Addressing Security in the Agile Space

Tue, 8/30 2:33PM • 51:25

SUMMARY KEYWORDS

security, products, understand, environment, vulnerabilities, christine, controls, devops, agile, hr, project, tools, approach, attack, security requirements, surface, organization, system, terms, culture

00:15
Well, good afternoon, LinkedIn Live community and those out there in the webinars space. My name is Charles Maddox. And thank you for attending our monthly webinar. This month, we're focusing back again on security, and how it's impacted in the Agile space and within agile development. This time I got my esteemed co guest and co host, Christine, I catch and she's also going to give you some perspectives. She's with Akuna consulting, and we're great and so much appreciative to have her here to share some of her wealth and knowledge around this topic as well. Oops, introductions here. My name is Charles Maddox. For those that don't know, I'm the founder and CEO of the eye for group. We've been in business for the last 10 years in the Agile space based out of Dallas, Texas, a lot of expertise around this cybersecurity space, as well as the Scaled Agile Framework, and Dev SEC ops as well. And yet we were been here in the community, we love to, to talk with you more. But without further ado, I'll turn it over to Christine for her to give a brief background on herself and what she's been doing over the last few years.

01:32
Hi, everyone, I'm Christine I coach. Yeah, I'm start my career within it. It was long time ago, we don't need to go there. But and then I moved to project management, program management and so but last 10 years, I'm concentrated on teaching practices and coaching. 20 years ago, when Asia alizee Man, you know, introduced, I was one of the one first one adopted this comparing to traditional Predictive Model Management. That's why I applied this. And then of course, over the years, security become much more important and cybersecurity become now more important. That's why the importance of thinking AGL, having AGL mindset and following HR principle and practices becomes much more important. That's why I am here last couple of years, with economic consulting in Washington, DC, we concentrate on the you know, HR training, as well as the you know, creating learning journeys.

02:45
All right. Thank you so much, Christine. And yeah, I've been fortunate to work with Christina over the last several years, with training opportunities, and just brainstorming and leadership topics. So it's been a great, great journey thus far working with Christine. Well, what we'll jump right into it to give you an overview on what we're going to talk about today is, you know, we're really focusing this this topic to those that are in the security, cybersecurity space, as well as those that are in the Agile space. And the the topics here are meant to give us the opportunity to find some shareable or collaborative ways of looking at how we come together as a unified organization or unified team and in dealing with these

these aspects of agility and security. So if you look at this, quote, here is a good way of kicking off this discussion. There's no silver bullet here, or you can't build more secure software unless you understand the threats in your system. Meaning that there's really, you know, there's no silver silver bullet that you can implement, that can solve all the problems within your software development space with regards to security, it's something that you have to continually evolve and get better and better at and and learn more and more about your domain and how it's growing and how things are changing in the environment. Okay.

04:19

Another thing to consider being in this, you know, information age that we're in this digital age, there are more digital products springing up, left and right, from our vehicles, to our watches to our headsets. I mean, this digital technology and software is embedded in everything. And with that there's an opportunity for vulnerabilities and someone to attack that system. And it's the quality gaps in the holes and Nienow practices that we may not implement along the way that give rise to the growing number of you can see trillions of dollars in revenue As in costs are being expended are forecasted to be expended on these security issues in the cost that it causes. We're talking about things in terms of systems downtime, you know, patches that have to be installed, you know, going back and, you know, recalling some of the deployments and releases that have been put out there because of, you know, faulty products, but the cost is, is ever growing, because of the number of digital products that we continue to put out in the market. So we need to take, you know, close a close look at how are we building these products? And how are we aligning ourselves around more secure products? So this Gartner report is actually gives us some some guidance on looking at how, you know, where are these vulnerabilities at in our systems, so they call it the attack surface expansion, we're going to build on that that word a little bit more here attack surface and what that means, but an attack surface is is anything in your system, that there's a potential for a vulnerability. And so we need to acknowledge what those surfaces are. And, you know, monitor and be ready to act to be able to prevent in sometimes even in the very, we call advanced areas, we even apply artificial intelligence and machine learning algorithms to be predictive and understanding where these vulnerabilities might be on our attack surfaces. So as I said, as the digital product complexity grows, so do the preventative technologies that we have to implement onto our products that help that help us with expanding our knowledge and preventing our attack surface. The identity system defense, that's another area in you might, you know, an easy way to understand this from those that might not be in a security space is like Single Sign On authentication into systems. So knowing who the user is that are that is coming into our system or using our system, to then also to to prevent potential attacks from, you know, erroneous or fake identities that are out there that are trying to exploit our systems. Okay. A big impact into the supply chain management. So, as we know, you know, we're paying like what, in here in Texas, almost close to $6 a gallon of gas. And we know that there was some market issues in the supply chain issues that may have been a carryover result from the COVID debacle that we had, but, you know, another again, we can see how sensitive our markets are to supply chain issues. And if you have a big attack on a supply chain that can drive a lot of downstream impacts to you know, prices going up into not being able to use your systems and, and ultimately to companies having downtime, not being able to ask as usually, if you have a big

