Ep. 42 Vulnerability Management for Federal Systems

00:00
This is John Gilroy from the Federal tech podcast.

00:02
And this is Willie Hicks from Dynatrace.

00:04
Today we're going to talk about observability and federal technology hit the music cloud.

00:14
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 podcasts.

00:37
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Everybody wants to know what's going on, they want to have visibility into their networks, so does the federal government. So today, we're gonna maybe chop that up into small little pieces, we're gonna talk about hybrid networks, network visibility for Federal Information Technology, we're going to drill down to some specific suggestions made by an organization called Sissa. And hopefully, in 30 minutes, when you're done, you'll walk away with some some, at least some concepts about observability what companies can help, and what CES is doing to help our listeners maybe understand a little bit better. But first, I have to introduce my guest. He is Willie Hicks, federal CTO from a company called Dynatrace. Dyna T R A, C. E,

01:21
Willie, how are you doing? Well, in Great to be here?

01:24
Well, we set the stage. Now we gotta do the hard part. It's always easy part, you know, you know, during COVID, everyone's online and and you were to handle that to him and staff. So they switched everything to the cloud, hybrid cloud, public cloud, private cloud. And what's happened is some people are looking at and going, well, we're vulnerable, because a lot of these situations weren't as carefully vetted as they should have been. And maybe it introduced vulnerabilities in the systems that could not have been there if they're more careful. But we survived COVID. And now we have to consider the whole idea of looking at vulnerabilities. And maybe

for the benefit our audience, you give us just a little 22nd nutshell description of Dynatrace. And, and the topic we're gonna talk about today.

02:07

Yeah, okay. And well, first, let me just say it's a, again, a pleasure to be here again, with you, this is my second time. And so Dynatrace, we are an observability company. And what that means is, is that we provide agencies with the ability to understand their applications, their, their application landscapes, their software, and to understand it from what we call the full stack standpoint. So from the end user all the way to the desktop all the way to the database. And that allows users in and agencies to get unprecedented insight into their security posture, their application performance, how their users are interacting with the applications, and so forth. So it really all of this is tied together with AI, Enzo is all kind of predicated on this idea of automation. So we tried to do this super simple and make it as easy as possible for our customers.

03:07

So Dynatrace, we could have this conversation walking down the streets in St. Louis, because big companies have problems removability. And we can do this, you know, in Rio de Janeiro, everyone seems to talk about this. So let's drill down. And let's talk about how companies fail how organizations typically fail with this whole concept of observability?

03:26

Well, when I think about how companies fail, I think about it from a couple of vantage points on what I see with, with agencies, what I see with companies, they try to do it themselves, kind of they take the DIY approach, they try to, you know, stitch together multiple tools. So in this is this is kind of this is typical in many agencies where you've got this, this tool that you've got a lot of tools out there, for collecting logs for like collecting metrics, you now got the clouds. So you you're bringing in metrics from the cloud. And so for observability, to work, you've got to have all of these data sources, kind of, you know, combined all this data into, you know, they call it a lot of things now, data, Lake houses, data, lakes, and so forth. But you've got to be able to collect this data, to understand this data to analyze this data efficiently. And what I see a lot of times is agencies, they tried to do it themselves, they sometimes they throw in the middle, maybe a correlation engine or some way, and then they'll do some dashboards on on top of that. And ultimately, what they find themselves doing is just still back in the war room trying to figure out with how to solve a problem. And sometimes I also see the kind of the opposite of that, where they're not bringing in multiple tools, but maybe they're focused on one just logs that just may be scraping logs. They're just trying to use that to understand not just you know, their security posture, both performance and when there are problems. They're always digging through logs to try gotta figure that out. And And honestly, those methods, especially as environments have become more and more complex, they just don't work anymore.

