Micro Focus Reimagining Cyber Episode #37 Ty Sbano

Fri, 7/8 11:45AM • 26:38

SUMMARY KEYWORDS

security, startup, interview process, product, understand, cyber, business, talk, people, organization, metrics, folks, starting, multi year journey, cyber resilience, plan, ciso, build, success, reimagining

SPEAKERS

Ty Sbano, Rob Aragao, Stan Wisseman

Listen | Read

Ty Sbano 00:03
I'd like to quote Mike Tyson here. “I think everyone has a plan until they get punched in the mouth.” And I think that first 100 days, we all have this glorious idea of 30 60 90. But in startup land you must be willing to adjust accordingly.

Rob Aragao 00:18
Welcome to the Reimagining Cyber podcast where we are short and to the point perspectives on the cyber landscape. It's all about engaging yet casual conversations on what organizations are doing to reimagine their cyber programs, while ensuring their business objectives are top priority. With my co-host, Stan Wisseman, Head of Security Strategist, I’m Robert Aragao, Chief Security Strategist, and this is Reimagining Cyber.

So, Stan, who do we have joining us for this episode?

Stan Wisseman 00:45
Rob, our guest today is Ty Sbano. He is currently the Chief Information Security Officer at Vercel. Ty has had the opportunity to be in security leadership roles for very large firms as well as for startups. His primary career focus has been developing application and product security programs for companies like Capital One, Target Lending Club, and JPMorgan Chase. Ty it’s great to have you with us today, really looking forward to this episode. And this opportunity to speak to you. Anything else you'd like to add about your background? For listeners?

Ty Sbano 01:18

No, I think that's pretty good. I'm starting year number 18 in information security, if I don't consider like my undergrad time when I was working full time, which this would be year 20, to be honest with you. But in the grand scheme of security, IT, and tech work, it's crazy to think how long I've been doing this. And I really always appreciate a chance to pause, stop think, and reflect. Having these types of chats allow me to look back and really analyze my career track of how I've gotten here. And thank you for asking me to join today.

Stan Wisseman 01:50
No, it's great. You know, whenever anyone takes a leadership role, right, they should take time to assess and understand the current state of the organization, and then make a plan and execute on it. Now, now, when you come into cybersecurity, leadership roles, and you've had the opportunity to do that at many organizations, how do you establish your priorities? And, and I know that sometimes, as we've talked about, preparing for this, you've been brought in to help clean up somebody else's mess. But that's not always the case. But how do you typically engage and make your plan and prioritize?

Ty Sbano 02:30
Yeah, I think it really starts even prior to actually getting there, right? It's the interview process, you start to gain a lot of intelligence and intellect. And I think the idea of the interview process, everyone's putting on their best foot forward, but I think the right companies, the right culture, pull no punches. They really tell you the story, they tell you the challenges, they say where the opportunities are, if it's all glowing, and great, you know, it's not going to be real once you get there. There's going to be a lot of the odds and ends of like, this isn't what we talked about. And I can tell you like, within security, because of your expertise, because your time and role and your subject matter like focused work, once you get there, you're going to reveal things folks that don't have that level of depth and knowledge, you're just going to uncover, and you have to adjust accordingly. Right. So, I think you have to start during the interview process to really ascertain what am I actually going to do. And I think the best CISOs out there, start building their plan before they even get there for their first day, which is something I highly recommend. And I know it's counterintuitive. But if you want to be successful, you got to come prepared. And I think within security, it's you know, if you don't have a plan, and you're making it up on the fly, like it's probably not going to be that good. So, I think from that point, when you have your first day or your first week looking at the agenda of like, how do you get on board? What are the controls? Why were you even brought there? And I think my career in the past, you know, five, six years has been very different than the first, you know, 10 and 12 years, which was very hyper focused on application product security for larger organizations. And startup plan, you must be a lot more agile. And I'll focus the conversation on narrative there. So, I think once you get to the shop and a startup, where do you start because anywhere is going to be okay. But in reality, your first act matters so much to building or destroying the confidence of what you're going to do there at that organization and if you're on the tail end of you know, not so great experience or maybe they hired the wrong folks for the role or you got to help move someone out of the company or you got a disruptive big old project that's not been working well. I've been that, you know, and I love to just work on tough problems, because I think that really drives creativity. That drives a lot more of your own internal resiliency of working through adversity and honestly 18 years deep, I am at a point where there's no emotional reaction to a lot of this anymore regardless of the incident regardless of the mistake regardless of the error. It takes a lot because I think just even in these past two years, we've seen more physical warfare. That's come into my frame. We've

seen pandemic responses that we've only drafted in plans and dealt with like swine flu back in the day or like little things. But now it's really that adjustment. So, I like to quote Mike Tyson here. And “I think everyone has a plan until they get punched in the mouth.” And I think that first 100 days, we all have this glorious idea of 30-60-90. But in startup land, you must be willing to adjust accordingly. And I think we're going to kind of touch on that a little bit more as we keep going.

