FEDERAL TECH PODCAST

Ep. 66 A Better Approach to Intelligence Analysis and Data Visibility

00:00
This is John Gilroy from the Federal tech podcast and this is Matt Thompson with so cure this is Jordan Barris was Okay, today we're gonna talk about identity verification, hit the music Mani.

00:13
Welcome to the federal tech podcast where industry leaders share insights on innovation, with a 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. We have two guests today. Our first guest is Matt Thompson. He's the senior vice president General Manager public sector solutions for Soke here, we also have Jordan Burris, Vice President and Head of Public Sector strategy for Souq here. But first, I would be remiss if I didn't tell the audience that we are recording this at Ford's fish shack in lovely downtown Ashburn, Virginia. Why here? I think everyone listening knows that 70% of the world's internet traffic flows through Ashburn. What better place to talk about identity verification than right here. Maybe it flows right through the restaurant here. Maybe the very, very kitchen, who knows? So we're gonna talk about identity management, anything else. But before we begin, I have to tell about goals in life. I talked to Matt before the show, he tells me that his goal in life is to have a beard as good as Jordans. Is that true? That's very true.

01:34
about somebody finally admitted it, I admired every time we're on the Zoom call together.

01:38
And I don't want to pick on Matt, but also it's his birthday.

01:45
And it always corresponds with identity management day, which is a thing that we celebrate as well. And it's kind of like Captain America having his birthday. On the fourth of July, Matt Thompson has his birthday on identity management day,

01:57

Captain America who doesn't have a beard quite as nice as Jordan. So let's talk about identity management. Now, I tried to find a hook for this interview. And I searched I did research. I went to Gardner I listened to videos, I saw Jordan is all over YouTube, if you want to see Jordans all over YouTube. But then it dawned on me. It's Simon Sinek. It's why so why am I interested in this? Well, the why is very obvious. It's tax time, I just had to write a big check to the government. I gave him a big chunk of my money. And guess what, according to CNN, $5.4 billion, small billions of business loans are questionable social security numbers, they may not get that money back, Hey, that's my money. That's Jordans money. That's man's money that's going out there. So I'm very interested in identity verification, because I don't want my money wasted. I don't think anyone wants us money. So So why do you work for secure? What's your motivation? What's your why?

02:50
Matt? Yeah, my Y is to improve the trustworthy access to digital services, whether that's across government agencies, or in the commercial space, I think we have a fundamental right to control our identity information, how it's used. And I think, today, a lot of the solutions in the market don't do a good job of protecting our identity. I think there's an opportunity to help government agencies in particular, improve the way that people assert their identity to them to access their benefits and services, as well as the flip side of what you were saying is the manipulation of your identity information and having that used by criminals, cyber criminals, identity fraudsters to use your information to commit crimes via identity fraud, with benefit programs that ultimately impact you as well.

03:43
So Jordan, how do you ask the Simon Sinek question why so why so care?

03:47
For me it's really about it's a spin on what Matt was talking about. And it's about confirming that everyone, regardless of race, socioeconomic background, etc, has the opportunity to engage in a digital ecosystem. Far too often and going back in my career, you know, back in 2018, when I used to work for for the government, there was a push and initiative to find different ways to bring people in verify who they were online. Why? Because we found that far too often. The underserved populations were those that were being left out of the process. Fast forward to the pandemic, this hit mainstream, where you were hearing it time after time, and every benefit benefit program that folks were not able to get access to their benefits. While fraudsters coming from nation states or, or criminal rings, were intercepting those benefits in particular, for me, something had to change. And so I joined secure because I believed in the product and what we are doing to transform really what is that digital experience for the American public

04:47
that Thompson's is really that I get breaking news at a restaurant breaking news, breaking news, I have a press release in front of me zero trust maturity model version 2.0 released this morning on your birthday, and you look into The old little table of contents here, and what's the first pillar identity? So I guess we're, we're playing to your hand here, aren't we?

05:08

Yeah, no, I think there's a reason that identity is the first pillar of the zero trust strategy. Now, while that specifically focuses more on the enterprise side, and really has a focus on authentication, you know, at the end of the day, I think the government has a responsibility to extend their thinking around identity, to meet citizens where they are, and the Biden administration has improved customer service as one of its top initiatives, and digital identity must be included in that effort. From my personal experience, in my work experience, a more trustworthy digital identity system is a top priority to restore Americans faith in their government. And I think that plays in with the broader philosophy around zero trust

05:53
Jared, I'm very, very sophisticated and a high intellectual. And so to do research for this, I went to Google and typed in identity verification, and a strange name popped up the name of Jordan Burris. And I see this guy all over YouTube talking about identity verification. And also there's an article here that you wrote, and it's called from money mules to synthetic identities. I had never seen that phrase before. So So what is the synthetic identity anyway?

