FEDERAL TECH PODCAST

Ep. 18 Splunk's SURge: How To Get Immense Value From a Small Team

SUMMARY KEYWORDS
ransomware, splunk, security, problem, people, data, trust, agencies, podcast, incident, surge, network, research, team, defense, phrase, asset inventory, federal, books, big

00:04
Welcome to the federal tech podcast where industry leaders share insights on innovation, with a focus on reducing cost and improving security for federal technology. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcast.

00:28
Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Our guest today is Mick baccio, global security strategist at Splunk. Surge. Nick, how are you?

00:39
I'm well, thank you, John. Thanks for having me. How are you this morning? Good,

00:42
good, good. Well, word Splunk. I think most of my listeners know about Splunk. I mean, have been around for since 2007 or something. And I think, you know, when they think about Splunk, they think about you know, understanding data, okay. And when I introduced you people heard Splunk surge is a different company. I mean, so Splunk, sir, so, so tell us about this word surge and you and what this all means for our listeners? Sure,

01:05
well, surge is a research group inside of Splunk that was officially stood up, I guess, in October of last year was announced at comp, but we've kind of been working behind the scenes, since if you want to pick an incident, I think SolarWinds was what started it for us. A group was inside Splunk you know, surge, the distinguished strategist, Ryan, Kosovar he, you know, lords over the team. And the idea of Splunk, you know, strictly a kind of a network defense, you know, Blue Team, just to help the security part of using Splunk. That was the research group, the initial idea behind it was, hey, how can we kind of help all these blue teams out there, these network defense types, and that's my wheelhouse. So I've been a Splunk user for a super long time ever since back at the CDC was my introduction to Splunk. So I always viewed Splunk, as a security company, I didn't know the other uses for Splunk outside of security. When I finally you know, ended my federal career

had a chance to join Splunk when I learned Oh, it's it's just all you know, how to how to manage your data. That's what Splunk does, you know, whether it's IT ops, whether it's availability, whether it's, you know, the million different things, my aperture was just security. And having that background and network defense. Ryan had the idea of, hey, look, let's let's, you know, the the mantra with blue collar for the blue team is just kind of putting that work in solving all the problems responding to incidents, and how Splunk can do that, how us as a research team can do that. And so ever since solar winds, you know, some of the bigger incidents, whether it's Casaya, whether it's clinical pipeline, we've managed to pretty quickly published out whether it's a blog, whether it's guidance about how you can use Splunk, to kind of aid in that response effort, that network defense effort, I think the biggest kudos that can give that the team was the log for J incident from our log for show, just the, the holiday kind of ruined for everyone. We got wind of that incident. And we had a blog out and I think we published, it may have been a day earlier. Some guidance for for all the network defense teams out there a day earlier than Sisa published their notification, which was fantastic. And it just gives speaks to the effort and just the work that team has put in to kind of get, you know, Blue Team work out there kind of help network defense teams across the enterprise respond to incidents. And that's kind of what the one of the core tenants are. Another one is, we said research group, right? Surge is a research group, as Shannon Davis put out a fantastic white paper on ransomware encryption speeds. Basically saying, hey, look, here is 100 different ransomware binaries, we're gonna let them go and see which one works faster. Like if you had a quadrant of performance for ransomware binaries, this is what you would find out. And we had seen it before, right? It was a ransomware affiliate that was advertising, hey, use us because we're the fastest. And it was weird to advertise that right? It was the same thing you would see from any vendor, and our software is the best. And we didn't believe it, right? We're like, Oh, that's weird. So like I said, Shannon sent the research out, we found out when you get hit by ransomware, you've got anywhere from four minutes to four hours. That's it. And you know, part of that problem in your response becomes, you're not going to stop or it's very hard to stop ransomware once that binary is launched, but that binary is the last stage in your ransomware attack. So all of the other things that you can kind of do to change that response strategy to, you know, stop ransomware before it happens and what's left Boom, I guess is the phrase we use a lot, which I hate, but it's pretty, pretty descriptive. Once that ransomware binary launches, there's not much you can do before that there are steps you can take to detect ransomware once you've been targeted, and you know, that's kind of what we wanted to get out there, hey, ransomware, here's how fast it is. But here are some steps you can take to kind of change your strategy. So that's the, you know, one of the other things, we're really proud of it search. So it's really just a lot of network defense, you know, Blue team efforts to kind of help Splunk users Splunk customers, get ahead of problems out there and control or not control, I guess, use that data, they already have to solve security problems.

