PhD student goes from 'hackademic' to funded founder with cybersecurity solutions

Wil Gibbs spins DARPA competition-winning AI research into a $1.5 million startup

By Kelly deVos, ASU News
March 6, 2026

Every morning, computer security engineers slide behind their desks, open their dashboards and brace for impact.

A thousand warnings. Red flags stacked on red flags. Automated scanners screaming about code injections, memory corruptions and compliance violations. Somewhere in that digital haystack is a needle — a real, exploitable vulnerability. But good luck finding it before a hacker does.

The tragedy of modern cybersecurity isn't that we can't find bugs. It's that we find too many.

"Out of those 1,000 issues, there are only about 50 that are really important for you to fix," Wil Gibbs says. "But the problem with having 1,000 warnings is that you don't know where to start."

Gibbs is a computer science doctoral student specializing in cybersecurity in the School of Computing and Augmented Intelligence, part of the Ira A. Fulton Schools of Engineering at Arizona State University. He also earned his bachelor's degree in computer science at ASU and now works with Associate Professor Adam Doupé in the Center for Cybersecurity and Trusted Foundations. Gibbs says he's done watching engineers chase ghosts.

After spending two years building artificial intelligence systems that find and fix software bugs as part of a competitive cybersecurity team, he's now the CEO of a startup called Artiphishell, and he's betting $1.5 million that he can turn academic cyber-wizardry into something enterprises will actually use.

Born in Vegas

To understand Artiphishell, you have to start under the fluorescent lights of DEF CON in Las Vegas, where 30,000 hackers gather annually to probe systems, uncover weaknesses and make technology more secure.

There, Gibbs co-led the 25-person Shellphish team that competed in the AI Cyber Challenge, a moonshot program backed by the U.S. Defense Advanced Research Projects Agency, or DARPA, to build AI systems that can automatically find and fix vulnerabilities in open-source software. The stakes were national: rising cybercrime; more than 3.5 million unfilled cybersecurity jobs worldwide; and open-source code, which can be exploited by hackers, underpinning everything from hospitals to power grids.

Shellphish built an AI-based system called Artiphishell that can analyze software, identify security flaws, patch them and retest the system. The team took home $2 million in prize money and proved something radical: AI can meaningfully assist vulnerability research if it is engineered carefully.

But Gibbs saw a drawback.

“The problem, almost, is that the AI is too exciting,” he says. “Many people hear AI and then instantly say, ‘I’m in. Let’s do it.’”

After two years in the trenches, Gibbs knew better. Large language models can sound confident and look correct even when they’re wrong. In cybersecurity, those kinds of mistakes can lead to a breach, resulting in lost data and dollars.

“If you’re not really paying attention when going through the results, you’ll think it is correct up until the point that you have a problem,” Gibbs says. “And then you ask, ‘Where did this all go wrong?’”

Cut the noise

That question set the stage for something new. So Gibbs and several teammates spun out a company.

Artiphishell doesn’t try to replace the bug-finding tools enterprises already use. Those automated scanners are everywhere, and they work. The real problem is triage. To meet compliance requirements, companies run static analysis tools that generate thousands, or sometimes tens of thousands, of alerts. Most aren’t critical. Some aren’t even exploitable.

Artiphishell ingests that flood of reports and pressure-tests them. Instead of hunting for new bugs, the system analyzes existing warnings, determines whether vulnerable code is actually reachable by hackers, attempts to reproduce the flaw and, if successful, generates a patch. If it can’t reproduce the issue, it gets deprioritized.

“During a test of 1,000 warnings, we were able to trigger and reproduce about 50 of them that represented real vulnerabilities,” Gibbs says. “So instead of spending thousands of hours sorting through every warning, you spend 10 minutes reviewing the ones that actually matter.”

Artiphishell’s differentiator is evidence, providing reproducible results that security teams can verify themselves.

“We give you a concrete value or report that you can then run yourself to reproduce results and be confident in them,” Gibbs says.

The pitch has resonated. The company raised roughly $1.5 million in initial funding as Gibbs prepares to graduate and run the business full-time.

Making security spending pay off

One of the ironies of cybersecurity is that success is invisible. If a company’s data defense is good, then nothing happens, and executives struggle to justify the cost. If they underinvest and suffer a breach, the consequences are public and brutal.

Gibbs believes that Artiphishell can flip that equation by giving back developer time. Instead of sifting through noise, engineers can focus on architecture, innovation and proactive defense.

By the end of this year, Gibbs hopes to raise a larger round of venture capital funding to help the company scale up. New products are slated for release within the next 12 months. The long-term vision is to build an AI-augmented security workflow grounded not in hype, but in proof.

Doupé says Gibbs combines deep technical rigor with a builder’s instinct.

“Wil has demonstrated outstanding leadership and research skills throughout his time at ASU,” Doupé says. “He’s leveraging these skills to start the entrepreneurial journey, and I’m confident that he and the team will succeed.”

