Ep.59 How to Deliver Software with Impact

00:05
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Today in the studio we have two distinguished gentleman. We're gonna talk about software development and fishing practices for the federal government. Our first guest is doe Han Luca. He is the Principal Fellow for modern software delivery, and Keith Meelo. Our guests in the studio today are doe Han who Luca. Again our guests in the studio today are doe Han hula, co principal, fellow modern software developer and getting that name hook up. Try that again. Do Han Doohan, Doohan, Doh, Doh, Doh, Doh, Doh, Doh, Han goolka. Here we go. Okay, here we go. Good pause, try again. Our guests in the studio, our dough Han goolka, principal, fellow modern software delivery, and Keith Meelo, Engagement Manager from a company called Excella e XCELL a.com. If you want more information, they have all kinds of stuff on their website, all kinds of activity on the Twitter feed. They specialize in software and modern software delivery. I think this is a big question for many people who are listening here. Today we're going to talk about four or five main topics, we're going to delve into something called FISMA. High impact. We're gonna talk about supply chain, maybe touch on the ever present zero trust, maybe see about it. So what actually sells different? What's your special sauce? What's going on here? Before we begin the gentleman with the unusual first name, tell us about your background and and you can criticize me for not pronounce your name correctly, if you want.

01:41
Hi, John. Great to be here. That was a pretty decent pronunciation. So no criticisms there. I am, originally from Turkey, you know, came, you know, immigrated to the US, once a Virginia Tech for computer science. But 15 plus years into my career as a software, developer slash author slash speaker, I write about technology. I like web development, cloud architecting, and delivering agile solutions.

02:18
Right. Great. That's gonna head on. And Keith, maybe a little bit of background, please.

02:23
Sure thing, John. Thanks for having us. My name is Keith. I'm, you know, from Maryland, I did my undergraduate degree there and my master's program. I we've been working with federal Consulting at the government for probably the past 20 years, and through various number of agencies, and currently working with the national security market for Accela. And I've been partnering with Ilhan to help our modern software delivery practice, you know, deliver some of the most secure code that we can be, you know, contracted to deliver for the government. One of the things that we've been trying to do is exceed the compliance outcomes that typically, you know, our clients are looking for to comply with FISMA regulations, and go above and beyond and delivering more outcome based results.

03:22

Well, Jeremy, I didn't realize it, but I would expect N D now we're gonna get an executive order. And it's gonna mandate John Gilroy to say, an acronym every 32 seconds in these podcasts. So I gotta have an acronym. I don't have a choice here, gentlemen. So we got the acronym of choice, I'm gonna reach into the grab bag and pull out an acronym. It's going to be FISMA. High impact. Okay, so when it comes to software delivery, so 100, what does FISMA high impact mean? And how does your company work with the government to achieve that? Absolutely.

03:51

So FISMA stands for the Federal Information Security Modernization Act, it was a law that was passed in 2002 to ensure a baseline level of security for information security systems that are deployed within the federal government. So high impact there stands for High confidentiality, high integrity and high availability. There are also medium and low impact levels. And, you know, currently, Keith and I have been working on a high impact solution. And you know, as he mentioned, in the past

04:26

four years. So normally, this is contrasted with different category called FedRAMP. Ah, so maybe a quick discussion on both those how they compare?

04:34

Sure, yeah. FedRAMP is the is the public facing side of it. So if I had a product that I wanted to operate within the federal government, it would have to go through the FedRAMP program to be certified at a low, medium or high impact level. So, you know, for example, in our FISMA high impact solution, we can only use FedRAMP High certified products. Got it. Got it. So

05:00

two completely different subjects, as long as our listeners know, this different sides of the same coin makes it Yeah. So Keith, my question to you is, in preparing for this interview, I read all kinds of articles about software development. But everyone's got a different number 80% of all software code developed today is from off the shelf software. It's 72% 59 out of two percentages, but I think people are starting to worry about, you know, memory safe languages, you reusing code. And so So where does this fit in discussion with secure software?