05:44

Now, if you're listening to this, and you want to get more information, Splunk search strg EEG or the website, they have form, you can sign up for newsletters, and this this is free. This is not give me some money. And I'll pick my brain for a few hours or something. Now, this is all free stuff. And I mean, I think the first white paper you came out with years ago, was detecting supply chain attacks. I mean, very practical down to earth things that, you know, here the tools. And and so what kind of expertise Does your company have? Well, 92 of the top 100 companies use Splunk. I mean, and when you see that's like your I don't know why you guard at a turnpike or something, you see something can you see enough cars come through? You kind of make some

you know, observations about stuff, you know, and I think that's, I think that's a strength of search is that it is a widely available information from people who've been in the trenches. And and I didn't even mention your background. I mean, Mike's got 20 years experience, military background, many agencies, executive officers, the president, he's got all kinds of experiences. So if he's sitting at that toll booth seen some guy he's gonna have some strange and he's gonna tell you about it. And so that's I think it's it's interesting response that the company Splunk has had no spunk could easily have put that pine paywall brought the MEK I think it's really been part of the community, isn't it? I think

07:01
it totally is. When you look at any kind of response efforts or security efforts, if we just did our research, and the Honestly, my background being what it is I kind of focused on nation state, you know, so nation state X is hacking nation state why? And if there's a specific, you know, malware binary that maybe only affects six people in the world, that's super interesting to me. But again, that doesn't help a lot of people. So I think we'll be focused on are in addition to those type of incidents, just the general things, how can we help the security community as a whole, you know, when you look at the search team, I guess, to a dozen people now, and obviously, that wouldn't scale? You know, we couldn't talk to everyone one on one. So things like the blogs, the white papers, the videos that we do, we kind of make all that free, because it's just helping folks and raising that security bar overall. That's kind of the goal. While we're all here, isn't it? Yeah, but but

08:02
they also have a separate research team, don't they? I mean, spawn cutter research team, and then you guys are they combined?

08:07
So the threat research team, Jose, the gang there, they are fantastic. When you talk about building detections, when you talk about things like attack range, that is the in the weeds research team. So we're kind of taking, I guess, a knot in the weeds approach kind of a step back, and making it more consumable, kind of more widely available information. When we work pretty much hand in hand with the threat research team, they are kind of our technical lifting when it comes to detections, because the work they're able to do. It's a fantastic team who, who, you know, we wouldn't be where we are without the threat research team,

08:48
but specifically from my audience, the federal IT professionals and their partners, trusted partners, given your experience at the different levels you've been at, and you know, what's your background? I mean, how many people on the LinkedIn profile have sons Alaris on there?

09:03
Yeah, well, I'm a bit of

09:05

sounds like, you're pretty much down to the the bits and bytes. And then you know, the CPUs. So I mean, then when someone like you says, Well, this is a threat, this is really should consider and here's your options, people aren't just gonna walk away and go away. You know, it's, you know, so that's a, I think it's a fantastic service you're offering. And in the federal government, there's trending phrases, as you know, and because I'm an old radio, I can see the phrase of pace. And so zero trust architecture is eta, that's the phrase that pays and so mandate every 32 seconds, I've got to say, zero trust or we're not getting any credibility. So we got

09:42
to pay royalties when you say zero trust.

09:46
And so we have this big mandate executive officer present. This is a big dogs that coming down on you muster August 2020, or else we're going to come and get a baseball bat and come get you and then we have the agency saying, Well, you know, I want to deployed for zero trust. But I think I think one of the problems I have is, was, who do you trust? I mean, how and how do you know? And I mean, so this is a, this is maybe an area that certain surge, or maybe sponsors can help. Just going through that this eat a healthy diet. Well, what does that mean? So go to zero trust in two years? Well, you're not helping me. And so where does zero trust fit in this discussion?

10:21
I view zero distrust, I guess, as the updated version, you know, the esoteric defense in depth, right? If you go back that dinosaur discussion where, you know, layered defense defense in depth, it's purely just do I trust, you can read the NIST, I think it's 801 19. For the zero trust architecture, the model, it's more of suggestions and a mindset and specific guidance. And I think that's part of the problem, but also part of the solution, zero trust as a whole, you look at things, you know, multifactor, authentication, asset inventory, you know, network segmentation, you know, those are kind of just the things you would do holistically in a defense in depth architecture. It's a heavy lift for a lot of agencies. And I think that is a huge problem. And because there are specifics on it, I think that's where some folks might get tripped up. Like, I can't say, Hey, if you want zero trust, do XYZ, because I think it's more of a mindset, and how you build out your network and how you how you how you look at security, but you know, at its core, multi factor authentication, asset inventory, and patching and ID, that's kind of when you look at any internet controls. That's number one and two, right? I think CIS is asset ID and inventory, which is honestly, I think it's the Holy Grail of any any network,