06:19
Yeah, absolutely. So synthetic identity is it falls under two different buckets, right? It is identities that in some way have been manufactured, such that they can perpetrate being a real person. At the end of the day, it plays on one of the legacy links in the chain, if you will, that exists for identity today, the reality that we're still as a society within the US very heavily dependent on what is the credit ecosystem, in order to assert or establish someone's identity. Think of it as like the gatekeeper, ultimately, and synthetic identities are created when you have either someone's real PII. So what combination of their their first name, their last name, their address, and their social security number, someone may decide to change a piece of that, right, they may change the social security number that originally, you know, links to Jordan into either what would be someone else's social security number, or what could be, in some cases, that complete fabrication where they're just making up a person that doesn't exist, the way that credit ecosystem works is that you know, the first time you go to assert this information, they have to keep a record of it. Now, you may not get approved for that credit card. But if you keep coming back enough times, eventually you'll come through because from a history standpoint, they're now realizing that someone is trying to assert who they are. And this quite often can impact for an example, folks who are newer to the country who are coming and they're they're now just getting this their identity information, promulgated through systems in particular, so with synthetic identity, whereas it's been around for decades. Now, at this point, it's hitting mainstream because of the ease of access that fraudsters have to data that's been breached time and time and time again. And really the these weak links in the chain, as we say, the credit over reliance in the credit ecosystem, which has put us in this position where, you know, at given enough time, given of resources, any fraudster can start to grow what is a synthetic identity and use it? Funnily enough, we actually put out a report not too long ago about synthetic identity, and really the state of it. And we found out that, you know, one of the most common synthetic identities that exist is an individual named Mike, Michael Smith, mid 30s lives in Texas has a Gmail account, in particular has a pretty average, you know, credit profile, and in terms of, you know, what, what, what he's doing at the end of the day was in reality is completely fabricated, and quite often used for, you know, what it'd be moving, moving money nefariously, or intercepting benefits from from citizens that need the most. John,

08:54
if I can add just quickly, synthetic identity fraud, you know, is a more sophisticated type of fraud that we have seen traditionally in financial services. And what makes it also unique is the fact that it's victimless. So there's no actual person that's, that's being notified that, you know, a fraud event has taken place, we are starting to see spikes in synthetic identity fraud across government use cases. So I do think it's an important thing for government leaders to be more educated on and understand the problem so that they know how to solve it.

09:28
In the article that Jordan wrote, he talks about knowledge based authentication and put that in the back of my mind, I'm thinking about rolling around. And I'm trying to describe so cure. I mean, if I was on the metro tomorrow, when someone said, Well, what's so cure all about? Or if you're on the metro tomorrow and says, Would you say it's a it's like a predictive analytics platform or it could get a lot of different information? So yes, yes. There's in fact, Jordan, is that what you do?

09:51
Yeah, that's, that's part of what we do. I think there's more than one piece to it. The first piece that we talk about is the identity The verification piece or identity proofing, which is where we're making sure the identity elements that are being submitted correlate to a real human being, I often say a carbon life form that this data all this data matches a real person that, by the way, is still alive. One of the key things that we've seen across government fraud is a high likelihood of fraudsters using deceased people's SSN. And, surprisingly, that's happening from family members. So you know, I have a parent who's deceased, I'm using their SSN as part of applying for benefits. So they're applying for benefits with deceased people's information. So we want to make sure one, it's a real person to that that person's alive, because if they're not alive, hello, why are they applying for a government service or benefit, but that's only half of the equation. And the other half is making sure that it's actually John Gilroy, who's entering John Gilroy is information. That's actually the harder part and why that's harder is because all of our data has been breached, and number of times at this point constantly being breached. And one of the impacts of the all these data breaches and ongoing data breaches the fact that it's easy for fraudsters to get access to our data and submit all of your real identity, all of your current identity elements, what's the harder thing to solve for is, is this actually that person submitting it. And so that's where we get into the predictive aspects of our platform, which really focus on the different types of identity fraud, third party identity fraud, synthetic, which we just talked about, and we're moving more into first party identity fraud as well.

