

# 2023-04-11 - Dez Rock

[00:00:00]

[00:00:23] **Christophe Foulon:** Welcome to another episode of Breaking Into Cybersecurity, and today we have a special edition with a cybersecurity company founder. Her background comes from leading a red team company and now switching to Blue, . I will leave that up to Des, who is our guest today, to share her background and why she wanted to come on this podcast to help influence the next generation of leaders in cybersecurity.

[00:00:52] **Dez Rock:** Thanks Chris for having me and thanks. Hi to everybody out there. You're absolutely right. Before we were Blue Team, which you know the [00:01:00] company as you can see, the logo behind me are, if you're listening that it's called See Monster. We were definitely red team. A lot of people don't know what Blue Team Red team is, so maybe we should get into that.

[00:01:09] **Dez Rock:** Blue Team is DEF Defense when it comes to cybersecurity and red is proactive. Pen testing and things like that. And we had a background of red team a history of BR red team, hacking for years and switched to blue, I must say cuz we're talking about breaking into cybersecurity.

[00:01:25] **Dez Rock:** I am. Technical, I don't have any of the qualifications that you do or do all the things that you do. However, I am a founder and a co-founder, I should say, in this area. I have, the company is ours and I lead. And I am the c e o. I suppose the first thing we can say is that you really do not need to be technical in order to be in this space.

[00:01:46] **Dez Rock:** There are room, there is room. I don't think I could have done it on my own though. I definitely needed my co-founders. Yeah. So

[00:01:52] **Christophe Foulon:** what initially prompted you to found a company focused in cybersecurity? What your co-founder. [00:02:00]

[00:02:00] **Dez Rock:** Okay, so when we were Blue team red team we had a c clients and regular clients.

[00:02:05] **Dez Rock:** One of them was blue Scope Steel, which is the fourth largest steel manufacturer in the world with locations all over the place. So their data security issues were quite unique. They were in mines, they were

everywhere. And we would keep, we would do the pen testing and they asked us at some point, is there software that.

[00:02:26] **Dez Rock:** Is there software that we could use to help protect us and we didn't know at that time. And then through that, trial and error and learning, we actually learned about seams where that there was such a product. And we introduced them to Splunk. This is a really good origin story.

[00:02:42] **Dez Rock:** Fantastic. And to which they turned around and said, you know what, Splunk is way, and this is a very large organization saying Splunk was overpriced. So they asked if there's anything else we could do. So we started with open source tools and I started to build a team and we thought it was a side project and it's become [00:03:00] now the main event.

[00:03:00] **Christophe Foulon:** Wow. And as a thinking from a founder's perspective, for those that are not technical and you're looking to. Get into this space as a leader. What do you need to do to ensure that you're having the right conversations with the business? Yeah. When it might be more technical than you are or having individuals asking those types of questions, how do you keep up with the industry?

[00:03:26] **Dez Rock:** So for us, we. We found a need within the industry and then decided to fulfill it. And I suppose that's the first place to start if you're looking to become a founder. So becoming a founder is different to leading in this space, by the way. It's different skillset. Becoming a founder is, just relying on your entrepreneur skills to see, look for a A possibility in the industry and then fulfill it.

[00:03:47] **Dez Rock:** Leading is a different skillset. Leading is that you have a team behind you. You've built a team, and it's the style that you bring in order to make that team better, to literal literally carry that team or [00:04:00] lead the team. The names suggest itself. So those two are different skillsets and to break into them leadership skills are synonymous in every industry, cybersecurity.

[00:04:09] **Dez Rock:** It does tend to have a lot more neurodiversity. So if you're not good with working with neurodiversity, you're probably not the industry to be leading in. And for founding, I think there's a lot of opportunity out there, for sure. Yeah.

[00:04:21] **Christophe Foulon:** Thank you for bringing up neurodiversity. I think it's often not covered enough.

[00:04:26] **Christophe Foulon:** And as you mentioned that, what are some of the skills that are really needed to lead neurodiverse workforces.

[00:04:35] **Dez Rock:** So I think that we've all, we are very used to cookie cutter solutions. Like we all go to school. It's the same thing, like we reward the person who puts their hand up and answers questions and stuff like that, and ignore the quiet one sitting in the corner.

[00:04:47] **Dez Rock:** And we try and train people to all have the same personality. What I'm saying is it's almost like a societal standard. And when it comes to working with people and working with neurodiversity, it's more than just a personality trait, right? So the [00:05:00] neurodiverse person communicates in a different way.

