bugcrowd

SOFTDOCS ENGAGES BUGCROWD TO HELP SECURE THEIR EDUCATION-FOCUSED ECM PLATFORM

Crowd-powered Next Gen Pen Test and Bug Bounty Programs provide insights, education, and risk-reduction

Softdocs Mission

Softdocs develops enterprise content management (ECM), e-forms and process automation solutions exclusively for the higher education and K-12 markets. The company's Etrieve platform reduces the need for paper while improving student service and employee productivity with complete control over how content is captured, processed and distributed. A wholly digitized experience consisting of some of the most precious and therefore vulnerable data available, student information, necessitates serious attention to data security. With the help of Bugcrowd's crowdsourced security programs, Softdocs is committed to ensuring the security of students and educators everywhere.

The Value of Student Data

The information held by Education ECM platforms can be highly personal, and therefore vulnerable to abuse or misuse. For K-12 students, information like name, address, phone number, social security number, health, medications, etc. are often necessary for enrollment, as well as proper communication, care, and protection thereafter. In higher education, financial information and valuable intellectual property might join this already lengthy list of data points, as students engage in the loan process, and begin to attach payment information. The cost of compromise for this data is grave — valued at more than **$300 per affected record**, second only to healthcare, worldwide. While reputational damage can be costly, it pales in comparison to the personal and financial devastation for affected students, parents, faculty, and staff.

Softdocs

Launched: April 2016
Type: Next Gen Pen Test and Bug Bounty Programs

"Softdocs' partnership with Bugcrowd is a key strategy for securing the Etrieve product for our customers. In today's threat landscape, focused, crowdsourced attention to our digital footprint is important to securing the integrity and privacy of their data."

Mike Williamson
VP of Development

Security at Softdocs

While it's important for a software provider to recognize why it might be targeted for attack, the most evolved spend their days thinking about how they might be attacked. As conscientious stewards of their education client's content, Softdocs embraces this approach through a variety of security strategies and tools focused on preventing as well as responding to malicious attacks. Extensive internal application security testing by Softdocs is further complemented by Bugcrowd's managed crowdsourced testing programs to provide greater depth and breadth across all of Softdocs most critical assets. Through adoption of what's known as the "hacker mindset," Softdocs proactively defends user data with the most organic approach to real risk possible.

The Value of Bugcrowd at Softdocs

With a number of strong security investments already in play, Softdocs was looking for a solution that would enhance their existing operations, without draining an already tightly focused team. They chose Bugcrowd for a fully-managed approach to security testing that leverages human ingenuity to surface more high-value vulnerabilities. Platform analytics and workflows enable rapid vulnerability triage so that Softdocs can fix quickly. After seeing success through Bugcrowd's Managed Bug Bounty programs, Softdocs has leveraged the Bugcrowd platform to meet additional security testing use cases, including On-Demand Targeted Testing, and Next Gen Pen Test.

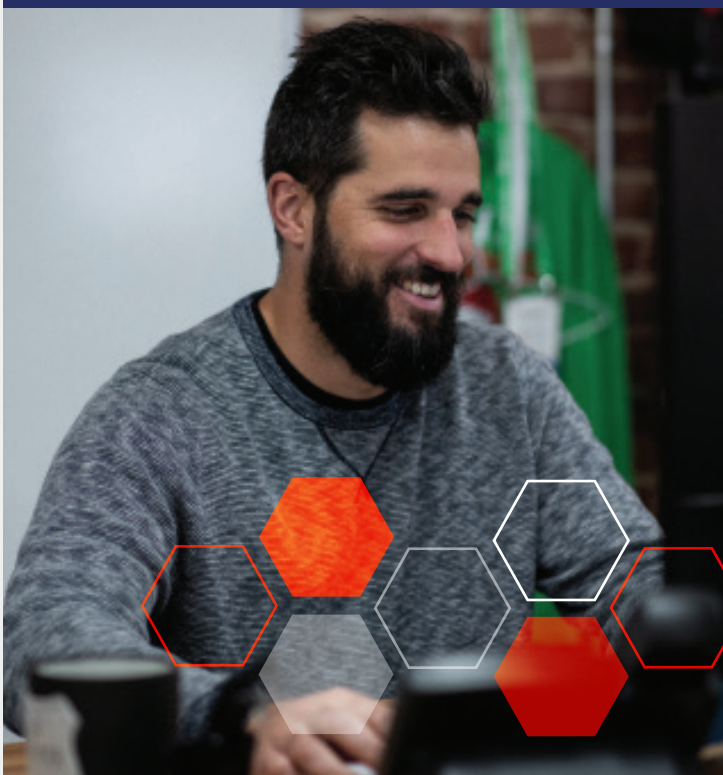
Softdocs cites several key benefits to Bugcrowd's competitive crowdsourced testing:

1. **Unique perspectives:** Varying testing styles and focus areas applied simultaneously reduces blind spots and complements existing testing efforts
2. **Pay for results:** A cost model built on results rather than effort provides more value for money
3. **Competitively motivated:** Rewarding unique discoveries delivers more high value results, faster
4. **Bandwidth back:** An elastic team of testers enables Softdocs to refocus internal resources on remediation efforts
5. **Risk reduction:** Negative testing (testing that surfaces no new flaws) provides validation of a secure foundation, enhancing overall security posture
6. **Education:** Surfacing those patterns that are exceptions to, rather than flaws in code, provide a chance to learn and grow from things not typically targeted

"Since we pay for results rather than effort, we can scale out to many researchers, and the cost is inversely proportional to how secure we are."

"During our program, we've gotten some very interesting and unexpected traffic from a variety of researchers, and I think that kind of testing exercises our product more thoroughly than would be possible with conventional testing with staff or contractors."

