IT Matters Podcast - S1 EP 23

Mon, Mar 04, 2024 10:32AM 29:57

SUMMARY KEYWORDS

canary, mdr, red, threat, cybersecurity, edr, detection, people, customer, organizations, focused, alerts, managed, brennan, cloud, security, response, identifying, respond, confirming

SPEAKERS

Narrator, Brennan Manion, Keith Hawkey

N **Narrator** 00:07

Welcome to the IT Matters Podcast where we explore why IT matters and matters pertaining to IT.

K **Keith Hawkey** 00:16

Brennan Manion, welcome to the IT Matters podcast. How you doing my friend?

B **Brennan Manion** 00:20

Thanks, Keith. Great to be here, really appreciate you having me on. I've listened to some of the podcasts and it's great to actually be here as a guest. So thank you for having me.

K **Keith Hawkey** 00:28

Yeah. My pleasure. Really excited about the conversation we had today. First of all, for those of you that don't know, Brennan is a new father. So tell us, tell us about the dad life with young young Finnegan.

B **Brennan Manion** 00:44

Dad life is great, it really is a blessing. It's pretty wild, just to just see the miracle of life come together. And I know there's a lot of books on being a parent, but I don't know if there's like any set manuscript or process you can just follow 100%. But I do believe that God just puts these powers inside you that when you kind of hold the baby and you see it, you just kind of know in your heart what to do. And it's been really great. The legend is true, you do get a lot less sleep

when you do have a baby. So that's happening, but you know, thankfully, I've got a great wife that you know, keeps me in check there and helps out with that. And it's super fun and thanks for asking. We're really enjoying it.

K Keith Hawkey 01:30

Yeah well. Glad to see another Manion in the world. We need more of you. Look, quick intro. Brennan is an account executive at Red Canary. They are a managed detection response organization. And today we thought about focusing on what what is MDR? Red Canary? How did you get into the industry? Brennan? We're coming up at the end of 2023. We'd love to talk about where do you think the market is going next year? What are some of the trends that you see happening as of late? Brennan, tell us tell us about how how'd you get into cybersecurity and how did you end up at Red Canary?

B Brennan Manion 02:20

Thanks, lots of great stuff to talk about there. So for me, you know I first, I'm from Charlotte, North Carolina. So for those that are familiar with Charlotte are gonna know what I'm talking about, for those that aren't it is a banking capital. It is big time. If you go to the local YMCA or at church or just you go to a restaurant, there's a good chance that somebody next to you works at one of the big banks. And when I was trying to figure out what I wanted to do 15 years ago, when I graduated college, I went ahead and talked to a bunch of people. And I quickly realized I did not want to be a banker after going to some of the trading floors. I just love interacting with people. I cut my teeth with my first sales job. I was the rich, the rich guys trash man. I sold a computer recycling service. And it was pretty cool. I called on hospitals, universities, I actually called on the big banks, all different types of organizations. And it was a really great way for me to learn and begin my craft and in sales and really start to fall in love with that. I then started to realize that I wanted to move and elevate my game up. I wanted to focus on something IT director or that C level executive is interested in, not necessarily the garbage they're trying to get out of their facilities. So I actually went to this conference called Varrow Madness. There was another reseller back in the day that had the same colors as Opkalla and a lot of people loved them just like they love Opkalla today, but the company was called Varrow. And I was there thinking I was going to get a job at Cisco or EMC or any of the companies there, Palo Alto started to become big at that timeframe and I actually fell in love with the reseller community of Varrow and just listening to the CEO give a presentation. I got connected with the VP of sales and he connected me with another and I actually found a home in Varrow and ended up working there for about four years. Along that journey of selling data storage, connecting to the internet, networking, security, I just really was passionate about, hey, there are people out there hacking organizations, stealing credentials, creating ransomware like, that's exciting. It's the modern Wild Wild West in my opinion. And it just got me fired up so I kind of attached my cart to those horses, focused on cybersecurity. I found a lot of enjoyment in that. And being from Charlotte and growing up here is an amazing city that has grown and it's so beautiful, but I didn't really know anything aside from Charlotte, so I actually decided to go double down, bet on my career a little bit. And I decided to go find myself at no other place than Bay Area, California. I ended up moving to San Francisco, San Jose in the peninsula in Palo Alto. And I actually worked for a cybersecurity company there by the name of CrowdStrike. And felt really fortunate I got there in early time, right before they had really started to launch. I actually worked at CrowdStrike, when it was challenging to sell CrowdStrike. It had not totally hit that