[00:05:02] **Dez Rock:** Their brain works in a different way, and they require a different way in which to be handled. So what I've seen is that people like, it's the, it comes down to the same. It's the same thing. It's not oh, you have to treat them any, it's the same thing. You make your staff comfortable and it's whatever makes them comfortable.

[00:05:19] **Dez Rock:** For example, it's a small one, but my staff don't like to come, especially they don't like to come on camera, so in meetings, so I don't make it a point that you have to put your camera on because that's nothing to do with their job skillset. That's got nothing to do with whether they can do the job or not.

[00:05:35] **Dez Rock:** That's just it's a requirement outside of that. And so therefore I, and I know it makes a lot of people uncomfortable to be on camera, to make the eye contact and things like that. So it's not a requirement for us. The way you dress, the way you are. And the other thing is if you wanna work from home, cuz I know a lot on Neurodiverse, people love that I fully support that we've been remote before the pandemic and continue to be yeah.

[00:05:56] **Christophe Foulon:** Nice and. Camera off [00:06:00] communications. What are some of your recommendations for a leader to be able to communicate effectively? W with a broad population, especially if you're remote.

[00:06:10] **Dez Rock:** Okay. Tools are very handy, collective tools, no matter what you use I do struggle at times, to to get this right.

[00:06:17] **Dez Rock:** We also deal with people where English is not their first language as well. So you. In that case, I actually, what I do, because I'm the one who wants to communicate I actually use tools like Capture or any other video recording tool and will record myself saying whatever I need to say and screen share showing whatever I need to show.

[00:06:36] **Dez Rock:** Therefore, I'm covering Audible, visual and any other communications. So what's important is that they understand my message, right? So I don't need them to be on camera to, to listen, for example. So I will use that tool a lot and it works really well for people who, where one, it's recorded so people can go back and listen.

[00:06:56] **Dez Rock:** And two, the fact that You are watching, my gestures and stuff and what's [00:07:00] important to me, especially screen sharing when I'm talking about certain things especially creative stuff that I need done. It's it's a really valuable tool in that case. Yeah.

[00:07:09] **Christophe Foulon:** I love the use of the audio visual as well as it sounds like you're using caption as well.

[00:07:16] **Christophe Foulon:** When it comes to influence, how do you recommend that leaders develop their influence when they're not in person, they might be remote to work on those types of skills?

[00:07:27] **Dez Rock:** So with. Listen, we've had the pandemic, so everything's a bit topsy-turvy, but prior to that we were meeting at least once a year and dragging everyone into the room.

[00:07:35] **Dez Rock:** And although as reticent as people are, everyone does enjoy it because you do get to break some barriers down in your team. You actually sit down and have a meal together and things like that. They are team building exercises, which are important, and they do bring the coercive, it's coerciveness to the team.

[00:07:52] **Dez Rock:** That's important. I also encourage some banter as well, and. Important to share the good things and the bad as well.[00:08:00] So yeah, I the re the other way, what I really do is actually get to know the person I'm dealing with because I think, and I spoke about this earlier, I try not to treat everyone as the same.

[00:08:11] **Dez Rock:** So not everyone is the kid who puts their hands up and knows all the answer using the school classroom metaphor, right? So if you're

the quiet kid in the corner, I will find a quiet moment to come sit next to you and then see, how you're doing and if you're okay. And do you understand everything?

[00:08:24] **Dez Rock:** Because a leader, much like a good teacher, must know who they're leading. And their style in order to reach them. And a

[00:08:31] **Christophe Foulon:** as, as you think about developing leaders within your organization, how do you create that talent pipeline for them to grow and lead in your organization? So

[00:08:40] **Dez Rock:** that's the thing. I can't lead everybody.

[00:08:42] **Dez Rock:** Obviously I have to mitigate, like hand over that task to other people. So I pay very close attention to the corporate culture that I'm building, really close attention. So I will hand mold the people that I want to lead for me. And work closely with them. And they're the people that I'm talking about.

[00:08:57] **Dez Rock:** So once they know my style and I trust them, then I expect [00:09:00] them to then carry on exactly the message and the style in which I've done. And that, to be honest, is the hardest part there because we have such a disconnection between. Executives and workers, nobody likes CEOs. You just need to go on Twitter to see that.