11:45
I guess that's where smoke would fit in. If we started looking at logging and numerous log standards, we're looking at transparency and seeing what's on the network, looking about, you know, getting a reliable asset inventory. I mean, I can go to my garage and get an asset inventory, but not the GSA. Who knows, I mean, and also, I think, from the federal perspective, 135 agencies, you may some have, some agencies are pretty high, and the maturity level on this, and some that are kind of low, maybe the federal government needs to put together a zero trust architecture surge, where they share their information among the agency. So maybe you can get an AmEx,

12:27
you know, and I think, in my experience in the government, that's always been a problem is that the the credo is, you know, kind of blanket statement, it's a, it applies to all agencies every level, but the budgeting and the resources that some agencies have compared to others makes those mandates just nigh impossible to accomplish. And that's, you know, that's, I think that's a problem. That's where problems come in, or that's where, you know, kind of cutting corners comes in. But I think, you know, the breakfasts are out there, I think it's a really good model to move to, when you look at other governors, you know, he was m 2131, a lot of the passive DNS work that's coming out, it's the right move. And that's why we're kind of fortunate, lucky at surge, because we're just going to put out what we think height and think you can accomplish that, right, here's how I would use Splunk to model parts of my zero trust architecture, here's how I would use Splunk in a passive DNS solution. And there's parts of that out there. But I think it's a rough road for a lot of federal agencies, being able to comply with those executive orders with a zero trust mandate with you know, a lot of the modernization you've seen come out,

13:39
one thing is obviously subscribe to surge newsletter, at least they'll get regular updates of, hey, this would happen to this organization. And this is how they handled it and, and talk about, I mean, I've read the study of the hospital in the state of Washington that was hit by ransomware. And they very detailed study of the timeline is almost like a history major. Okay, there's, there's a timeline to this. The other thing, I never thought of coming up and coming to the White Paper, okay, well, take a look at this timeline between 20 different types of ransomware. It's, it puts, I think you're in a position to put these concepts in more analytical level, maybe more, I don't know what it's called advanced level

14:15
100% trying to do is a quantitative research, right, and we were a strategic research team. So with that ransomware research, we're not saying, hey, and this is how your security program should be. It's just hey, when ransomware it hits when you have a ransomware infection on your network, and I think there was a paper recently that gave it around five days from the initial, say a phishing email five days later is when that ransomware binary is going to launch and there you know, then it's really, really bad day for everyone. But in that five day dwell time, here's what you can do. What we try to do with the white paper, the ransomware white paper is just kind of echo trying to stop ransomware after the binary and launches is pretty futile focus on the strategy detection before it. And here are some tips along the way

15:09
earlier in our interview, use the phrase that I think it's a security as a data problem. And, okay, your data problem. Back in the days of Sun Solaris, you had 20 megabyte hard drives or whatever you had, I mean, small monitor is small. But now, I read a statistics this morning about IoT devices. Apparently, there's 7 billion people in the world, and I don't know 12 billion endpoints and rapidly increasing. And so, back 20 years ago, when Mac was trying to figure out Solaris, he has a couple of hard drives to worry about. And that was hard enough, but I can't even count the hard drives are the amount of endpoints come into hard drive. And so what's

15:49
the I think there was a phrase by Bruce Schneier years ago, it was data is the exhaust of the information age. And I think that's beautiful. But also, yeah, that's a problem. We like you mentioned IoT, a human. And then with that comes a whole new data set to monitor. And we still have the problem is with with PII, pH, I, with corporate data with intellectual property, we just security data, and we're growing more and more that the world is becoming interconnected. And you mentioned around 7 billion people, not everyone's got a phone, right. But there are folks that have multiple devices. And each device begets more data begets more data, and kind of finding a way to manage that, and corral that and push that around. At its core, that's what we do at Splunk is kind of help you move around whatever data you need, whatever data you're collecting, and from my aperture of just being a security person, it's all of that log data, whether it's DNS logs, email, logs, event logs, you know, all of those different things that helped me kind of paint a picture, you mentioned that very specific timeline to paint a picture of an incident that happened. And that's what you can do with data. Before COVID.

