Heather (00:03):

Welcome to the Hurricane Labs Podcast. I'm Heather, and today I'm chatting with Tom, Roxy, and Dusty about the cybersecurity skills gap and what we can help do to bridge it. To kick us off, Tom, you were talking a little bit earlier with me about some pain points and areas of struggle that learners face could you tell us a little bit more about that.

Tom (00:34):

Yeah, absolutely. So I think there's a lot of different areas that are kind of interesting for this, and it's something that I see both sides of and also interested in hearing how the rest of you on this discussion feel about it. But kind of one of the challenges I see is being well-rounded in this industry, it's really easy to get super focused on one aspect, whether that's technical or whether that's something else. And then professionally we're asked to do so many different things in this industry. It's hard to be able to accomplish both. So a lot of times I'll see people coming out of school or being in school and have a really heavily technical focus. And they'll be really sharp in different technologies, they'll be good at programming, they'll be good at doing security assessments, whatever, but a lot of times you put those people in front of a manager or a client in they'll lockup and not know how to have that conversation with another person, how to relate those technical concepts to someone else. Likewise, I'll see people who struggle the other way. We they'll have a little, have a very strong interpersonal communication background and be able to have communications with other people, but they'll struggle with knowing the technologies or having enough of the technical background in order to be successful and relate with some of the other people on the team. So I'm not saying everyone has to be, you know, equally strong in both, but having a working background in both of those is definitely really helpful.

Roxy (02:11):

Yeah. I mean, that's, that's certainly true. We have a lot of gaps when it comes to things like ethics as well. I know that it's very common for people to be aware of the technical aspects, but then when it comes to things like vulnerability disclosure, for example, it seems like security professionals can't agree on vulnerability disclosure. And there's also is everyone reading the NDA's that they're signing? Is everyone familiar with what they can and can't disclose? I mean, there's just a whole bunch of various topics that don't really get touched in technical training. And also working with clients like you mentioned, Tom, some people are really at working with clients and working with other people.

Dusty (03:03):

I mean, especially with being able to speak and explain your findings is extremely important. You can be the best red teamer or whatever, but if you can't explain how you exploited something, it makes it a whole lot harder to learn from it and improve the situations. If you aren't able to explain and speak to non-technical people about what the issues are.

Roxy (03:33):

One of the things that I really struggled with in the beginning was when I did something wrong or when one of my coworkers or my company did something wrong and we had to admit it to the client. That was very tough for me in the beginning because I was anticipating the client being upset with me personally, even if I didn't actually do it. And so I had to learn how to communicate in a way that just explained simply what happened and what we're going to do to fix it. That's another skills gap I think that we have is just admitting that something wrong happened and knowing the process to make the client feel like we actually are doing something to fix it.

Dusty (04:23):

I also feel like that can be helped by having leaders and mentors that are willing to share their own failures so that it doesn't become an atmosphere where you're afraid to fail. But knowing that whoever's training you or are mentoring you has had their own failures can help to make that burden less.

Tom (04:46):

I think that's also a case where good management really helps too. You have a situation where a manager, a bad manager will say, 'Oh, this new person screwed something up. That's their fault.' A good manager is going to say, we ran a new initiative and we're working to resolve it, and not make it the fault of the person, but the fault of the organization and turning that into a learning opportunity for the person who's new. Because that knowledge that, you know, if something happens, your management has your back and is going to help you address any issues that come up, that's going to make a big difference in you being confident to handle those situations and try new things and not be afraid that you're always going to face consequences for making mistakes, as opposed to learning from them.

Dusty (05:32):

A part of the skill gap can also be either a lack of in-house experience or lack of trust in your senior people to be able to train new talent or new employees, to a point where they're self-sufficient. You hear so often about entry-level cybersecurity roles that are looking for either a good amount of experience or just unreasonable expectations for entry level positions. And that makes me question whether or not there may be a lack of trust to train up people who don't have that experience.