Back at DEF CON, under the neon glow, the Shellphish team once bet big and won. Now Gibbs is making a different wager — that careful, evidence-based AI can cut through cybersecurity’s thousand-warning mornings.

Because in a world where everything runs on code, the real jackpot isn’t prize money.

It’s knowing which 50 security flaws matter before someone else does.

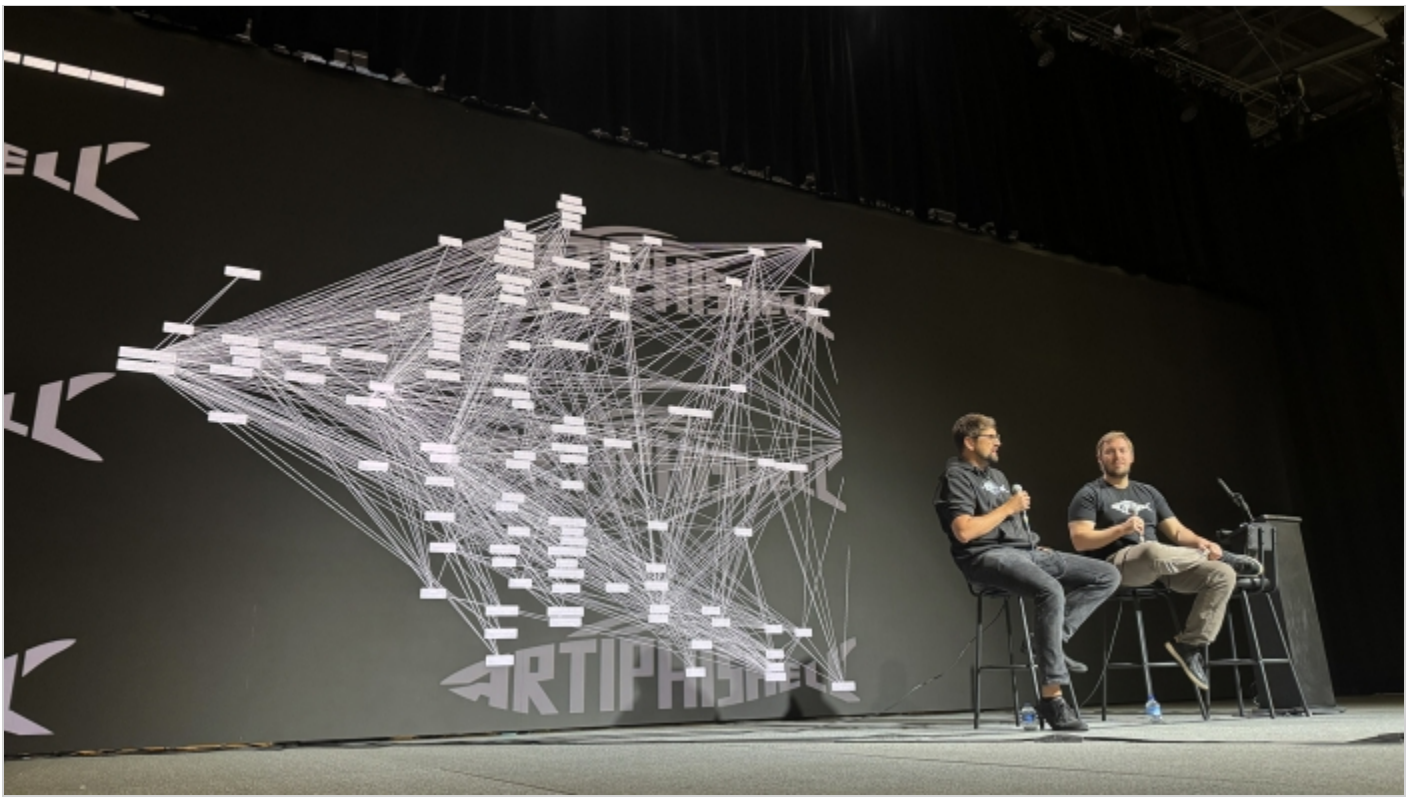
This story originally appeared on ASU News.

Main image

As Wil Gibbs — a computer science doctoral student in the School of Computing and Augmented Intelligence at ASU — wraps up the work for his degree, he has parlayed his doctoral research into a tech startup that will provide cybersecurity solutions powered by artificial intelligence to industry and enterprise clients. Photo by Erika Gronek/ASU

Text image(s)

Wil Gibbs holds the Shellphish team trophy awarded at the U.S. Defense Advanced Research Projects Agency's AI Cyber Challenge at the DEF CON 33 event held in August 2025 in Las Vegas. Gibbs co-led a team that received $2 million in prize money to fund their efforts during the competition. Photo by Kelly deVos/ASU



Wil Gibbs (right) speaks with Artiphishell co-founder Lukas Dresel onstage at DEF CON 33, where the pair presented the technical underpinnings of their work to an audience of cybersecurity experts and enthusiasts. Photo by Kelly deVos/ASU