Ep. 4 Identity Management and Federal System

SUMMARY KEYWORDS
identity, agencies, julie, biometrics, identity management, yosh, security, organizations, people, continue, cloud, federal, years, identities, called, focused, attacks, securing, trust, swim

00:00
Well, that's a good point. Ah,

00:03
I'm going to start with you again. Here we goes. We're at nine. Welcome to the federal tech podcast. My name is John Gilroy, and I'll be your moderator. Our guest today is Julie Smith, executive director at identity defined security alliance and Yosh Prakash, Chief Strategy Officer and marketing officer at CVS. Now, most of my listeners have heard of Savion. They're pretty understand what they're all about identity management, but many of my listeners have not heard about Julie Smith. So Julie, tell us about your organization and how you can benefit my listeners, please. Sure. So

00:34
the organization that Iran is called the identity defined security alliance, we've been around since 2016, originally, but 2019 as a standalone entity, nonprofit, I will say, and our primary mission is to educate security professionals. So seek chief information security officers, security leaders, architects on the importance of securing digital identities, and then we provide resources, education, advice on how to prevent identity related attacks.

01:09
Okay, let me try to put this in perspective now, in the federal government to make this big transition to the cloud. Part and parcel of that is using different clouds, hybrid clouds, no, maybe they're intuitive and systems and, and so identities a key component of that. So yeah, I'm gonna turn to you and say, Well, what benefit would my listeners get from learning about the identity management conference coming up from Julie's company?

01:33
Yeah, John, I think it's a, it's a great opportunity to, you know, just assimilate a lot of information that's going to be, you know, put together as part of the identity management day. This is the second year that IDSA is hosting the identity management there. It is, as you probably know, and most of your listeners also recognize identity has become the core of security. And in the day and age where cybersecurity attacks are increasing, we are to understand more about identity and the role it plays in organizations security effectiveness. So what is in store is a lot of good content from various partners,

various practitioners in sharing that information on what's working and what organizations should do to improve their security posture. So it's, it's an it's an important event for, for ideas, then assess supporting that. And it is it is great for your listeners to tune in as well.

02:35
So, yeah, I just got a quick list here, Julie. So there's no lack of organizations associate with the federal government that help with identity. So where do you fit in this whole stack here?

02:45
Yeah, so our focus really is around educating and raising the awareness of identity. So we do a lot with the National Cybersecurity Alliance. Last year, we partnered with them for the first ever Identity Management day, as Josh mentioned, this is a second year, and also with the National Institute of Standards and Technology, right nest, and the NCC OE. So what we do is raise the awareness of identity in these existing security frameworks, there's a number of them out there. And a lot of them just traditionally have focused on network, the network side of things, right, the, the, as we we've talked about for a number of years, 10 plus years, the traditional perimeter is gone. And identity is now considered the perimeter, because people are everywhere and it and accessing corporate resources and through, you know, through Wi Fi, unprotected Wi Fi, in coffee shops at homes now since COVID. So identity is really the important component and the way to protect assets. And it's also the target for hackers. It's the it's the primary attack vector, as we've seen through our research and other research. So these frameworks that are that are out there and are recommended from the federal government are incredibly important, but we want to make sure that identity has a leading role in those frameworks and in those control sets.

04:20
So Julie, I went to the website, I DEA s alliance.org. And I see the information about identity management day. And one of the topics is trends in a securing digital identity. And so this is this is not a book on the shelf, you take and read the book. This is like it's something's changing all the time here. So federal IT people have to be appraised of what's going on currently right now, don't they?

04:44
Absolutely. Yeah, absolutely. And you know, our research shows that 79% of organizations out there have suffered an identity related attack in the last two years. That That's pretty significant. And 61% of all hacks are identity related. So it's it's an it's very important topic. You know, we saw last year, two of the biggest and most impactful breaches were tied to identity at its core for identity hygiene. So it's it's an it's an important topic, whether you're in the public or the private sector.

05:18
So yeah, you look at the federal government's all kinds of numbers thrown around, you know, some people project that federal cloud spending will be $8 billion, here in a couple of years. And so if you combine that with the fact that hackers don't break in, they log in, this is a big problem for a gummies, isn't it?