Heather (06:14):

So like new people coming in are expected to know things without having been trained within the company, instead of accepting that you have a new person coming in with no experience, and you're going to have to train them on certain procedures.

Dusty (06:28):

Exactly.

Heather (06:29):

Something that I've heard some folks talking about is when it comes to investing in training opportunities, there seems to be a discrepancy in how much is invested in red team versus blue team. Have any of you seen that in your experiences? Yes, actually, I've seen a lot of training available for red team and a lot of emphasis on red team. And I mean, it is the most glamorous side of cybersecurity. It's the side that a lot of people are attracted to, but when it comes to blue team training, and I guess this might be because blue team is a encompasses more topics than red team, but red team training, you can find all in one package, blue team training, you typically have to seek out different pieces of the skillset that you're trying to develop. I'm sure there is a blue team course somewhere out there, but it's more common to see when people are talking about cybersecurity training, it's mostly red team. If it comes together in a package.

Tom (07:42):

I mean, a lot of that comes down to what gets all of the press too. And what people talk about. It's like you break into something everyone's going to be talking about that you're giving talks places and all that fun stuff. If you are stopping something, you're probably not going to get the same level of attention, although different places do cater to torture in that information. I find reading about that stuff. Fascinating. It's just not as general interest as so-and-so broke into this thing and caused all this stuff to happen.

Dusty (08:14):

I also feel like it's easier to create a training for red team because it's easy to create a vulnerable sandbox for people to hack, but it's much harder to create a realistic hacked environment for a blue team to go through and really get a enterprise feel of a blue team, because it's hard to recreate the noise and regular activity that you see in an actual enterprise in more of a sandbox.

Roxy (08:48):

And we have NDAs as well. So a lot of people on blue team can't even share what they're doing. Blue team is the silent–.

Heather (08:58):

The unsung hero.

Roxy (09:00):

Right.

Heather (09:01):

Dusty earlier you mentioned unrealistic expectations that a lot of the community and employers have about what a potential employee's home life or college experience might be. Do you want to tell us a little bit about that?

Dusty (09:16):

Yeah, in the more outward facing InfoSec community, it always seems that in order to get into InfoSec, you need a home lab, you need to be doing a ton of stuff on your own, and you need to really almost dedicate your life to getting into and staying and in InfoSec where at the end of the day, this is still a job that you're working for an employer, and there should be a healthy home life balance that a lot of times feels like you almost can't have with the industry kind of presents itself as being. I know I've fallen into that a lot where I've spent more time than I should have on outside stuff at home, like on working on work stuff at home, where you can't apply that standard to everybody. Because at the end of the day, this is still a job, not your life.

Heather (10:13):

I mean, some of that can be pretty expensive too, I imagine. Not everyone's going to have the resources to delve quite that deeply in their personal life when it's not being work provided equipment. Right?

Roxy (10:24):

Yeah. And another thing it's not just a matter of money resources, but time is a resource as well. I'm a single parent and I just did not have the time to set up a home lab. I have never set up a home lab to this

day. I barely touch the router in my home. So some of us just don't have the time or the money or the resources to set up a home lab or do stuff on our own. There's also the issue of courses that are way too expensive, way too–even though these courses are really, really good courses. And I'm not disputing the quality of the work. It's just, when we're talking about bringing people into the field, I can never recommend that people take a SANS course. I have never told somebody coming into the field, 'Oh, you need to purchase a $3,000 SANS course or $2,000 or whatever it is.' I know that they probably can't afford that. If they're trying to get into the industry, they're probably not making enough money to be able to afford that. And they were always like a one-week, in-person course in Arizona or something. And I just didn't have the time or the money or the ability to be away from my kids for a whole week. There are a lot of obstacles like that, and we have to do our best to remove those barriers for people.

Heather (12:09):

I think that also ties back to employer investment. Like this sounds more like something that if companies want their staff to have this training, then it should be something that companies are willing to invest in to get their staff this training.

