# DATATRIBE

## DataTribe Challenge Finalist Q&A: Dr. Anita D'Amico, CEO of Code Dx



DataTribe recently closed submissions to its second annual DataTribe Challenge, a global competition to identify and develop high-technology startups with a vision to disrupt cybersecurity and data science.

Three finalists [were announced](#), who will split $20,000 in prize money, and the winner will be eligible to receive up to $2 million in seed capital from DataTribe. The investment could also potentially include a follow-on investment of up to $6.5 million in Series A venture funding from DataTribe and AllegisCyber, a Silicon Valley-based cybersecurity venture capital firm.

In a new Q&A blog series, we are interviewing all three of the finalists to highlight their innovative business models, how they are disrupting their respective industries, and why they chose to participate in the DataTribe Challenge.

For this installment, we spoke with Dr. Anita D'Amico, Chief Executive Officer of [Code Dx](#), provider of an award-winning application security management solution that automates and accelerates the discovery, prioritization, and risk management of software vulnerabilities.

**Q: Tell us about your background.**

**Anita:** I have a background that is a bit different from others in cybersecurity. I have a PhD in experimental psychology, which I have applied to many domains over my long career. For most of my career, I've led teams of really talented people to conduct R&D and develop solutions that improve human performance of complex cognitive work. I've worked to improve human performance in the merchant marine, the space station program, surveillance aircraft, and cybersecurity.

I've been working in the cybersecurity domain since the 1990's when I was selected to initiate the first Information Warfare integrated product team (IPT) at Northrop Grumman. In 1999, I joined Applied Visions, Inc., a small software company, and created its Secure Decisions division to conduct R&D and develop new software technologies in cyber security. During the next twenty years we received funding from DARPA, DHS, Air Force Research Lab, and Naval Research Lab to do some really interesting research, and develop new cyber security technologies to improve cyber situational awareness and the performance of cyber analysts.

About 8 years ago I became interested in software security, and started pursuing R&D funding to develop innovative technologies in application security. That led to several research projects that developed new processes to improve efficiency and remove barriers to testing software for security issues. The Code Dx technology came out of that research.

Now, through Code Dx, I am improving the performance of people who are responsible for assuring the security of software, and of organizations who value application security.


**Q: Tell us about your business/idea.**

**Anita:** Most data breaches can be traced back to an attacker exploiting a software vulnerability. In fact, more than 90 percent of breaches in the Information Industry involve an attacker exploiting a vulnerable web application. So, the question is: Why aren't these software vulnerabilities being discovered and fixed before a software application is released?

A major reason is that developers and security analysts have been slow to adopt the Application Security practices that would discover these vulnerabilities early in the software development lifecycle. And why are they slow to adapt AppSec practices? Because testing software applications for security issues is labor-intensive and costly, and it produces a mountain of results requiring days of further analysis.

In short, to find most vulnerabilities in software, security analysts need to run several different types of AppSec testing tools against the code base and combine the results. Unfortunately, these AppSec testing tools are hard to configure and run, they produce a boatload of results, and the correlation and de-duplication of the results can take weeks of time.

Then the analysts have to prioritize which security issues to fix first, collaborate with the development team to show them what needs to be fixed, and track the entire remediation process. Then they report up and down the management chain about what they found, what was fixed, and whether a specific software applications' security risks are getter

better or worse across the software development lifecycle, or what is called the SDLC. I'm exhausted just talking about it!

Our ideas to solve these problems were: first, to remove the barriers to adoption of AppSec practices by making it easy and faster to do AppSec right; and second, to provide visibility into an application's security risks across the entire SDLC. We do this by automating the most labor-intensive activities in this process; and by providing a system of record that keeps track of everything that has been done with respect to securing the software through its lifetime.

**Q: What was the original inspiration for your company/product?**

**Anita:** The Code Dx technology started out in 2010 as a Phase I Small Business Innovation Research (SBIR) contract, awarded by the Department of Homeland Security (DHS) Science and Technology directorate to the Secure Decisions division of Applied Visions, Inc. We had $99,000 and 6 months to come up with a proof of concept for a new technology that would correlate the results of static application security testing tools (like Coverity, Checkmarx and Fortify).

I've got to give credit to the DHS S&T program managers who were aware over nine years ago that AppSec analysts needed to run and correlate the results of several static analyzers in order to find most vulnerabilities. The National Institute of Standards and Technology (NIST) and NSA had done benchmark testing of static code analyzers and found that none of them found most vulnerabilities. You have to combine several together and correlate the results to get good vulnerability coverage. DHS S&T issued a call for someone to develop a new technology to automate that correlation. We came up with a proof of concept that worked, and we received a Phase II SBIR worth $750,000. From there, we strategically bid R&D to start building out our plans for what eventually became Code Dx.