08:00

alright. All right, I thought I heard a little bit of background noise come back. But no, no, no worries there. But so yeah, supply chain issues are another major area that could be that could make our costs go up exponentially if we don't have a way of monitoring on the supply chain. Vendor consolidation. So one thing that we're also to looking at from a cost standpoint is how do we optimize the vendors that we're using and the tool stacks that we're using, for example, on security management? So that's going to be a big trend coming up as well? How can we be more efficient in that? So is that that dev SEC ops approach on how to shorten cycle times making sure that we're being as reactive and responsive as possible, and it's saving costs in that area as well. Okay. Another area that we want to look at is the cybersecurity mesh. And what we're talking about, you know, if you're familiar with the IoT environment, where we're talking about cloud data centers, we're talking about devices and understanding those architectural, intertwining, that also need to be monitored and, and have security applied in that level of infrastructure as well is another area that is a trend that Gartner predicts is the up and coming big area of impact. And then the distributed decisions that need to be made in terms of an organization's applying their security practices in a way that can be in a somewhat centralized fashion, but also to allow for a decentralized model for decisioning. When you have a remote workforce, for example, that is, you know, being global, in that case that there may be data centers across the globe and how do we how do we maintain that that environment in a secure way, when we're distributed in such a fashion. And then lastly to number seven is beyond awareness. And we need to be ahead of the game ahead of the curve in terms of what are the human behaviors that we need to be accounting for, and also to, you know, taking progressive steps into applying into our algorithms, ways that, again, can account for potential human error, human behaviors, and you know, the human interface reaction, the human interface aspects of a system as well. Okay. All right. So I mentioned before a little bit on the attack surface. And then on every attack surface of a product, oftentimes, when we look at these terms here, and these approaches to cybersecurity, we're talking about already deploy products. And, and we haven't gotten into the Agile development piece yet, we're gonna get into that. But when you look at the product itself, when it's out there in the market, you know, from a DevOps perspective, that's just a part of the cycle, because we need to be reactive and be able to build the next feature and be able to, to patch the system properly, or address the security issue. So with our deployed products, there are attack surfaces. And then we actually have an aspect that's being exploited, that we call that an attack vector. And you can see here some of the common attack vectors that we might be familiar with, I know, you know, you don't working in an enterprise environment, you have these, these phishing emails that come back, you know, come through your, your accounts, just to make sure that you're being aware that you're not downloading some virus into the system. But you know, what we're what we're showing here, these common attack vectors are very common on, you know, deployed software products. And so we need to be aware of those, we need to understand where it is at in our development process that we can to prevent some of these from the very beginning. And we want to be, you know, cognizant that these are some of the things that we're ultimately trying to protect our software products from, right.

12:12

So when you're managing this process, from a cybersecurity perspective, you're managing the attack surfaces, and ultimately trying to prevent as much as possible any of these attack vectors from coming in, they oftentimes call this a vulnerability management program, you're managing these vulnerabilities. at a large scale, you have a program of doing my monitoring, assessment, potentially running some

