FEDERAL TECH PODCAST

# 100 Ep.100 Understanding Threat Intelligence for Federal Systems



00:00
Hey it's John Gilroy from the Phil tech podcast.

00:05
And this is Dave Monae with Tim comer.

00:07
Today we're gonna talk about how to understand threat intelligence for federal systems hit the music Manny. Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is David Monia a chief information officer, chief evangelist and team Connery Fellow at a company called Team Comrie, David, how are you?

00:28
I'm great, sir. Thank you. How are you? Good, good, good.

00:30
Talking about threat hunting and threat intelligence today. And I think anyone who's listening to this is read articles. They know it's very important, especially in the federal government. In fact, just last week, these folks over at CES talked about bolstering there's the word there bolster threat hunting. So David, why in the world bolster threat hunting? Have we done this for years and years and years?

00:51
So we have certainly been aware of the idea of threat hunting. And I think, you know, for listeners, it would be a good idea for us to frame you know, what is threat hunting? What's the, you know, what, where does this fit in? And threat hunting, when you think of it in traditional terms, you know, when kind of security policies and whatnot began, events would happen like this, you get compromised, or you get attacked. And hopefully you catch that attack and then mitigate it somehow. But typically, that isn't how it happened, because people weren't actually able to detect the attack stage. In typically, they would catch the misbehavior of a already attacked already compromised device. And then they would go into remediation. Right? And that's expensive and unfortunate, because there's typically, you know, a scope of impact effort that has to go on because like, how do you know that only this one system was compromised? So then along came the idea of, well, let's start to be more proactive, let's start to understand what could be done to us. And that's where kind of the idea of you know, red teams started to emerge to kind of test security postures, to see how your policies work to make sure your controls were applied correctly, and things like that. And then, as time went on, though, people

started to realize, you know, it would be great to be able to actually try to better understand adversarial movements and what adversaries were doing. Now, in the federal space, that capability is certainly available, in particular, through some federal agencies that you can request support from national security agency, for example, if you're, you know, critical infrastructure, you can say, hey, you know, we have this and how can you help us, you know, better understand this, they run these programs that are absolutely fantastic. But the problem is, is you have to start with something very specific, right? And you get back a very specific answer. And that's all, you know, legal obligations, title 18, and whatnot suggests this is how all this has to happen. So, but what that leaves is, kind of a space for being able to quickly assess in event. So you have an IP address, and you want to know, well, what else has it done on the internet? Who is it doing to and giving that type of context. And that's where we come in. And we would say that we've evolved threat hunting into what you could actually describe as threat reconnaissance. And threat reconnaissance is, like I described, so you've identified some source of malice, that's affecting your infrastructure affecting your network, and you want to understand context, is this, you know, is this a random drive by where it's, you know, somebody's just spraying the whole Internet looking for a specific vulnerability? Is this a industry specific thing? Like, are they targeting just federal agencies? Which, you know, again, kind of suggests, more more nefarious than, say, the, you know, average, just exploit everything on the internet? Or is the thing that probed you talking to nothing else, but you? Are you the only thing that they seem to be attacking? And that level of understanding is game changer, right? In particular, you know, imagine it's, you know, Friday 4:30pm, this event happens. And now you need to know, like, am I working over the weekend? Or is this something that I can triage and understand that, you know, hey, this was random, we're not being specifically targeted. So what we do is we make available what we call pure signal. But you can think of it as you know, collection, data lake of largely IP metadata, but also some other data sites that allow you to illuminate the sources of events and understand what else they're doing in one of those things that what else they're doing is who's managing that infrastructure? And then you can pivot off of that and understand what other infrastructure might they be managing. And this would allow you to create a true proactive security posture and apply. You know, as you see, the adversary standing up new infrastructure, you could already update your border policies to, you know, say deny that traffic. And that's just one of the applications. There's also great use cases around third party management. So supply chain thinks supply chain observation, you could look into your supply chain to see if they appear to be compromised, you can use it for asset discovery of your own infrastructure, as networks have grown over time, we apply our peer signal products for that exercise as well. But really, you know, we provide global visibility towards, you know, a lot of defense use cases where we have pushed the ability to apply policy in a defensive Stach status far left of the event stage so far to the left or far left of bang, if you will, and less so helping organizations break out of that kind of reactive approach to security.