Roxy (12:25):

Oh, absolutely. There are employers that will pay for your certifications. If you can get an employer to pay for it, like absolutely do that. It's just not always an option. And it seems like employers don't always make it a priority when this is an item that if they budgeted for, they would be so much happier with the level of expertise that their level one security analysts have. Instead they're expecting them to have all that experience before they're even hired. And there's so much value in training someone specifically for your company's needs.

Heather (13:13):

So to address some of these pain points with the skills gap, what can candidates or learners in InfoSec do to help bridge this gap?

Tom (13:25):

One of the things that CPTC challenges students to do is to kind of step outside of the comfort zone of just being technical and having to communicate professionally, behave professionally, have conversation with management type individuals and all those different skills that you don't necessarily get if you're doing a college program focused on like the technical side of things. So I know it's called a collegiate pen testing competition, but I really try to position that more as a collegiate consulting event, where you learn how to do all kinds of those different things that you wouldn't necessarily do outside of actually working.

Heather (14:03):

And in addition to courses and programs like CPCT, learners could also go like seek out mentors, right? So what sort of things should they keep an eye out for when seeking out a mentor?

Roxy (14:15):

It's really hard to find good mentorship in cybersecurity, because I guess this comes from my experience as a feminine person. I'm sure it might be different for other people, but there are a lot of predatory mentors and you don't really find out why they're so excited to mentor you until it's already like, 'Ooh, I

need to block this person.' That's something that happens sometimes. And so, you know, it's also a matter of like, is that mentor actually going to give you the resources you need? Like, are they knowledgeable in what companies are looking for and what they're hiring, is that going to be helpful to you? People gravitate towards looking for a mentor because the lack of accessible low cost training.

Heather (15:09):

Roxy, what about gauging training or mentoring opportunities, whether it's like during the hiring process or as an employee in a company?

Roxy (15:19):

Well, if you're already working somewhere or you're already interviewing somewhere in the interview, you can ask them for what's a typical training plan or what's a typical career path for this position. If they have something planned out and they can tell you exactly what the training plan looks like, or if they can tell you, once you hit these metrics, we're going to give you this type of training, something like that, some sort of idea, or outline, then you can be assured that they actually have a plan and it's actually for everyone. But if they start saying things like, well, it just depends and you can't really tell like what the metrics are then it's like, okay, well, I don't know for sure if I'm going to be one of those employees that they invest in, but if you're already at the company and you're trying to figure it out, one of the things that I started doing, I asked my manager as a security engineer, I asked him, what type of training do you think I should be provided? He answered that I should be getting Microsoft Office training. And so as a security engineer, so I was like, okay, I guess I'm not getting that Linux forensics training that I've been promised for over a year.

Tom (16:41):

I'm guessing the office training, wasn't trying to embed things into macros, right?

Roxy (16:46):

No, no. It was because we used Microsoft Excel and I needed to learn how to make graphs or something. It was something like that. That was just like, okay, that's, that's not the training that I was asking for, but okay. A lot of times, if you're already at the company, you can't really do a whole lot if they're not willing to train you or invest in you. So there are other companies that will.

Heather (17:16):

What sort of advice would you give someone who is working for a company that is supporting their learning adventure? Should they just go through like systematically and just like start hitting each of the topics and, you know, learning everything they can?

Roxy (17:29):

That's actually something I forgot to mention was even before you work in a company, picking a specialization is super important because cybersecurity is so broad that if you're just trying to train yourself in the general, the types of things that you see on the CISSP, for example, the CISSP covers a wide range of topics, but it doesn't cover them in depth. And so finding a specialization where you have in-depth knowledge on something can make your resume stand out more and different companies have different goals. So it's not a matter of picking the best specialization. I would say, pick the one that you think you can perform well in. So if you're really good at investigating things, or you're really good at

forensics type stuff, just go for forensics, you know, because there's going to be a company out there that's going to have that as their goal for someone to hire. So you need to look like more than just the average entry level, you know, cybersecurity engineer.

Heather (18:40):

Now for the flip side, being on the other side of the desk what advice do you three have for the companies who are looking for potential candidates? Where should they start?