penetration testing, oftentimes, and making sure that your system is preventing such attacks. And and also to try to get ahead of the curve in terms of you know, assessing and simulating remediation support, and doing a running reports on an ongoing basis. So a vulnerability management program oftentimes is what an organization puts in place to make sure that they have these aspects manage as much as possible. Alright. So ultimately, we're trying to reduce the vulnerabilities on the attack surfaces with that vulnerability management program. You know, so you're seeing something, you know, some of the aspects being called out here is like identifying, you know, your physical assets and digital assets, do you have an accounting for them? Do you have a configuration management plan that, that has these under control, constantly reviewing policies and controls within your organization, to making sure that we have these things under control, we're gonna get to two as well. Again, we're, there's a connection here between existing products that have been deployed and new products that are under development. So the policies and controls can also apply to how we apply our development practices, going forward to make sure that we're accounting for reduced attack surface and ultimately, reduced Attack, attack vectors coming in, alright, trying to reduce complexity within our development products, also to try to strengthen our systems in terms of their vulnerabilities. So ultimately, maybe removing an attack surface altogether, that it doesn't exist or reducing the threat of the vectors coming in at on that particular attack surface. And then, if you can't remove it completely, you can also to try to shrink it, you know, make sure that there's not as many opportunities within that potential attack vector to that we, that potential adversary could exploit. Right. So overall, when we take like an assessment of our security program, our vulnerability management program and what we're putting in place in terms of controls and procedures and policies and tools, rules and monitoring our monitoring approach. How are we posturing ourselves, and that's what we call our posture. That's your security posture that you're, you're showing. And it really is your level of visibility to the inventory and the assets that might have vulnerable attack surfaces, and the controls and procedures that you do have in place that that are innate, that are able to detect and contain potential attacks. And then, of course, your ability to react to potential threats when they come come down the line. And then also to last but not least, your ability to be optimized with your approach and how many controls and things that you have in an automated fashion being applied in your environment. So that's what we call your posture, and how you're measuring and making this approach visible to the outside world. Okay, one tool to do that, or there are many tools to do that. But oftentimes, you might employ a framework to do so which gives you guidance on how to lay out some of these monitoring and these policies and controls that you need to use to help you evaluate and, you know, manage your security environment and then presented a certain posture for your organization. There are many different frameworks, as you can see on this slide, very popular one is the the NIST or the National Institute of Science and Technology, that there is an organ as a government organization, that actually is a partnership between government and private, the private industry that have put together a framework that allows for the benefit of the

16:46

private industry and government industry in government use quite a bit, but as well as in the private industry as well. But then there are other you can see there are other frameworks out there, the PCI CIS, and one of the things about the frameworks, just to just to know is that they can be very catered towards certain industries. And certain areas of focus, you know, maybe some is ours, some are it, some are more, you know, government related, you know, there are different focuses and different coverage of controls and compliance as well. And you could see here in the scale gives you an idea of,

the more robust are the ones that are have a lot of controls and coverage versus the ones that are more weaker, and are probably more in a more geared towards specific industries of focus. Okay. So, when you start to look at the development process, when you're building new products, and services, how do you take into some of these? How do you take into some of the security controls that might prevent, you know, abroad abroad, or to attack surface or certain attack vectors, you know, to be in existence in the first place. So, you know, coming from like a framework that I just showed on the previous slide, you may select out certain controls that might align with your requirements and planning process, your continuous integration, continuous deployment process, and then that way, you have specific things that you're trying to gauge and measure to make sure, you know, right from the beginning of new product development, that you haven't, you have identified a need to have a secure product, and you're trying to build secure products, right from the start. And then how you might implement some of these products are in some of these are some sorry, some of these controls are in some of the common tools that that are out there. There. You can see here, we've overlaid a lot of the planning your traditional agile lifecycle approach here, the from a planning perspective, a continuous integration and deployment. And it's a continuous operation, there are certain tools that we can use to implement and track some of those controls and policies with our within our environments or development environments. So that would be a way that you can, you know, there might be a tool stack in here, that might be something that you're currently using. And you could see that hey, well how how might some of these controls be implemented through either logs for, you know, a definition of done that you might be tracking through, you know, a program like JIRA even and have a team aligned on some of the criteria to make sure that you are hitting the right control points that you are wanting to achieve in terms of maintaining a good secure development approach.