By 2014, we had an alpha version of Code Dx Enterprise and we deployed it to several early adopters. In 2015, we spun out a separate corporation to commercialize the successes of our DHS-funded R&D, and started putting our own funding into the product. We were later referred to as a "DHS SBIR Success Story."

Our product and our company has grown by consistently listening to our customers and incorporating new capabilities into our product. Customers and evaluators seem genuinely surprised when they see a new release that incorporates something they mentioned in the past; they say something like "You actually listened!"

**Q: What's your vision for the future … "What will the market you are pursuing look like in 5-10 years?"**

**Anita:** Hopefully, the market for securing software applications will be much less siloed than it is right now. The AppSec market is currently very distinct from the network security market; the users, buyers and suppliers for AppSec rarely venture into Network Security and vice versa.

However, I think that the boundaries will be blurred in the next decade. I foresee that the CISO will be buying products and services that completely integrate all types of cybersecurity and provide both a unified risk picture and the ability to focus on specific sources of risk, as diverse as firmware, software applications, network connectivity and people.

I also foresee that the CISO will have just a few dashboards that pull together every type of security risk into a single place. There will be fewer standalone products; everything will feed into a central place using standardized information exchange formats. The CISO and the security analysts will be able to trace security risks back to their many different sources – including insecure software applications, embedded systems, connectivity, devices, even people – and be able to see how different levels of security at each source affects the overall risk picture. And if they are developing new technologies – for example, through manufacturing or software development – the organization will be able to assess risks at various stages of a solution's development.

**Q: How does your business address pressing cyber and data challenges for the commercial sector?**

**Anita:** Commercial companies are terrified of data breaches, and many realize that most breaches can be traced back to an attacker exploiting a software vulnerability as a vector into the enterprise. Code Dx helps these companies to discover and remediate software vulnerabilities before an attacker can exploit them.

Commercial companies are also concerned about being able to demonstrate that they were proactive about reducing risks from insecure software during its development and release. To address this concern, Code Dx provides visibility into application security risks throughout the software development lifecycle, and serves as a system of record that stores data about AppSec testing and remediation that was done through an application's lifetime.

**Q: What attracted you to the DataTribe Foundry? Why did you choose to participate in the DataTribe Challenge?**

**Anita**: DataTribe is an investment company that understands cybersecurity and bootstraps new entrepreneurs. It's unusual to find investors who have long-term experience in, and actually understand, cybersecurity technology.

DataTribe rapidly grasped what Code Dx was about. They saw that Code Dx could make a difference, not just make them money. DataTribe also has resources to help new CEOs like me. Most CEOs of technology start-ups understand their technology, but are not necessarily savvy about the infrastructure needed to support the business. DataTribe provides access to accounting, legal, marketing, product management and other essential support services.

As a new CEO, I'm constantly facing issues I've never dealt with before, and I want the ability to call a trusted resource for help. DataTribe is that type of lifeline. Their foundry concept is based on helping new entrepreneurs to get through the business end of things so that we are in the best position to introduce new technology into the market.


**Q: What's your long-term vision for your business?**

**Anita:** My vision for Code Dx fits right into my vision for a future in which the CISO will assess security risks from a centralized platform. Code Dx is becoming a single pane of glass for assessing risk across the software development life cycle.

I foresee Code Dx as automating many parts of and managing the entire process of securing software, from the earliest stages of software architecture, through the entire coding process, and into post-production.

Code Dx will continue to expand the number and types of information sources it can ingest and correlate. For example, we recently began incorporating the results from network vulnerability management systems; this allows us to see risks to an application not just from its code base, but also from the network infrastructure in which the application resides. We will expand to other information sources as well.

But the biggest vision I see for Code Dx is to get the information we collect and process as the AppSec system of record into a form that reaches decision-makers and is actionable. Most systems present details that are meaningful to technical people. I want to develop new reporting capabilities in Code Dx that package the information into a form that the CISO can rapidly comprehend and take action on.

My longer-term vision is to be able to package up summary information about software security risks into a form that is easily understandable and meaningful to a Board of Directors. That type of data presentation will include insight not only into the problem areas, but also the operational impacts, and what is being done to reduce risk.


*We would like to thank Anita for speaking with us. Don't miss out on the opportunity to see the three finalists present and answer questions from judges on November 14th at City Garage, Baltimore MD. Click here to request an invitation to this event.*