Elizabeth Boggs: Nine out of 10 software breaches begin with vulnerabilities created in the coding process yet 90% of companies do not begin applications' security testing until code is in production because until now integrating applications security into development has meant a trade-off between security and time to market. Our next company up, Wabbi, has built a new SecDevOps Orchestration platform that enables large organizations to assimilate application security processes into existing development pipelines, to produce more secure code without having to sacrifice velocity or agility. Brittany, I invite you to unmute yourself and take it away.

Brittany Greenfield: As Elizabeth said, I'm Brittany Greenfield, I'm CEO and founder of Wabbi the SecDevOps platform that enables enterprises to deliver software faster and more securely. We all remember the Equifax breach, right? It's hard not to when they had to pay $700 million. And it's why it keeps coming up in the news once a quarter. But do we know why it was really considered the Seminole application security breach still to this day? It was because it was about a breakdown in processes. Equifax, like every other organization, set a policy, not to use a specific component, the patch [inaudible 00:01:17], on projects with personal information.

However, the developer being completely siloed off from the security processes still moved forward with it without applying the patch or even just using it because he didn't know that policy pertained to the work he was doing. And so fast forward two thirds of a year, before Equifax could find and fix it nearly half of America got some of their most sensitive information stolen. And while we may think this is the exception, the reality, this is still the norm that even though nine out of 10 breaches are due to software defects, 90% of organizations are beginning security after code's already in production. This is tantamount to moving into a house without checking to see if your foundation is stable and your wiring's faulty. They're not doing it because it's faster or cheaper. They're doing it because as development models have evolved, the security models have failed to keep case. And it's easy to understand that when this is what it takes to secure today's modern development pipeline and application.

So, this is where Wabbi SecDevOps Orchestration platform or Secure DevOps Orchestration comes in. What we do is analyze the existing tools out there, whether they're scanners or other controls, you then get to view that information in the project specific context, both in Wabbi, as well as in your existing DevOps and SecOps workflows.

And then Wabbi creates informed actions whether automated or a good old fashioned educated decision back in those tools, such as breaking the build in Jenkins or preventing a branch being committed in GitHub. And what we're focusing on here is really enabling people to do their job better. So how would Equifax have been different with Wabbi? We would have started in the same place where they would have set that policy not to use who's open source. However, the developer now having the application security processes integrated into his existing workflow would have been informed even before he started coding, not to use that component. However, of course, trust but verify, Wabbi would then call on the appropriate tools to check if the component was used and if necessary block the code from advancing.

This is about increasing human efficiency. If we think about some of the biggest developments in both development and security over the last decade, it's been about letting the team do their jobs better and automating the manual processes. Whether it's GitHub and GitLab or Datadog on the development side or on the security side, CrowdStrike, Demisto, and Phantom. This is about orchestrating and automating and centralizing these processes. So you can get APSEC owner, the focus that he needs to go help resolve problems. The PM can de-risk project delivery, because nowadays it's not just about decreasing cyber risk, but about business risk and what you need to know to remove bottlenecks. And the developer gets to make sure his code is going to keep shipping. He's not going to be that bottleneck.

And while this may just feel like common sense, the reality is here we are three years after our birth, and we're still the only platform that is fully integrated into every step of the development process. While you're certainly seeing some of the larger or global organizations doing homegrown, nobody, and DOD is no exception, wants to maintain that internally. Legacy providers have tried and failed to reverse engineer their products into the modern development pipeline.

There's of course, a new generation out there. However, they're taking this from securities approach and it's just shifting the bottlenecks and services are of course always important, however, they're not scalable. We want to keep services focused on helping strategy, not trying to just do more manual work. And this is not a move shot. By the end of this year, 60% of rapid development teams will embed these processes in their solutions. It's up from 20% two years ago. This is one of the reasons we're here today. We've just been awarded an SBIR around continuous ATO, which is really a natural use case for us, but the development organizations and the DOD and the broader federal government do not look any different. And this is exactly the problem that Wabbi is solving. How can we take specific contexts and then automate the decisions after it so we always know we're developing code with our specific security standards.

It is well accepted between security and engineering now that it is a shared responsibility model. And for us going through the VP of engineering, not only means that we're the sole security tool in their chain and we're not swung by other security spending, but we can finally start translating security into hard benefits. It's no longer this nebulous part of your nonfunctional requirements. We can improve efficiency and decrease the cost of developing secure code. Wabbi is incredibly sticky, scalable, and flexible. We're not just an orchestration platform. We're really the application security infrastructure layer in the DevOps tool chain. And we can be deployed rapidly. We do not have to be enterprise wide to get started. We can start no matter where you are in your DevOps or security maturity, even down to an individual team and then scale from there.

So why did we come here to Starburst? Why did we want to be talking to you and your broader community? Because you all are dealing with the top teams that are tackling the toughest problems and trying to set a new standard. I was recently asked by an investor, what's the difference between your commercial and your federal strategy? And I said, "There isn't." Federal organizations, like the DOD, had undertaken some of the same strategic digital transformations that the commercial sector has. It's about removing bottlenecks. I always love this Einstein quote to finish off with it, "We can't solve our problems with the same thinking we use to create them." This is why security has failed to keep up with development. And SolarWinds is a great example of how fragile the software supply chain is starting with application security. With that, I'll open up the floor for questions. Thank you for your time. And I look forward to continuing the conversation.

Adam Wong: Thank you so much, Brittany. A lovely presentation, really enjoyed it. My first question is if you can talk a little bit more about how your tool differentiates itself from other automated use case testing tools.

Brittany Greenfield: We're not doing any of the testing ourselves. What we're doing is we're processing that information against our policy engine, which you have to think of as being the contract between security and development for what your tolerable risk level is and how you control for it and what you're willing to let out. So we're processing that. That's different for a training platform than it is for a mission critical drone. We hold that master record and that's what differentiates us with our platform. And then we do the calls for you so you don't have to do the manual, work with that.

Adam Wong: Very good. I had a question with your long experience in cybersecurity, if you were to make one cybersecurity recommendation to everyone, what would you make?

Brittany Greenfield: There's no such thing as perfect code and there's no such thing as perfect security. And if we can all adopt that mentality, whether it's at the application security level or the network level, and stop trying to build walls and build better systems so we can respond, that's my number one recommendation is stop this binary approach to security and saying it's never going to be perfect, how can we at least be prepared?

Adam Wong: Very good. Thank you so much for answering my questions and for your presentation, Brittany.