19:51

And then what we know from this is, you know, it's a very popular term that we call out this these days is called dev SEC ops. So it's a dev. It's a DevOps approach with a, a tighter focused on security, making sure we're calling out those security requirements throughout. And then you can see here, as I laid out even more specifically, around the security aspects and the actual lifecycle aspects, how might you use some of these tools in this dev SEC ops approach, in a continuous way? And then ultimately, as we know, that, you know, to actually make an artifact or manifest of this from an agile perspective, we call it our definition of Done. And a definition of done is the the manifest of what are the what is the level of doneness when something is done and deployed? Knows in an agile world note we're talking about here? What does it mean to be done? And what does it mean to be done, done, not halfway done, develop, develop, done, but not security done? Or is developed, done but not released? Know, what does it mean to be done done, and done doesn't mean there's only one thing, you know, it's done when it's in the customers hands, and they're using it and is secure is a high quality deliverable that is secure. And so just like any other requirements that might be non functional. And maybe in this case, a security requirement is non functional, that we need to account for it in our definitions of done. And so ultimately, the things that we just caught up in the previous slides in terms of these controls, the output of these controls and the measurements, and the compliance of these controls, they would also to be captured in a, quote unquote, definition of done for our products. All right. All right. And then lastly, here, I wanted to call out that, you know, here's a good slide that, you know, those are listening in, you might want to screen capture this, but these are some common terms in the dev SEC ops environment, that just account for a lot of the things that I just shared. And things that from an agile practitioner, if you

haven't been in a security environment, for that long, these are some good words to understand the definitions up, we cover quite a bit of these already. But I would, you know, challenge you guys to go out and research and just, you know, Google and find out what the definitions of these very common terms used in a security environment that it's, you know, we're trying to build either building security products, or we're going to be moving into this environment one way or another. With these products, as I mentioned, you know, in these days, everything has a security risk potentially. So good, a good list of DEV SEC ops terms that I would advise that any agile and security practitioner, understand and know, in that way, we'd be more informed and knowledgeable about what's going on in our environments. So with that, security and agile finding the right balance now, you know, how do we know? So oftentimes, we've looked at security as being something from an Agile team perspective and development teams say, hey, well, that's a security group over there, they handle that stuff. They handle security scans, and the policies and the compliance and that. But, again, as we know, from a DevOps perspective, we have shared ownership, we should be looking at this as a shared responsibility across the board for our teams. So what is the right balance? And Christina is going to want to bring you in on this and help us understand this a little bit better. But when we're talking about having the right balance, you know, what do you think about this?

23:45
Okay, you talk a lot. All right. I'm gonna put a couple of things. But we have actually poll questions. I like to put this forward first. Okay. Let's get the feedback first from the audience. Okay, Mohammed, can we run?

24:13
Great. Right, Christine, can you see the poll question? Did it pop up? Yes.

24:17
Yes, it did. Hopefully, all the participants. Let's see what type of answers we will get it because it will help us to address their questions and so on.

24:30
So the question is, how do you feel about the increased focus on security in the Agile space? All right. Let's see here.

24:52
A few more people that can go at least Okay, I think we're pretty close to. Yep. All four people took the poll. All right. Do you want to go on to the next poll? Christina?

25:16
Yes. The next question is how do you feel about the secret of HR projects, you know, having security embedded into the HR projects? For your projects, I mean, think about your organization. But you think about it, are we sure that it is handled, you know, or you are not sure how HR projects handle security, or security is concern for you, but you'd like to learn more about how they're addressing and or security is a major concern for you. And HR projects or other codes are not what you are thinking that we want to know. Or think?

26:07
How many you might have to run that next poll for us?

26:12
Well, okay,

26:15
so both questions should have been, they were both answered. Okay, so on question, one, we have 100% on glad that security is being taken care of being taken seriously. And that our team is doing everything possible to protect our data. For question number two, we have 75% that I'm confident in the security measures we have in place, and 25% of security is a concern for me, and I'd like to learn more about how to address it in Agile projects.