05:32

Yeah, it's one of the things that we try to look at is, you know, how does the supply side risks vector factor into the solutions that we're delivering from the off the shelf products that you purchase, and you implement it on the client site, to custom code that you're building, although you may use open source libraries, and some of that may actually, you know, contain some supply chain risks. And from that, we need to, you know, have a high degree of vigilance and not, you know, trust the sources as much as we do and kind of tails into the zero trust stance of always making sure that there's no service within your boundary that you implicitly trust. At, you know, the the process that we're working with, with our clients in the national security market, we're doing a lot of custom code development. And with the FISMA, high impact systems, there are a lot of principles that we need to meet, I believe there's in excess of 700, different security controls. And we need to build to those FISMA, high impact settings for anything that comes through the door, whether it's an off the shelf implementation, or if it's a custom code delivery. And we're also looking into building compliance to those security requirements in our AI and data analytics offerings as well. So if there are data processing systems that are happening within the federal government space, we're applying the FISMA principles to that as well.

07:23
But that's, that's a hot topic, you know, I mean, everyone's talking about this, this of artificial intelligence. So maybe you just chime in here real quickly and talk about how this can help a software development just a little bit.

07:33
There's been a huge insurgence of AI assist tools that came out recently, it's kind of started with GitHub co pilot, and burst into wide adoption with chat GPT. And now, Microsoft has moved that technology into being and they have also announced moving, you know, similar technologies into the Microsoft Office Suite. So with AI assisted tools, it's a great way to learn, and understand new topics that were unfamiliar with. However, we need to recognize that, you know, when we ask AI to generate some kind of code for us, or, or, or, you know, it tries to improve what we've written, it's merely a suggestion, it's just someone tapping you on the shoulder and telling you, hey, you know, consider this, it is otherwise a huge risk to just simply copy and paste code. And this is similar to other tools like Stack Overflow, it's just in general, a big mistake to just, you know, copy paste code, and use it without understanding it, because we've seen it in the supply chain, some bad actors sneak in, you know, inconspicuous looking code into a project widely used project, and then they later tried to exploit that, and similar exploits exist in the AI space as well. bad actors train the AI to you know, develop bad code, basically. And unassuming developers can easily put that into their software and introduce a vulnerability that they're not aware of into their systems.

09:24
Yeah, at one point someone smart told me once you have a choice between people writing bad code or computers writing bad code. I think, you know, people writing bad code is is what the government is looking at. With that the these AI models also are hungry for inputs. So as you go through and you're putting your code out there, you're using the variable names possibly that are integral to your systems. If you have to pay attention to whether that is, you know, pushing information that should not be pushed beyond the government boundary into the AI model itself.

10:12
Keith, I'd like to maybe jump away from Ai, maybe another topic down the road, I want to talk about something even more difficult. And this topic is human beings. This is the hard part. I once worked with a brilliant guy, I mean, software engineer, he's, he's worth multi multi millions right now. And he would not use a seatbelt. He just has a thing he drive around with, I think beep and, and he just, he was smart. He knew everything he could code he could do engineering is a whiz, he was an athlete. And he hated using his seat belt. And so so my question to you, Keith is, so how do you? How do you control the human part of that? where's the where's the user base? How do you get buy in from the user base on the software? Security? It's, I think it's a big part of the discussion.

