Ep 46 Software Project management and the Shift Left

00:12
Welcome to the federal tech podcast where industry leaders share insights on innovation for the focus on reducing cost and improving security for federal technology. If you like the federal tech podcast, please support us by giving us a rating and review on Apple podcast.

00:36
Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Our guest today is Jeff kalamar. Chief Technology and Innovation Officer XLR, we're gonna talk about security and software development. But first, I have to tell you, we're recording this from mongst barbecue in lovely downtown Purcellville. And after this interview, that's been a while sober and get some barbecue. So what are you gonna order today?

00:56
Well, they have they have something at the top of the menu that is my favorite. It's called The Boss Hog. Oh, yeah, the Boss Hog is basically every smoked meat that they have. And there will be leftovers involved.

01:08
So it'll be wonderful. It's going to be a good afternoon. Okay, let's get serious here. I love to start off with quotes because I love quoting smart people. One of the smartest people I know is a guy named retired brigadier general Greg touhill. He's running cert now in Pittsburgh. And he famously said that security must be top of mind throughout an applications development. So agree disagree from a federal perspective? I mean, that's obvious. But how do you incorporate it in large projects? Yeah. You can't,

01:35
you can't argue with the generals Security does have to be top of mind. The problem comes in is when you realize all the other things that have to be top of mind to meeting the mission need getting the work done, operational stability, reliability, quality. Oh, and yeah, and security to there lots of lots of considerations for for teams to have top of mind to be able to do the job well.

02:01
So maybe it's a matter of priority. You can you know, you can Google list and find this I did the research this morning. This year 2023 federal agencies have $11 billion to spend on cybersecurity. So so how do you prioritize that expenditure? Isn't isn't worried about zero trust isn't worried about, you know, software bill of materials is worried about open source software? So where do you prioritize?

02:24

Yeah, I think it's, it's for sure about prioritization. I mean, yes, we have to, we have to make hard choices about what we're going to do and what we're not going to do and what we're going to buy and what we're not going to buy. But over the last, probably seven or eight years, I've also realized that maybe there are some both and choices to get to, and a lot of roads lead back to DevOps for me or DevOps dev SEC ops. And one of the things that the DevOps movement taught us was that you don't have to trade off throughput and stability. So you can get both of those things by implementing certain practices and having certain capabilities. Well, I think the same thing is true for security, too. So wouldn't it be great if it were, if we could get work done, we could get fast, frequent changes, we could have operational reliability and stability with our systems, and those systems could be secure. And I think that the the the evidence and the practice and the research and the stories, and even our own experience bears that out that you can't have all three of those things all together, there aren't any trade offs involved. So is the short phrase shift left is that we're talking about here to incorporate security in the early stages of development? Yeah, so Exactly. shift left is a is, is a phrase or term that's been been thrown out recently. And that is a key strategy for being able to improve our security outcomes without having to make those least as many of those hard, hard trade offs. So let's talk about what shift left really, really looks like? Well, first, let's talk about left of what and the traditional view of security or quality or testing or you know, a lot of these things is that it happened at the right side of whatever that schedule, Gantt Chart diagram, workflow process look like. You got your requirements, you build the system, you do all the things and then and then right before the system went to production, or is deployed to production, the security group would come in, you know, they do they do all their scans on all the software until you all the things that needed to be fixed before you actually went to production. Well, so we're talking about shifting left from that and integrating security concerns and perspectives and requirements as early in the process as we possibly can. That's in the architecture. That's the code. That's the components that we're using. And the behavior that's different is the teams and the programs are built Seeing these these systems, like, hey, reach out to your security counterparts, get them involved when in the planning of this, you know, whatever it is that you're going to do get them involved in the architecture of whatever it is that you're going to do. Get them involved in the technologies that you're going to be choosing and keep them involved throughout the whole process for whatever the life of that system is.