[00:09:14] **Dez Rock:** But everyone wants to be a found, everyone wants to be their own boss. And so there's a disconnection there. And and I agree there is a disconnection, but what's interesting is that both sides can often contribute to that. To that, to that workplace toxicity. So it's important to catch it. I, when I see it, to catch it and remove it, that's part of it.

[00:09:34] **Dez Rock:** So it's all about training the people who I want to manage other people,

[00:09:38] **Christophe Foulon:** So you mentioned training the people who who grow, who. Grow and lead other people. What are some of the skills and competencies that you look in those people? I know you mentioned your style, but for those listening you're looking for that, those tips and tricks.

[00:09:54] **Christophe Foulon:** So what would you recommend for them to work on to become a leader?

[00:09:58] **Dez Rock:** Good questions. I [00:10:00] think that the base of it would be is to recognize that people are emotional creatures and that decisions made from emotion. Is not good leadership, right? That you must be able to put aside, you can get upset, you can be very happy.

[00:10:17] **Dez Rock:** It doesn't, whatever the emotion is, feel your emotion. We're not robots, but to make decisions while you're in that heightened state is the number one mistake right there. So not to do that, and also not to take things personal. Because the, this isn't like to use the Godfather, it's not personal, it's personal, it's business, right?

[00:10:34] **Dez Rock:** So it's that, which means I'm asking people to, and I'm looking for people to remove ego as well, to be more skill orientated or goal orientated and to remove ego so that it. In order to do that's a really nuanced part. You need to be able to show vulnerability. You need to be able to not have a bit of humility and be humble to say, Hey, listen, I made a mistake.

[00:10:55] **Dez Rock:** I need to know how to do better. And often there's a little bit of untraining as well. If you've [00:11:00] been, like I, if you're an executive, you've been in a different organization where they have a different corporate style, you're bringing. You're bringing all of that to my new to, in this and you're trying it on now, you might not like it.

[00:11:11] **Dez Rock:** You might have left because of the corporate culture was so toxic. But unbeknownst to you, you'll often bring those attitudes over as well. So it's about recognizing your own behavior as well and being willing to change. And those are the people that I want on my team. Those who can actually Adapt to do that.

[00:11:27] **Dez Rock:** Because what happens is, and you and people might say, Hey, listen, this is all sounds a bit soft and lovey dovey, but once you actually get people comfortable and happy in their workplace, they are far more productive. It's as simple as that because people do not work for money. It doesn't matter how big the paycheck is, if you're treating them like They're proverbial.

[00:11:47] **Dez Rock:** I won't, yeah, they will leave. They'll look to leave anywhere. They'll say, I just, because, I don't need this. I will find another job and then I'll transition over. Nothing is worth this. It tells you that we spend a lot of hours at work. We [00:12:00] spend lot, more than we do often with our family, right?

[00:12:03] **Dez Rock:** So our relationships with our work. Should not be toxic. And it's funny because we speak a lot about toxic relationships and we know we have toxic relationships with our boss and all that sort of stuff, but there's not enough discussion about. What to do about that. So all of your questions about how to lead, my first thing would be is that ex, if you wanna be a good leader, focus in on that.

[00:12:24] **Dez Rock:** Try and remove a lot of that. And it's not because one a ha, like I said, a happier pl. A workplace is a far more productive workplace. You're inspiring people to bring their best, not because you're paying them to.

[00:12:35] **Christophe Foulon:** Earlier you mentioned there's a lot of neurodiverse individuals. Wi within this.

[00:12:41] **Christophe Foulon:** How do you help those that often have been very technically focused Yeah. But now are interested in leading people to switch from that individual contributor mode Yeah. To that leadership mode.

[00:12:55] **Dez Rock:** I know exactly. Yeah. So it's, to be honest, Sometimes you [00:13:00] could my suggestion would be this, and that is to break it down as a flow chart, right?

[00:13:05] **Dez Rock:** So you, to lead effectively, you must say, I need something done, and then I need a result from that. And I, and then, so that's the flow chart, right? So I need e, my staff to do this, and then I need to know that it's done. Basics, right? And then we break it down. It's if they don't do this, then it becomes like a, if that, then this situation, if they don't do this, what is my course of action?

[00:13:26] **Dez Rock:** And so you can start building it out. Am I helping you visualize like a pathway? You can start building it out. If they don't do this is what I do. If they don't do it again, I escalate to this and then this is, and you fill that out. Now of course you fill that out in a way. Will work for you, right?