10:58
Well, for me, it starts with the team, the the folks that are putting these software pieces into place, the people from the government that are managing either the off the shelf solution, or the custom coded solution, or the AI and analytics solution that we've put together. Getting people to care about the outcomes is is really key to making a team very security conscious, mission focused, whether you're working with Immigrations and you want to, you know, ensure that people coming to America to participate in the American Dream have the smoothest transition possible. Or if you're working in a law enforcement system, and you want to make sure that the downstream users, the people might be, you know, special agents or something like that, that they have the right level of support, and not put in harm's way because of, you know, failing security practices, you know, at the level of building software, so aligning the government mission to the team's mission, and building that level of buy in, you know, helps helps people put their seatbelts on. And one of the things that has been really integral to the way Excel works, and the way I've definitely managed my engagements is to try and build a culture of trust. And with that culture of trust, we have people on the ground who are able to identify security shortcomings and bring them to the attention of both the government and both the everyone on the team so we can have an open discussion and find the best ways forward. It's not always the case that something like that happens sometimes, if you're going through code, maybe even code that you wrote, and you take a look, and you haven't, oh, no moment, I shouldn't have done this, when I put the code in a year ago, let me just fix it real quick, and not tell anyone that's kind of an anti pattern, what we try and do is, you know, bring that to the forefront, we have the conversation in this realm of trust with the client with our people, and we figure out the best ways forward. That is really key to getting everyone like you said, to put on that seatbelt to do the right things. And it's something that we found our federal clients have really appreciated.

13:28
Well, Don, I know from Turkey, I'm going to introduce you to how they speak in rural Oklahoma. I go there all the time. And the phrase that you're using or Oklahoma's you got you a die, lemme die lemon, let me give you a dilemma here. The dilemma is the federal government wants to move to zero trust. And the other hand, you know, they have a lot of legacy systems that maybe a tough fit. And so the dilemma is Do you rip and replace do you what do you do and how do you make that choice? And you know, legacy systems? At what point in time is it? No, we gotta, we gotta hold good home to carry can't fix that motor anymore. So, so, how do you answer the dilemma of moving to zero trust in a timely manner

14:10
moving to zero trust is a is an attitude that needs to be shared across the organization. And it is impossible without the right enterprise level software available to everyone at the organization. Because there you know, lots of IT systems that require admin access, etc. And if it's not, if that access is not maintained in a manner, where you know people can you know, check in and check out or only you know, the amount of time time they need it, you know, we we kind of break the zero trust circle right then and there. It is easier to implement in newly built you know, Greenfield systems and your for example, at a current system, you know, We don't have access to the runtime environment, we don't have access to the production systems. So, you know, whenever we need to do something, we need to declare that we're going to do something. And if, you know, if we don't declare that we consider that a, a bad act in and of itself, so we train every team member, to be very careful about, you know, how they behave around the system. So it's an attitude from the, you know, most junior team

member all the way up to the top, and it requires, you know, Thoros, support and, and, and rip and replace, in some cases, because the DNA of that zero trust has to be built all the way into the internals of the application. One mechanism we use is least privilege access, which the users of the system are only given access to functions that they require to perform their jobs. And they can only see the data that they need to see to operate within the system. So it's about, you know, reducing the attack surface. It's about limiting access, and the time and the window of opportunity to do something bad.

16:22
Okay, so I have a question about the early days of the Internet and a question about today, and involves names. I don't know, maybe, maybe you or maybe your father, study this. But in the origins of the internet, that's something called Archie, they had something called Veronica. And they had a lot of fun with these early names. And it was kind of a light hearted thing. And that's continued to some ways. In some ways, it hasn't. And today, we have something called Google's Dora Gra, have nothing to do with Archie. But so tell us about Dora. And where's this fit discussion, especially the way that Excel handles software development?

16:53
Well, I was gonna say the door research project is, you know, being run by Google, it's a collaboration of 1000s of different contributors. And it is trying to answer the question of what's the best practices in in the DevOps world. And as they dug farther into DevOps, and the the research project matured, over time, they realized that they were uncovering not just what's good for a DevOps world, but what is good for software development, what is good for organizations to, you know, enable actions to happen. And they started with, you know, taking some key measurements, and they prepared, you know, the state of DevOps reports on an annual basis, the most recent one just came out. And it's a, you know, a very handy resource for folks that are looking to dive into the modern software world, to begin to figure out how these different tools and components that everyone's been using, kind of fit together and lead to, you know, what we call elite performance metrics. And I'm sure Don is our Principal Fellow of delivery would have a much more in depth and

18:23
and I think that's what the listeners want to know, they want to know, okay, you know, Excel has had drastic growth in the last 15 years, I've seen it, and it's got to be a reason for it is that just, you know, best talent, the best process or so what's the secret sauce? Oh, hon, what's the magic?