wave where most companies are now utilizing them in some fashion. And it was pretty cool, a great, smaller company at that time, the one right behind me, Red Canary, got connected with me, and we knew about them, we had a nice partnership. And they asked me if I would wanna be the enterprise account executive for the Bay Area and that just sounded so exciting to me. And I decided to go forward with Red Canary and I've been here for over five years, and they've been a great company to work with. And I've made my way back to Charlotte. And I've seen so much change happen in the security community. And I've watched our company grow and change to that. And ultimately, it's really nice, we're really focused on being a security ally, and empowering others and really do our best to keep companies out of the news headlines. That's the number one goal at Red Canary is to avoid a data breach or compromise and give the confidence that they're going to be protected. I know that was kind of long, but that's how I got my start in IT to where I'm at today and just really finding enjoyment in cybersecurity,

K Keith Hawkey 06:38

Well, it's you've landed at a good place, and getting the, having the background CrowdStrike, I'm sure helped along that path as well. CrowdStrike has become a you know, one of the leaders in the endpoint detection response marketplace, and they've grown since then, as well and expanded capacity. So Red Canary, Red Canary serves a very important role in the cybersecurity threat landscape within the Managed Detection Response area. So when you think of MDR, Managed Detection Response, what is MDR? What if you have an IT leader that is looking for, they don't have the internal resources to have 24/7 eyes on glass, in that they're watching the screens that are doing the threat hunting, and they're thinking about outsourcing that task and they you know, they know they need MDR. What is MDR? Who should be, what should they ask providers to validate they're doing a proper job of this?

B Brennan Manion 07:49

That's a great question. So that's so funny, too, because MDR means so many things to so many people, it really does. It easily can be defined different ways. And funny enough about Red Canary is when we first started, it was just called Red Canary, like MDR wasn't really the definition at the time. We weren't sure exactly where to put us into the box of what category we're in. You know, from a security leadership and security practitioner looking to really level up their security and harden their posture. You know, when you're looking at an MDR provider. Yeah, you want 24 by seven eyes on glass. If you're, if you're most of the ones in America, you're gonna want your SOCs to be USA based, you want to have USA support. Those are all kind of generic standard things that you should be getting from an MDR. If those aren't part of the equation, then I don't really think that even fits into the MDR category to begin with. But what really stands out to, at least in my lens and how I'm viewing it, you know, MDR should be somebody who's looking through, they're doing the threat hunting, they're confirming the threat, and then delivering that confirmed threat to the end user. And what's what's wild about that Keith, is there an MDR is managed detection response. When you're bringing a threat to somebody and confirming it, that's just MD, that's managed detection. If you're ever going to add an R, you have to have a response component to it. So what that means to me is, hey, you're either able to stop that threat in its tracks, you're able to remote in, you can share screen, you can get online, the R should be the level of response and detail that customers should be looking for. What can my MDR provider do once a threat is identified? How can they help me respond to it? Because it's quite interesting, Keith, you see this every day talking to

different organizations. They might have some really smart people on staff, probably at the same level that Red Canary does for some of their incident response. But as you see, they only have maybe one or two like cyber, I like to call them cyber ninjas. They're just going to be scary good at their craft. But then there's other people that have really focused on networking and storage, and they're kind of moving over to cybersecurity. And you gotta find a way to empower those people to be successful at it. And at Red Canary, this is something that we do every day, we are professionals at identifying threats and responding to them. So when we're partnering with someone and we're defining MDR, it's a partnership where we're working with you and your team to make sure that, hey, we did pick up a threat in your environment, we've confirmed it's legitimate, it's time to respond to it. And we want to work with a team to respond to it however they best see fit. And it's really important that we do it quite quickly because speed does matter in the security industry. So for me, managed detection responses, it's somebody who's identifying the threat, confirming, confirming that, and then helping the customer respond to it, however, that customer sees the best fit.

K Keith Hawkey 10:55

Yeah, and, you know, like, like you said, I think for a long time, many IT departments have dealt with having to, they're focusing on detection, and they're getting fatigue on the number of alerts, and they don't know how to remediate. And it's, they don't have, you know, the cost of the cybersecurity specialists, depending on how tenured they are, skyrocketed during COVID and are still very, very, very high. And for most organizations, they don't have dozens of IT people, they don't have the spend to invest in that resource and much less invest in a SOC that's going to be 24 hours. So they invested in tools that give them telemetry and it's it's a full time job to have the know how, of how to respond. And I'm sure you've you've walked into situations where there's SOCs that are embedded within an organization. And they're saying that, you know, we maybe we have reduced alerts, but we still don't seem like we have a partner beside us that's going to help us respond to the threats and even remediate on our behalf and in some circumstances. So yeah, I think that the response part of MDR is, is probably the the biggest differentiator among the providers in the marketplace. What is so you know, in terms of Red Canary, where did where did Red Canary begin? What is the origin? What is the company focused on now? I guess what, how does Red Canary standout in the MDR marketplace? How's it different?