11:35
So Jordan, I mentioned this zero trust maturity model version 2.0. Francisco released this morning, believe it or not, there's also executive order released just for John Gilroy. And it mandates me to say artificial intelligence at every podcast. I gotta say, artificial intelligence. So when I think of what your job is, I think of artificial intelligence and thinking. Now, if I'm trying to break into Jordan's account here, I can probably use artificial intelligence and maybe, maybe come up with a password or something. And so So how is artificial intelligence being used to compromise credentials?

12:06

Yeah, absolutely. So when you're thinking about identity, in particular, fraudsters at scale are using artificial intelligence or machine learning, in particular, to in order to be what would be, for example, bot detection attacks, or a bot detection mechanisms within systems as they're, you know, submitting information, they're using it to, you know, input information into forms. At a quick clip, they're learning where there's weaknesses, inside of processes that exist for the government, today, and they're taking all of this information, all this feedback that they're getting, and they're sharing it across their networks. And then they if you go to the dark web, or you go to forums, where fraudsters are living, they're telling the story of what to attack was successful, where and how they were able to exploit funds. That's why we see, you know, news stories out of Maryland, for example, with SNAP benefit programs of folks having their accounts intercepted, in particular, and then not being made whole. Ultimately, a lot of this comes from, you know, using technology, as it were in order to augment their capacity and help them do things at scale faster. And unfortunately, we haven't seen necessarily the compliment on the other end of the spectrum, which is where, from our standpoint, it's so cure, we're leveraging machine learning to fight back ultimately. So we were using the same type of tools to find a way in which we can better analyze identity as it is being as a transaction taking place as someone is engaging within a digital channel. So that way they can we can have that level of assurance that they are who they claim to be ultimately,

13:47
you know, Matt, this is not your first time at the rodeo, you've seen a lot of things. And I think we'll

13:51
I like to stay on the ball for longer and eight seconds.

13:53
Maybe do that your birthday parties? Yeah. Well, I don't know if it's hard, 35 agencies, and I would bet that there's 135 different identity solutions out there. Maybe more. I mean, each agency has little nooks and crannies and they're smaller everything else, man, my age is like to say the word legacy identity verification systems. But some I'm trying to fit where you fit in with this multiplicity of approaches to identification. And so so where does secure fit in candidate help? Just the novices can only help that a high end people are where do you fit in this whole solution to the government?

14:24
Yeah, well, for starters, it is a problem that every agency is kind of doing their own thing, if you will. And you know, you're the same John Gilroy when you go to the IRS as the same John Gilroy when you go to Social Security Administration is same John Gilroy when you go into HHS, so, you shouldn't have to be re verifying that you're still the same John Gilroy and proving all the same information over and over again. You know, that said, there's also not a one size fits all approach to identity verification. I mean, if you're just accessing, you know, some weather information out At NOAA, you shouldn't need to have the same level of vetting as if you're filing your taxes or claiming your refund at IRS. So, you know, there's there's different levels of vetting. in the identity space, it's called assurance. But at the end of the day, there needs to be flexible identity solutions that can verify lightweight aspects of your identity all the way up to your full legal identity and every aspect correlated to get back to that really strong proofing event that we talked about earlier. The way we fit in, you

know, and we don't solve the entire digital identity problem. What we solve specifically is around those two pieces that I shared earlier, which is, you know, is this a real human living would be good if they're applying for benefits or services? And is it that person that's submitting the information, so identity proofing identity verification, relatively synonymous, as well as, you know, the identity fraud piece, and we do that empirically, more inclusively, more accurately than other solutions in the market. We think it's a time It's time now for government to put best in class solutions in place in this space. Because of all the challenges that we had during the pandemic.

16:17
Jordan, we're recording this in the restaurant. So I got to ask you a question about gourmet cooking. My avocation is gourmet cooking, believe it or not, yesterday I cooked in the house and I was got a bunch of ingredients and called for some white wine. So I went up to the Safeway in Leesburg. This is true. This is literally happened yesterday. And I'm an old guy with gray hair, and I can barely walk. And so I went up to buy this thing. And the woman said, Okay, I want to see your ID, what do you mean? Take up my wall and show you my ID really said yes. I said, That's it. I threw my hands up in the I walked out. He said, That's it. I can't take it. I walked away. Now, there's a parallel in the federal government, let's say cod, Jennings Jr. Works for the federal government to say pick out a name of a hat somewhere. And he goes through multifactor authentication. You know, there's something called MFA fatigue, where causes I'm, I'm sick, I just let you through I'm sick of it. I mean, it's, it's so you get the point where so where's the net under that, you know, all of a sudden some malicious actor can get in because of MFA fatigue. And so so the failsafe is identity verification, is that what it is?