05:55

Now, before we started this interview, I told you I had a little background and radio. And, you know, it has to spell things out. For example, your website's kind of hard to remember, but I'm gonna spell it out for audience. It's team dash, c, YM, r u.com. And you'd all kinds of information there. And what's easy to remember though, is report you folks have called voice of a threat Hunter. So website hard to remember, it'll be in the show notes. But voice over threat Hunter, I remember that report may be downloaded. Thanks for that. Yeah. So what's it all about? What's the voice for 300 is all about and why should our listeners download? Yeah, well,

06:32
it really dives into and much deeper detail, what I just described, the ways that we you have, we have kind of evolved the landscape for a defender, allowing them to have visibility and near real time on adversarial actions. And it has moved to the concept of threat hunting, you know, into the next era. Frankly, evolutionary, not just revolutionary, and the capability, you know, again, the resources available, in particular in the federal space are vast and massively capable, right. But that all takes time, you have to fill out requests, you have to wait for some type of response. And all of that takes time. And time is the only resource you can't get back. Right? You can make more money, you can print new drives, you can I mean all you can make more of everything but time, right. So having access to instant answers, nearly instant answers that provide situational context, related to adversarial actions is frankly, priceless. So that's all kind of spelled out in the voice of threat Hunter. And you could think of it as it's not just attestation you know, in the voice of a threat Hunter part, you know, it's not just that attestation. But it is a very good paper that kind of highlights how people should be thinking about proactive security in the modern world.



08:03
And what people are thinking about as podcasts, and you're a guest on my podcast, and David, if I'm not mistaken, you have a podcast as well tell our listeners about your podcast, please.

08:11
Yeah, absolutely. So we have a podcast called The Future of cyber risk. We, by the

08:17
way, that's easy to remember, you go to Google and type that in Kancha, the future of cyber risk, bang, we get to take this podcast. Finally something easy.

08:26
That's right. Yeah, no, that's right. So but the podcast is really geared towards kind of demystifying the positions of, you know, risk managers. So that's, you know, your CISOs, your CIOs, your policy and framework advisors, you know, all that kind of the full gamut. We have a varying range of guests from kind of the technologists, who executes up to kind of the policy advisors to law enforcement who see through the process to the end, we have had guests from around the world. North America and Europe, I think I've largely, you know, taken over the numbers wise, but we've had guests from around the world. And what we tried to do is, like I said, we tried to demystify what is risk management in the amount of world, you know, legal obligations around around the world, in particular, around certifications and things like that, and regulatory concepts. They often have requirements for specific titles to appear in organizations, where there's simply not enough people to kind of fill those roles. So there's a lot of people that meet kind of educational requirements, but not the experience requirements, who find themselves in these situations where, you know, suddenly they're trying to understand well, how do I be a CISO? I worked for the policy office previously, you know, and suddenly they have to understand all these new things that can be overwhelming can be daunting. So what we try to do is we try to bring in SMEs that can provide insight And, you know, if not defang the topics, at least demystify them in the objective being, you know, leave them with some idea that, you know, hey, maybe I've never done this before. But this has been done before. And I can tune into the future cyber as podcast and hear how

somebody else did it. And you know, what I should be thinking about and what perspectives I have. And then even if the listeners aren't in those situations themselves, it's been very informative for folks to just understand what are the thoughts that these people in these situations go through? So it helps them to kind of understand what is the security ecosystem? In what do you know what responsibilities and roles and thoughts and philosophies do all the people who have in the in that hierarchy? You know, how are they what ones are they looking at the world through



10:53
your amenities, people attend to events like Blackhat? And I think you folks are at BlackHat. And just put this in perspective. I mean, there are other organizations that do threat hunting. So what's the differentiator with you folks? Why should our gummies listen to this? Maybe I'll listen this podcast. So what's your differentiator? David?