B Brennan Manion 12:45

Yes, so Keith, the reason that Red Canary was created is ultimately we just saw a problem in the marketplace. And the problem was, teams are getting alerted with so many different security alerts from all the great tools that they utilize in their environment, from firewall to NGV, EDR, to identity, you name it, right? All these tools are generating alerts, Red Canary's whole goal and mission was, hey, let us collect in that data, let us help identify the threat really, actually be very strong and confirming what's a threat and having a high accuracy percentage, and then helping that customer respond to it. That's the main goal and focus that we have and there was a problem that we saw in the market, basically.

K Keith Hawkey 13:27

Yeah. And then and that definitely means a lot. Is there are there particular, where's Red

Canary going right now? What what's what's the frontier look like? What what is r&d look like in terms of the, you know, robustness of the service, and the next year, where are y'all set as far as developing the industry.

B Brennan Manion 13:54

So you know, Red Canary's cloud first, and we're a cloud native solution, we can support on premise technologies, but we're ultimately betting on the cloud, we're seeing more and more users starting to deploy into the cloud right now. And we're definitely wanting to be the leader of managed detection response on cloud use cases, anybody who's using containers, Kubernetes, any of the major public clouds that you all are familiar with and positioning. Red Canary wants to be on the leading cutting edge and identifying threats and responding to them. You're pairing that, we feel like we've really created a nice workflow when we identify a threat, and confirming that it is indeed legitimate and then helping the end user respond to it. The next iteration and phase of Red Canary is is adding additional integrations, right? There's been some new technologies that have hit the world, really, and hit the world by storm. And we want to get those integrations involved with Red Canary. So that's something we support many of the major ones that most organizations organizations use, but at the newer ones that are really starting to stick and people are finding value in them, we want to have eyes on that when we've collected that data feed, we want to provide value and context there. Those are the main pieces. And ultimately, what we're going to keep asking and leading into our customers a big core value, the number one core value at Red Canary is we do what's right for the customer. So the way that we do that is by listening in, understanding the challenges that they're facing in their security operations, and our goals to really meet that and let them know and really deliver the confidence that we're handling those threats and keeping the environment safe and secure.

K Keith Hawkey 15:40

And speaking of confidence, I think that Red Canary at this point has a pretty good track record in terms of you know, false positives, particularly, I said, what is the data on that? I know that I've got some numbers in my head but, I know I'll get it wrong, that that certain percentage.

B Brennan Manion 16:01

We have a 99% plus thread accuracy rate. So many people on your, in your target audience of listeners are probably going to say that's a bunch of BS, it's actually very true. So we just did just shy of 34,000 confirmed threats across around 1000 customers this past year. And 286 of those threats were false positives. So if you look at that, we're doing about one false positive per 125 true detections right now, which is putting us at a 99% plus, it's like 99.2 dot dot dot is what our accuracy rate is, and the way we do that Keith is our software and our human element. So as data comes into red Canary, it immediately goes into the detection engine. And that detection engine is super sophisticated. But its real principles are quite basic. It's looking for new behavior, bad behavior, suspicious behavior, any one of those three things you can be rest assured, it's going to be reviewed, not by one, but two tier two and above SOC analysts to confirm, hey, do we have a threat on our hands or is this a false positive because there's really nothing worse. Well, there is. The worst thing you could have is you could have a threat get past by you, and you have a compromise. The second worst thing is having a vendor that

you're paying good money to that's helping you respond to threats and confirm them, ship you a bunch of fake alerts. You don't want to have that. And that's something that we're really good at sussing out and giving a confirmed threat to an end user. So when that does happen for our customer base, our customers are very interested to know, hey, Red Canary has got a real threat on our hands.

K Keith Hawkey 17:38

Yeah, that can save an IT or cybersecurity team immense time for sure. Another another question that I get from a lot of IT leaders is they have a solution that, they have an EDR solution and endpoint detection response. And then but they have providers to come in and they'll do managed EDR and then they'll call it MDR. And then there's XDR that's a lot of Rs in this world. So what are what are the differences between EDR MDR and XDR? How do we categorize these buzz words?