26:45
Okay. Thank you for the replays, guys, what is first of all, what I want to bring it up, whether the you're running HL adaptive project metadata methods, or predictive traditional project methods, it doesn't matter security should be part of it. Because you listen, Charles, all the way till this point is the time has changed now, you know, 1020 years ago, having you know, implementing Single Sign On was, you know, good solution, it resolved bunch of issues, but today's world, we are living in different worlds. That's why the just pre prepared the, you know, the solutions, you know, just adding a couple lines on the project plan, it is not going to resolve the issues. If you want to be reactive, you have to be step ahead of the current new cybersecurity issues to whatever is happening on the market. Okay, if we can close Yes. But how we can find the right balance of course, you know, you're gonna run the projects and if you start thinking all those security related items, how it's going to work, I can hear you saying this because security requirements is extremely heavy as well on the you know, project and we are trying to be more adaptive, understand what needs to be done run iterations. And so it's the same way actually, how the HR principles works, if you can move to the next slide, because I have quite simple overview over there. You see, because we know and also you know that last year we celebrated 20 years of age I'll manifesto principles publication, right now is quite widely employed. But understand that you know, the what we are talking about the scrum Kanban lean it and all this DDS TTS other two you know system they are methodologies frameworks, the idea is having the mindset understanding that you know, continuous learning also is the key in this field is not there is no one standards structure, it says you know, you are HR now, actually there is no such things, because if you are agile, the changes, you will keep adopting it and moving forward. You will be keep learning new things. Okay. That's why actually if you have this mindset, it works with security, all the security related items 10, new inventions, usage of the new tools and everything works very well. That's what I'm trying to say there is no one training there is no one book that you will read and you will say okay, next 10 years. I am good with this knowledge That's why understanding to security requirements and what needs to be done actually it is quite benefits to your project and that's why if you add this mindset to the security mindset as well as HR mindset to your current tasks, activities projects, actually you will have much better speed and flexibility Okay, that's why a when we talk about to HR practices or HR development, we ensure that is not being a jewel, but employing to DevOps and Dev sack up is part of the structure

because whatever your needs, you should be open to accept those changes. And until you have this you cannot mitigate security risk in your Agile projects or traditional projects whatsoever.

31:02
Yeah, hope this makes gives you some clarity on this the expectation you know, there is no one magic pill actually, I want to go back to Charles at the beginning you mentioned that you know, there is there is no one solution fits everything there is no one major curl you know, you will such such described it and will resolve all your problems, all your security issues, unfortunately, there is not not such a thing, but you need to do you need to learn to continuously learning continuously understanding what is happening on the innovation side of tour, what are the stuff is available for you and for for your personal life and, you know, that's why the impact to the our privacy, all this comes with you know, understanding and continuous learning and being open minded and accept the change, because the change is happening quite so fast. And sometimes it's tiresome, I can understand but this is the environment 21st century theory. Okay, Charles, can we go to the next slide? Or I can stop if there is any question I see there are some questions or hybrids, someone says yes, I am not too much fuss about methodologies, because it should be work package team members, you know, work streams, they need to make a decision about the methodology they use is not a methodology, whatever the methodology fits your environment, your task, your activities, you should be using this important thing, understand the security part of it. Understand, you know, if you are dealing with external vendors, if you are Oh, you know, your tool is going to be used by the public or open to other system and all this stuff needs to be understood. Okay, this is the key. That's why I don't think too much about you know, which methodology to choose within HR umbrella, any methodology, whatever fits your development structure, where your team your environment, is the right tool, right methods just ensure that you review the security requirements, privacy requirements, confidential requirements, all this stuff comes in a package, you know, it's one and you should consider all this stuff. So if there is no other question, we can move on to the next slide. Anything else? Great. Okay, if there is no question I see that there is a slide upcoming webinars Yeah.

33:54
Christine, there is a question we just wanted to the public is how do we manage security in cloud

34:00
it's this guy's it doesn't matter the weather the cloud or the your next room? Data Center? Is the of course how do you choose the cloud? I mean, I'm not talking about you know, for the organization using two coffee shops, cloud services, but it doesn't matter. The cloud is just the flexibility it gives you you don't need to you know, get your hardware and manage the all the security pieces within your infrastructure located in one location. Cloud gives you quite flexibility that you can add remote server infrastructure and depends on the you know the cloud service you are selecting, they can provide the services as well. Here my only distinguish is whether you are small business large enterprises that you will choose because if you are a small business currently Right having to datacenter in house is quite expensive from the security perspective. That's why the cloud actually provides better solution. But again, it's depending on your situation. But from the project management perspective, it doesn't matter of security needs to be part of it, you have to ensure that you know, all the security requirements handled in the clouds environment, as well as your local database data center. So you remember the

hackers that attacked the data center without the cloud. Cloud didn't create the cybersecurity issues, the defects and the you know, mistakes and the environment and the infrastructure creates those issues. Not the cloud.