William Scalf
Security Architect



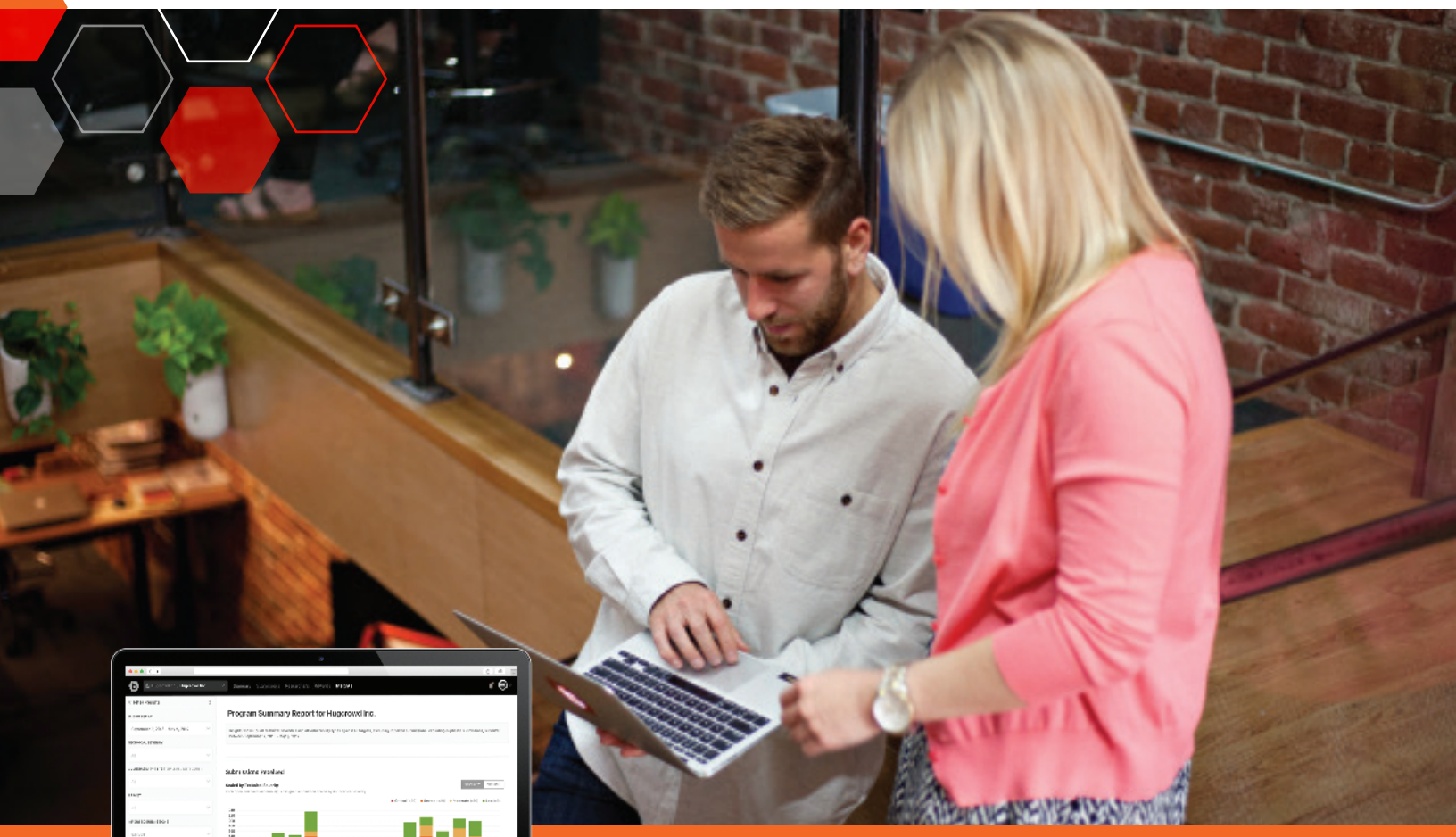
Overcoming Challenges, Together

Crowdsourced security can be a powerful tool in the fight against malicious attackers, but also requires support from many business units outside of the Security team. Legal, Finance, and others will likely have questions that must be addressed prior to engagement. Softdocs was no exception to these important internal discussions, and leveraged Bugcrowd's expertise to guide conversations, and craft a customized program that would fit all stakeholder requirements.

Understanding How Researchers are Vetted and Selected:
Bugcrowd assesses researchers for program fit based on a variety of features that can broadly be understood as measures of both trust, and skill. Some programs require participants to reside in a particular location, or be background checked before enabling access. Bugcrowd provides Softdocs with researchers that make sense for their business, as well as their platform security initiatives. Additionally, Bugcrowd enables customers to determine disclosure policies that range from strict non-disclosure, to- coordinated and mutually-agreed upon disclosure of Researcher findings in order to share learnings and best practices with the wider security community.

Understanding the Incentivization Model:
Many Bugcrowd programs entail a "bounty" component that is used to monetarily incentivize researcher engagement. This element is fundamental to Bugcrowd's ability to deliver high priority vulnerabilities faster than any other testing solution. Bounties of varying amounts are awarded to researchers based on validity and severity of findings, and the "Bounty pool" is topped up as needed to continue active programs. Bugcrowd works with Softdocs to ensure continued researcher incentivization and engagement by arranging bonus periods, and creating appropriate reward ranges that still fit budget requirements.

By teaming with Bugcrowd, Softdocs can deploy the crowdsourced security programs that meet business requirements, compliment existing security operations, and, most importantly, help secure Softdocs' customer data.



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