Rob Aragao 05:30
Yeah, definitely.

Like the Mike Tyson analogy, getting thrown in there, appreciate that. Talk a little bit as it relates to when you're getting into, you know, startup land. And as you said, you kind of you know, you're at day zero, because you've gone through the process of kind of the mutual interview process, right, as you talked about the culture and understanding of what's real within that organization, and what they're trying to drive at it kind of the key business outcome is what you're going to end up flipping back into how you're approaching it with your cyber program overall. So, let's talk a little bit about, you know, the approaches that you've taken, as it relates to getting to know, right, what they're trying to accomplish, what the desired business outcome is they're going after right to market and competition and all of that. And then how you kind of say, okay, now this is how I'm going to take the steps and framing the way I'm going to enable them to achieve those things. From my support in the cyber program, I'm going to initiate or completely pivot from what they've had in place. Maybe explain about that. I think that'll open the minds, so people understand the reality of how fast and important it is not to miss when you come into a site startup.

Ty Sbano 06:39
Yeah. So, I think when you get there, you have the interview information, right? Like where or why am I even here? Like, what is the context for me being here? Am I starting at a series B? Early enough where maybe there are some good decisions, and I get to really build it from the ground up, we're more recently, starting in a series D. And it's different. There is maturity wise, that look like a series B feels like a series B, but we got 300 some odd people running around. And there's a lot of processes that haven't matured at the same rate. So how do we prioritize? How do we think about that? And again, were you brought in at the right time? Or are you working, kind of on your heels trying to drive forward? And I think that's where you really need to understand who's your constituency? And what is the network of champions and change leaders that you're going to associate with? Or are you just going to be an army of one sitting in a, you know, an ivory tower in the corner, because your security and it's like, I'll be honest, in startup land, and that does not work, you need to be integrated, you need to find the forums, you need to be invited to the forums, you need to be kept invited to the forums, right, like you can't be kicked out. And then also, I was like, well, why is security not good? Because I don't have visibility, why don't you have visibility, where you don't invite me to meetings like that, that should be a telltale sign of like you're not fitting in? So, the thing that I found very natural is getting as educated as you can in the business and defining what is the threat model? How are you looking at the world? And I sit down with the executive and each company in the very beginning to say, here's how I'm looking, you know, we can talk about business impact assessment, we've talked about all these buzzwords within security that, honestly, you as a CEO or the CSTEP, you don't need to know. What I want to understand is when I prioritize things, or when I talk about a security incident, or I'm driving a business

value change, like, hey, we're going to go build on sales enablement, so we can fill out security questionnaires faster. So, deals can close. Or one's going to go, Yeah, we want deals to close faster. Well, here's the thing. We can't do that until we have a security program. So, if we start filling out questionnaires as quickly as possible is like, well, we don't have this, we don't have that, we don't have this may slow down on the whole thing. You know, and I think when you talk about that threat model of where are our functional risks, are we in alignment and agreement on what our exposures are, what our attack surfaces, and also the strategic roadmap of give me at least two quarters, if I can have two quarters, great, but in most startups, you're going to get like, two weeks, two months, two years is not feasible. And I think when I look at my track of previous publicly traded companies, having a three-to-five-year plan was realistic, because you need it. You need to bring a lot of people along for that journey when your security teams 350 humans versus I got a team of seven right now I have IT, I have privacy, I have some legal stuff. And I have security. And then I have this fringe thing called fraud, abuse, trust, and safety that I don't have any time for neither do my peers, but we're working through it. And we have a dedicated team. But strategically, we're not we're not kind of grinding there. And I think even in that communication, I have the confidence that I'm working on the right things. And I say this last thing that I mentioned, it's not a priority for me because we have some folks doing it. I just can't jump in there because my skill set my background, what I'm going to bring to the table for speed of execution is this stuff. And this is where we're going to drive forward and I think if you have that threat model firmed up, most folks will start to understand. Okay, so you identified additional gaps, you understand where we're prioritizing if you're elevating the right three things, right? And then any executive, you start getting into 5, 10, 20. And I bring a matrix like the NIST CSF, way too fast. No one cares. And I'm sorry to say this to all security professionals out there, they don't have time to care about it. That's your job. You need to communicate effectively to say, okay, of the things I've discovered so far. Here's where I'm focusing my time. Are these the right things? This is what it's minimizing. This is what it's reducing. This is what you know what, maybe we just don't care. But one of the first acts I really liked to always pump for folks. And I got this from Mark Dorsey. He has over at Netlify. And he's a competitor of Vercel, but we're friends. And we've been friends when he was at HelloSign. And I met him at a meetup. And he just gave me good advice. He's like, before we do anything as a CISO. Get an incident response retainer. And I'm like, you know what, that's always in my playbook now. Because when I get there, I don't know what I have. I don't know what I'm going to run into. And you know, what, what CISO wants to walk into the shop with that surprise of like, hey, we got breached. And we didn't tell you about in the interview process. I know plenty of CISOs that have bounced from shops, because they were blindsided very, very much. And it's unfortunate, but that type of support with an incident response retainer gives you the confidence to say I can keep moving forward. And I have the backup and support in case something goes wrong. Because if I burn out in the first 100 days, and then what where's your program going, I couldn't tell you because I'm too tired, I'm exhausted. And I didn't sign up for this stuff.