11:10
Well, you know, first of all, it's absolutely zero hype. So it's not a lot of commercials, it's not, you know, no one can pay to get on the program. It's not positioned like that. So it's not, you know, whatever you want to call that edutainment or, you know, I forget what the term is, you know, but it's not a place to add. It's, you know, I'm not an academic I, I'm a Marine Corps veteran, who went to the Marine Corps right out of high school, I happen to be born with a natural aptitude towards understanding how digital systems work. I've worked for 27 years now in the industry. And but as a result, I don't communicate and with lofty language, I don't communicate with marketing buzzwords, I communicate, very frankly, simply, because that's the lexicon that I could draw from. And that's my favorite chance to use that word, by the way, is when I talk about how I don't have a strong vocabulary, but anyway, but no, I, I would really like to think that what we do is we produce a very easily digestible, zero pressure media, and our podcast is easy to listen to, it would be as if you were joining us, you know, for a cup of coffee, and you happen to be sitting at the table between two cybersecurity experts having a discussion that you can actually feel like you're part of. So, but having no hype is definitely I would say the leading thing.

12:42
So what about your company itself?

12:45
What differentiates us is our global access to insight. So, you know, we've set out for 20 years or so now, to facilitate services to the internet community as a whole. So think the organizations that actually make the Internet work. And in return, we have unparalleled access to the data that the internet produces. So we can answer more questions about badness than anybody else. I know, there are other people who make that claim. But I will tell you that those folks are also typically our customer. So but we are the source, we have products that deliver this insight to people, both via a UI UX. So like think of Portal, but also via API. And it's you know, near real time, threat intelligence that is applicable to like I said, provide context that really nobody else has, unless for perhaps you work for the Department of Defense somewhere. But otherwise, we have, we have more visibility than probably anybody in the world.

14:02

And so what people normally engage with you they'd have some kind of a platform digital risk platform. Is that what you call it? Maybe you could expand on that a little bit? Yeah,

14:11



that's correct. So we have three views. We have, as far as digital risk goes, we have an attack surface management platform that's been popular in the federal space. It's called Pure signal orbit. Then we also have for threat hunters. We have pure signal Scout, which is a very quick answer, nearly instantaneous contextual view, not a deep dive. However, it's, you know, Hey, these are the certificates that this host says this is where we've seen them. This is a basic view of kind of what the conversations that we've seen this host having with other hosts in the world, and what is the malice potential for those conversations? Again, our focus is primarily around maliciousness. So our data does have a tendency to have a bias towards bad Add, we don't get to catch a lot of false positives, we don't start by looking for them. But we do our collection methodology is kind of a, you know, total information awareness approach, if you will. And so we collect everything, not just TCP IP, or UDP, IP or whatnot, we work with a data format that operates at the IP level. But it doesn't just pull those three IP protocols out. We look at all potential 255 IP protocols. So we can see tunneling protocols, we can see things that stand out, but often avoid policy devices. So you know, your firewall certainly blocks TCP IP, certainly blocks, TCP, UDP, certainly blocks ICMP. But sometimes, you know, they don't pay attention to for example, GRE and nation state actors are aware of that. So they will sometimes make use of these alternate IP protocols to conduct exfiltration to maintain persistence, you know, things like that. So, our visibility includes all of that type of stuff. So but you can see that in Scout get a very quick answer that via its API, you could hook it up into whatever front end tool your analysts may be using, whether it be multigo, or, you know, potentially even something like Palantir, or something like that, if someone wanted to help us work with that, if they have that requirement, we could certainly figure out how to hook our API's, you know, in that direction. And then lastly, we have what you could think of as our flagship, which is pure signal recon. And what recon is, is a deep dive. So think of that down to granular visibility of all of our upwards of 45 or 48, something like that, datasets that are visible in the platform. So scout and recon working from st data, Scout gives you an amalgam ized, kind of short, pithy answer. And recon gives you you know, the nitty gritty, all of the data types, in particular, and recon are pivotable. So what that means is, is like, you know, let's say you look up an IP address, that IP address has an SSL certificate, Well, where else has this SSL certificate been seen a click of a button bang, you can see where else it's been seen in the world, it helps you understand because, you know, it sounds crazy, but Criminals are lazy, whether they work for a government to foreign government, or whether they work for themselves. So they will reuse deployment images and things like that. So even that small method that I just described of looking for SSL certificate reuse, in particular self signed, certificate reuse can oftentimes lead you to other pieces of nefarious infrastructure that you were unaware of. And you should update your network policies to keep them from being able to reach you as well. So those are kind of our three primary things. And then we also have threatened diligence feeds that are available as well, where if people just want like, just give me a list of IP addresses to block this, these are very popular amongst ice ax and a couple other federal offices, where they just had a requirement to purchase those, I forget the name of the program. Now. It's evading me but it's similar to basically we're in the book we're in the catalog aren't this defeats offering is, I believe, will soon have scout and recon in there as well. But there was a federal program that's put together for sourcing. And like our feeds, people can just open up an order it and it'll show up, we've

