

Refactor: A Team of Superheroes Breaking Down Silos to Empower Every Tech Team to Collaborate Securely and Automate Everything



Michael Fraser
Co-Founder | CEO | Chief Architect
Refactor
<https://refactor.it>

Contact:
866.493.9367 x801
mike@refactor.it

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: *Mr. Fraser, would you tell us the vision behind Refactor?*

Mr. Fraser: We started Refactor in order to solve a problem. There are many organizations that want to be able to get into DevOps and DevSecOps using existing open source automation and security tools

out there. These tools require existing DevOps engineers and cloud security architects to be able to create tool chains for DevSecOps automation. These resources are the bottlenecks because they are in high demand and there is a low supply of them; the ability to collaborate with other technical folks is impossible if they don't know how to use the same tools. This is compounded by the fact that a lot of organizations are not only looking to get into the cloud but also modernizing towards digital transformation and need to get all of their existing talent onboard with automation, which is really about making the company more agile on the technical and security side.

We wanted to build a platform that would cater to the broader technical audience out there who create automation content, folks like DevOps engineers, but also enrolling those who consume this content, which are a large percentage of the technical folks out there. We built our platform to do that because those who consume content out there are visually focused, so we built a platform that is visually focused. There is a drag and drop component and ways to do things visually that existing Ops and security folks are used to, as they expect that. The other side of that, the DevOps engineers expect to be able to live in code and work within the tools that they are already building stuff within. Therefore, we married those together to have the best of both worlds in one unified platform.

CEOCFO: *What were the challenges in creating the platform and technology?*

Mr. Fraser: You do not ever get it right from the beginning. I think you have a good idea and you want to build something out and be able to get it out there as quickly as possible. Being able to take feedback and actually pivot is essential when you create new innovation. Receiving feedback from original customers and taking it to heart, as well as in the interim earning interest from the DoD and specifically the Air Force. We were able to fine-tune our overall approach and found our sweet spot is with organizations and vendors who create their own automation content and use the open source tools we support. It was critical to have feedback from customers and feedback from prospects to have the platform evolve into what it is today.

CEOCFO: *What were you surprised about that people wanted?*

Mr. Fraser: They wanted us to support open source automation tools natively. We thought originally that we were catering towards those who wanted it to be easier to use, so we steered clear of that at the very beginning. What we realized is that many organizations started understanding what their overall needs were and the actual requirements to migrate to the cloud or even support hybrid cloud type of environment. We originally were completely cloud focused and we concluded that customers we were catering to from midsize to enterprise, managed security services providers (MSSPs) and government customers like the DoD, were very keen to use open-source tools, so for us to support those tools was essential to what we have currently in our platform.

CEOCFO: *How do you reach out to potential customers and how would someone find you if they are looking if they are looking for help?*

Mr. Fraser: I have been participating in thought leadership speaking engagements, and lately, specifically around DevSecOps both in the commercial and defense space, like the Defense Innovation Network Summit that I spoke at recently. I also am going to speak at BrightTALK, and various industry events like RedHat AnsibleFest, All Day DevOps and DevOps Days. For me, thought leadership is critical for us to get our name out there, but also enlighten the community about our new perspective to DevSecOps. Aside from that, large industry events like the major security and cloud shows like RSAC and AWS Re:Invent. Those types of industry events are also critical because that is where a lot of organizations are looking for the latest and greatest, the next wave of technology that is coming.

"Our platform enables the wide breadth of technical talent that an organization has to assist with, as well as addressing the talent shortage, while enabling true collaboration when it comes to DevSecOps, but also empowers those that are trying to retrain and master new skills to be able to leverage some of the automation technologies available, from open source automation tools for infrastructure as code to security tools out there. We will continue to support a wide breadth of open source tools to support whatever solutions organizations need to create and iterate on for their organization long term."- Michael Fraser

Thought leadership is the main focus for us and a more grassroots type sales approach where we are focusing on sales folks that are able to get the word out for us. The other piece is having MSSPs and Vendors getting us into their midsize and enterprise customers, in a one too many sales approach. We even have some MSSP customers that focus solely on government as well. We recently closed an Air Force SBIR Phase I award, which stands for the Small Business Innovation Research contract that gives us the ability to do business with any entity in the entire government realm that wants our DevSecOps platform.

CEOCFO: *What are you learning about working with the government?*

Mr. Fraser: We know, as a startup, that we have to be careful about that, however, the good thing about this current engagement that we have with the Air Force is that it is all about dual-use technology, so you have to have commercial adoption in place and actual paying customers before you can even get into this program. Anything that we do that we create in our platform for features the Air Force wants, once we get to Phase II, which essentially is an engagement where we set up certain requirements that they have that we will build into our platform, those have to be dual-use because they very much want to make sure that we do not build features and functionality that are only government specific, so it does not pigeon-hole us into government only.

The other piece, I would say, is with this current program, they are really trying to fast-track and make it as easy as possible for companies that are innovating to be able to start doing business with the Air Force and the broader DoD as this was the first program that was joint, so there is also involvement from the Navy, Army, NGA and National Security. The goal is to get our technology to the broader government so that it does not impede them to also be able to use technology created by innovative startups because they understand that startups like us are creating the next new wave of technology that they want to get access to, when prior government red tape hindered or prevented it completely.