18:39
That's one of the most difficult questions to answer, because we always pay in ourselves when we are writing, you know, responding to RFPs RFIs. You know, how do we explain the way we work? And because, you know, well, when it comes out of the washer on the other side of it, and we read our competitors, our RFPs, and our fives, you know, everyone's capable of writing beautiful sentences, and, you know, use the right buzzwords and everything, to, you know, on paper to represent themselves. However, at Excel, you know, we've been at the forefront of agile from day one. And, you know, it is always shocking to people who join Accela just how agile we are to the bone. Being able to iterate and push forward relentlessly is, is one of the keys to our success. And, and also, you know, just part of selling the core tenants of, you know, the way we work is, you know, speed to value, you know, we deliver value faster than others, you know, we're not, and I'm

not talking about we deliver our technology faster than others, we deliver value faster than others. So it's really important to distinguish between those two things. And then we operate at elite performance. You know, we've taken the door research program to heart how it can It's DevOps, things like continuous development and tie that to developer happiness, or, you know, customer outcome. And then we also focus on delivering organizational impact just beyond the project that we deliver. So for example, when it comes to cybersecurity, we focus on delivering security outcomes, and not just compliance. It's, you know, kind of, once again, relatively easy to sit there and check boxes with a compliance officer. But it's really difficult to actually, every week, you know, have a team check in about security, and make sure we're secure, it's really difficult for an engineer to self identify an issue they found. And then we celebrate that, as a team, congratulate them for finding that vulnerability and coming forward. So so that trust and freedom that we give to each individual on our teams, and this also includes subcontractors that we work with work with everyone becomes a team member, equal team member. So you know, all these factors combined, I think is part of why we succeed. Every opportunity that we get to be on

21:08

case Compliance would be I go to your garage, I hope you got Yeah, you have a seatbelt. And it worked fine. So going beyond and looking at the outcomes is I sit in the car and watch you drive and write your seatbelt. So that's the next step, isn't it?

21:24

Yeah. Even in kind of our, our practical situation, we deal with government agencies that are experimenting with cloud native architectures. And I say experimenting, I mean, it's something that's known in the outside world, but in the Gulf cloud, this is something that they are, you know, embracing, some agencies are embracing it quicker than others. But there are some things that we have to go in, as, you know, Excel consultants and remind the government that they, you know, should put passwords on their GenCon notes, you know, it's, you know, it's not necessarily in the purview of us delivering a software package to the government in which the vulnerability arises. But we are active, curious, and engaging our government clients on many levels, to help them better their security position. So, yeah, it's almost like going in to make sure the seatbelts are there on the car, but also checking the brakes before you

22:33

Oh, boy, next level up is really good. So Don, I have a friend who works for BP. And he's software developer, and, you know, regular complaints, and I'm talking about hot sauce, and all the regular stuff and everything else. And I'm just thinking about no your job and keys jobs a little bit different than that. I mean, you got like, you're like you're both in the race is my friend, but you gotta like a log carrying you behind you call the compliance log. It's the cell arrays. And so I think everything you're trying to do as far as agile software development, I mean, it's difficult and hard to accomplish, but you have this added burden of compliance has got to get a ticket to the next level, maybe that's a differentiated with Excel is that it can also accomplish this magic trick with all this burden of compliance and security.