05:38

Indeed, indeed, and I think cloud acceleration is an opportunity for federal agencies to really bolster the security. I mean, this is this is a lifetime opportunity, because, you know, agencies are moving away from archaic, you know, systems on the cloud, right. So while there are definitely vectors that, you know, the hackers and attackers can exploit, but this is also an opportunity to put in the right practices in adopting a zero trust approach. And, you know, baking in all the necessary security and privacy controls that are described in this or in ICANN, or several other guidelines that have come out in the past. So I think it provides an opportunity to strengthen the security and making sure that the cloud systems, the new systems that agencies are building, are resilient, are robust, and are able to deploy and employ, you know, strong identity management, technology.

06:46
You know, Julie, I'm in the classroom a lot in a classroom tomorrow night, and I have these things called books I have my students read and, and Simon Sinek wrote a book called Start with Why. And so I'm gonna start with you. So tell us about this conference. So why should our listeners visit this conference? To see what's going on? Give us two or three reasons.

07:04
Yeah, so the identity management day virtual conference. So this is the first year that is the second year of identity management day and the first year that we expanded our content offering and, and our, our day itself. So there are just so many aspects of this identity management problem, and and we decided to put together a series of sessions that would kind of hit on every single topic. And so it really offers something for everything. So if you're an SMB, your small to medium sized business, we've got a great session, that includes an individual from the mitre Corp, someone from the Center for Internet security controls, and then also an MSP, focused on how to address this identity and security challenge that SMBs are facing, right, they're small, doesn't matter, they're still a target. And the impacts can be significant, as we saw with Colonial Pipeline, for example, zero trust, a hot topic, especially in the federal space. Right now we have a session, John, that you're going to be moderating. Thank you for doing that, with a couple of celebrities in the zero trust base. And we're going to focus on zero trust and the role of identity and zero trust strategies and why that's important. And we're going to talk about what it is and what it isn't, and some misconceptions. And then we're also going to talk about identity related attacks today. So what is going on in the environment? How can organizations What strategies can they follow to prevent identity related attacks today, and that's our keynote panel. And that's going to be another fantastic one. So those are three sessions right there that I think can span, really again, back to it hits your GAVI audience, especially in the zero trust side, but also in the SNB. And some of those agencies that are smaller. And it hits the private sector as well, organizations of all sizes. The other aspect of it is as individuals, we have different personas, we have different identities, as individuals, as employees as third parties that may be interacting with customers. And we all need to do a good job of protecting our own passwords and digital identities. Because when those fall into the wrong hands, and they will, they can be used to do some pretty serious damage. So I think just the overall day is around education from the perspective of identity management, a virtual conference, and then awareness in terms of sharing best practices, let's come together as a community and make sure that we all stay secure because we are all very interconnected in the world we live in today. So yeah,

09:46

I have a memo in front of me from the White House came on March 21. And I want to read it but first, you know, one of the best ways to keep up with the fast changing world technology is to attend webinars. You learn at your schedule and get continuing education In credits, the best webinars are from Fed insider.com. And they're free. Just last week, they had Dr. Ernest Moy from the VA talking about using technology for the underserved populations. A lot of veterans, of course, are in rural areas and a lot of innovation with the VA. And I'm sure they're interested in identification management as well. And I'll get this this thing for the White House now. I read these things all the time, but March 21 2022, this is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience. Yeah, this was this is a this is really like a call to action. It's like pounding on the table Yosh wake up, wake up, isn't it? Yeah,

10:41
I mean, I think the the overall environment has changed substantially over the last year. And actually, for the last several years, where we see not only the hackers want to do it for monetary benefit, but more importantly, the state sponsored actors are behind a lot of these attacks. So what the, what the White House statement is highlighting the fact that that is only going to increase because of the geopolitical reasons that we all know. So every agency will become a target, every private enterprise will become a target, because you never know what data is used is there and is can be exploited. So which is definitely a call to action, as rightly pointed out, that every agency needs to be thinking about bolstering the security, ensuring that their systems are resilient. I mean, you can think of many high profile attacks that have happened that Julie was alluding to last year, and many more might happen. So I think having robust defenses and increasing the resiliency of the systems is going to be extremely critical. So that they you know, I definitely think that the the order that or rather, the statement that came out was a very much, you know, relevant in this context. And every every agency should pay attention to that.