B Brennan Manion 18:19

Well, when Red Canary was first born, we just did managed EDR. And it goes back to what I've been kind of harping on the whole call, it's we listened to the customer and that's helped us evolve to be where we're at today and Red Canary's absolutely a managed detection response or a managed XDR however you want to spin it. I like to think of XDR as the great term next gen that we all saw about three years ago in the IT space. It's another way just if you park cloud in front of it, it's gonna gather more of a target audience. It's kind of one of those buzzwords, you know, EDR endpoint detection and response MDR managed detection response, XDR extended detection and response. The way we look at XDR is, you've got all the different tools in your stack, from your networking, to your identity, to your cloud, your SAS, your apps, any of the great tools you've got that you've invested in your security strategy, those are falling in the category of XDR. What Red Canary wants to do and does do is we're ingesting the XDR data so all the different tool sets coming into us we're helping manage and help solve that problem for them. That's how we're addressing it and that's kind of how the market has to find all those different acronyms that we've got.

K Keith Hawkey 19:34

Does Red Canary provide any of the endpoint protection technology today? Or do you guys

B Brennan Manion 19:42

Yeah so, we're big believers that if you're going to create something and do it really great, let's not go ahead and recreate one that somebody's already done really, really well. So for us, we're partnered with the best of breed providers when it comes to networking, email security, endpoint security, you name it, right? You know, Red Canary's proprietary data is our managed detection response. We did create our own Linux EDR, we felt like there was an opening in the market there so we did create our own Linux technology there. So we did create that ourselves. But primarily, we're interested in in utilizing the great tools that companies have already invested in. It doesn't really make a whole lot of sense for us to try and go compete with the

great, great endpoint and networking and email companies that have already been proven and tested and validated. Our goal is to help customers manage them and operate them at the best performance level possible.

K Keith Hawkey 20:45

So Red Canary, your your value add or one of the main ones is that regardless of the investments an our organization has made, Red Canary can come in over the top and add increased value to the initial into those investments. You don't have to there's very little change that they have to make in their environment to have Red Canary perform the SOC services and the MDR.

B Brennan Manion 21:16

That's exactly right. So you know, when I look at the customer profiles, Red Canary, you know, people are really partnering with us because they're they're either, the number one reason that they partner with us is they want to do everything they can in their power to avoid ending up in the press, in the press release, or the news with anything of a negative connotation behind it. They want to really focus on keeping the brand in the best highlighted version possible. And Red Canary is good at identifying what's a real threat and empowering their team to respond to it really quickly. Many of the customers when we're talking to them, and they have not yet partnered with us, a top pain point they have is hey, I have bought best of breed technology, I have that in place. I do have people on my staff. But the problem is, I'm still challenged with trying to manage that and go through all of the alerts and do that effectively. Also, I'm taxing my team, we're running 24 by seven, there's people that are challenged with some of the on call support you've got to do or the eyes on glass we're having to do on holidays and weekends. When people are partnering with Red Canary, our customers are able to close their laptops and walk away without that anxiety in the back of their mind of, hey, my laptop's closed, I'm out doing Christmas shopping right now, I really hope something bad doesn't happen to my environment when I'm not in front of my machine. That's exactly what Red Canary is solving. They're empowering their customer. You know, a lot of people like to say, hey, come by MDR and we'll release all this time so you can go focus on the things you got to do. That seems like some fluffy BS, in my opinion. What Red Canary is really doing my man is we're giving the customer confidence. Because there's a lot of alerts coming in. I'll never forget, I met a guy at a large bank back in the day and I was talking to him. He was a friend of a friend and he worked on a SOC it just happened to be that we were at the same party together. And I said, Wow, you're in the security operation center. No kidding. Tell me about your job. He goes oh well I'm going through these alerts. I manage them, I'm going through a sim, I've got networking endpoint. He's like, Are you tracking what I'm talking about? I'm like, Yes, I do. I know exactly what you're talking about. And I was like, I've got one question for you, my man. Are you able to go through all the alerts in your environment? And his response is, he started laughing and he goes Not a chance. And that let me know that a large organization like him that has a lot of funding to be really successful in their security practice let me know that Red Canary is solving a real problem out there that many companies are facing every day.

K Keith Hawkey 23:50

Yeah, no yeah, you're right I hear it all the time. Mostly the most of the IT departments today

are running very lean, they're in the weeds, they don't have time to work on strategy, they are looking to bring in services that can supplement their team not replace them so that they can take a vacation every once in a while. That should be you should be Red Canary's tagline.