gone through already all of the federal procurement exercise to get in the book. So easily, easily available and easily applied. But those are kind of our four, our four prongs, product wise. In addition to that we do all kinds of effective community outreach and no cost services as well. I would encourage people to take a look at the Community section of our website, we are kind of a staple service of the backbone of the internet as a whole and can be for your network as well.



19:12

You said API and kind of like a flash and kind of flashed, I've, I've interviewed several people about cybersecurity and, and some people argue and maybe you can look at your 20 years experience and see if this is true or not. What what people have told me is that the attack vector now is not necessarily a firewall, but the API itself. You see attacks on the API itself as part of the you know, your observations here. Yeah.

19:37

So, you know, there's another number of avenues of threat there. First of all, weak credentials, whether those credentials be you know, a login password or whether they be some type a shared secret. I have seen very poorly implemented instances of those, in particular, because there's no web interface. There's no interface typically, which by the way, HTTP, you know, and Anytime you use a web browser, technically you are using an API. Right? They just happen to, I guess you can say that yes, probably. Yeah. Yeah. It's a it's a protocol within a packet. You know, I mean, so by definition, arguably, that is one of those. And what we're seeing today is kind of a resurgence of kind of the same pitfalls that happened previously. Right. So poor assumption, well, who's going to talk to this without knowing it's an API? And who's gonna then if they do talk to it, who's going to know how to talk to it because you know, API's are, typically have some kind of schematic way to communicate with them, right? You have to ask your question in a certain format. Well, again, just like HTTP, these things are often published, right? So an organization makes their service available via an API, the API has a schema document so that you can write your tools on the other end, that document gets in the hands of somebody that it shouldn't, if the API stream itself is not hardened, using some kind of crypto, you know, SSL, what have you, then maybe people attack it just plainly. But then once people do get authenticated access to it, a lot of the same early application pitfalls that people used to see. And I'm talking in the 90s, early 2000s, where it was very easy to escape, don't do using escape character attacks and things like that, where you can access all wrong parts of the system and things like that, we're seeing a lot of that happen again. And that's why I think people are for lack of a better word down on API's. But I have bad news for them. You know, they may not like it, but just as HTTP as a protocol, had, you know, earn its earn its way through the world and has been abused umpteen times, in passing history, API methodologies are going to be as well. So people need to kind of grow up adopt a modern API approach. In most of all, from a business perspective, they have to understand that users in the marketplace insist to have these API's. Because you can't have 50. browser tabs open. If you're all some type of if you're you know, you're doing software as a service, via some kind of platform, you can't have everybody logging into 30 platforms, it breaks the workflow. It's not, it doesn't create for like a continuous process work, you know, thought process as you're working through an incident, right? You didn't, if you have to keep switching windows, and, you know, undoubtedly, you'll have to use the restroom, you'll need to get something to drink, you know, the workday will end I mean, there's a bunch of scenarios, right, where you have to interrupt that workflow. And if you don't keep track of exactly what tab you're in, and things like that, it breaks. So the modern workforce, in particular, you know, security analysts,