Stan Wisseman 11:34
You're setting an expectation and leadership saying, look, something is likely going to happen even later down the road, we need to have something prepared just in case there is an incident so we can respond effectively and have in the right amount of speed. So, your communication is key with the executives, even before you join the company, certainly with the executives understanding what the priorities are. But when you're looking at trying to quantify success, whether it be to the board, to the

CEO, for yourself. Are there some metrics that you typically are trying to capture? Or is it again, so dependent on the organization, and in the context of what you're dealing with, there isn't a rule of thumb that you can go to.

Ty Sbano 12:25
I have a non-standard metric. And while I appreciate KPIs, KRIs, I think at startup land like you're shooting tourists those trajectories, but you don't have the functional business processes, you probably don't have the people, you don't have the data.

Stan Wisseman 12:40
You can't feed them.

Ty Sbano 12:44
Yeah, you cannot feed your metrics without information. And I've been on both sides of this paradigm where metrics really influenced me in such a way that I've pivoted my career to go focus on BI and data for four years of my life. And it was very valuable, but like being data driven, is critical. But all that aside, when you're in startup land, or you're starting a security program, if you start with metrics, I think they can be inspirational, but you're going to lose your audience, because you're typically in a fast-moving shop that wants to realize value. And to get to that value statement. You're talking about nirvana. And it's not feasible. So, MVP, or minimum viable product, I know it's an overused word. But where can you start small and get your key wins while you're building your strategic wins to get to the next phase? And my question is simple. Do people want to work with me and my team? That's it. You know, what? If the answer becomes No, well, I'm not doing my job. I didn't show up, right? I didn't present right. Or maybe this company just didn't want me to be here. But I can tell you, in the interview process, once again, before you sign up for any of these gigs, you should have a clear established idea of like, what am I there to do my there to disrupt a lot of stuff and piss off a lot of people? Well, I want my contract, I want my work agreement to reflect that. Because if I'm there for one year, I'm not going to be able to do a multiyear journey. My preference is to find the place where I'm in a multiyear journey, it's important to understand why you're there. So even before that point of asking that KPI and that metric, like having that defined success criteria of like, what do you expect me to do? By the time you're one rolls around? And if there's no answer, or it's like, well, you're going to tell us. I love when I get hate, you're going to help us, inform us what is it that we're going to measure and why and success or not? Because if you're getting compromised every day, and no one cares, then whatever. But if you get compromised once and you get fired, then it's a different story. Right?

Stan Wisseman 14:38
And I just following up on that. I do agree in that context of if they don't perceive value in that they're not going to invite you to that meeting. But going back to your experience for the whole product security side of the house, right. I mean, there's the in your role as CISO to a startup that's coming up with a product or service you're trying to ensure that your organization is secure. But you also have a more than most at awareness of the importance of ensuring that whatever product or service you're offering is not going to introduce risk to your consumers. Right. And so, you know, again, looking at your perception of success, or where you need to focus your time, how much of it typically is on the organizational side versus what you're providing as a service or product?