05:21
Every now and then I get to use fancy words because my wife's a Latin teacher, and so she once told me about this phrase called nomenklatura nomenclature, so I got to dive into nomenklatura here. All right, so there's a debate in the community about DevOps versus dev SEC ops there. It's kind of like, I guess, Red Sox, Boston fans, Yankees fans, they hate each other. So is this is this a topic? Or I guess what start with what what part of the divide you stand on,

05:46
that's part of the divide, I am on the side of the divide. That helps organizations win, and people find joy in their work. And if that means standing on the DevOps side, okay, if that means standing on the dev SEC ops side, okay. I try not to get too wrapped up around term terms and terminology. And try to look at the outcomes that we're trying to get here. And if the outcome is, hey, I want to I want to be able to deliver better higher quality software more frequently with higher, you know, higher stability, and I wanted people more engaged in their work, and I want to make sure that bad stuff doesn't happen.

Like, I think we can all probably get behind that, regardless of whether we call it DevOps or dev SEC ops are fluffy, pink bunny number four.

06:36
Well, we're recording this from a barbecue place. So I got to talk about cooking. And so if I were to bake a cake, and I was the big cake at 350 degrees Fahrenheit, or bake the cake at, I don't know, 130 degrees Celsius. Cake could take can taste good, no matter what you can call it, Celsius or Fahrenheit, we'd have that outcome, and the outcome is a good taste in cake or a good tasting barbecue here,

06:56
right? That's right. That's right. It's about the outcomes. And I find way too often that people get wrapped around the axle on drawing bright lines around terminology, and this versus that. And sometimes we lose sight of the why behind a lot of these things. And the faster and more focused and clearer we can be on the why I think 10 Things tend to work out a lot better.

07:17
Many of my listeners are involved in very, very large, complex projects. And they're using the hybrid cloud. And we know that there's a dearth of people actually working some of these projects can't hire people. So people talking about automation. So what do you view the role of automation is in software development, maybe looking for vulnerabilities in code?

07:36
Yeah, automation plays a huge role in being able to improve security or security outcomes. And so going back to that shift security left, framing in the in the typical way, traditional way, what would what would often happen is teams would would build whatever the system is, and then they sort of effectively pitch it over the law to the security group, who would, who would run their scans, you know, they take they take that magical security tooling, and they'd run it against the software that's been built, and they'd look for vulnerabilities. And again, that was happening really, really late in the process. And it was also really manually intensive, you know, to being on the other side of that of the pitching over the wall, those security teams were inundated with, I gotta run scans on all of the things because there's all these teams that are trying to make changes, we got to make sure that, you know, we're not introducing introducing risk, or at least mitigating the risk of the enterprise. And so that will take a really long time, and the teams will be blocked from going into production. Well, what if we turn that dynamic around, and just as a start, take those same tools that the security group is using, and bake that in, so that the teams who are building the software could actually use the same tools with the same rules to run those security scans in a similar way that the, you know, the security group is doing. And that's a start of that automation story of how we can get the throughput and the stability and the security all at the same time. We're all using the same tools. And we're using that automation to be able to do things that automation is really good at, which is run things really fast, really consistently, and give us the feedback that everything's okay or that there's things that we need to fix. And so baking those security tools into here's one of my favorite terms, the CI CD pipeline. Yeah, this is very good terminology nomenclature. Yeah. So baking those security tools in so we're looking for code vulnerabilities. We're looking for vulnerabilities in the packages or the other components that were the third party components that we're

using to build our systems. And we're making all those checks to make sure that we haven't opened up any holes or done anything that might leave us open to badness.

09:51
So see, I think in the in the spy movies, or like informants or something, but we're not talking about citizen performance here. We're talking about continuous integration.

09:58
Yes, that's right there stripe and having those tools consistently run repetitively run frequently run, like multiple times a day on every check in. That's the thing that's gonna keep us safer than we were before Anyway,

10:10
okay, let's say we have this perfect world. You're sitting downtown with a CIO of an agency, and you say, ABC, we should do it this way. And he goes, Well, yeah. And then another person or team goes, yeah, and and you all agree and, and it's a perfect situation. And then you're into the buzzsaw. And the buzzsaw is acquisition. Yeah. And so a lot of times with people in acquisition, they may not be trained on some of these types of continuous development, continuous integration. And they may want to put into a certain checkbox or something happens at one time. And and what would Ron Popeil say set it and forget it. Right? And so so where does acquisition? Should acquisition, learn more about flexible software acquisition, continuous improvement? Or where do they fit in this time?