35:50
Let's make sense. Yeah, actually, Christina, I reply in the type in answer to that, too. I didn't, I didn't realize that. It didn't show to everyone. But yeah, I made the same points that you made that security, a security, whether it be cloud or non Cloud products, one benefit that we do have with the Cloud products is that they knew that that was an issue, like take AWS, for example, they have, you can become an AWS security practitioner, because they they know that you can get training on their tools on how to manage security. So from a tooling standpoint, they've, you know, they got some tools that you can use, that can help you monitor and report on and help prevent those attack surfaces and vulnerabilities that I was explaining. But, but yeah, so if you don't, you know, you don't have an advanced tool, like an AWS or an Azure that can account for those tools or account for those security threats, then you got to, you know, you got to have another way to monitor and address those those threats. So

36:59
definitely, definitely, it's that's, that's why it's always look at the from the holistic perspective is not just a one to one server one, you know, environment is a problem, you have to look at holistically this whole solution. Yes.

37:18
Do you have any other questions or comments that anybody wants to bring up? Right now? I think we've moved into the end of our, our webinar here, and we're open for comments and questions. While we're waiting for some questions, for Christine, to pop up, I wanted to get your opinion on something. You know, when we were now the security has become a big focus for our teams when they're building products. You know, we didn't always used to have to work very closely from a development team, with people with security backgrounds, and how can we build a better alignment? Understanding because there is, you know, the security group, they do have their own initiatives are trying to build. And then we have development teams that have their own initiatives that you're trying to launch these products. But there's a big overlap here. Yeah. I mean, building secure products. So how do we build better relationships between these two groups? And what have you seen? And, you know?

38:29
Yes, yes, it's unfortunately, this is what I see as well. But as soon as I start, you know, initiation initiated project program, that's why I introduced to ensure that, you know, everyone understands what we meant with HR, what we meant we did DevOps or dev SEC ops, because DevOps is a nice short term, but doesn't mean just developers and operations, but the testers, the security, the architect, needs to understand that we are on this together. And you're absolutely right, because what happens, I'm smiling, because all the time I see the same thing. You know, when you identify resources and Security says, yep, 20% we cannot tell you the who will be the one whoever is available, will attend your meetings, and you know, we'll think because they have their own looks, work as well. But this is the biggest mistake, you see, the security cannot be taken lightly, especially if we are dealing to you know,

the products with the end users. No, you have to do everything possible to prove that you need the security folks embedded within the team. They are there at the beginning as a designer, so I understand during to you know, the testing the execution, and so, the role might be you know, reduce from full time to part time or 25% And, but they have to include it and what is good about it, that what you show was at the beginning, all the slides, I know we will share with the participants and you know, they should take this and share with their project sponsors, executives. And so this is key, because you don't know where the vulnerabilities, you know, you don't know how the end user is using where they are going to use it. You know, because we have everything on our cell phones today, you know, they might be you know, the less on data, whatever the reason, or they cannot reach to, you know, they are vendor data, they might hook up to the, you know, coffee shops, internet, you see, you don't know where the vulnerabilities is. It could be anything, because I have my sunglasses with microphones. I use as a headset, but you don't know what is, you know, what else is going out from my, you know, coming out from my speakers on my sunglasses with this is, that's why the security who is going to use this tool, how they are going to use this too. That's why you need to full time security resources, especially at the beginning. And your slides was very right on, they should use this to you know, create the arguments with the sponsors.

41:22
Yeah. Another question I have, too, is that the culture, oftentimes that maybe an organization doesn't have an you know, you know, I'm a new, I'm a CISO, coming into an organization. And we're building products that we know, are going to be potentially at risk for attacks. But I'm coming from an organization that they just don't have a security focus culture. And also to there's a culture where people kind of work in silos. So have you what have you seen as a way of kind of breaking that culture? mindset? I mean, how do you get it to that

42:10
age? Yes. Yeah. Okay. That's it is it is very important, what I found actually running, you know, 1520 years is a project program manager. approach needs to totally change, you know, now is in my projects, programs, I have coaches, I have leads, and more people actually, you know, create trusted environments. You see, this is because this is the only way you can change the culture, culture doesn't change, top down. culture doesn't change, when the executive says email, oh, we are moving to Agile tomorrow, everyone is empowered. It doesn't happen this way. Culture change happens from the bottom up. And for this unique people on the grant, supporting two teams, explaining that I was just in a meeting this morning and saying, No, give us a plan. I'm saying no, we I like to build the plan, with your inputs over there. You see, but because we need to train those folks, we need to explain them the approach and then taking ownership without thinking firing. And you know, like, they will lose their job, if they make a decision or to take the ownership that's required, then, again, on this front training. And continuous learning is important. But the team should have a group of people they can trust. It could be that's why the new names for this the coach, it could be coaches, it could be program manager, it doesn't matter. But when they have the trust that people they will be more open. share the information. This is the key. And my next webinar on PMI that's I'm talking about the collective intelligence. This is the reason you see bringing teams intelligence to the upfront because there is a loss of intelligence expert knowledge in the teams that we lose it because they don't speak up. See, they don't participate for whatever the reason, but this we need to bring up we need to change the culture, make it more