05:08

So we got a big problem here. A lot of people in the cloud, a lot of people observability true as companies is true and federal agencies, okay, okay. So Dynatrace can help companies with a platform that makes it easier and saves them money to have this good observability into what's going on the system. But this, this whole problem of what's going on, is not just isolated to the commercial world, I mean, the federal government

recognized in fact, Sissa it just in November, last month, they came up with a binding operational directive saying, hey, hey, Willie, we know what you're going through buddy. And and here's a few ways we can help suggestions. And this has been a kind of a big deal in the industry as far as data management, and it's kind of a big deal, isn't

05:49

it? Oh, it's a huge deal. And you know, what Cisco came out with? So so this is, so what CES is talking about here from this binding operational directive around vulnerability management, the reporting of vulnerability is very, very important, is a subset is a part of the observability landscape. So this is something we need to obviously always have our eyes on. And that is, you know, and a lot of this came from, you know, you may have heard of this thing called log for J. And I think probably everybody in the country at some point has heard about log for J, and a lot of the vulnerabilities that have have popped up, you know, really appeared not just not just in the last few years, it's this has been going on forever, but it's becoming more and more evident to, I think, the general populace that, you know, cyber criminals are taking advantage and exploiting, you know, weaknesses in the system. And a lot of those weaknesses are introduced or open source through vulnerabilities. I'm not saying Open Source is a bad thing. It's a fantastic thing. But the problem is, a lot of times what we see with agencies, what we see with our commercial customers, is they get hit by vulnerabilities that are well known. And so you know, you've got these known exploits, you've got these known vectors into your application, but they're not patched. And so this is where Sissa is really kind of, kind of, I shouldn't say put the hammer down, but really saying that we have got to do a better job at vulnerability management, we've got to do a better job at continuously monitoring for those vulnerabilities and remediating those because, I mean, honestly, I think of this as low hanging fruit, if there's a known vulnerability out there, it should be patched, it should be, you know, isolated, and we should make sure that, you know, we are closing all the avenues to our adversaries and to to cyber criminals, and so forth. So they can't have a you know, they can't attack or systems. Now, granted, it's kind of a Cold War, there's going to always be this back and forth, we close one door, they're going to try to find another one. But we've got to make sure we keep on top of these, if that makes sense. Dateline November

07:57

10 2022, Sissa. Got it right in front of me, transforming the vulnerability management landscape. And so I want to, I want this to be an interview that will appeal to people who are novices and pretty sophisticated at it, but but to paint the picture is that over the years, CIS has come up with known vulnerabilities, we know that I think it's a KV or something. And so and so an agency can go out on their own and say, well, this software package I'm buying does have any known vulnerabilities. And I think the way NIST and other organizations have structured is that the burden is put on the agency to figure it out. And I think when I read this transforming the vulnerably met Well, I see the transformation going it the onus is going off of our poor, overworked coveys to the vendors and the saying, hey, vendors, you got to jump in on this and help us is that a good summary of this document?

08:50

So I think that's that's a good, so you're talking about this excellent blog that was released by I think, Eric Goldstein, and yeah, and the interesting thing is, and I think you're right, you are 100%, right, that this needs to

be a public private partnership. I know that's kind of always talked about and maybe overplayed, but this this truly needs to be where industry, where vendors are really stepping up, and providing, you know, being able to interface with things like you know, the you mentioned, the, the vulnerability exchange or the in the KV, I think it's the KGB, the known exploited vulnerabilities catalogs, and they're the catalogs they're these databases, they they your rice, so in other organizations, we they always are keeping these, the CVS and these these vulnerability and exploit definitions up to date. As soon as they come out. They go into these databases, they go into these repositories for you know, and really for one main purpose is well obviously they're out there they're known but then they can be automate So you you have to have, I think a key part of this article was also how we achieve automation by publishing these these advisories in a common framework. So I think they called it the common security advisory framework or C SAP. So, you know, being able to publish these in machine readable format, so we can automate. So we can, you know, automate, the, the scanning, the remediation, all those other capabilities. And I think we're industry really needs to play a part in this alongside all of these other topics. But there's, there's something we haven't mentioned yet. It's a part of it. But being able to deliver s bombs, or what we what we call as an S bomb is a basically a bill of materials a software bill of material. So industry, when I deliver when Dynatrace delivers software, I should deliver a full account or a full account, a full bill of materials and everything that goes into that software, every piece of third party software, every open source, you know, instance, whatever might be in there, because this also needs to be in a kind of in that machine readable format. So when agencies run into another law for J, they can quickly scan and say, okay, all of these are all the salt. This is all the software we have in house. These are all the vulnerabilities, this is what we need to go and remediate. We shouldn't be just like law for J I remember when it happened. I remember meeting after meeting being cancelled, because everybody's off, you know, trying to isolate what systems we have out there that have law for j. So it was all hands on deck. We have to make this better. We have to be quicker at this because the longer it takes, the longer we're exposed that it does that make sense?

