FEDERAL TECH PODCAST

Ep. 130 Protecting identity in the hybrid cloud

00:00
Hey John Gilroy here. It can't use the hybrid cloud without identification. Yet 80% of breaches involve credential abuse, often identification hit the music Mannie.

00:16
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 podcast.

00:39
Welcome to the federal tech Podcast, the podcast that connects you to federal Technology Leaders. My name is John Gilroy and I will be your moderator. Just as you heard in the tease, we're talking about identification today. In the virtual studio, we have Jimmy McNary. He is the AVP for federal solutions for a company called Sampras, Sc, M p e r i s. So, Jimmy, Do I have your identity correct at the beginning here?

01:05
You do is Jimmy McNary. Correct. Right. And

01:08
that's important, the hybrid cloud to identity. And that's we're going to focus on today. I've been doing some book learning this morning about identity. I tell you what, you know, if you want to figure out where to start with zero trust, you got to start with identity. Every one of these five pillars, six pillars, the first pillar is always identity. And so let's talk about Sampras champion, and how you can help my federal listeners maybe, maybe help them with the first part of the first pillar of zero trust.

01:35
Yeah, absolutely. So, you know, I came to some Paris last year, to help out build out this defense in depth starting with identity Corp. Right. So just a quick background on my my history. So, computer technology has always been in my blood. I was a kid writing code on the Atari 800, the Commodore 64, the Radio Shack trs 80, model three. I grew up using the 300 baud modem in the late 70s and 80s and war dialing into bulletin board systems so always enjoy different types of technology, and ended up joining the military after college with my military career in the Navy. bringing me here to Washington DC area. I worked with various federal system integrators like north of Grumman, SAIC, Raytheon, and went to work for various sim companies like ArcSight securonix, are focused on correlating tons of log data to help find those bad actors. And I learned a lot about hackers gaining access to various methods used across the enterprise. One of the most prevalent

themes I saw was hackers gaining access to identities of users that they needed the access for right? Actor directory is the core identity store for 90% of organizations worldwide. This was a message that resonated with me when I met with Mickey our CEO, here at Sun Paris, if we can protect the core of the enterprise and environment, the identity store, that to me is a home run. The sun Paris mission is to be a force for good. Having worked in cybersecurity for over 25 years. Now. That is a mission statement that I understood. Well, here's

03:14
the mission statement that I have if everyone's eating pancakes at the restaurant, and must be pretty good pancakes. If Sampras is one of the 60 fastest growing cybersecurity companies. You're either lucky or smart or you're focused on on something I mean, I mean, we know that large enterprises do tend to use Active Directory more than smaller ones. And so so your target audience is probably going to be large organization like the federal government. Is that right, Jimmy? Absolutely.

03:38
So the value that some parish brings with the federal leaders today, John, you know, according to Mandiant, researchers, nine out of 10 cyber attacks involve active directory. Let me say that again. Nine out of 10 cyber attacks today involve active directory that is staggering. That's unbelievable. You know, it's something I always knew subconsciously. And clearly, the founders here at some Paris already knew that importance of creating a great product protecting a core identity store. Late last year, NSA and Sissa really released a list of the most common vulnerabilities in enterprise environments. And to no surprise to us here at some Paris, many of those on the list directly involved Active Directory. To answer your question, the direct value here some Paris is, you know, we have over 150 plus combined years of Microsoft MVP, expertise, expertise, and experience on staff, and over 25 plus former Microsoft premier field engineers, on staff as well. Many of those engineers are very long careers with Active Directory, including working in Microsoft. The knowledge and expertise they bring to creating the products we implement for federal leaders today is monumental. Did you know Active Directory is turning 25 This year,

04:57
created Actually Actually I didn't know that I remember it was released. Yeah,

05:01
great in 1999, it has stood the test of time, right? of evolving from RFCs as early as the 70s. And, and initially Released with Windows 2000 Server Edition, it has been a core identity store for many, many years. And so Paris has created some great products to help protect it and recover from disasters that may occur with it as well. And we are seamlessly out of the box integration with many of the top sim companies out there today that are correlating information from across the enterprise network.

05:32
I know like Databricks are having a show in town next month, aren't they? Yeah, absolutely. Good, good, good. So I go to a barbecue place in town with all my neighbors named Patrick Sullivan. But a year ago, I was sitting and talking. And he said, Well, you know, people started talking attack API's. And I said, come on. Oh, yeah.

After API's. Now is that your website this morning? S E MPRs. And, and they're attacking Active Directory, that's an attack vector really, the going after that?

05:57
Absolutely. You know, if you think of a defense in depth, strategy or model, right, or if you think of an onion, right, and you peel back the onion, the defense in depth layers, right? I did a CT is right in the middle of that onion. And it's essential to protect that identity core. And again, you know, the attack surface is usually measured by looking at the potential threats to the enterprise, right, we have built into our DSP, which is our directory services, protector, the ability to scan and evaluate the identity landscape, and quickly notify the administrators of vulnerabilities or have automated orchestration, that can rollback potential changes in the identity store, like Active Directory, before an attack vector can be used and the compromise and the actual account occurs. Identifying these potential vulnerabilities in real time as they're occurring across a wire allows us to reduce the overall attack surface for those bad actors.