10:51
Yeah, acquisition plays such an important role, not only the security, but really quite honestly, for the federal agencies to meet their mission and to get the goods and services that they need to do that. And that set it and forget it philosophy. Just to offer an opinion, I don't think it works anymore. Not in this this world of constantly changing stuff. I mean, let alone technology technology is changing in such a fast pace, I don't know how you you write a contract with a particular requirement and not expect that that requirement is going to change at some point in the very, very near future. So to the degree that we can incorporate change into our contracts, and value the importance of that change in our contracts? Well, that that is the role of acquisition is to be able to to continuously change to be able to meet the evolving needs of whatever the whatever the customer needs, I have

11:49
interviewed many companies. And when we talk about software, the concept of open source always comes up. And more and more people tell me is that, you know, most software today is really a developer, grab some code off the shelf, or from a library and plugs in here plugs in there. And, and they're all open sources, increasingly important model federal organizations. And so what role is open source and software libraries have and making sure the software is solid, and it can actually be continuously improved?

12:17
Right, this is an area that a lot of modern enterprises are really looking at, because they've had that realization that you just shared, which is more so today than ever software is to a large degree being

composed rather than created. So we're pulling all of these third party libraries and services and components, as you put it off the shelf. Hopefully, it's an approved shelf, that's a vetted shelf with stuff on there, but how do we how do we trust that those software components are, are good for our business or our mission. And, and there's a lot of organizations now that are spending a lot of time trying to understand what there is another term for your software supply chain looks like, and making sure that it is a trusted software supply chain, that we're not inadvertently or accidentally incorporating vulnerabilities into our, into our enterprise. And that is a it's a really complex problem. And it's an evolving area. We just if you want to look back to the executive order that came out not quite two years ago, so May of 2021. There was it was a lot about that it was a lot about being able to to manage and the software supply chain for the federal government in a more intentional in a more unintentional way. And and hopefully that promotes better security outcomes.

13:43
introduce Jeff earlier, he is the Chief Technology and Innovation Officer of Excel. If you want more information, you're the website, e x, c e, ll A. And if you really want to treat follow Jeff on LinkedIn, Ji AE l li, I mra. Why every day he comes up with I don't know how he comes up, he must have at four o'clock in the morning and in compose these things because he'll take an aspect of software development and and dive right into it. He'll dive into training, he'll dive into continuous improvement. And it's almost like a thought of the day or something. I'm wondering he should assemble those into a book or something because you really put some thought and he's linked to that, please haven't yet.

14:15
i Yes, i Yes, I know. I sometimes, you know, I It's like 10 o'clock at night. And I'm still thinking like scratching my head is like, what am I going to come up with? What am I going to write some most of it at this point is just got the habit of being in writing, being able to express thoughts clearly.

14:33
I'm thinking about the person who manages monks over here. I mean, they have management challenges, they have changes all the time, and have certain supplier difficulties. So I think some of the things you write about apply to the people who wrote monks here, down the street. I mean, some of your front areas it's it's a it's almost beyond soccer. Another software is managing what we can manage barbecue, you can manage ribs, or you can manage software

14:55
development, I guess. I also think that on that same point, I think there are a lot of fun things that the software and the technology industry can learn from other industries. I mean, touching on that that s bomb concept or software bill of materials, like, it didn't start out software bill of materials, it started out bill of materials, you know, the physical world of building stuff, you know, the ingredient list or the component list of what the stuff that's in this thing. And we applied that concept to software. And there's a lot of examples like that