17:05
I would be untrained and go to events, I'd meet gummies all the time and sit down next to him and say, we're thinking spunk, oh, yeah, they analyze machine data, okay. description of it. But what you folks doing a surge is, is you're putting in work boots and showing people exactly what it means. And I think this increase in amount of sensor data coming in. I mean, it's getting to the point where I don't mean it's these to say about garden hose fire hose. I think it's a tsunami, it's way beyond this water comparison. So artificial intelligence must play a role today in analyzing machine data with spunk, I mean, how can it not?

17:37
Oh, 100%, it becomes the amount of data that we're parsing as an entity, as an agency as a business of any size, it's exponential, it's too much for one person is too much for a team of people. And with that, you're relying on the tools that you purchased. Now, those tools have to be trained at AI, you know, when you talk about interoperable interoperability, or explainability. It's a whole other discussion about you know how that AI is to and how machine learning is used. But that is something with the amount of data that we're seeing every day, you have no choice but to rely on that tooling, to kind of augment your process does not replace things, but augment them and kind of free up resources to focus on other problems, you know, because you're just kind of raising the bar.

18:28
Okay, we're coming to the end of the interview, you had other problems. And let's talk about other problems in the future here. Before we began this interview, I mentioned a Gartner study that came out and it talked about talent shortage, and they say, well, it's gonna be a lot of ransomware. But the real problem is gonna be a talent shortage. So So do you agree with that? And how can spunk maybe automation was fun can help make existing technical professionals more flexible, more adaptable, more power? What they call a force multiplier, what do you think about the sound shortage and spunk in the future?

19:03

So two parts, the talent shortage,

19:06

I believe, 100%, there is a talent shortage. And I think the way to one of the primary ways to go about solving that talent shortage is to look outside the background that we normally do, and we're hiring people in security. Some of the best people I have met in the security field and not start off in security. It's just something they fell into when they love or you think are hired because of that curiosity. So I think the talent shortage is, is there. But I think there is a very big pool of people that we can choose from and look at that. Maybe we didn't initially consider and started doing that. On the other end of that, what's going to happen? I ransomware. You know, you can't have a podcast without talking about ransomware and I don't think that's going to be a very, very big problem, I think It's going to get worse from a ransomware perspective where it's not just ransomware, it becomes not ransomware as a service, but start thinking in the terms of cybercrime as a service where I'm not hiring this affiliate, just to perform a ransomware activity, I'm hiring them for any number of offensive, you know, toolings that they can, it's in their portfolio. Sites. Ransomware is a business it that's bigger than ransomware. And I think those steps, those basic things that going back to zero trust, you know, Id or assets multifactor, network segmentation, no, what you can do and what you can do when you start talking about automation, you're not automating people out of jobs, you're just automating simple, repetitive tasks, and you're freeing up resources to focus on other problems. And it all comes back to data, you know, whatever data you generate, know, how you're managing it, and where it's going. Know how that packetized traffic moves to a network. And what happens then, and I think starting in, you know, just that that culture of security is the big thing. Every day, we're going to have security problems, and that's not going to change, but how are we respond to them, and how we're making the overall security community better. I think that's just the way to go. And hopefully, it served, were able to do that and keep doing that.

21:18

I'm in the classroom a lot. And my students always want to know what podcasts you listen to and what books you read. What books should I read and, and so I just wanted to end this with tapping your brain here. There's podcasts called darknet diaries on if you listen, only security podcasts, listen to the thinker with wild for our listeners, then ask you the book question next.

21:36

I am a big fan. I give a shout out to beers with Talos

21:41

super awesome crew over there. And obviously your gang over to cyber wire. And Johnson's podcast was fantastic. Plugging ours here served we do coffee talk every other week. And that's always a good time. But yeah, a lot of there's a lot of good security podcasts out there. But I think I do listen to beers with Talos and listen to afternoon tea with and a lot. So those do I'd recommend anyone out there.

22:09

Books just outdated. I mean, the authors I speak to they make more money from the audio books and the physical piece of paper books. So I'm a big book believer. So any books worth even considering or or is that just too too slow?

22:22
I got two books.

22:26
One, her name is Laura Lippman, a collection of short stories called both Baltimore noir kickbacks. Fantastic. Really good. And then Neuromancer by William Gibson. Read that that's fine. And that's the book that made me want to go do to cybers. So that was it. Yeah, so those two

22:50
that's pretty good. Pretty nice. Well, really appreciate your time today. I think it's given our audience a better perspective about Splunk. And, and the information I mean, some like the dream team got together and sharing information for our federal audience thinks a great idea. You've been listening to federal tech podcast with John Gilroy. I'd like to thank my guest, Nick baccio, global security strategist at Splunk search.

23:11
Thanks for having me on.

23:12
And thanks for listening, everyone.

23:15
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 podcast.