11:49

Yeah. I come from a humble background, a blue collar background. I had neighbors who were factory workers and refrigerator repairman and longshoreman and I never forget that. How're you doing? Oh, I'm overworked, underpaid. This was a blue collar limit 40 hours a week on the factory overworked and underpaid. That phrase may apply to the federal government. I think a lot of federal systems managers are going crazy. They're understaffed, they have a tremendous amount of work to do. And really what I view this as is transforming the vulnerable, it helps them manage their vulnerabilities better it I mean, they're overwhelmed. They have they have to do something, I think automation is going to be the key this they have to automate. It's just, it's just a whack a mole with that's 20 feet long, you're running hitting the moles and you're not getting so I think this is another key aspect of it, I think is is having observability what's on your system, and know the vulnerably the weaknesses on there. But also this is going to help you know our people keep safe. Yeah,

12:45

John, you're exactly right. And I come from a similar upbringing. And granted, I'm a little bit further south. My My father was was a landscaper and and I worked with him, and then he owns a little side businesses and things like that. But you know, all same thing overworked, underpaid, and I see that with, I see that in the federal government. And on top of that, you know, I I am always, you know, proud of the work we do at Dynatrace in the work I do for the federal government, because, you know, often these paid often these, these

civil servants are, like you said underpaid, but also an overworked but also they're doing this out of sense of patriotism, they're obviously not doing it for the money. They're not doing this to you know, for fame. And so, you know, I think it's our duty to find ways to help augment their work. You know, I think with automation with AI, I'm never talking about replacing people. I'm never talking about replacing the the security operations centers, I'm not talking about replacing the NOC workers, I'm always talking about augmenting their capabilities and observability does that it helps bring in all of these, you know, millions, sometimes billions of data points, but on top of that layer, artificial intelligence AI so you don't have to spend hours sorting through data sorting, through logs, sorting through vulnerabilities sorting through all of the security information, you can actually isolate where the problem is isolate the root cause sometimes automatically remediate it. And then you know, if you if you trust your API to do that, but at the bare minimum, you can then take that data and instead of spending hours and hours sorting through this yourself, take a few minutes and then you can move on to your your your actual key tasks and things you should be working on

14:46
and prioritize to because everything doesn't have the same value. You know, the military guys say if you defend everything you defend nothing, it's an old military adage from 500 years ago. Same is true. I mean, what if, let's say system a Gilroy software's got the vulnerability and your agency doesn't use Gilroy software? Well, I mean, you don't have to worry about a day. I mean, you can prioritize where the few out in the 40 hours week you're in there, you can prioritize and go to the right system. Maybe the Hicks systems got a vulnerability, and you happen to use the heck system. Okay, forget about Gilroy, I mean, the whole idea of prioritizing, I mean, how else can you be efficient with the limited time that we have,

15:23
you are so right in that and and prioritization, especially, you know, any of these cases, with performance issues with security vulnerabilities, it's, especially when you have a major kind of going back to log for J, when you have a major outage, when you have a major vulnerability, a major issue that you need to resolve, you need to find those most vulnerable systems, you need to find the ones that are the, you know, you know, we bought for J, you know, everything was a level 10 You know, we got to get everything remediated well, maybe, maybe not, maybe I should focus first on those top 20% 40%, whatever it might be 50% of systems that might be for we're facing, they might be constituent facing, they might have access to the internet, they might have sensitive, or confidential or, or secret datasets, datasets that I need to protect, those are the ones I need to focus on. First, there might be 20, or 30% of those that get lost for days on the system, it's not actually even being used, it's in a dormant, you know, module not being used, I can handle that later. So to your point, being able to, to actually quickly isolate that and prioritize completely, that that is completely right. And using another military idea, situational awareness is is another kind of key part of this. And that's, I think, what we're talking about this idea that, you know, in the, you know, the military's, you know, this is kind of one of their minds as being a knowing their environment, knowing the environment that they're working in knowing all of having as many data points as they can, because this is how they make decisions. This is how they make really quick tactical decisions is because they have, you know, the best information they can have at a given time, I think it should be the same way with our systems, you should have as much in the best data that you can have to make those decisions and to make them quickly so you can isolate problems and move on.