cyber analysts, they prefer to use a front end tool that a single pane of glass, if you will, that can reach out to multiple datasets, and then bring that back, do a correlation and present to you what matters to them. And that's just reality. You know, I mean, whether people like it or not, who are out producing PAC software and delivering services via API, you're not going to be able to tell the market, how they must use your tool, it's just not going to work that way anymore. They already typically have their own method that they want to access data, it may be the platform that is authorized for use in their infrastructure. So maybe it's completely out of their hands. But almost certainly it is, if it's not mandated to them, it's the tool interface that they prefer to use, because they're most efficient. And well, again, you know, I'm not necessarily promoting any of these products, but for example, Maltego, I've used for, you know, 20 years because I prefer to use it. And it talks via API to any data source that I want to write a plug in for. Now, granted, I'm, you know, you know, hacker nerd person, so I can write these plugins, but you know, there are lots of tools out there in particular in the federal space, that are already existing, and these analysts in these types of locations are typically working through a pane of glass that they're accustomed to, and your data source if you're in the marketplace has to plug into that not the other way around. And that's just reality of of modern cybersecurity.



24:25

Yeah. Great, great take on API I'm sure there's a lot of truth in there. Let's stick with acronyms. Three letter acronym topic topic is real raccoons. Okay, as a podcast and Tom, you got a podcast and the podcast in DC called Feds at the edge. And everyone's talking about the edge and edge computing and, and COVID people are remotely coming in there at the edge. Now we have sensors on trains who have sensors on satellites, all kinds of edge. So this IoT does that stand for the Internet of threats are so what about IoT in your world? I mean, how is that wrecked your world?

24:58

So the internet of targets So, yeah, so you know, we're uniquely positioned. So we see, we see the internet as a service of IP addresses, right. And they are predictive, every IP address that has ever existed and will ever exist is already a known quantity. So in our case, we look at it from the outside in, we look at almost everything from the outside in, whereas an edge policy mechanism would look from the inside out, Inside Out has its advantages. In relation to granularity of events within your enterprise, obviously, that's important, Inside Out has its advantage in time, right? Because once you see it, it's typically Well, it's on your network. So we're talking millisecond responses to be able to do things. But it has its massive disadvantages, because what the attacker is doing other than talking to you, you don't know anything about. So our outside in approach allows us to look for IoT in the wild and look at who is probing them. What else there probing, you know, this type of context. So IoT to us, you know, was an expected outcome of making the IP addresses, we knew they would be used at some point. And we knew to be looking for them as they did. So when ipv4 Exhaustion came around, where the address space, you know, really started to get much smaller, you know, available ipv4 address spaces is like, Rock Bottom right now. And to us, though, that's a blessing, it gives us more known objects to potentially look at and see what they're doing. And understand, you know, what is the surface of the internet at any given time, now, ipv6, obviously, we've just started to scratch the surface of the you know, potential address space for it is absolutely, you know, galactic in size. So, you know, we try, we look at this space as well, but you know, it's a little trickier, you have to pay attention to, you know, what prefixes have been assigned, and try to, you know, focus your discovery on those assignments. But as far as ipv4, you know,

as ipv4 address space exhaustion happened, frankly, it made us, you know, kind of looking at the surface of the internet easier, because there weren't so many potholes of empty address space, that you have to, you know, skip over. So, but IoT is definitely the future. But I will tell you, if you put your devices on internet, make sure that you are in communication with your vendors, make sure that you are on every possible announcement was that they have, so that you can know, when there is an issue with those devices, I have to tell many people over and over again, that these devices typically are designed for a very specific use, and they do not have the update tempo of say your Apple laptop, which is designed for very general use in therefore they have to be much more rapid and ready with security patches. But IoT devices, statistically, and historically, are lagging way behind on that front. Because as kind of the trickle down effect happens, there is a very long development cycle, going into putting patches into the IoT wild because if these devices crater, if the patch causes problems with these devices, oftentimes lives are at risk, you know, so in particular around operating technology, so OT, but IoT stuff is just as critical. Like you said, Imagine, you know, if the trains controller systems were to fail, that could be, you know, terrible situation. So that patching process, that remediation process takes a very long time, relative to kind of, you know, general computing. So if you are responsible for IoT infrastructure, it's imperative that you take all of that very seriously. Because by the time you are notified that there's a problem with one of these, not counting, you know, special access announcements, because there are obviously critical infrastructure groups within the federal government where you can get that information in a skiff and start to get in front of that type of stuff. But generally speaking, in particular, in civilian government work, that's not the case and you're just a regular customer though your mission is maybe arguably more important than say, you know, a dentist's office or something which is seemingly arbitrary. You're not seen by the vendors as that much more important because the you know, there's only just so fast they can work. Because like I said, they have to do all this regression testing, they have to do all of this stuff. So the sooner you can find out in apply updates to Your IoT infrastructure, the better, because a lot of time has likely already passed. And unless you have a Wayback Machine, and you know can go with what's his name Sherman and Mr. Peabody, and go back in time, you're gonna be already behind the gun. So that's my advice for IoT. Hopefully not too scary.