17:22
So it's it's about understanding that there's different parts of the problem in which things can go wrong, right, like a lot of the focus and conversation around the federal government today or even historically, has been around multi factor authentication. And don't get me wrong, that that is an important piece of the puzzle, it is absolutely necessary. And more importantly, moving towards phishing resistant authenticators. Ultimately, things that are, you know, scissor rightfully called out, and there's zero trust maturity model. The problem though, is that with all of those authenticators, it typically has to be some type of fallback. So you talked about it being fatigued, I talked about it from the perspective of maybe I'm just really absent minded. And perhaps I have a token on my phone, or perhaps I have a UB key or something to that effect, and then I lose it. Well, now I have to go reassert and reestablish that identity. Depending on how your processes are set up, folks are either allowing you to do a very quick recovery with not much assurance that is the right person, or they're making you go through a long drawn out process in order to reassert your identity. Identity Verification, honestly is like the, the the path that is, if not protected, could lead to disruption or interception of most of the credentials that we see today. It's been put far too often to the backburner in terms of agency priorities and strategies. In particular, it's because there's been this notion that, you know, folks really only have to assert their identity once and we can manage it from there adversaries, fraudsters are getting more and more sophisticated. They're learning that as we deploy these new techniques, these new authenticators, they have to move upstream. So now my goal is to get earlier in the process. Why? Because not only can I now pretend to be John Gilroy, and take the account from before he even has the opportunity to get it. But perhaps I want to do some type of recovery activity, I can now steal it from him as part of the process. And so if we get identity

verification, right, we can keep them out holistically, if we get it wrong, then you're going to continue to see the stories that we see today, where folks are being locked out of benefits, or they're having their benefits intercepted and taken from them. Ultimately,

19:23
Jordan, I can say unequivocally that no one on the planet has ever tried to act like they're John Gilroy. There's only one

19:31
I guarantee you your bank accounts, your credit cards, your 401k You've had a lot of fraudsters trying to attack and take over those accounts. I guarantee you. You just don't know. Yeah. Oh, I'm not sure I'm right. I'm sure I'm right.

19:47
Wow. Yeah. So Matt, you've got a military background. And so the military folks got to saw locked in this is only for civilian agencies are they got it all down or where they fit in this conversation? They should have been It Better identity metal verification the other shouldn't Yeah, I

20:03
think there's there's evolution there within the DOD space. Defense manpower data center really runs a lot of the ID management for the DOD. They've done a good job they you know, they've got a, a relatively secure, credential based system today of using smart cards, effectively, which everyone that is on your podcast should should understand, I think where you know, they are working to evolve is around mobile base credentials, more portable credentials, more flexible credential, so that it's not carrying around your, your common access card, as the only method of proving your identity to different resources. But I think you know, the problem for people that serve as really when you get out of the military, and then you have to prove that you had served at some point you become a veteran. That was really, you know, the starting point for when, when I had co founded what is now at me was around how do we solve that problem of giving people who had served in the military a way to continue to prove that they had served? And that's a big problem. That's a big challenge. But um, yeah, I think, our main focus today, because you can't boil the ocean and government at the end of the day, I think our main focus is really those agencies that have high constituent engagement, where they're providing benefits or services to the public. And they need to know that those benefits are going to the intended end recipient and not to, you know, organized fraud rings over in Nigeria, or Russia or China, where we saw lots and lots and lots of taxpayer money going during the pandemic, because it was so easy to commit identity fraud, and use John Gilroy as information to fraudulently file for benefits from countries outside of the US.

21:55
So Jordan, one hour ago, a gentleman sat in that chair at Ford's fish shack and record an interview. And we talked about network visibility. This is a challenge because the hybrid cloud public private legacy system is kind of a challenge. And he talked about the dark data. What do you mean, there's a lot of data we don't know about on systems. So we can't really draw data from there. Now, in your article, you talked about the dark web.

So So what role does the dark web play in looking at vulnerabilities, especially when it comes to identity verification?