23:14

Initially, it was a log, however, we've kind of conquered that process, and became great partners with our information security officers, and that whole security operation center. And by the way, you can notice me I'm trying to avoid acronyms as much as possible,

23:36
we'd have a mandate, every 12 minutes, we have a mandate here,

23:40
I can make my sentences much shorter by dropping a minute. So we've become partners. And you know, working with the CIO level and down, we have switched our technologies to the right one. So we shifted our systems were set our security to the left as closer to the developer as possible. And we've also leveraged that shared responsibility model with AWS, where we leverage technologies like AWS fargate, where AWS is responsible of the runtime environment, and we just run our containers on top of that. So all of this has allowed us to master the compliance aspect of things to a point where now, we are the ones as a team that are letting the organization know about vulnerabilities that are coming up in the wild, as in, you know, not only we apply our patches before there can even be guidance issued in in the agency, but you know, we've patched them pushed out to production already, but we're also practically communicating that vulnerability. So, if you play with the system and work to improve the system, it is very possible to become, you know, to gain champions within the federal government to help you succeed. And, and you know, remain very productive. In fact, when we pushed, we shifted left, we've reduced our own M budget operations and maintenance budget by 90%. That's a staggering amount. That helps save a ton of resources for our team to be able to further innovate and further push those not bleeding, but leading edge technologies that can further improve our efficiency.

25:30
So Keith, I'm taking notes here, I'm writing down elite performance, reducing cost. And I'm trying to come up with a title for this podcast you're on. I'm thinking the title may be these five words, organizational impact beyond project delivery, because yes, it's the seatbelt. Check the brakes, too. That's what you're doing. You're going beyond

25:50
I liked that title. That's that really kind of syncs up with our delivery philosophy?

25:56
I don't have any acronym. There's no hunt. So we're in trouble have gone with an acronym the donee? Yep. Well, I'm gonna ask you both a quick question that we have to cut off here. Everyone likes projections next five to seven years. So I'm gonna ask Keith, first, where do you see this whole system evolving the next few years? And then we'll toss to DOE Han. So Keith, project development next five years, what's gonna happen?

26:20
What's gonna happen? All right, I'm putting on my, you know, Magic Hat not being over what pops up in the magic eight ball. I will say that there have been a lot of executive orders and presidential memos that have

come in up recently. This has prompted folks, especially OMB to take a look at contract language. And I'm getting a feel similar to early 2000s. When FISMA came out that, you know, there will be an across the board update to contract language, which will be mandating zero trust principles, either compliance, in part or in whole, for the NIST definition of what zero trust architecture is. So I see that gaining momentum. I also see the government looking outside of top down regulation. So one of my clients in the national security market has taken a look at the key measures from Dora research project, and has begun to systematically create metrics around those for their project portfolios. So we have folks in the government agency that's looking to private industry, and in these best practices for software development, to implement their policy as well. There are some additional kind of innovations happening. One is AAS cow, which is almost going to geek out a little bit. It's like a markup language for FISMA compliance policies, those 700 Plus policies for a high FISMA system, you can actually tag your code where you're complying. And you can show how you're complying. And you can meet all the requirements. So you don't have to do 1000 pages of documentation, when you get your authority to operate on a FISMA high system, you can actually just mark up the code. And, you know, that lets the security personnel, the ISOs, the information security officers understand when something's changing, rather than relying on the project team itself to come back in and have that conversation. So those are my predictions. Yeah. So.

28:45
So Kate says more shift left to Han, what do you say?

28:51
More legislation? Hmm. So I've had a unique journey, you know, because being a, you know, hands on coder to now being several layers separated from that. It's kind of like watching a musical it's, at some point, you realize that all the C level sweet folks and managers and non technical folks, they're just looking at the play, but they don't know what's going on behind the scenes. And from my perspective, software development is still having its, you know, wild west moment. So it's like, where civil engineering was maybe in the early 1900s, or late 1800s. And, you know, today we don't, it's unacceptable, if not criminal to build a bridge, that that will collapse and, and, you know, kill people, and it is extremely scary. The systems that we rely on are built with just very little checks and balances, there is no personal responsibility, and we need to kind of get to a place where we treat Software Engineering as seriously as civil engineering or architects. And perhaps at the state level, we need to start certifying folks and and you know, there needs to be consequences to delivering bad code.

30:17
Well, we're gonna have to end our conversation our kind of running out of order. I would like to thank our guests doh Honolulu cup principal, fellow modern software delivery, and Keith Meelo, Engagement Manager from Excel. Thank you, gentlemen. Thank you, John. Thank you for having us.