B Brennan Manion 24:16

I love it. That's a great tagline.

K Keith Hawkey 24:19

That someone someone's watching watching the ship. Where do you see where do you see the market going in 2024? Generative AI is is on everyone's tongue today. Is Red Canary leveraging I'm sure, I know the threat actors are leveraging generative AI, particularly to impersonate key individuals that organizations. I've heard of phone calls being, you know being replicated. Certainly we see it in email, certainly we see it in you know other more human oriented reaches. Large language models, generative AI. What do you see, what's Red Canary doing to implement that or fight against that?

B Brennan Manion 25:10

Yep, so we use AI at Red Canary in helping us identify and build off detections, to honestly operate faster and be ahead of the attackers. And of course, we're crowdsourcing our data so when we do see detection on one, we're populating that for that detection to be identified across all. For us, you know, I'm going to kind of hop back into what I said on the cloud, we're really focused on providing the greatest level of support around cloud when it comes to MDR. We feel like there's some gaps in that for some of the workloads, and we want to be the very besta at supplying that. And the other thing that we're working on is just having a better tighter integration on the new tools that we're seeing. So we just released integration with Wiz, we have MDR support across Wiz platform, we've seen a lot of success with that. We've got that coming for some newer other technologies and have gotten a lot of really strong press in the market, we're seeing people adopt them, the different technologies out there. And Red Canary is looking to be the top MDR provider when it comes to that. We've listened a lot to the customer. And we've heard, hey, it's really great that you're helping us out with these threats, it'd be awesome if you could actually respond or remediate on it for us. So we've done and released active remediation where Red Canary can remote in hands on keyboard, do the full remediation on endpoints. We're now starting to dip our toes into that and seeing Hey, can we go ahead and do an actual active remediation when it comes to an identity threat, when it comes to an email threat? Can we even do that on firewalls? I know customers probably are not going to want a company like Red Canary or any company like that doing changes on their firewalls. But there might be some organizations that just don't have any IT on staff that would like that level of support. And we're definitely dipping our toes and potentially offering more there as well.

K Keith Hawkey 27:09

Well said Brennan. So we're coming up at the end of the podcast here, we always like to give it

give a chance for a guest to to disseminate a message. You're going to provide a message to any cybersecurity professional out there that that's under said, or that's just not prevalent enough in the intelligencia of the cybersecurity landscape, what would you what message would that be?

B Brennan Manion 27:42

You know, that's a great question, Keith. I am, a couple of things come to mind here. And I think that the biggest one is I would just tell people, any of your listeners to just go for it. You know, there's, there's a saying that I like it's fake it till you make it. And sometimes you're just gonna keep faking it. And then one day, you're going to recognize that you've arrived. And I would just want to give power and confidence to anybody out there, whether it's IT security, sales, whatever it is that your position is that you're passionate about, just go for it. I mean, you you only have one life, go go do the best that you can out of it. And if you believe in something, be confident and go for it. You know, you don't want to get out of the guard rails and be disrespectful. You always want to have high respect and nice manners always. But go out and go go for it. If you feel strong about something, push the button. And you'd be surprised at the amount of greatness that you can bring the world.

K Keith Hawkey 28:38

That's awesome. I think that's an excellent note to leave on. Brennan, how can people get a hold of you? How can people reach out to you?

B Brennan Manion 28:45

You can use text me, call me, smoke signal, email, LinkedIn, you name it. So I'm on LinkedIn, that's probably the best way if you don't know me, my email is first name dot last name at redcanary.com. But LinkedIn is a great spot. That's that's probably the premier social networking for business professionals but I'd be welcomed to anybody that wants to connect and learn more and I'd love to help any way I can. And if I'm not the right person, I'll do everything I can to find the right person to help someone.

K Keith Hawkey 29:17

We'll make sure to include that in the show notes and Brennan, really appreciate you being on the podcast. Thanks a lot for your time.

B Brennan Manion 29:23

Thanks Keith really enjoyed it. I love being a partner with Opkalla. You guys do great stuff and it's always fun to work with really fun and great people. So thank you.

K Keith Hawkey 29:31

Well that's that's very nice. And we will see you guys next time. Take care.

N Narrator 29:39

Thanks for listening. The IT Matters podcast is produced by Opkalla, an IT advisory firm that helps businesses navigate the vast and complex IT marketplace. Learn more about Opkalla at opkalla.com.