[00:13:42] **Dez Rock:** So threatening and cajoling and all that sort of stuff may work once, twice, and then that doesn't make you a good leader, right? So the same thing if they do that, What do you do? Like you must, do you praise, do you say, well done? Do you say, how do you reward them? What's their best reward? What is their what matters to them?

[00:13:59] **Dez Rock:** So I'm trying [00:14:00] to break it down in a way cuz I do know how the neurodiverse mind works. I'm trying to break it down in a way

in which you can see it. That there are pathways that you can actually learn to say. This is what to do in this situation. And then how do you report back to your superior?

[00:14:13] **Dez Rock:** What are you saying? How are you communicating? How often are you communicating? What is it that they want to see from you? And good leadership is thinking always outside of the box, and, but you can actually quantify that too. Do I wanna make everyone just a little bit more happier around here?

[00:14:27] **Dez Rock:** It's like, how do I go about doing that? Or do I want, I need productivity up. See, here's the. Old style of leadership is I need productivity up. The manager gets out of his office, walks into the, the work floor, the floor, and says, work harder, and then returns back, sits down, job done right?

[00:14:42] **Dez Rock:** So I will argue that's not leadership. Yes, but neurodiverse people can absolutely lead. It just means that they would recognize that what is required, like what does leadership look like Once you understand what leadership look like, and remember the whole adage of lead, a really good leader will have people who want to [00:15:00] follow them, not because they have to.

[00:15:02] **Dez Rock:** That's when you know you're a very good leader, right? Because they want to follow you and you inspire loyalty as.

[00:15:08] **Christophe Foulon:** Yeah. I love how you've been able to group the different aspects of delegation, collaboration, communication, all, all into that flow chart. A and kind of an adage to the company that you're leading right now, a sim company being able to do if thens and understanding how data's flowing through it.

[00:15:29] **Christophe Foulon:** Correct. Let's pivot over to the company side, if you don't mind. Okay. As you shifted from an adversarial approach to now a defensive approach with your companies, how Yes. How do you help individuals make that mindset change? In order to better defend their companies and to grow as technical individuals?

[00:15:50] **Dez Rock:** Are you talking about my staff or my customers?

[00:15:52] **Christophe Foulon:** Your customers because in order to be able to utilize a good SIM or any [00:16:00] other defensive product, you have to start



potentially from a threat model approach and kinda take that adversarial approach and then go back and go, okay, so well, this might happen, so let's look for this.

[00:16:11] **Christophe Foulon:** Let's ensure that we log this or we do. How do you go about and educate your customers on the need for your product?

[00:16:20] **Dez Rock:** Oh, I see. For starters, regulation is doing a great job and so is the, so are actual black hat hackers doing a great job at marketing on the reason why we need security.

[00:16:28] **Dez Rock:** They're like, I couldn't market the way they do for me. And also regulation as well. So now we're getting more regulated because we have data. It used to be just banks, you need, if you've got money, you need to be secure. That was the way it goes now. Hospitals are being targeted, universities are being, like anything where there is a lot of information are being targeted and used in inappropriate way because data is valuable.

[00:16:49] **Dez Rock:** It's as simple as that. Like your health records are valuable as well. So there is an obligation, there is a moral obligation for the companies in those areas, or any industry really, where they're holding data, [00:17:00] personal data about somebody that they need to protect them. That sells itself, right?

[00:17:05] **Dez Rock:** That's, that sells itself. So it's a matter of what tool you use, and here's where we get into how people make these decision. And I'll be frank with you, people just usually Google or use what everyone else is using. Usually the Gartner quadrant, you know what everyone else is using. And you know what's really interesting, Chris?

[00:17:23] **Dez Rock:** All of those breaches that you hear in the news, they all have security software and yet none of them are working. And that question is not being asked like, what were you using that failed you? And now you have a breach, an embarrassing breach that you have to, do a pr, recovery. What were you using?

[00:17:39] **Dez Rock:** How did you make that decision? Who made that decision? Will you reconsider that software? Do? Do you know what I'm saying? It's if we were to use an analogy, the one I like using about the security in a house, for example, or a building, right? You employ security guards to monitor your building and you get robbed.

[00:17:56] **Dez Rock:** Do you sit there and say it was bound to happen. Or do you sit [00:18:00] there and say, who did I, who was protecting us? Like where is their responsibility in all of this? Were they, did we leave a door open? Did they leave it? You know that, so that's what you're asking yourself. You would reconsider and maybe up your security.