12:17
Yosh in Washington, DC, we have seasons, I know, in LA, they don't, but we have cherry blossom season. And over the weekend, my wife and I drove downtown. And we probably drove around five or six federal agencies. And I was going to talk to her and say, you know, each one of those agencies probably has a different level of competency when it comes to identity management, and she would have punched me or something. I said that but But 10 agencies 10 Different levels of competence when it comes to identity management. And so so where does your company fitness? Hold discussion? Josh?

12:45
Yeah, I think you're just to address the question of 10 different agencies at 10 different maturity levels, John, and I think both sides will as this have done a great job of, you know, putting out several, you know, frameworks and tools that are that are helpful in understanding the conformance of they're an enterprise or an agency is at right. So, when you look at this specific guidelines, 800 Dash 63 which talks about, you know, various, you know, you know, three different you know, guidelines that NIST has put out across identification Federation as well as credential management, one thing that you will realize is or no is that there are different assurance level within each of these. So, what it means is, depending on the business need, agencies connect, can can select or can say that I want to be at

assurance level two, for this particular application. So on one soap, so one thing to note that is that agencies can do that in essentially conform to those assurance levels. And now, what I have seen with agencies as well as across the corporate world is that it's not the conformity which is a problem, but it is more of how how much of adoption you have had in the sense that you have 1000s of applications or you know, hundreds of systems that you have within your environment, how many have been brought under control, how many really are under the governance of the identity management identity and access management system. So that basically is the majority challenge that I have seen in, you know, across corporate public sector as well as the private sector. So, yes, there are going to be you know, different levels of maturity and different levels of adoption. But there are guidelines to really see how to measure the maturity of identity management across the board. As I mentioned, the conformance levels and the assurance levels provide that guidance. And it's extremely helpful for agencies to follow that.

15:05
You know, Julia gets website in front of me here, identity management day 2022. And I bounce around and talk about this classroom again. So he has his class tomorrow. And I sent a message to my students today. Now, Georgetown University, I had multifactor authentication to send out an email. I mean, I have to like have five IDs, and my fifth grade teacher before I'm allowed on campus. I mean, they're very, very strict about that. So is, is multi factor authentication, kind of like a baseline starting point for this discussion, or is that advanced, too far advanced?

15:37
Well, let Yosh weigh in on this. But I would say, I would say it's a it's a requirement, regardless of user type. Now, you know, the more barriers you put in place for someone who has a credential, a valid credential, but they're using it for, not for not for the reasons that it should be used any, any way you put a barrier, and I think is a good thing. You know, once you start to get into more advanced technologies, like understanding the risk posture of that individual, so maybe it's based on their behavior, and maybe it's based on the device that they're using, and maybe it is the device itself, that device identity itself that has information that you can then bypass MFA if that risk level is very low, right. But I think at the core, and even if you look at some of the attacks that happened last year, if MFA had been in place, they might not have happened can't can never say they wouldn't have happened. But I think they definitely would have slowed down the attacker, and they may have gotten bored and moved on to something else. So I think MFA at its most basic is a requirement regardless of the user type, and the access type as well.

16:55
So you actually got a question about James Bond. Ready for James Bond? Question? Yeah, I've been in out all kinds of data centers in the Pentagon on Capitol Hill, I've been everywhere, I think. And I was in the state of settlements in Ashburn, Virginia. And there was an eye recognitions thing there, you know, and, and, you know, it seems like a funny thing to talk about, but I don't think there's any little working groups on identification with biometrics on this is just a separate topic completely. We're just this esoteric world data centers.

