. Given the variety of technology stacks, scale and different applications in their complex environment, hiring the amount of internal penetration testing staff to continuously test assets was unrealistic.

MONASH University

Industry: Higher Education and Research

Program Launch: August 2020

SUMMARY

Challenge — The cybersecurity team needed to gain visibility and manage hundreds of applications in a complex, ever-changing, global environment

Solutions — Bugcrowd Vulnerability Disclosure Program, Bugcrowd Bug Bounty

Outcomes —

- 100-fold increase in actionable intelligence using Bugcrowd's Vulnerability Disclosure Program for the cost of one traditional penetration test
- Lowered operational overhead
- Gained assurance from improved visibility and guaranteed continuous coverage/testing by vetted cybersecurity researchers

By leveraging a VDP and subsequent Bug Bounty program with Bugcrowd, Monash can edge closer to realising their goal of continuous cybersecurity coverage. “Bugcrowd gives us much more assurance that the right things are being tested all of the time by a group of vetted cybersecurity researchers. A once-a-year penetration test is very expensive, point-in-time and has a limited scope, where the very next day things could change. We have continuous visibility now,” said Maslin. With these programs, Monash benefits from an elevated vulnerability submission process, providing efficiency, safeguards and assurance as researchers continuously test the environment.

Salman Khan, Cyber Threat and Vulnerability Specialist for Monash, highlighted some of the operational benefits of having Bugcrowd’s Vulnerability Disclosure Program in place. “There is a much lower operational overhead now. For individual penetration test engagements, you have to plan it out and involve multiple parties. A lot of time is spent doing that. The Bugcrowd offering reduces resource drain through validation, triage and prioritisation. You also get shared access to top talent with a good combination of skills and experience.”

Triaging, Re-testing and Reporting

One priority for the team at Monash is to have increased visibility into their whole environment so they could better understand where assets in their attack surface sit, identify trends or patterns, and know what areas need improvement. Bugcrowd’s Vulnerability Disclosure Program has enabled that increased visibility, along with additional benefits.

“The Vulnerability Disclosure Program is one of the best value-for-money services that we have. The annual cost of the program is the same cost of one traditional penetration test for us, and the VDP has given us around a 100-fold increase in actionable intelligence,” added Maslin. “But it’s not just submissions. You get the bonus of triaging, prioritising, remediation advice, proof of concept and re-testing. It’s not just about the quantity, it’s about the value and quality of submissions. That’s all wrapped up in the Bugcrowd offering.”

Monash also found Bugcrowd’s executive reporting functionality to be especially helpful. “Being able to provide the different levels of data from the platform has been fantastic. We’ve really hit our objective to significantly improve visibility,” said Maslin.

“Bugcrowd’s Vulnerability Disclosure Program is one of the best value for money services that we have. The annual cost of the program is the same cost of one traditional penetration test and the VDP has given us around a 100-fold increase in actionable intelligence.”

Dan Maslin
CISO

Looking Forward

Since launching their VDP program in 2020, Monash has experienced a simple implementation with immediate results. “Onboarding with Bugcrowd was really smooth. The team helped us introduce the program and align us on a ‘crawl, walk, run approach.’ We’ve had fantastic results so far,” said Khan.

As Monash continues to embrace a “crawl, walk, run” strategy, their new Bug Bounty program enables the team to target specific and high-risk systems. They hope to get to the point where point-in-time penetration testing can be wholly replaced with this crowd-powered approach.

As they expand the scope of their programs, achieving a level of assurance is always a main goal. As they continue to lead the way for other universities across the globe, they shared some advice for those looking to start utilising crowdsourced security. They recommend planning out your scope and engagement with those system owners, starting small and targeted. They also emphasised the importance of helping internal groups understand the offering and possibilities of crowdsourced security. Lastly, the team underscored the value in building internal processes to triage and remediate vulnerabilities.

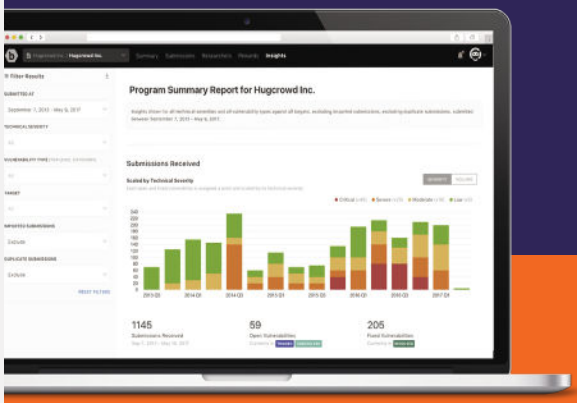
Crowdsourced cybersecurity has transformed vulnerability management at Monash University, helping them to stay secure, expand visibility and gain increased assurance as a leader in higher education and research.

“When protecting against 21st century threats, you need a 21st century solution.”

Salman Khan
Cyber Threat & Vulnerability Specialist

“Bugcrowd has given us confidence that a crowdsourced approach for quickly identifying weaknesses does scale to our ecosystem of hundreds of advanced research-led digital systems. We have a challenging environment —it is constantly evolving and is increasingly connected to the world beyond our institution’s boundaries. Yet we have observed that researchers and the Cyber Risk & Resilience team alike have embraced the transparency and responsiveness that this approach provides, giving us confidence that continuous assurance can be achieved.”

Dr. Steve Quenette
Deputy Director, Monash eResearch Centre



Learn why hundreds of companies have turned to Bugcrowd:

www.bugcrowd.com/get-started