Ty Sbano 15:28
Yep, it depends on kind of the product itself. And it also depends on why I've joined if I'm starting with the base program build, which is something I'm doing at Vercel now, starting with a lot of the enterprise controls, but I brought in someone that I've worked with in the past, Aaron Brown, an amazing security engineer, now head of cloud security here at Vercel, that I'm interesting, because we've done some of this journey together in the past that I can say, Cool, you go work with product. You know, I'm here, like, that's all I've ever really done. And I love to do, and I prefer to do that work, but I can assist you and watch you get that part done too. And in all honesty, it's not at the executive tier that the product really moves. And that's a difference in my observation as well, like, yes, I can help. But if I'm sitting down to explain, like, you know, here's how we're going to establish DDoS protection within our product to sell this to customers. I don't talk to the executive team too much about that. I'm talking with the directors, the product managers, the sales team, like I'm working cross functionally across the org. Good and bad C-level titles can do some of those things. But when we pull a lever, say we have something bad like secrets management isn't good. You know, I can say this out loud. Most of the shots I've ever been at secrets management can be great in certain areas. It's not great everywhere, right? And we all know that that cred, leak creds go to the wrong place. Sometimes it's just speed of movement that must get something done and I text slack it to you DM it to you over LinkedIn, whatever it is. Sometimes we must take those degraded stances. But when I when I look back at like enterprise versus product, I don't always kind of conflate the two, because if I'm charging after the basics of hey, what third parties do we have in our show? What endpoints do we have for all our employees? And if I can't answer that, why am I going to go narrow and deep on the product to build out these crazy cool features, that is going to empower the journey and help sell this more. When we all know massive breaches and issues really occur from basic flaws? No 2FA the most recent one that's out in the news with I forget how many billions of people's information through, you know, that was from a blog post. And it had a secret in it, and someone recovered it. And then now they've extracted this and they're selling, you know, billions of billions Chinese citizens. Now, that's the perfect story, an example of like, well, we could have done all this great stuff and the product, but they didn't matter. Right?

Stan Wisseman 17:57
Right.

Rob Aragao 17:58
You know, you kind of hitting upon where I want to go next. And it's about the will, I'll say keyword positive security culture. Alright, so establishing that you talked about, you know, you're meeting and engaging with the different directors, the product leaders, right, kind of, you know, how do we go to market with our solutions? How do we ensure that people are thinking about security as you're creating the different products and services and capabilities to continue to grow Vercel? What's the aspect I kind of one of those, you know, you talked about kind of quick, visible wins is what I like to phrase it as right, you get in, it's like, here, here's what I'm thinking about doing. We agree that we should achieve these things, and you achieve it or overachieve it. So, you're sure that positivity back right to the business. But when you think about kind of instilling that positive culture across the board, not the easiest thing,

right? What are some of the things you've seen work? What are some of the kinds of, you know, lessons learned as well?

Ty Sbano 18:50
I think it's as simple as carrot versus stick, you know, there was a powerful book called the “Carrot Revolution and the Carrot Principle” that I kind of read way back maybe 12 years ago, 10 years ago. I really appreciate the sentiment there. Because I think one of the things that we've already talked about is coming in on the tail end of a rough team, or maybe a team that's already in place. I think that's been one of my magical, behavioral traits that has allowed me to excel within the security space. Because a lot of folks come into this with that negative view or very critical or their traditional curmudgeon security person. It's not customer oriented. And I think as someone that started purely in consulting, you must put your best foot forward, you're there for the customer in that ideal that everyone is your customer changes the narrative. So, I think when you treat your employees, your folks within your company, your direct reports as customers of your service, it changes the narrative. And I think that's something we must think about. So, going back to that previous question, like do people want to work with me? I consider that to with people that report to me, and sometimes the one long one that are on the ship must hear the message over and over. And they're like, you know why? Why is this person so positive? Like, why do they focus on this narrative or these data elements to drive change versus like, telling people, it's bad. I'd rather have that conversation internally as a team, than go and lambaste someone. So even as something as simple as a security incident where someone falls victim to a phishing attack, you know, when you do phishing training, do you end up firing everyone that clicks on the link? Right? Like when I hear those stories, I cringe. Because I'm like, that's not a learning moment, you're dispelling trust. So, the element there for me is like, I'm trying to establish trust in so many of these customers that it only takes one mistake, and only takes one miscommunication and takes a lot of this. So going slow to go fast is important. I firmly believe in going extremely fast, but with respect with positive intent, and I think that resonates back because people trust you. And when people trust you, guess what happens? They self-report issues, they fix issues, they partner with you on things, when they don't trust you. They don't want to work with you, you don't know what the issues are, you'll never know what that tech debt is. The skeletons remain buried somewhere behind you.

