For more than 35 years, OSIsoft, a member of the Microsoft partner network, has been empowering people with data. The company develops and supports software used to capture, process, analyze, and store any form of real-time data. Today, employees use OSIsoft industrial intelligence solutions to make critical business decisions based on more than 1.5 billion streams of operational data gathered at 19,000 sites in 127 countries. For customers in oil and gas, power, chemical, pharmaceutical, life sciences, pulp and paper industries, and the public sector, OSIsoft and its flagship PI System help to maintain reliable operations. And when the ramifications of downtime can mean unscheduled wind turbine closures, or power outages for citizens, it’s obvious that for OSIsoft, the reliability and security of its industrial intelligence solutions is critically important.

“The things people take for granted today—like gasoline, clean running water, safe medications, and power—are what OSIsoft helps to deliver through our software,” says Bryan Owen, Cyber Security Manager at OSIsoft. “That’s why, when it comes to ensuring the security of our solutions, we test for security bugs using Project Springfield, from Microsoft.”

Ease of use simplifies security testing
Up until recently, OSIsoft developers spent a disproportionate amount of time and IT resources performing security bug testing, or fuzzing. Fuzz testing is a technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.

Different OSIsoft product teams incorporated fuzzing into the software development lifecycle for the company’s most mission-critical solutions, but the amount of security bug testing done at the company was always curtailed by its labor-intensive nature, and the less-than-reliable results. “I could spend four or five days writing test definitions for our current fuzzing platform and even when I fuzzed our product, I got no results,” says Zdenek Ryska, Senior Software Developer at OSIsoft.

So when Microsoft Research approached OSIsoft with an invitation to join the Technology Adoption Program (TAP) for Project Springfield, a security bug testing service that runs in the Microsoft Azure cloud computing environment, the company was eager to participate. “We thought the cloud aspect would simplify how we performed fuzzing at the company,” says Owen. “We had 16 developers participate in the TAP between June and August of 2015. The service was so easy to use and delivered such great results that we have been a customer ever since. Thanks to Springfield, there is a five-fold increase in the number of teams using fuzzing at OSIsoft. The result is an improvement in the quality of our code and ultimately, the solutions we bring to market.”

Martin Peter, Senior Software Developer and Security Champion for OSIsoft SQL products was a TAP participant: “I was really impressed by how easy it was to get up and running with Springfield. After a brief introduction from Microsoft, I built my first application and began fuzzing in a couple of hours.” According to Pam Hawkins, Senior Software Developer and Security Champion for the AF Team at OSIsoft, the solution’s ease of use adds extra layers of testing to the development cycle. “We quickly learned how to write programs that created and loaded seed files so that it was feasible to add an additional layer of testing that we would not previously have had time to get done within our release cycle.”
Cloud-based service saves time and money
The OSIsoft PI System is capable of “wide queries” that handle big data—a popular product for many customers. Recently, Ryska used Springfield to test code as he added functionality during development of the product’s latest iteration. He found hundreds of bugs, reducing the number to zero over five development cycles. “We believe that any time you can do security testing earlier in your development, it’s better and saves time and money,” says Owen. “And because the service runs in Azure, we don’t have to budget for computing resources or staff resources to get the job done.”

Enhanced code coverage builds confidence
Today, developers at OSIsoft are a lot more confident that their fuzzing efforts are producing results. For Ryska, the level of uncertainty using the company’s previous fuzzing solution directly impacted his confidence in the code’s security. “Our other fuzzing platform was only as effective as you could write the test definitions. It could take months to fine tune them and you still have no idea how much code coverage you are getting,” he says. “With Springfield, in two days we had reports showing results, while with the other tool, we ran it for three weeks and got nothing. The confidence that we will find a bug, if it’s there, is huge.”

Hawkins agrees that a significant value of Springfield is the enhanced code coverage. “It’s fantastic that Springfield runs through so many scenarios based on your seed file. I can’t begin to think how much time it would take to test all my code paths without this offering.”

More secure code enhances business continuity
Rigorous testing is the norm in the industrial software market, but with Springfield, OSIsoft is set to raise the bar even higher. Thanks to the easy-to-use, cost-effective security bug testing service, OSIsoft can deliver even more secure solutions, boosting its reputation among customers who depend on its business intelligence solutions. “Springfield helps us to deliver higher-quality software,” says Peter. “That’s because we can use it more frequently to test new protocols.”

More frequent security bug testing that delivers actionable results mitigates the risk of service disruption at OSIsoft. A critical security bug detected in the field may take developers from across the company a month of concerted effort to develop and test a fix. “The cost avoidance we gain by reducing the risk of this kind of disruption to the business is of great value,” concludes Owen. “But the real reason we are so excited about Springfield is that, at the end of the day, our developers feel confident that they are building the best products they can for our customers.”