17:27

But if you enjoy this conversation, you may want to listen to an Episode Episode number 32. I did with a guy named Dr. Steven McGill from some type, he talked about the s bomb, you know about the software bill of materialism. And that gives you just a different flavor different aspect on it. I'm going to turn the tables here. And instead of examining, you know, the number of hours that a federal CIO puts in the office and doesn't, let's look at the vendors. And what one could read this, like an attorney could read this and go Hmm, it looks like they're turning that spotlight to the vendors and saying, you know, the vendor is going to have some responsibility here for for telling the agencies they work with about known vulnerabilities revolving business system now, no one wants to talk about their dirty laundry. But, you know, I think that that's, that's, I think that's the case is happening here.

18:14

Right? It is critical. Yes, we don't as industry, we don't want to expose ourselves, like, you know, yes, we've got vulnerable modules in our software. But I think what everyone needs to realize industry and agencies is that, you know, this is the world we live in. We all use open source, we're all using different types of, of different coding techniques and different ways. Now, we should be using very safe coding practices, we should be using the best practices out there. But ultimately, things like this happen. And for I get a perfect example is law for J, almost every company out there was using it, every agency, it was everywhere, and you know, for and what we found out later is that this vulnerability had been there for years, but it no one had discovered it. So it just kind of proliferated. So we can't be you know, industry can't be just held accountable if no one knew now, if we knew and did nothing about it now, that's a whole nother story. Now, the I think where it becomes negligence is when, you know, when we when we tried to hide things when we tried to cover it when we tried to, you know, protect our, our interest by you know, kind of, you know, not exposing that we had this problem. Well, we're putting agencies, you know, we're putting our commercial customers, we're putting everybody at risk, and nobody wants to do that. So you know, my, you know, Dynatrace we are very open. We publish all of our vulnerabilities, we publish our timelines to meet them. We're very open about that. And we act upon these things quickly because they do happen when question that often comes up with s bombs, though is that, you know, if we put out there kind of everything that you know, everything that we that's used to make our products and like all of our secret sauce, well, we don't have to put, you know, down to the code level, but like all the modules, everything we're using, you know, then there's sometimes there are people as well do we want our competitors to get a hold of that wheel, there are ways for us to kind of control that. But ultimately, we need to do what's right for the country, what's right for our customers. And that means kind of, you know, honestly, being open, and about all of this, Willie,

20:32

I'm listening to you carefully taking notes. And every time you say s bomb, you know, I spent 25 years doing live radio, I always like that. So I'm gonna tell you that much, and never got in trouble with the FCC because of it. So that's a light hearted approach to this problem. And

20:47

I don't mention that going through the airport. But

20:51

I want to say that we're either I'm an expert in one day, like, Hey, Willie, it's football season. And there's some silly team in town with a crazy name. And we all know that and, and, you know, when a defense looks at, let's say, the Chicago Bears, they looks at and they say, Oh, this is what they do, then sir Tennessee and this person, and then the winner the game, and all of a sudden, they toss it to the split, and it's a new play. And so my point is that there are known vulnerabilities, you know, you can scout a team, you know, what they're gonna play, then there's unknown vulnerabilities. And so, so this is one critique of that offers a fair critique or not, but that we can say, well, you know, these are known vulnerabilities, and she thinks is a fair critique or not a fair critique?