06:54
So this is really kind of interesting. I understand if you have data needed to be backed up. I mean, I know that a hole drilled and recovering from but recovering from an ad attack, that's, that's new, I guess, I'd never thought it was possible. But I guess it's there. Ha, yeah, it absolutely

07:10
has to occur, you know, if you think of, you know, the ransomware, or even nation state attacks, right. So if they get into the Active Directory, and they've modified or they've changed the Active Directory, you've got to be able to put your system back into a pristine kind of environment. Right? And, you know, what's, what's alarming is, a lot of organizations today, they believe that as long as they have a backup of the Active Directory, they're good to go. But you know, you don't want to be able to roll back to a system that already has malware infected, you know, maybe a year ago, right. So if you think if you bring an old image back into your environment, that's maybe six months ago, you might still be good, it could still be corrupted with malware, and you could still be right back where you were, you know, with the problem again, so, you know, we have a technique or approach that's very unique to us is approach where we backup, the Active Directory, parts of the product, or the objects to groups, users, or roles are all maintained. Part of our accurate dri backup, which is separate from the OS. This is really cool. Some Paris technology allows us our customers to backup and be running again, in a very short amount of time. Here's

08:23
what surprises me is that I can kind of I can understand recovering quickly. I kinda understand that. But But I guess your product also can intercept it before you need to be recovered. Hmm, exactly.

08:34
Right. So we use what's called in stream technology with Active Directory. So we're not actually monitoring logs to look for, you know, malicious activity within Active Directory, we're actually monitoring the streams, the actual Active Directory streams as they're occurring. As the objects are changing, the users have changed in the roles are changing. We're monitoring that in real time and looking for nefarious activity, and can act on that

very quickly, notify administrators very quickly or have some type of orchestration that takes care of those problems immediately.

09:08

But 10 years ago, I worked for a company and they would get HP servers then and and the system administrator would provision the servers and I always think of provisioning servers and an access like that. However, I think there's an application here with identity. I mean, what happens if John Gilroy leaves the company? What if John Gilroy leaves an agency? I mean, my name could still be in there for I don't know how long and I think this may be the last people that's on the checklist. I don't know if this is on the checklist of get John Gilroy off of access. And this is something I think you have to consider because there's a lot of strange things out there that people will happen all of a sudden is from someone who's had access five years ago.

09:46

Exactly. So we also use machine learning capabilities, behavior analytics into our product. And we can look at the overall patterns of the way users are using the system with Active Directory. So we have ability to actually see that users are no longer using the system or no longer actively using the different objects or roles that they have assigned to them. And we can take action on those as well.

10:12

I was at a, an agency one time, and let's say it had involved with education and but talk to the people there. And apparently they had some older systems from legacy systems. Well, it's a surprise. I think that's probably true for many companies. I think it's true from 88. And I think large organizations probably have those somewhere. And so does that throw a monkey wrench into the works when you try to have an advanced system like some Paris, or work? How do you interact with legacy systems? Yeah, so

10:40

we treat all systems the same way. Right? So they have at the core of their product enterprise is the Active Directory, it's where all those objects and rules and roles and users are stored, right. And those objects are protected by our products. We have products like DSP directory service, protector, NFR, which is the Active Directory, forest recovery product, and these products will constantly monitor your environment. Look for those vulnerabilities. We're looking for, you know, the iOS indicators of exposure, the IOCs indicators of compromise. And, you know, we're implementing frameworks like the mitre attack and defend and antsy frameworks and others to, to look for those those type of events as well.

11:29

I got a bunch more questions. But many times, people, it's my podcast three or four months after it's recorded. So if you're driving down the Nationals game with some friends, and you're listening to podcast, and you want to learn more, at your website, there's a pretty good blog there. And I'll put this link in the show notes. It's called comprehensive identity protection and resiliency. And most people don't think about resiliency when they think about their ad. I mean, I always thought it was like a refrigerator. Maintain your refrigerator maintain at well, yeah, I never think of that this kind of, and guess what happens? People looking for the vulnerable Lincoln, and this may be the vulnerable link. And so you have to protect

12:06
it. Yeah, absolutely. I mean, there's there's three stages that we look at, at some press, it's the pre during and post attack, right. You know, continuously monitoring and zero trust are core to our product. You know, we mentioned layer defense across the entire lifecycle of the Active Directory tech, you know, for pre attack. We support our customers by finding and fixing your Active Directory security vulnerabilities, therefore, thereby reducing your attack surface, continuously monitoring identity store for configuration drift, constantly updating iOS IOCs. And like I said before, operationalizing, the mitre attack and defend in other frameworks. During the attack, we're able to detect those attacks at the replication stream again, which bypasses having to monitor any log streams, we actually see those changes happening in real time on the Active Directory, C string stream, something that is very unique to our company. Obviously, we enrich the Sims and sores and sock tools in real time. And we can roll back the malicious changes in Active Directory and Azure AD as well. And then post attack. We are with you as well. We can automate the active directory forest recovery process which provides a huge reduction in time. Widespread attacks that exploit Active Directory can cripple your organization. And when ransomware or wiper attacks, takes our domain controllers takes out domain controllers. recovering your active directory forest can drag on for days or even weeks, risky malware reinfection, the process but with our product, Sampras active directory forest recovery, you'll be back in business in minutes or hours rather than days or weeks. Well, you've