[00:18:13] **Dez Rock:** That's something that would happen naturally. Like your brain would go there. I don't know. Because we all have a saying in this industry, you in this industry for long enough, you know that no one gets. For using a Gartner Quadrant product. Okay. So it's a safe bet. Is it a secure bet? No. If it was, we wouldn't have the breaches.

[00:18:32] **Dez Rock:** We did.

[00:18:32] **Christophe Foulon:** Yeah. I'd go there. And then I'd also say, I'd also look at understanding have you properly used the software? Have you properly configured the software? I agree. Have you tested the software to. Ensure that it does what it says it does.

[00:18:50] **Dez Rock:** I agree, but I think definitely, I think that exactly.

[00:18:53] **Dez Rock:** But there's also software limitations as well. So if you are, yeah. Got a price point. So for example, we're talking about C, right? Because I, [00:19:00] this is in my area that I know a lot of. If you are talking about price per node, right? So endpoints, you're being priced. You all of a sudden are now making fiscal decisions on what you're going to protect.

[00:19:11] **Dez Rock:** Now you tell me, Chris is. Securing your network or are you picking and choosing for the best of your knowledge? So I'll secure that door, that window, that door, but the back door, I'm just gonna hope no one gets in there. Because I can't afford to put a lock on there to use the analogy again. So that's not, so here's what we say. That's not security. And the reason why we say that is because we have been red team for so long, we know exactly how to find that damn backdoor, right? So that's the difference, is that it's not about just securing. Knowing how to configure, although I agree with you, that's a really big and important point that you must know how to use the software that's put in front of you.

[00:19:47] **Dez Rock:** But also is the software, is the pricing point of the software allowing you to protect your entire network? Yes or no? And if you don't put a sig ring around your entire network, are you secure? Yes or no? Ooh,

[00:19:59] **Christophe Foulon:** [00:20:00] Now that's an interesting point. We're now in a world where everyone's remote.

[00:20:04] **Christophe Foulon:** So a ring around the network is hard cuz everyone's everywhere. Absolutely. Now we get into risk-based decisions. Correct? On understanding what your, what are the most valuable nodes to protect? Correct. Because they hold the most sensitive data. And then the ones that might not have anything on there, they might not be critical infrastructure.

[00:20:27] **Christophe Foulon:** Those might go unmonitored, but you ensure that your critical assets get that protection. But

[00:20:33] **Dez Rock:** that's not security. That's. Wishing hopes and prayers. That's what that is. And I'll tell you why. Because the, remember the great role of China was never infiltrated by an army. It was infiltrated by bribing the guard at the door.

[00:20:46] **Dez Rock:** So it's the weakest link that will actually let you in. True. Actually, I'm not even sure if that analogy is true, but I've heard it so much. It must be. But Point is that, again, I reiterate reason why we double down on this. If you're not protecting everything, you're [00:21:00] not secure is because of our red team days, we would get in by the most unlikeliest manner, right?

[00:21:07] **Dez Rock:** So if we were doing that, And then we, and we, now we've switched to Blue team, right? So we say, here's a product in all good confidence. We cannot offer a solution to people and say, here you go. It's the best we can. You know what I mean? Just like you said, the most important data centers, just protect those and you're good to go.

[00:21:25] **Dez Rock:** That's not secure. So if you've got a worker working from home, accessing that data, or whatever, then you do have a vulnerable point right there. So that's okay. So we are getting to, product features and I know we don't need to go there, but that's not, we would, I would say that's not secure, that's not security at all.

[00:21:43] **Christophe Foulon:** And similar to that, but saying now taking that approach and going zero trust, where when you design your architecture, you design it Lease privilege, lease access, all these things. Yes. Then does the same [00:22:00] analogy still apply?

[00:22:01] **Dez Rock:** So yeah, we would have, we layer our, if you're talking about our product, we layer our our, our privileges for sure.

[00:22:06] **Dez Rock:** But we also have Agents as well. So you know when you were talking about remote situations and stuff like that, which becomes a nightmare for people because you're literally looking at different tenants, like different areas and that's where we shine, right? Big data in all over the places where we shine.

[00:22:19] **Dez Rock:** Cuz remember we modeled this after Blue Scope. Remember that? They were like everywhere. So small data everywhere, but collectively big data. So you know, security. By even putting an agent on a local small area, could be a home office, could be anything. So that becomes your collection point if there's a disconnection.