CEOCFO: *When you are speaking to the right person in any of the organizations, do they understand intuitively what you are doing?*

Mr. Fraser: The issue that we have currently with the new paradigm we are creating, is that there is definitely some explanation on the front end, particularly if they are not looking to try to automate in-house so they are not releasing their own software or they do not understand agile methodologies to how they deliver technology. I think that for us there is some education work for sure, however, I think that as companies are adopting further into cloud options, they are trying to become more agile in general as an organization and it makes the education on our end much less intensive. This is especially true for organizations like the Air Force or enterprises out there that have already gone down this route or they are already developing software in-house. For those that are not, then there is a little bit more education that is required from our standpoint. I would say 2020 versus even five years ago it is a lot easier to get in and quickly educate because a lot more organizations are up-to-speed on what the cloud is, and they want to be able to automate more as everything IT becomes software defined, or as I call it, IT-as-Code. Many, now, are even understanding terms like DevSecOps, which even a couple years ago they did not know anything about DevOps or DevSecOps.

CEOCFO: *Refactr was recognized as a Top Ten Security Automation Solution Provider by Enterprise Security Magazine. Would you tell us about that recognition?*

Mr. Fraser: Yes, absolutely! We have had a lot of inbound interest on what we are doing and that adds a level of credibility to what we are offering. The response has been good. We have vendors to enterprise companies that have come in asking to work with us around security automation specifically. While some of the other products in that list are more like SOARs (Security Orchestration Automation and Response), companies are realizing that they want something of a more general purpose from an automation standpoint to include security, not just being security-only focused. I think it has helped, not only with our narrative, but for people to understand the wide breadth of capabilities that we have as a platform and a company as well as that we are focused on ensuring that security is part of our DevSecOps automation platform. Organizations are using our platform to automate on the security front, as well, leveraging existing automation tools we support, like Red Hat Ansible.

CEOCFO: *What is your geographic reach today?*

Mr. Fraser: Primarily it is the United States and Canada. We also have interest from all over the world from South America, Brazil, and all the way to New Zealand. I would say that we are definitely looking to expand internationally in today's global economy and the ability for people to reach out and show interest in us all the way across the globe is really awesome but we also have to be realistic about how we are able to expand what we are doing here in the US. We have international interest with customers currently engaged with pilots outside the United States so we are looking to expand globally in pretty short order.

CEOCFO: *Are you seeking funding, partnerships, investments, as you grow?*

Mr. Fraser: With the Air Force SBIR Phase I contract we were awarded, on top of the Phase II grant that we will get, that will be anywhere from \$1.5 million to \$2.25 million, the Air Force will also match investment dollars one to one. Therefore, for every dollar we raise in our current funding round, they will match up to \$1.5 million, once we are awarded the Phase 2, and that is very enticing to investors. With this funding round we are looking to accelerate, because with all of the current momentum we have, we need to expand our company quickly. We are also very interested in establishing strategic partnerships, working with vendors in the cybersecurity space and enterprises that have dual use focus that can help us expand our footprint inside both enterprise and government entities.

CEOCFO: *Please tell us about your United States Air Force AFWERX award?*

Mr. Fraser: First off, as an Air Force veteran myself, I am excited to come full circle, to be able to bring innovation to the Air Force. This has always been a dream of mine, and now it has become a reality. The United States Air Force AFWERX Phase I award we received this March was super interesting. In November 2019 we launched the new version of our platform and messaging, focused on DevSecOps automation. The Air Force had also started a DevSecOps initiative in 2019. Through a contact of mine in the Veteran in Residence program that I was a part of through Bunker Labs and WeWork, I was introduced to the CTO of LevelUp, who is spearheading the DevSecOps initiative, Platform One. He saw a demo of our platform, and said we needed to apply for the Phase I program. We contracted with Long Capture to help us with the proposal process, and they were amazing. The proposal process started in mid-January, and we were able to submit ours before the February 12th deadline. Less than a week and a half later we got a letter from the Air Force saying we were tentatively selected. There were over 2000 proposals submitted, and around 400 were selected. Due to the fact this was a competitive process, we also have the ability to go sole source directly to Phase III, which means we can contract with any government entity directly and never have to go to bid with our platform. The next step for us is a

Phase II, which is up to a \$1.5M contract and can be extended up to \$2.25M, and includes fund matching, 1:1 for every investment dollar we bring in from when we were awarded the Phase I through 90 days post Phase II award, which will be July (90 days past that is October). So up to \$1.5M raised will be at least \$3M total in Phase II for Refractor.

CEOCFO: *With so many companies to look at, why should Refractor stand out?*

Mr. Fraser: We are solving a unique problem where there is a major talent shortage in cybersecurity and generally in technology across anywhere from DevOps engineers to software engineers. I think that organizations like the Air Force and enterprises are all looking for ways to enable their existing technical talent with products and tools that they can, not only get more out of but, help to retrain them into the future of IT, which is getting into public cloud and being able to turn everything, into a term I came up with a few years ago, IT-as-Code.

Our platform enables the wide breadth of technical talent that an organization has to assist with, as well as addressing the talent shortage, while enabling true collaboration when it comes to DevSecOps, but also empowers those that are trying to retrain and master new skills to be able to leverage some of the automation technologies available, from open source automation tools for infrastructure as code to security tools out there. We will continue to support a wide breadth of open source tools to support whatever solutions organizations need to create and iterate on for their organization long term.