17:27

No, I think I think the other objects in different form factors through which, you know, you identify individuals or, you know, people are machine identities for that matter, biometrics, and multi factor authentication, as Julius alluding to are, you know, obviously, different ways to authenticate and continuously verify whether the, you know, the identity is who they claim to be, right. So that is extremely important in case of human identities. Essentially, you know, biometrics and PID cards are often used in the federal space more. While biometrics may not be the most common form factor in the enterprise or corporate America, but I certainly see the need for that biometric based authentication in federal agencies, and especially in DOD, and other defense, you know, defense contracting in other agencies. So, biometrics do play a significant role. And if you really look at both the list guidelines that I was referring to earlier, the six, sorry, SB 863, I think it clearly articulates all the different, you know, authentication methods that agencies should employ, and even I can architecture does talk about different tools and systems that agencies should employ. So yeah, biometric biometrics will continue to be one of the primary authentication factors as machine identities become more and more relevant. I mean, obviously, there is no biometrics associated with that, which is where the PKI and other certificate based authentication mechanisms should be applied. Across the board. I mean, you know, you're talking about data center. Now everything is in the cloud, it will be CalCloud. But everything is in the cloud. So how do you essentially continuously authenticate or continuously verify those machines? And that needs to evolve as

19:39
Julie earlier I mentioned fed insider, they have continuing education credits for the webinars, but I'm on your website here. I D s. alliance.org. And it looks like you can earn ISC two CPE credits, continuing education credits from some of the courses you offer, maybe even from this event, is that possible.

19:56
That is correct. Yeah, we are an approved ISC square. CPE submitter partner. So we have 28. Webinars, I think out on our BrightTALK channel, our content can be submitted as personal study. And actually the the other thing that's super exciting is for practitioners who want to get actively involved in the IDSA, they can earn CPE credits through their active participation by giving back to the community. And and we've just introduced two new membership types that are focused specifically on security practitioners. So yeah, that, you know, earning CPE credits and giving back to the community and learning about identity related. Security is, is definitely something that we offer. So thanks for pointing that out.

20:43
So yeah, Ash, attending this conference is obviously a public private partnership. And, and believe it or not, when Garvey's hear about something that a small business is doing an Oregon or a bank is doing in Dallas, they lift up their ears, and they're very interested because these are people who are out on the street and getting beat up and knocked around and learn a lot. So So actually, this is not just for commercial people, I think the government can really benefit from this conference, couldn't they?

21:08
Oh, absolutely. I think it's a great opportunity challenge for all the galleries to really attend this. Again, as Julie was pointing out, this is more to increase the awareness. Yes, this is primarily for it. This is

focused on security levers, security practitioners and architects. But I think the essence of this is that identity is core to every every organization, and everybody within the organization should understand the importance of identity. So this identity management is to raise that awareness across the board. And there will be more specific, you know, information that will be shared, you know, the experiences that the bank in the, you know, Dallas or whatever organization in other parts of the US have had and share that experience with, with everybody else. So I think it's going to be extremely helpful. It is a partnership, I think one of the things that came out in the fight us order, exhibiting water last year was two countries that intelligence sharing. Now, intelligence sharing can happen within the agencies and DOD, but also the information sharing can happen between private and public enterprises. Right. So I think this is this is an opportunity. This is more knowledge sharing, but it is nonetheless, important sharing information that's happening on the identity management. So Julie,

22:36
I'm gonna hold your feet to the fire here. And I want you to give us a prediction where you come back in five years and make sure it's true. So so how do you see this evolving in the next four to five years, as far as hybrid cloud identification, all these threats attacks we see coming in? What do you see evolving in four or five years?

22:52
Well, I guess just purely from my perspective, I would hope that that number I mentioned previously, percent of organizations, you have experienced an identity related attack drops dramatically. You know, I've been in and around this industry for about 13 years. And it's always interesting to me that we seem to be talking about today, the same things that we talked about 13 years ago, ways that you can protect digital identities, the fact that there's more identities that need to be managed and need to be protected now more than there ever have been. And, you know, I sure hope that five years from now we're in a winner a better place than we were before. I think, you know, we do have a session that's at the end of the day on identity management day conference that's focused on the future of digital identity. And I think there's a lot of interesting things happening around portable identity around bring your own identity, and how that impacts organizations, as well as us as individual as well, as you know, governments, how can we how can we move across the globe? Using our digital identity, our portable identity, I think is going to be an interesting topic to watch.