open, understandable, acceptable culture and agreeing on to you know, this agreement. We can be disagree, but still you can talk or you can say you're, you know, thoughts and everything. agreeing or disagreeing, you know, this is a key, but talking is important. That's will require the cultural change. And I know it's certain organization especially The more traditional organization is more difficult. But I think it could be done. It could be done. Definitely.

45:08
Got it. Yeah, that one thing to just like to share, and I know, you know, we do, I'm actually a researcher at the University of North Texas, in this space of agility and security. And one of the findings that that I've found, through researching all the research papers that are out there, that was that's like, the biggest hurdle that people have found is this cultural issue with trying to implement better security practices within their development environment, it's just that they had a culture, you know, they've inherited a culture. And you want to focus that, that closely on that. And they also to have a culture that just not that collaborative. And so with those two things, that that combined where you just don't have a very security focused culture, and you have a, you don't have a tradition of having a very collaborative culture, that is a very risky culture to having big vulnerabilities pop into your environments into your product. So that's one of the key things that I've found so far in some of my research out there. So though this

46:18
really interesting research you do is you mentioned that, but it is important. Yes, you're absolutely right. You're absolutely right. All right.

46:30
Questions, comments coming in from anyone? See, anything on the link? Y'all got this going on LinkedIn live as well. And I'm not seeing anything there either. Well, we can do we can move on now to upcoming webinars, actually. So Christine, you want to give an overview of the elite agilus program?

46:58
Yes, sure. That's what one day

47:05
you give an overview of this and what this is about? Yeah, if you can see, can you see it yet?

47:14
Not yet. I thought it was the next slide. Anyway, we can share with the participants that Erica, this is actually the second consulting we created this elite HR this website, there is punch of information, membership site created everything anything related to HR, from the you know, the frameworks to approaches, the methods, tools, everything is available today. It's over there is Kurupt you can have the you know, the short version of the videos, the blogs, V logs, and content a bunch of content is over there. With this opportunity, we are giving three months free access to all the participants information is in here the in detail, but I'm sure we can share this information with all the participants because if you use this link, we will not ask you to you know, put your credit card or any information, you can just register and see what is in it. If you like you can stay if you do you know, if it is not something for you,

you can just browse it and put your comments. We are quite open to comments, but it is good site. It gives you an idea what I like as I mentioned the V logs and the podcasts information and Webinar recordings are over there is just you know, you can just listen pick and choose whatever you need. It is good site, I recommend to register.

49:01
Alright, thanks, Christine. Another opportunity for those that are out there too, is a training program through the i Four groups Academy. So newly launched Academy for those that aren't aware of cyber agility dot Academy and cybersecurity agility professional. And essentially, kind of what you're looking at is a combination of product management, DevOps and Certified Ethical Hacker. So it's, you know, giving you an idea of the security environment that we're in the opportunities of vulnerabilities and threats. And then how might you within a DevOps environment account for some of these from a product management approach. And so that's the that's the goal of this program. And yet, please visit cyber agility a cat cyber agility dot Academy to get more information about this program. All right. Have any last questions or comments before we close out? Well, thank you, Christine, so much for your visit with us today and sharing some of your knowledge and hope we can do this again. And this was some good news, the topics to discuss today.

50:25
Yeah, it was great. Thank you very much for inviting me. And looking forward to feedback. Any questions, the folks can reach me as well as you, you know, we are here to help you get this. All this knowledge share. Thank you.

50:40
Thanks, Christine. And then yeah, this this webinar will be published it will also be to on on YouTube and will be shared with those that attended or registered, and we look forward for you to join our next webinar. So be on the lookout soon. Again, we have a monthly webinar, usually the last Thursday of the month. This time it got extended because we we were a week over we postpone this this webinar this time, but usually the last Thursday of the month. 1pm or 12pm. Central is the is the typical time we we give these webinars so until then, thank you guys so much. And we will see you next time. Have a great day.

51:20
Bye for now.