15:24
you mentioned about compose, and in one of your LinkedIn updates, you talked about going down to the county center. Yeah, my wife and I've been the case since right place, and use the word compose

and I thought of orchestrate composing of orchestrating and, and one thing I noticed at the Kennedy Center is that when that orchestra played that piano, didn't move that piano stay in the same place, when you orchestrate things this piano could be moving could be going upside, she could be, you know, contracting outside bringing stuff in. So orchestration is a lot more complicated. It comes to software development than just a plain old symphony. Yeah, that's right. The rules, the rules have changed in the in the software world are are kind of different than the world, the rules have changed in the physical world, at least in terms of cost and friction associated with that. This is probably a whole other discussion. But that's where we got the Agile Manifesto from is realizing that that the world of software was very different than the world of, you know, building buildings and submarines and things like that. I got to put on your historian, there are people listening, this may not know what that references, it was about 1518 years ago, there's one e two and this top. Yeah, it's a developer. I said, we got a lot of troubles here. And one of the main troubles, by the way, was airline problems back then. And they figured, how can we solve it and they come up with some principles, like the Agile Manifesto, which is really had the repercussions even till today.

16:41
Yeah, it's a set of principles and values, all intended to discover new and better ways of building software. And I think they're still just as applicable today, maybe even more so than they were 20 something years ago, we still follow them.

16:59
Let's talk about orchestration and composing things. If you look at the different tools that are out there, and I've done 1000, podcast interviews I've done with people with platforms with tools, people with scanners, all kinds of things. And there are a lot of great project management tools out there. There are a lot of great code repositories, there are a lot of great X, Y Z's out there. But the problem is, is going down to Kennedy Center an orchestra. I mean, so Okay, Jeff, you got to put this all together, you got a diesel motor, and you got a plow tire, and then you got a barbecue pit. So make a big barbecue pellet. I mean, it's just it's hard to do, isn't it?

17:34
That's right. Yeah, it is. There's, there's no shortage of tools out there. And unfortunately, I think that's where a lot of people gravitate to most first is while I just needed a new tool for this. There's a new requirement out there, and let's just go out and find the tool that's going to it's going to meet the need, and they inject yet another tool into their, into their environment. And a lot of times those decisions can be counterproductive, because you neglect the maintenance of those things you neglect the training, appropriate use, you know, is it actually giving us the value that we thought we were going to be getting from the tool. And when encountering those situations, there are a few things that I'm clear about, that I've learned in my career. And generally speaking, the place that I want to start and that I advise others to start is you start with the people first, you get the right group of people together with the right skills, expertise, perspective and motivation, you're going to solve most of the problems just with that, then you can work on supporting them with the right process and the right policies in and putting those in place. And then once you get that figured out, then you can use that bring the technology to bear on making those things faster, more efficient, more effective, but start with the people first. And if you are

going to inject a new technology, and there are great ones out there, and there are many of them that you know, we should all be using. But start with the people first.

18:59
Let's talk about people in downtown Percival here, two blocks from here, there's a mechanic named Mike bridges, bridges automotive. And I'm sure if you went into his shop, he'd see a certain limited number of tools. He doesn't, you know, run to a problem by no the tool maybe occasionally. But he optimizes the tools that he has now. And I think maybe this get another tool. I mean, I'm sure that if you did a survey of let's say, a federal agency, you might find some tools that aren't ever being used. That's right. And so Mike's got a small shop here. He's got to use every nine sixteenths wrench that he has. He can't have three or four different kinds there. Yeah. And so I think the discipline to use a great tool or may not think that, you know, one tool is got the answer is something and the idea of maybe humans can can integrate with these tools look better. I mean, there's a shout out to Mike bridges. He's my mechanic. I've been reading up reading up on dev ops and Dev SEC ops and everything and there's a company called GitLab. It's the middle of this game and they do surveys. They did a survey in August of 2023. And they said, security is is the driving force behind DevOps? Yeah, security is all of a sudden 20 priorities is getting the top of the prayer instead of efficiently. It's at the top and security wasn't mentioned that mountaintop 22 years ago, was it it was there, but it was certainly