30:23
Scary. We're gonna wrap it up here. Can you give us a quick little prediction here for the next few years in your business? I'm kind of a negative person, I think there's going to be an event and people are going to start scrambling. But I've seen a lot of things. So So where do you see your industry heading in the next four or five years?

30:40
Industry wise, I think from internal aspiration, there's going to be a huge application of AI. Looking to streamline what you could think of as problems too big for humans, typically. I mean, there's, you know, you have your Mega humans, who can you know, like your rain man's who can just see these things. But that doesn't scale. Right. So as far as general cybersecurity workforce goes, people will be looking to apply artificial intelligence to do like, you know, anomaly detection is correlation. You know, stuff like that, but you'll still need a human being to determine causation, I think that's going to never go away. So I see that as happening. I am also in the camp of you, I think that we are looking in a societal term, I have a bad feeling that we are rocketing towards some destination that no one has really thought about. We are digitizing absolutely everything I was in the

OPM leak, for example, in my OPM content dated back so far back that I had no, I had no recollection of even seeing a computer when I was in the Marine Corps at the time. So somebody had gone and taken analog paperwork and digitized it at some point, and then it was breached, and accessed, you know, by people outside. So this is the kind of push for digitization. I understand the ideas behind digitalization. But what I don't get the feel is is that anybody has really, really contemplated, you know, what are the bad outcomes, right. And I'm not even necessarily talking about adversaries, a coronal mass ejection could easily, you know, one, one sunburst could easily cause massively disrupted situations. And when you couple that with a massive reliance on technology, that I would argue the majority society has no idea how it works. In fact, if you go to ask them for things that they use every day, like email, if you say, How does email work? They'll use words like click and open and stuff like that in send, but you'll never hear them mention SMTP you'll never hear them mention IP, you don't I mean, never. But yeah, those are the actual aspects of it. And there's a whole galaxy of detail inside SMTP. So but yet everybody's super reliant on these things. If you look at an automobile, you could go ask people, How does an automobile work, and there's people who could at least point to the motor and say, These are the motors, these are the tires, this is the exhaust, I mean, they have some understanding of this thing that they rely on, right. But when it comes to digital, electronic aspects of it, I don't think that we're prepared for them being gone from our life suddenly. And I don't think that we understand them well enough to actually be able to measure that risk to our life into our society. And I'm with you, I have a feeling, whether it be some type of cyber attack, which there's high, I would say there's a high chance of are higher than higher than average, I would say, given all of the political tensions that are afoot in the world, or just plain technological failure. I could see that happening sometime in the future. But luckily, the good news is, is you know, there's plenty of folks who do understand these things and are working on it, that we don't scale as effectively as we could. And that's why hopefully, folks will reach out to us and see how we can help get them in the fight to understanding what adversaries are doing to them and their network.



34:11

That sounds like a true marine determine the fight. Oh, rock. That's right. Yeah. Well, we're running out of time here. Unfortunately, even you have been listening to the federal tech podcast with John Gilroy. thankthank my guest David manyI, Chief Information Officer Chief Evangelist and team curry Fellow at Tim Curry. Thanks, David. Thanks, John.