24:04
No, yeah, sure. In the Los Angeles area, I go there a couple times a year, a lot of different neighborhoods and cities all around there in the Washington DC area, there's an area called Woodbridge and I have a friend who owns a small company. He's a small businessman, he's got 30 employees. And his number one concern is paying for health insurance is number two concerned is what to do about COVID. And then number three, oh, you got to make a profit. And then oh, by the way, there's taxes. And then we'll What about cybersecurity? And so every time I meet with them or have lunch, I say talk to ya talk to yes, do something you're gonna get beat up here. But But I can see how even federal agencies, I mean, there are people in harm's way in the Pentagon right now. And they have to juggle so many things. So Yosh, is this juggling going to be better in the next five years or what's going to happen next five years, what's your prediction?

24:53
I think that that juggling continues to be the case, John, I think obviously the of attacks. And in basically the changes the digital transformation, the cloud acceleration that we are seeing, will continue to evolve and continue to become mainstream. I think we need to obviously learn to live with this and continue to strengthen our defenses. So I think the the organization's agencies small or large, will have to focus on continuing to strengthen that. What I also predict is, and continuing on Julie's extending on Julie's thoughts is that decentralized identity is going to become a norm. And what that will help is, you know, bringing identities, validating the identities and public agencies having the ability to identify and authenticate these, you know, these these people across across different agencies as well as common people who are accessing and taking surveys so. So decentralized identity and identity in general is going to make a big push, especially when you look at some of the changes that we are going to see in the financial ecosystem with digital currency coming into picture identity will continue to become the core focus in terms of managing, managing and securing the different digital environment. So I think the effort will continue in terms of ensuring that we are secure in identity will continue to be that that core piece of the puzzle, the cybersecurity

26:38
so if you're listening this podcast and want more information, I DEA s alliance.org. Sign up I think it takes place on April 12 and find out new developments because it's gonna be part and parcel of moving to the cloud part and parcel of zero trust. It's just something you've got to keep in your your quiver. You got to have three arrows in there and have one of those arrows in the quiver. Is there any management? You've been listening to federal tech COC? You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest Julie Smith, executive director at identity defined security alliance and he ash Prakash Chief Strategy Officer saviant Why didn't 730 interviews with federal Tech Talk? It's hard to get that out, you know, every week for 15 years federal I gotta say federal tech podcast.

27:26
Oh, I saw that. I saw your update John on LinkedIn couple of weeks back so yeah, I mean, he did it is a long time.

27:37
Yeah, it was one point million downloads and 730 shows and all kinds of actions. So we're just moving on to new things. So I'm gonna do my own here. And what I'd like to do is do face to face in town like if if Julie comes in town, like sit in the lobby of a hotel and get two little microphones and have people walk by and throw stuff at us and go But Julie what you're doing now oh, what's his ID you'll see his ID you know, and I think it's much I can be much much livelier i think i i was at the satellite show two days ago and I interviewed people live on stage and it was so much better with humans walking by and questions from the audience and this guy had funny socks and I said if he asked a question he'll give you a SOX and it was just it was just then we have some like Chase we can say this weekend sickly little Chase sky and pick on him and and so it's live is much better than zoom but Zoom is good enough. So that's good. If I can have a publicity photo, Julie from you and Yosh and a logo from both of you to we'll put it up and I'm gonna do a video in about 10 minutes to promote this and it probably err on the I think like the week before, probably in the fifth of April. So we'll get you out there. Okay,

28:52
excellent. Yep, I will send them I'll send over the logo for the organization and also for the day as well.

28:59
And so yeah, sure. August 3 I'll be in LA for that race. The peer to peer race to mile race. 1200 people

29:06
there holding the car.

29:09
Say hey, yeah, yeah, how I'm like the oldest guy in the race, but I'm not the slowest okay, I'm like, like 620 out of 1200 So not the slowest but maybe the old isn't running what kind of race is this a running race ocean open water swim two mile ocean? Wow. So 1200 aggressive young man, like Yeah, sure on the beach there and they shove a gun and y'all jump in the water. And this is called a washing machine start. And oh, yeah.