22:23

Yeah, and I think I've talked about a little bit it think of it as like a clearing house, right? Ultimately, if I'm looking to understand all the PII associated with with John Gilroy, or Matt Thompson, or even Jordan Burris, likely, in some way, shape or form, there's pieces of that there, if not the wholesale thing, I was involved in the OPM data breach. And as a result, I know for a fact my information is out on the dark web or many other forms. And anytime I get a letter, I just like, Okay, one more Avenue that's available. But even beyond that, it's not even just the data that may be available. It's the tactics and the techniques that are also being shared, right. So you know, one of the things that we promote within the cybersecurity community and the federal government is being able to share those, the TTPs, tactics, techniques and procedures for vulnerabilities and how do we combat them, the same exact thing is happening, and perhaps maybe even at a faster clip, on the dark web, in particular. So when a fraudster or someone is engaging in attack, they're they're sharing it in various forums, to say, hey, this worked, this is how it was exploited. This is how you can go about replicating the exact same thing. They're sharing tools, and making it more widely available. And in some cases, we're hamstrung because even beyond the federal government, if we start to look into state governments as well, that level of exchange is not taking place today. And so in some cases, we're fighting a battle with one arm tied behind our back, and for our adversaries, or criminals that are out there today. They're using the dark web to continue to further their enterprise.

23:55

I'm glad you brought up the idea of state attacks, because I'm going to California in August. And you know, there's some counties in California that are bigger than some states. I mean, it says, I mean, California alone is the size of a country. I mean, just that aspect alone, that all kinds of vulnerabilities there. It's it's really kind of shocking, and I think that I think this is the new attack vector, maybe they're going after fitting, they're going down the chain down to the states and local communities and tribes and so much going on. It's incredible. Matt, at the beginning of this, I talked about the money show me the money, you know, $5.4 billion, and I'm worried about my money and paying the government and, and I think traditionally I don't want to cast aspersions on humans character, but it could be possible that the Small Business Administration maybe other organizations use a pain Chase approach. They may say, okay, Jordan, no, yeah, we're gonna give you that money. Sure. And then it turns out that it's a fraud and then then they go after them rather than No, no, no, no, I want to see that ID I want to do this, and then a certified letter and a picture of your mom. Right. So so pay and Chase is expensive, isn't it?

24:55

It is and it's often you know, they're often it isn't much on the chase side, or much success and free side. Yeah, and, you know, allowing this criminal activity to go and check whether it's domestic or, you know, international, you know, is just not acceptable. I mean, at the end of the day, let's not care as much about how many billions, or 10s of billions or even hundreds of billions may have gone to fraudsters during the pandemic. And by the way continue to go, you know, we can't turn a blind eye to allowing fraud to be a cost of doing business with government, because it is funding criminal networks. It's funding terrorist activities. This isn't, you know, money

going to a mom and pop shops. Sure, some of it is, but the vast majority is going to organize crime rings, which by the way, are taking this money and investing in their own r&d and getting better at attacking these different programs and services. And if you believe as I do is I think your audience does, we're only putting more services more benefits online, not less over time, and we're trying to push more and more things digital, which means that there's going to be more money available to fraudsters that continue to attack the system. So we've got to do something. There's a lot of money being invested by the federal government and by many states now to modernize the way they're doing identity verification. And you know, at the end of the day, I think now, you know, is the time for government leaders to step up and address this problem.

26:25
But Jordan, this is the part of the podcast where I read a statistic and you agree, disagree, or throw the microphone up? So here's this statistic 80% of cyber breaches are due to compromised credentials. That seems high. Does that? Is that a good figure?

26:39
Yeah, that I would agree with that. It's, you know, one of the number one, attack vectors that are exploited today is identity. In particular, right? There's many ways identity can be exploited. We've outlined some of that as part of today's conversation. But the reality is, is that identity is the ultimately the weakest link in the chain. It's one of the reasons why when I got started very early on in cybersecurity, doing risk management and understanding all the flaws, if you will, with a system, I kept coming back to identity and realizing that most of my problems if I could just get that piece, right. And it's a hard piece to get right to be clear. It starts with identity ultimately.

27:16
Matt, Cristobal time, look down the road. So where's identity identity management, synthetic identities? Where's this all heading next four or five years?

27:23
Yeah, I think as we get better, so are fraudsters. Because as I just mentioned, I mean, they're also investing. So we've got to constantly be vigilant and innovating, to protect our the front door of our applications, whether they're government or commercial, to address this, but I do think this has been a big unsolved problem for government for many years. And I think we're getting the right leaders stepping up the right investment being put into the space, the right focus on identity as critical infrastructure in America that, you know, we will improve digital accessibility and we'll do a better job of mitigating fraud.

28:06
Oh, great. That's nice summary. We're running out of time here. Unfortunately, you've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Matt Thompson, Senior Vice President and General Manager of Public sector solutions that soak here and Jordan burrows, Vice President and Head of Public Sector strategy. And so thank you, gentlemen. Thank you.

28:24
Thanks, John.

28:27
This is George T's from Elastic listen to episode number 65 of the federal tech podcast where I tell you everything you need to know about intelligent analysis.

28:37
Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcasts.