FEDERAL TECH PODCAST

Ep 51 Putting it all together: the Dark Web, the FBI, and Federal Cybersecurity

Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Today, we're going to take a look at security optimization and platforms. And we're going to focus on a company called reliaquest. And our guest is Mike McPherson. He's the senior vice president for security operations at reliaquest. But before we begin, I have to talk about the elephant in the room. And no, the elephant is what you think it is the elephant the room is the Super Bowl. The Super Bowl is a couple of weeks back. But Mike's got a story about a football game and his company to tell us about your story about your football game and your company. The reliaquest bowl, is that what it is?

00:49
Yeah, sure. It's great, great talk to you, John, really, really enjoyed the conversation. Thanks for taking the time to talk to reliaquest invited me on, you know, we've been super excited about it back in, you know, early January, the reliaquest became the title sponsor of the reliaquest bowl down here in Tampa, which I know historically had been known as the Outback Bowl for years and years down here in Tampa, one of the one of the premier January 1, football, bowl games, college football bowl games. And this year, we took over the sponsorship at Apple, so super exciting time for us here at reliaquest.

01:24
And the reason I bring it up is because riot quest is a big successful company. It's operated well for many years, in fact, so successful it can endorse a whole football game like isn't, so they're very, very successful. And Mike's got a successful background also. And it ties in directly to the federal government. So maybe just a little, some thumbnail sketch of your background with the FBI. Please, Michael?

01:45
Yeah, I appreciate it. Thank you very much. I have been at reliaquest. Now, just just almost a year now, John. But before that, I spent 25 years in the Federal Bureau of Investigation. I started my career up in the late 90s up in New York City doing work on a Colombian drug squad, tracing drug dealers around New York City in the late 90s. Up until like September 11 happened, right and the the world was shocked by the terrorist attacks. And I was there that day in New York. And you know, I experienced that and witnessed that. And many times I say, you know, the world changed, you know, the FBI change. And I changed that day to have, you know, how, how I thought how I operate within the organization of becoming from this, you know, reactive organization is reactive person that we could go out and solve some of the best crimes in the world no matter what it was. But now this idea of becoming proactive and understanding the threat and getting ahead of the threat. And I spent my next 25 years kind of perfecting that and I shifted even towards cybersecurity in my years. And as I left the FBI and came to join the private sector, I realized that, you know, I am not ignorant to the cybersecurity threat that this nation faces. Because, you know, cybersecurity is national security as I see it, and I'm glad to still be

playing a role in helping protecting the nation's economy and my role here reliaquest As I transitioned out of the FBI, okay, so people are

03:13

trolling around for a podcast that might help them and they see this guy with FBI Background strong in this company, very successful commercial background. So from, from my opinion, but I deal with guppies a lot. I think they respect success in the commercial world. And so I think what I want you to do today is maybe convey some of that, well, look, we've been really good with banks and financial institutions, insurance companies all over the world. Maybe we can apply this to financial institution, the federal government, they sure have them, they have all kinds of health care opportunities in the federal government and, and the regular good old fashioned DoD type stuff. So I went to your website this morning, and I saw a couple of words, and what words can fascinated me, it was gray matter. Now my wife, I've been married for 39 years, my wife says I have no gray matter. So maybe you should be the expert on this. Because I just wonder so so what is this gray matter? Anyway?

04:01

Look at reliaquest. We're a cybersecurity technology company. So what does that mean? That means like, we offer our security operations platform, which we call gray matter. And this gray matter platform allows large enterprise customers. Those are those are customers of significant revenue, 500 million billion dollars in annual revenue. And we allow those customers to detect, investigate and respond to cybersecurity threats. across their enterprise. It doesn't matter where their data sits, whether their data sits on the endpoint endpoint or on premises or in the cloud. We're able to help them and their detection, investigation and response areas we like we like to say we're the force multiplier of security operations in this really complex world. Because you know, as our CEO and founder Brian Murphy says, you know, cybersecurity is the greatest technological challenge facing this nation today.

05:00

So the tagline for this is reliaquest, gray matter do what others aren't willing to do. And so you put your nose in areas that maybe it will be dangerous. That's what sounds like to me.

05:13

Yeah, look, this is a really, really hard space that we're in. It's not it's not easy, right? It's complex. There's, the threats are varied and deep. The ways to combat it is really challenging. There's a ton of tools out there to a ton of vendors who want to sell people things and say, here's the next best tool, here's the next piece of technology. And, you know, our clients and customers are out there trying to buy trying to acquire trying to stay ahead of the threat. And we help we help them right by giving the security operations platform, then backed up by world class security operations center by experts, that were able them to keep the technology, they have been able to pull their threats in and take a look at these threats across their environment, that are able to increase their visibility, reduce their complexity, and manage the risk. That's how we do it.

06:07

So manage the tech response. The tip of the spear here is response. So it can look and I can see a train coming and say on the railroad track and drink me get off that track. And so by response, what do you mean you coordinate with other systems or actual activities that your company can do to prevent intrusions?

06:24

Sure, like once once a threat is detected, and then we'll we'll help them investigate to see how bad the threat is. And then the response is everything from an automated response through the platform that can take an automation that can that can isolate a host that can take a take a technology offline, remove it from the network, if it's if it's infected, or, you know, semi automated, where we'll provide a recommendation to the customer and say, here's what we recommend that you do, we think we should do this. So we work in joint with the customer. And that's what they say we're a force multiplier for them. We know when to remove them from from the effort of we'll never know their environment has been as much as they do. But we can certainly work with them, and help them increase the visibility of what's happening on their network.

07:13

I went to your website this morning reliaquest RELIAQ usc.com. And saw blog had a great title, the blog title, something like top ransomware threats to watch out for and 2023 and a 13% increase in ransomware. and Equal Opportunity attacker, I mean, hospitals, federal agencies, John Gilroy donut shop, I mean, equal opportunity. And so there has to be dealt with rather than some small point solutions like antivirus. I mean, there's got to be a better response than these point solutions shouldn't there,

07:47

it looked at the threat of ransomware is not going away, you every day, you open up the newspaper, turn out, turn on the news, and you'll see another organization getting hit. And no one is safe. And depending who the threat actor is more often than not, they're they're trolling the environment looking for the weakest link, and they're gonna go out there and say who's not protected? Who can they take advantage of, that's who ransomware these criminal organizations. And if your defenses are strong, and if you're capable of perhaps I'll just gonna move on to the next person who's not next organization who's not as equipped to deal with them.

08:26

I've done hundreds and hundreds of interviews and one of my most memorable interviews is with a guy named Brigadier General Greg two hills tired. And he can do anything he can probably fix the transmission a car and train a horse and then fly a jet. So he's a great guy. He's he's running folks up at cert in Pittsburgh. And when I had him on the air, he had this really great quote, and I just wrote it out of kept it's really gonna quote, he said, complexity is the bane of IT security. I can't compress it. I mean, it. It's what you guys do from 3d blocks your posts is no, no, here's what we do. Got all this junk here, this junk there, right here. Take a look here. Here's the on off switch. So it reduces a complexity, doesn't it? What I mean,

09:03

that's exactly what our platform offers, right? It's those three things is that increased visibility, reducing complexity, and all in the hopes to help manage your risk. So when his chief information security officer when He's raising his hand, you know, to the board of directors and his CEO, saying, I'm going to protect your

network, I'm going to stand up and use all the resources I can, you know, he needs help to do that. He's having, you know, a variety of tools that likely don't even talk to each other, speeding towards him and his team who is probably limited and resources, he has to go back and try to justify every dollar he has to spend, or pivoting from tool to tool trying to correlate alerts trying to correlate metadata on what the environment looks like. And we believe we have that solution with gray matter to give him that one pane of glass that one place that he can look to pull those alerts in, enrich it, enhance it with data, add more data to it, because he has more visibility, and then help resolve it, helping that response portion of it as well.

10:07
You use the word visibility, let's unpack that word a little bit here. And many times, people look at networks and say, Well, what visibility is is finding what, where everything is on the network. And that's a challenge with shadow IT and everything else. But I think with visibility maybe applies a different your world, because the visibility I've read about your company, you try to try to make things that occur in the dark web more visible to potential attackers. And so this is an interesting aspect outside of the football, the reliaquest ball. The other most fascinating part is this whole dark web activity it's you have. So that's a component of getting an understanding of what threats are out there, isn't it?

10:43
Sure. Absolutely. Absolutely. We talked about visibility. One is like where your where your internal data sets, and we talked about that already, whether it sits on the cloud, or on the premises or any endpoint, you're collecting that internal data you want it to. But then there's a bunch of external data. Also, when we recently had the acquisition of digital shadows at threat intelligence company, just last year, we acquired that company, and they really specialize in the threat from the outside in what is on what's happening out on the dark web, what's happening on the internet, they can collect that understand that TTPs that tactics, techniques and procedures of the adversary, whether they're nation state actors, whether criminal organizations, and how to take that data from the outside, combine it with what we see from the inside of within the customers network, and blend those together so that a customer can understand know what the what the threat looks like, because you really can't protect against the threat unless you understand what you're fighting against.

11:47
And I think one of the biggest battles is fighting against complexity. And we think we've got that answered with the kind of platform you can use. So when it comes to risk management, you know, when I started 10 years ago, I didn't agree on risk management. I thought all through the software, no, it's financial risk management, I think they've appropriated that term into your world of risk management. So so how can a system like reliaquest assist someone at an agency federal agency, kind of manage the risks?

12:15
At the end of the day, you know, a lot of risk management that comes down to not deliberate decisions based on the resources you have, right. So you have to have the visibility into your network, you have to understand the threat that you're having. And then you'll have to make choices, investment decisions on how to combat that threat. And that Cisco, that information security officer has to go to the board of directors, and make a business case for investment that he wants to make to help protect that network with a promise he had. And

we can help them understand get the best out of their tool that they already have on their network to increase that visibility increase that they know the dollar cost value of their investment. Are they getting enough about it? And then how does that map against a threat? How does that map against Mike, the mitre coverage of standard of threats coming in? How are you covered against those different threat vectors? And do you need to apply more investment in certain areas? An investment could be in people, it could be in technology, it could be in a various different ways. But the whole point of it is making deliberate informed decisions.

13:18
Yeah, I think that's the whole part of the the part of the discussion where takes action, and something has to be performed. I deal with a lot of software developers, and a trending phrase is continuous development, where they're, you know, an Agile process that considers development. And this word continuous is, is is applied to continuous integration. But I think it's applied to continuous visibility and networks isn't so So I walk into your shop and I go, Hey, clean, clean bill of lading. A clean bill health, you're fine. Well, so what? And yeah, that it's 1201. And something happens. I don't know where so I think what's interesting about your product is that it offers this this no, we're not done yet. We're still in the middle of doing and you got to be proud of everyday this continuous application. I think this is a theme I've seen through software and through cybersecurity. So you offer continuous visibility, continuous automation and then measuring it to see how you did the month before a year before hmm,

14:11
absolutely. I mean, fibers security's continuous journey, right? Because the threat landscape changes, the tool to combat it changes and you constantly and the threat is different every day. Our adversaries getting smaller, but are better and faster. You know, time is the enemy in cybersecurity. So there's no perfect but there's always a better and that's what we say there. There's always a better than what we're doing it today. And we have to keep striving for that because, you know, we're a firm believer what we say is cybersecurity is a team sport. You know, you have to work with partners. We have to work with our customers to do it. There is no one entity to do that. And I learned that from my early days and the FBI and we're trying to you know, trying to fight terrorism and the big bad FBI we we had to be humble about it. Say we need to help, we needed help from local law enforcement needed help for the intelligence community, we had to reach out to the private sector and start sharing information doing that. And I see that in the private sector side, too. You know, most of these organizations are incapable of doing themselves because it's complex, and you need someone to come in and help you to do that. And that's a space that we reliaquest We're trying to help them solve for,

15:22
like, there's a podcast in town called Feds at the edge. And it's kind of appropriate, timely and appropriately named, because we see more and more systems being at the edge and many times the the data processing has been at the other edge, you know, that computes done at the edge and, and what at what point should you the commute and what's the most effective way? So I would think if you, if you and I are sitting or big ol room with a whiteboard, and I put a timeline on there, I'd say Well, looky here, this all this edge is this coat. And so this is must have impacted some of the way that requires reliaquest approach to security is so edge computing concept, doesn't it?

15:57

Yeah, 100%. And it goes, goes back towards the visibility of understanding what can you What can you see what are you what is your capability to see what's even what's on your network, right, and what's out there, and your capacity and capability to leverage the tools, you have to understand how you positioned against the threat.

16:18

Mike, if you go to Gartner, Forrester, you always see these charts, these category make up these categories. I don't know how they do it, they're probably do with a you know, maybe on a whiteboard, bunch of people in some beers, something. And so many times the acronyms associated with your organization's MDR and XDR. So I want to use a different acronym, I want to use MFA. So my, my daughter has a master's degree in finance. And she has a friend of has an MFA. And so I know what that is. And they said Master of Fine Arts, no, cut the wrong MFA. So multifactor analysis, the reason I bring it up is because the people I've talked to that don't want to display it, some people in the lower levels are managing systems, and they're actually the boots on the ground, and they get so many alerts, they turn some off. And then you get alert fatigue. And all of a sudden, you can have situations where the attend to have words today, and you don't respond as quickly. And so some person or something has to come in and say, Look, we understand, you know, you're turning off these words in secret, maybe there's a way to automate it, maybe an automation process can not reduce the number of alerts but help you maybe prioritize or decide which ones you should use your analytical ability to respond to. So I think this automation is got to be part of the Cisco too, doesn't it?