Stan Wisseman 21:17
And you stay in your ivory tower, right? You're in your way.

Ty Sbano 21:21
And then you can literally have that conversation with the frustrated engineers, the directors that are pointing and saying, well look at how crappy these people are in the security space. You know, like, that's cool. I'm not them, you know, or that's cool. That was in the past. And that's something I'm battling right now is like, that's in the past, let it go. Because I don't care anymore. That was six months ago, like how many things here? Do we talk about that six-month-old? Not a lot. So why are we talking about people that haven't had any impact on what we're doing? Now, today, I've rewritten the policies. I have adjusted the program, I'm talking to our customers, like I'm doing all this stuff. It's a new reference. If there's context setting, I'm so down to have that conversation. But if it's just to talk crap, you get one or two with me, I just, I don't want to have a third round of like, I just want to hear someone just getting bashed, it's like, you know, they probably had some positive things. Maybe they weren't set up for

success. There's a lot of contexts I don't have either. And we're hyper focused on something that's not building a sport. So, I think when you really focus on for progress, and always focusing on that step forward, like, it just changes your mentality. And I think a lot of folks see that and want to work with that. Because that's, that's the type of person I want to work with.

Stan Wisseman 22:36
Right? Well, hey, you know, this podcast, we're doing Ty is all around, how we can adapt what we've been doing, to do it better, and be able to honestly handle today's threat landscape and business landscape, right. And you're all about adapting and evolving, as we've been talking about. So, in that broader context of cyber resilience, you know, how can we evolve? What been we've doing for four decades on cybersecurity? To address today, and tomorrow's new threats. What do you think? What's next, you know, where do we need to go?

Ty Sbano 23:16
I think it's a continued movement towards less talk of injecting the word security into things. So, I've been stuck on this my whole career. And it started with application security with this idea of a secure SDLC. So, when we say hey, we're going to go in a secure SDLC. Does that mean everything else is insecure? And it's happened again, in my opinion with DevOps? Well, we're going to do DevSecOps, I'm like, well, I mean, DevOps already has quality into it. If we've all agreed that security is a subset of quality, then we don't have to have this conversation. And we're doing it again, you know, secure cloud, cloud security, posture management. It's just posture management, right? And I think I get it, I understand from the marketing side, I'm on this side of the sale now in startup land compared to like, publicly traded where you know, it's too big to fail. It's a very different scenario to understand the business model for what it takes to make a sale. And I get the search engine optimization, I understand why we must have those words, but as practitioners inside of your four walls, if you're beating down the door, and always saying security, special securities unique. Well, I think you're becoming anti-resilient, because you're creating these different tracks, you're creating these different places have documentation new, creating a different communication style. My recommendation is to be part of the resiliency strategy that's already there. It's not to break away and create something new. And I understand sometimes there's disambiguation that must happen with like incident response or security versus incident response for like PR and other things, which you may get involved with. But I really go back to just like dropping the terms of cyber security from those narratives and just talk as if I'm with the business because I am and I think that shows up well.

Rob Aragao 25:01
I think that's spot on. Personally, it's one of the things for me that, you know, we talked about. It's DevOps. There's no second the middle, because once you put that in the middle right now, just kind of distinguishing that there's some sort of separation, we need to kind of have a conversation and debate where we come in. No, no, no, it's built in. It's baked in right just to your pasture management example. So, I agree with that principle. Because it does set the stage correctly when you initially engage with the other audience that is used to doing their things. And now it's, it's simply kind of embedding the elements of security just into it as part of the equation. Well, so I listen, we appreciate you coming on and sharing your journey from the large organizations in your before, the kind of the focal areas you've been going after in startup land. But the approaches that you've taken is what I hope the listeners really

take, as lessons learned different ways to work with the teams to help enable those positive security cultures and drive programmatic success at the speed. A startup has to move out to be able to be a successful organization and grow. So, thanks for joining us to tie 100%

Ty Sbano 26:04
Appreciate you having me! Always happy to chat.

Stan Wisseman 26:07
Anytime. Thank you.

Rob Aragao 26:10
Thanks for listening to the Reimagining Cyber podcast. We hope you enjoy this episode. If you would like to have us cover a specific topic of interest, feel free to reach out to us and you can find out how in the show notes. And don't forget to subscribe. This podcast was brought to you by CyberRes, a Micro Focus line of business, where our mission is to deliver cyber resilience by engaging people, process and technology to protect, detect and evolve.