29:37
And then you get up once before I know exactly what you're with. There's 1000 Is everybody started at the same time?

29:44
Well, what they tried to they tried to have different so like, it's, it's crazy men go first, and then men and wetsuits and then women and women wetsuits and, but yeah, it's you want to go, you want to get in first and get out there. So Yeah. Wow, I've been doing for many years now. I'm trying to have about 1104 I'm trying to break an hour for that swim. So you've done triathlons, you know, but 2.4 mile swim. Hmm.

30:12
Yeah, I did an iron distance. I didn't do the run because I can't really run anymore. But I did an iron distance. aqua. Aqua likes us swimming by us. Awesome. That's awesome.

30:23
Suppose your time in the 2.40? God, I don't remember, ah, the most important thing

30:29
was to go back. And look, it was a long time ago. I'll go I'll let you know though. I'll go back in and look.

30:35
No, it's amazing. In the Washington DC area. I'm just like, you know, guy in the 711 or something. In Los Angeles. I swim with a surgeon, a banker, and two multimillionaires and a PhD student. So it's like, yeah, who are these people out here? They're all like, you know, I is not my, you know, guy across the street here is retired. So I don't. But now like they just have What a bunch of characters out there. I can't. Oh,

30:59
yeah. Sure. Yeah. So the one that I the race that I did, I'll tell you this was in the Russian River. So it was outside a Guerneville is where we swam in California. The river was so low that day, you can swim along and you like turn to breathe. And you could see somebody walking along the bank. It's like, well, you could have long.

31:22
So I do the Chesapeake Bay swim to its 4.4 mile swim. And I had a friend who was in the middle of the bay, you know, you alternating currents. And he hits something with his hands like hmm, and more she was more she went. Oh, he never He never does from again. After that. He got too scared. He didn't know what it was. I mean, mushy, you know, the NLA they have the drones that come behind you. And sometimes it's the sharks behind these big group of people. Nothing good sign. So I gotta have my insurance paid up in case a shark NABS me in LA, not a land shark, a regular shark. Okay, so I'm already for the event of the 12th. We're gonna have a warm up call, and then I get some good questions for the three people, my panel, 45 minutes is going to be a no brainer. So it'd be a lot of fun. So I'm looking

32:12
at a good crew. So I mean, I think they could probably, you know, any of them alone could talk for hours about because

32:18
one of them is an academic guy, too. So I can do the academic stuff, too. So Missouri. Yeah.

32:23
Yeah. Yeah. He's interesting. So he reached out to me a couple of months ago, there. He's writing a book with John Kinder bag about zero trust. It's yeah, so hopefully, he'll talk a little bit about it. But it's more along the lines of the Phoenix Project. So it's sort of a fiction kind of allegory, I guess, if you

32:42
will. In fact, Chase released one of those about three months ago, I read it. So

32:46
yeah, so yeah. So I make I'm excited about that. I'm excited about the whole day. I think there's some some great panels. So I think it's going to be a really good session. And

32:55
yeah, and I wanted to position it. So well, NIST has this and the DOD. But you know what, maybe you can learn from you know, someone else? Yeah, for sure. And the continuation credits, this is a big selling point in this town. CPS really is because GAVI has got a, they want to get promoted. And they got to have a sister things they have to show there. And so it's a real subtle thing, and they're not going to say it, but they want it because they have to prove that they go up to Yosh and go I want to get more money and and here's why. Because I owe and so this is how they prove because a lot of times the

federal government they can't. They're limited in some ways, but the CPS are a great way to justify moving to the next step.

33:38
Oh, excellent. That's great to know. Thank you for pointing that out.

33:41
It's it's something they don't want. I mean, Chase work for the government. I mean, a lot of people know things and it's just some subtle things that I think it's a slice ICP is like, Whoa, yeah, this is great. Yeah. And well, good. Awesome. All right. Okay. Sorry for the mess up. Talk to you soon. Bye. Bye. Thank you so much.

34:00
Bye