13:49
used the word unique a couple of times, and I'll apply the word unique to something at your company. It's called the purple night. So I have no idea what this means. So what is the purple night Naga? How would you go? Don't you remember that name? Yeah, you know, we

14:03
have a marketing team, right John? So they do that kind of thing. You know, purple night is a free Active Directory Cybersecurity Assessment Tool built and managed by our own Centaurus threat research team. The purple Knight tool has been downloaded over 10,000 plus times, helping organizations assess their overall security posture on their identity core. You know, according to Gartner 33% of organizations today use no Active Directory defense whatsoever. That's alarming to me. And what's even maybe even more alarming is you know, like I said before, these organized organizations believe they're protecting their active directory by merely doing system backups are a threat research teams or CEO or entire company wanted to provide a valuable asset or valuable assessment tool for organizations to look at their Active Directory and see where they need to improve the overall posture of this core identity store. You know, Jimmy,

15:00
I think if we were just informally were at a conference sat down with some, some federal leaders down there, I would think that 30% Number, I think that maybe, you know, maybe different than most people think I mean, how many I've had hundreds of conversations about secure 100 The conversation about backups, immutable backups, and no, no. What about the backup the ad? No one ever thinks of that. That's not even that that's not the checklist. Don't think so. And so that that has to be part of I think, a word, the phrase, a prudent approach. Absolutely.

15:30
So, you know, purple Knight has hundreds of security indicators, which can help organizations proactively evaluate their identity core security, Microsoft has actually said that, you know, 88% of the customers, that's, you know, nine out of 10 that were impacted by incidents, had insecure Active Directory configurations. So I'll say that, again, nine out of 10 customers that had incidents at insecure Active Directory configurations, it's, it's, you know, again, our intent and our hope to help guide organizations in closing those vulnerabilities. So with our free purple night tool, you know, it's listed on Cisco's website under resources and tools, you can download it for free today on cypresses website as well, you know, and also I'll tell you, John, we have a new tool that came out recently as well. To complement problem is called forced druid, another marketing firm, that we have purple Knight and forest druid, foresters another great free tool we just recently released, you know where purple Knight is focused on the vulnerabilities in your Active Directory setup. Force truth focuses on the attack path availability to take over those tier zero assets. So foresters free attack path discovery tool, natively compatible with Active Directory to help cybersecurity defense teams quickly prioritize high risk misconfigurations that could represent opportunities for attackers to gain privileged domain access.

17:00
Let's drill down into that term configuration, because you combine that with a word earlier, configuration drift. So when I was taking notes, and you're saying that I wrote down scope, creep, configuration drift, and I think if if John Gilroy company only used one cloud service provider, you know, might not have to worry about, but today, it's all hybrid, and things are moving back. I mean, there's repatriation, John Gilroy, goes back and kind of goes back out of the cloud. What about the provisioning there? I mean, I can, you know, I can understand this phrase a lot better when you think of the hybrid cloud, because configuration drift almost must be parallel with the hybrid cloud. Connected, isn't it?

17:41
I'm sure there's a large connection there. You know, we look at, again, how long Active Directory has been around, right? And in many of these organizations and enterprises today, they've probably had the same Active Directory they've had for many, many years, right? So you think about all the changes have gone throughout that Active Directory history, where it's been implemented in that organization, there is a lot of configuration changes, a lot of roles that change, right? People leave, they come back, or they go to a different operational organization, or they move to this organization that can continuously changing, right? So our goal within you know, Sampras is to be able to help give that knowledge and that information to those admins that are monitoring Active Directory to say, hey, look, let's look at these kinds of parameters that are being changed within Active Directory and see if that really makes sense.

18:33
So crystal ball time, let's cast your eyes into the future. And, boy, I gave up in the prediction game a long time ago. It seems like there's going to be more indifferent attacks. I mean, we talked about API attack and ad attack and everything else. And so where would the best way for people learn more about mean this innovative attack of attacking at mean, go to conferences? And I mentioned a blog earlier, where can they learn more about this? Jimmy? Well,

18:59
definitely our website has a ton of information we have, we have blogs, we have news articles, we post stuff on LinkedIn all the time, about the technology that we're trying to protect from a core identity perspective. You know, there's there's plenty of information, I think, on our website that can they can provide that information. If they go they're

19:20
good SCMP here as well. We're running out of time here. You have been listening to the federal tech podcast with John Gilroy, like thank my guests, Jimmy McNary AVP for federal solutions at some terrorists.

19:35
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.