21:35

No, that is 100%, of fair critique. And, you know, we, we need to, you know, they're kind of two ways I look at this from the known standpoint. But no one's we should just be addressing, I mean, that, that we know them on them, we know they're out there, they should be addressed, they should be addressed quickly, the unknown, that becomes a little bit more difficult, obviously, because they're unknown. So there have to be other approaches, there has to be, and I think this is where, you know, you you start looking at your, your, your different types of security tools, your seams, and all the different types of tools you're using that. And this is where I'm, obviously a big proponent for AI and machine learning and different types of approaches where, okay, so we don't know that there's a vulnerability out there. But there are probably heuristics and different things that we can use, we need to be analyzing for behavioral patterns, user behavioral patterns, machine behavioral patterns, you know, this is where again, observability becomes key, because understanding how machines normally should work how, you know, what should I see from, you know, a CPU standpoint, from a memory standpoint, network communication, what's talking to what if I see, you know, something very, you know, very simple, the system might have been compromised, is that it's not a known vulnerability, I saw no scanning, I saw nothing, but all of a sudden, I started to see traffic that I never saw before. And it's very sporadic traffic, it looks like, you know, you gotta be really good at the you have to look at almost every transaction, because how this this, you know, system is working is sending just a little bit of data at a time, it's kind of almost trying to mask what it's doing, you need to be able to see those types. And I don't claim to be a security expert, I'm an expert in observability. And that's, that's kind of key to I think, observability, which I think is key to security, being able to see the small changes to be able to understand those small changes, and then to act upon them. Because, you know, it might be a normal, you know, this might have been a code change. And this activity is completely normal. But we need to analyze it,

23:45

d y n a t r a c e.com, that's Dynatrace. No, I and there's a YDYNA, T R A, C, E. Well, Simon Sinek wrote a book, he says you got to start with why. And I think we spent the first part of this discussion with the why we did a lot of why. And now we got to transition to how. And when he talked about vulnerabilities, I think, traditionally, the How was, let's say Gilroy software would see a vulnerability, then I'd put up a PDF, and then maybe a federal CIO would go to my site and read the PDF and take action. And, you know, I guess technically legally, yeah, I announce it, it's buried, but it's a PDF somewhere in that transition I see in this document is that, hey, let's use a technique. Let's make it machine readable, and be able to distribute it in a

more efficient manner. Then some PDFs gilroy.com That no one reads I mean, this machine readable capability really, really puts you know, puts a lot of muscle into this, doesn't it?

24:46

100% and, you know, kind of the old way of doing this definitely was you know, I go out you know, monthly to a database I go out at night. Well, what abilities are out there, you know, and over time things Got a little bit better, and there's more automation and more. But now I think we're you know, and I look at it this way, too, I think that where where things are going is that I think industry, when they deliver new software, it should be just, every, every piece of software needs to have that software bill of materials, it needs to be in a in a format JSON format, or whatever format is that it will probably be JSON and, you know, whatever the standard is, that could then easily be translated into as part of the agency's automation process. So that's uploaded, and it's constantly just, you know, whatever, whenever there's a version change, whenever there's an update, there's a new S bomb. So that's part of it, then, you know, we're tied into also the, the known exploited vulnerability catalogs, and we're tied into the different vulnerability database. And so we're pulling these feeds the sources automatically, and you have whatever method you use, if you're using agents, if you're scanning, you're using, you know, scanning software, once a week, once a month, they should, we should always be looking, we should always be observing, and when something changes, when something, you know, becomes anomalous, when it becomes, you know, is not where it should be, that should be flagged, and we should have an analyst or an AI algorithm that can actually quickly look at that isolate has, is this coffee, does this look like it's been compromised, and then act upon it. Ultimately, I'm really big on automation of that, you know, I believe that what we see commercially and from agency standpoint is that the, the idea has always been, you know, kind of perimeter defense, you know, protecting you got your web application firewalls, you've got all your different perimeter tools to you know, really tried to prevent people from getting into the environment. With COVID, what we saw is the perimeter actually extended out nail to the home. So you got to hold another aspect. So you got to factor that in. I think that, you know, with observability, with this idea of kind of always monitoring, I'd say we pulled the perimeter in even closer to the application. So there are a lot of platforms out there that can do, basically, runtime application protection. So while you know, maybe having an agent at the application that's constantly monitoring it for performance and all these other things. But also, do I see a command line attack a SQL injection attack a, you know, a typical type of pattern that tells me that this application has been compromised, I should be able to stop it at the application. So I need to maybe tighten that perimeter up as well. So that's just another idea.

27:40

Yeah, I think it's all the people listening to this should take and, and go to CES and read this. I think it really, it puts a lot of the concepts we've been talking about observability and the whole machine readable language and software bill of materials and understand what you have, and it gives you the tools to actually accomplish some of the things they've been targeting. And I'm really glad we had John to talk about it. You've been listening to federal tech podcast with John Gilroy. I'd like to thank my guest, Willie Hicks, federal CTO, Dynatrace Thank you.

28:10

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 podcast.