bugcrowd

HOW SEEK LIMITED PROTECTS ITS LEADING EMPLOYMENT MARKETPLACE

SEEK Shows Commitment to Security with a Managed Public Bug Bounty

Security at SEEK

SEEK is Australia's number one employment marketplace, bringing together a strong portfolio of online employment, educational, commercial and volunteer businesses. SEEK operates across 19 countries with exposure to more than 4 billion people. At SEEK, users' security and privacy is paramount. The company takes every precaution to protect its information so that it can focus on bringing innovations to market through its products and services.

With an expanding attack surface and highly motivated adversaries, SEEK recognized it needed to create a consolidated channel for vulnerability reporting and improve internal and external security testing practices. To achieve this, they tapped Bugcrowd's platform and community of white hat hackers, launching its crowdsourced security program in 2016.

Crowdsourcing for More Coverage

To power the SEEK platform over the years, the team had incorporated varying technology stacks and "backend" systems for managing different parts of the business. Combine that with the highly sensitive user data shared on SEEK, and you have your hands full with creating a dynamic and effective application security program that incorporates security and privacy at every level.

SEEK does a number of things to help secure its platform, including:

- Code and design reviews
- Vulnerability scanning
- Dependency scanning/checks
- Helping build "secure by default" systems, so security is enabled by default
- Traditional Penetration testing
- Internal security training and CTFs.

Even with all these security layers, SEEK needed to ensure its diverse systems and data were tested further with a bug bounty program to catch vulnerabilities that slipped through our other controls. SEEK started working with Bugcrowd in June 2016. To get the business comfortable with running a bug bounty against the production systems, SEEK started with a small limited scope. This approach proved very successful and allowed the company to increase the scope of the program over time. After running a wider scope private program for a few years, SEEK took the program public in 2019.

seek

About the SEEK Program

Launched: June 2016

Type: Private to Public Managed Bug Bounty

Vulnerabilities Rewarded: 532

Paid Out: $136,990

"Unlike a scheduled penetration test, time is not a factor. And given the number of researchers on the Bugcrowd platform this means eventually the majority of customer facing applications end up being discovered and further tested. This allows us to 'even up' the playing field between security testers and the technology teams."

Zac Sims
SEEK Security Engineer

Benefits of Taking Your Program Public

By evolving to a public bug bounty program, SEEK gained a force multiplier of hackers, which increased the number of new findings, as the company's targets were exposed to more hackers with an even bigger array of skill sets, perspectives and abilities

With a public program, SEEK also increased awareness of its security maturity among its users. This demonstrates the company's commitment to protecting digital assets and responding to known risks.

> "It's like having a team of security researchers, all with different skills and techniques, testing your systems on and off throughout the year. This additional testing fits nicely with the continuous delivery approach that software development now typically follows."

Zac Sims
SEEK Security Engineer

Scale
Scale testing efforts to gain access to extensive skill set, diversity, and coverage at scale.

Awareness
Heightened security awareness and reassure stakeholders security is a priority to your organization.

Coverage
Ideal for publicly accessible targets such as web and mobile applications.

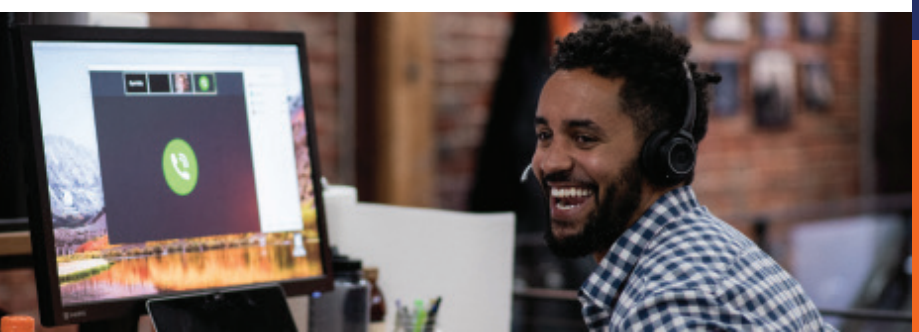
Working with Bugcrowd: Measuring Results

Over the course of both the private and public programs, SEEK has been able to maintain strong engagement across targets.

Bugcrowd has enabled SEEK to identify "patterns" of vulnerabilities that no one else had. These patterns may only be visible over months or weeks and will typically be in more than one system.

Identifying these patterns has allowed SEEK to establish secure defaults, that prevent these classes of vulnerabilities across all of its applications and services. The SEEK security team reviews bug bounty submissions weekly, which allows them to further identify patterns and fix these issues before they occur. SEEK's crowdsourced security testing coverage is wider than their normal testing processes, so they were able to get valuable findings from the older, less front-of-mind, systems.

For more information on SEEK's bug bounty program, check out this **blog post**.



532 vulnerabilities rewarded

$136,990 paid out

> "Being able to use real examples of previous bugs enables developers to look at their attack surface in a different way."

Pamela O'Shea
SEEK Principal Security Consultant

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