[00:22:38] **Dez Rock:** So that's redundancy there. If there's a disconnection with either the internet or power all your dialogues are still there. So when the connection is resumed, those. Are uploaded to your scene. Now that is, that's what we call, the double redundancy and all sorts of security measures that we think of because of exactly those situations, right?

[00:22:57] **Dez Rock:** So exactly those. That's I guess what makes [00:23:00] us uniquely different. We're constantly looking because we are constantly looking at holes in our own software, right?

[00:23:06] **Christophe Foulon:** Yeah. So a, another approach I've worked with companies. There's using products like this for compliance. And then there, there's, using products like this for value add.

[00:23:18] **Christophe Foulon:** Yep. It. The origin story of many seams were they weren't security products to begin with. Correct. They were big data analysis products. So how do you, what sort of use cases have you shared with customers where, okay, obviously it becomes a value add versus a cost center.

[00:23:37] **Dez Rock:** No, I agree because there's some people who would identify a seam as a d, searchable.

[00:23:41] **Dez Rock:** Database, and that's not what a CM is. A CM must have SOAR or X D R capabilities these days, right? So it actually has to do something rather than just collect data, because by the definition it's a incident event management software. Now you have to manage the DAM events. You can't just there's a database, let me just serve search it.

[00:23:59] **Dez Rock:** Do you know what I'm saying? It's like [00:24:00] just by, its very definit. There's a lot of people calling themselves a sim provider that

are not. So the value add comes from, and I do have an example of one of my customers who has C Monster. They, been using it for quite a while and they had a phishing attack.

[00:24:14] **Dez Rock:** A what do they call it when they want money from you ex ransomware, right? Yes. So they had a ransomware attack and the same with the X D R capabilities. Shut that down immediately and was notifying and notified The operators immediately so that it knew what was happening.

[00:24:28] **Dez Rock:** It was smart enough to know what was happening and it shut it down. And so here was an issue that would've been newsworthy. Absolutely. That turned into an ordinary day. It was like the security product did what it was supposed to do. So that is a value add right there. So to use the example of collecting data.

[00:24:44] **Dez Rock:** Now you said a lot of people use seams for compliance. Because you know you're being forced to, right? That's not because you take security seriously. So I would argue that if you hold people's data, you have an obligation to take security seriously. And [00:25:00] only by doing it because you've been made to, it's the open market, right?

[00:25:03] **Dez Rock:** There will be people out there who will offer security and people are becoming a lot more wise with that. People will becoming a lot more like intuitive who's holding my data? Where is that? Where's that? So just being compliant is a rather relaxed position to take. Yeah.

[00:25:17] **Christophe Foulon:** And how do you help your customers move from.

[00:25:20] **Christophe Foulon:** Security for compliance to security for that moral obligation minimum spend versus really achieving something

[00:25:30] **Dez Rock:** actionable. So that's the core of exactly like when you talk about the heart and core and the soul of the company. Exactly. That we did not want security to be gate kept by price. We.

[00:25:40] **Dez Rock:** Thought if we were going to do something, we, it's almost like democratizing security, right? It should be for everybody. So the price point is the one we attacked. Cause we knew that was the reason, the gatekeeping reason why people would not protect everything. So when you are with us, you are not just protecting for compliance.

[00:25:57] **Dez Rock:** You're literally, you have the ability to protect your  
[00:26:00] whole entire network. Now, by doing that, you are protecting your  
whole entire network. We're not letting you, we're not asking you to. Yeah. So  
that is your biggest benefit right there. You're not choosing to say, oh, just the,  
just these bits, just, which is, let's face it, the reason why we do that is because  
price, like it's costs a lot, right?

[00:26:18] **Christophe Foulon:** Yeah. Wow. We've gone from leadership to  
leading in security does, thank you so much for coming on. But before we go,  
any final advice you wanna give to future cybersecurity leaders?

[00:26:31] **Dez Rock:** Ooh. Find yourself a very good mentor. And yeah, that's  
it. Find yourself a really good mentor and o okay, so it comes down to the  
person in the arena.

[00:26:39] **Dez Rock:** Only take advice from those actually in the arena, not the  
people in the peanut stands telling you they can and can't do it better.

[00:26:45] **Christophe Foulon:** Wow. Des thank you so much. Really  
appreciate your time for coming on another episode of Breaking Into  
Cybersecurity Leader. Thank you for having me.