Tom (18:53):

Probably that job posting itself is going to be the first place to start and writing it in such a way that what you're asking for is first thing possible. And then also make sure that you're not trying to inadvertently exclude entire groups of individuals basically by your job description. But I know when I say, if something's possible, we always make the joke of, you know, 10 years of experience with server 2018 or whatever. It's just something that physically cannot exist. That is something I know it's a joke as much, but you do see cases where there are job descriptions that are looking for things that just practically can't happen. So obviously you don't want to do that, but to even look more seriously as if you're looking for an entry level position, you shouldn't be looking for five years of experience. Is that just not practical in someone with five years experience is going to pass over that opportunity and look for something else. Because quite frankly, it's not an opportunity.

Roxy (19:55):

And you never know what kind of ideas you might have from someone new that's coming into the company. Even if even the lack of experience can be something that you can use to better the company, because they're coming in with a fresh mind and they aren't set in certain ways yet. So in some cases, a skills gap can actually be an advantage because you can go through the process of training that person and they can look at documents and tell you like, 'Oh, okay. Actually between step two and step three, we need to add more information in here because that's not clear.' For someone like me, who's been in cybersecurity for so long, I might look at that and know exactly what's between step two and three. But if somebody that I'm training, it's not very clear to them, you know, then I need to fix the documentation and I need to fix how I'm training people. So actually having people come in with a skills gap can be a huge advantage if companies are willing to listen to them.

Tom (21:06):

Yeah. And like when I'm writing up documentation, I like to have people that are not only peers review it, but also people who aren't familiar with the process review it and run through that and just tell them, let me know anything that doesn't make sense and we'll figure out where the gap is in there. And then you just end up with better processes all around.

Dusty (21:26):

I also feel like it's important for companies to be willing, to take a risk on someone that may be more of a challenge up front, but has the potential to be a lot more rewarding down the road. Some of the best people I've seen in InfoSec did not start an InfoSec. They came from other fields and just had a knack to see and do well in the career do well in InfoSec. And then if you do hire that way, don't neglect it. Continue to build, not only yours, but also the people below use skills up.

Roxy (22:07):

Absolutely. Like you can't just hire someone say that you're going to train them and then train them for one month and neglect them the rest of the time.

Heather (22:16):

So now when it comes to mentoring, what should the mentors keep in mind about their role in helping someone gain footing and InfoSec?

Roxy (22:24):

So when it comes to mentoring someone or trying to train someone up, a lot of things that people don't consider is like we talked about earlier with the SANS course as being too expensive. There's also the fact that the person that you're trying to mentor or train up, maybe doesn't have the resources to even, to even learn what, what you want them to learn. So sometimes you'll have to provide those resources, provide the book that they need to read or provide the tech that you want them to set up in their home lab. You can't expect everyone to have the same resources that maybe you had, even though it was easy for you to do something. Something like a 10, $20 book is something that would have been an obstacle for me 10 years ago when I really didn't have any money. So you may have seen me, some people may have seen me on Twitter, giving books away and, you know, people used to give me Amazon gift cards, just so that I could give books away. And I haven't done that recently, but there are still people that talk about how that one book helped them or changed things completely for them because they wanted to learn, but they just didn't have the, you know, 30 or $50 to drop on, on a book.

Heather (23:52):

What last piece of advice would you like to give to anyone looking to get into InfoSec?

Roxy (23:57):

I just want to encourage people to, you know, it, it does look like it's difficult to get into cyber security, but you know, I just want to encourage people to keep going and keep trying.

Heather (24:08):

Alright. Well, thank you very much for partaking in this discussion today. We appreciate it.

Tom (24:15):

Thank you for having us, Heather.

Roxy (24:16):

Thank you for listening to me rant.

Heather (24:19):

Anytime. And that's all for today. Thanks for joining us and be sure to stay tuned for our next podcast, where I'll be chatting with two of our pen testers about how they go about attacking a network and then application. Until then, stay safe.