17:29

Automation is completely it's, it's a cornerstone of what we do in the environment, you know, they, we don't believe that an analogy, an analyst, whether it be in our customers, or in our own security operations center, should be working some of these tier one alerts, you know, we do the human brain, the human people we take, we want to remove what we call the low brain, I'm activity of the analysts, they the duplicate alerts that the small stuff that can be automated out, enriched and enhanced with data, so that our analysts are really spending time on the tier three, tier four, the threat hunting the big brain activity, which is why where we believe the human person wants to be and where they should be. And there's a lot of success we've had in our platform of being able to remove a lot of this noise from it. And a lot of people claim claim to do what we've seen. But we've seen great success with our customers, and being able to understand the problem that they're trying to solve for understanding their risk tolerance, and being able to cater it to that of based on whatever sector, whatever space or in the size of their team, when we see security teams may have two people on it, or may have 50 people on it. And our risk tolerance in that organization may be a little bit different. But no matter the size, we don't think any of those teams should have to look at a tier one alert, we should be able to automate some of that and rich it with the data and build it to make some of those decisions over and over for the person.

19:06

So I just dawned on me, the acquisition of the company, the dark shadow company, allows you to gather more information. And all of a sudden, the database you're using can help categorize or prioritize people in the federal government. So someone sitting out interior or female, or where we happen to be in town here, and

they get some of these lower level threats and whatnot. And I will do that after lunch. Now I gotta worry about the fire in the hallway. That's you're gonna have to prioritize it. Maybe they will it Oh, no, it's down. And if we don't get that we get the 10 for you to the fire. And I don't know, you have to prioritize things there. The all kinds of military people say if you defend everything, you've said nothing. So maybe that's your skill is that knowing where to collect information or to help prioritize and let them work more efficiently?

19:51
Right. So we want to pull in the data from all the avenues that we can right so whenever we have Some of the tools out there on the maybe on the customer network or some are external threat streams as well, too, we can enrich those together within our platform. Now you start understanding, okay, what is it this IP address coming from is associate with a certain threat actor. And I know these threat actors, this is their tactic. And there's the techniques and their procedures, here's, I know what they're going to do, I can start making some proactive actions of what they're going to do. And if I may, I know it's a nation state actor. And I'm going to function a little differently because of nation states, and then a criminal organization, all those things come into play, much of that early stages can be, can be automated, I know if my analysts have to do something by hand, it may take them two hours to do a comprehensive hand analysis. But if I use my gray matter platform, to save analysis, I can done in in minutes and less than 20 minutes to help make some of those decisions quicker, and then I can enrich it. And then I can add human analysis on top of that, but I'm getting to that decision point much, much faster.

21:01
So that's why someone like you can look at a series of events and go Well worry about this, don't worry about that. And that can help in prioritizing things and, and make sure people don't waste their time on the wrong thing. So it's interesting that your background combined with it's like these building blocks putting together it seems because it's pretty good, pretty good puzzle to help contact this incredible difficult heaven. And also, you talked about your company in the blogs earlier, I just want to leave my listeners with this. This is a very good book, by the way. It's called Top Top ransomware trends to watch out for in 2023. It talks about all kinds of ways. And, and it's not just a corporate pitch. It's a hey, we've encountered this stuff, and you're going to hit it too. So make sure you do this, this and this. And if you want to pursue it fine, but here's your chance to do so I thought it was very well done. I think it's a good thing to leave our listeners with any predictions for the future.

21:52
Look, this is the this challenge isn't going away. But you have to understand the threat to combat the threat. And I learned that in the FBI and it's in practice here at reliaquest. To is we have to understand, you know that adversary what and how they do it. And at the end of the day, we can make security possible when we work as a team. And that's one of the important things I think is being able to be humble enough to say, I need help to do this and no one person no one organization can do it alone. And

22:22
that makes sense to me. Well, great. You've been listening to the Phil tech podcast with John Gilroy. I'd like to thank my guest Mike McPherson senior vice president security operations at reliaquest