20:13
not in the same way. Yeah. And there's only there's only one word that I think I would take exception with with that, with that statement, security is the driving force behind DevOps, I think I would say security is a driving force. Oh, there are some words here. Yeah. So we all we all know that, that we want better security outcomes, we want them more efficiently, we want them more effectively. We want them for lower costs, lower cost, we want all those things. And we also want the work to get done. And we also want operational stability. And, you know, if if security is the top priority, well, then let's see what happens when your system start going down, because you've invested all of your money in in one thing over another and you haven't invested in other areas. So I think every organization is different. And every context for every organization is different, and their priorities and needs are different. And rather than talking about a one size fits all, and security is the most important thing or something else is the most important thing in all circumstances. I think for each organization, and maybe even each team, they need to find the right balance or the right integration of of all of the things that are important. I teach at

21:31
a fancy pants school, so I get to coach philosophers. And so I'm gonna quote a famous philosopher, and I want your observation stuff. So I'm gonna quote the famous philosopher, Yogi Berra, he said, The future ain't what it used to be. So when we look into the future of this complex environment, hybrid cloud, compliance, regulations, constant attacks, where do you see this heading in the next few years? Yeah.

21:56
The future is gonna be fun, John, the future is gonna be fun. With me, I

21:59
tell you that much, here's,

22:00
here's what I think is fun about it. First, first thing, at least, that I believe about the future. Things certainly aren't getting any less complex, they're getting more complex, that that's the trend. And maybe they were always that complex. And we're now just like, kind of figuring that out. But things are getting more complex. And so we have to be able to respond to that or accommodate that or operate successfully in that sort of environment. I think that's that's thing, number one. Thing number two is, things are speeding up. And it certainly feels like that a lot of people would say that it's been speeding up for, I don't know, ever. It's certainly in the technology world, the pace of change is just, it's just accelerating. And when you've got speed with complexity, that starts to be, you know, difficult, challenging to manage. And so the last, so the last realization is understanding that complexity is increasing, and the pace of change is increasing. What does that really say that we need to be putting in place? And that's the capacity or the capability to be to respond constructively to change. And that's at the organizational level? Do we as a, as an organization, a group of people that are aligned to a common mission? Do we have the ability to constructively respond to the changes inside and outside of our organization? Do we, as human beings, individuals have the ability to be able to respond to changes in our own environment constructively and grow and develop that growth mindset? And then from a technology perspective, are we bringing the practices and the capabilities into our organization to manage and implement and use and operate technology that is going to allow us to respond to changes in a constructive way? Because it's an inevitability, we know that something's going to change. When that happens? How are we going to be best positioned to respond to it?

23:54
Well, that's great information. And I think he may want to make a shameless plug for a book. I mean, I'm big fan of wanting to tell the listeners here, one of the shameless plug number one from Jeff kalamar. John,

24:05
I'm gonna be leaving this with you because I brought me up. Yeah, no. So this book is called investments unlimited. It's from IT revolution. So if anybody out there has read the Phoenix Project, or the unicorn project, or the DevOps handbook, or the book accelerate, I'm huge fans of all of those books. This is sort of like the next in the series. And it's written as a novel, just like the Phoenix Project to the unicorn project. We're, and by the way, if you haven't read those books, you really should, if you've read the goal, maybe I can expand the reach of people who can relate to this book, if you've read the goal by Eliyahu, Goldratt. Again, novel format, and I think it's the it's the subtitle of this book that really says it all. For me, that's a novel about DevOps security, audit, compliance and thriving in the digital age. So it's a narrative about how modern organizations can incorporate all of this concepts DevOps, secure Are the audit compliance in a way that looks different than it used to in the past and that traditional human review very document heavy kind of kind of way of working into something that's efficient and effective. It actually produces joy in the people who are doing this. And it helps the organization win. So this is the book about that. It's a narrative. It's a story. It's an engaging read.

25:24
You'll love it. You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest Jeff Gala, more Chief Technology and Innovation Officer Excella and we're signing off from mongst barbecue and lovely downtown personal Virginia.

25:38
Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcasts.