Speaker 1: Welcome to the Hurricane Labs podcast. I'm Heather, the technical writer here on today's show. I have three members of our SOC team with me to share a little bit about their career journeys, to answer some of the InfoSec questions we've been asked to be a social media and the talk about how they deal with burnout. Welcome Roxie, Tony and Kurt. Thanks for joining me today. Why don't you guys go ahead and introduce yourselves.

Speaker 2: Alright. My name is Kurt Wolf. I work in the SOC at Hurricane Labs. I've [00:00:30] been here for about three years now, total, um, two years was doing incident response, uh, for a year that I was one of India team leads. So in charge of running the, uh, SOC incident response team and, uh, for the last about year or so, I've been doing, um, psych architect work.

Speaker 3: Okay. I'm Roxy. Um, I started out in cyber security in 2013 as a network security analyst. I've also been a, sorry, I've been a cybersecurity [00:01:00] engineer in a SOC as well. And currently I do vulnerability management, pure Hurricane Labs.

Speaker 4: Hey everybody. My name is Tony Robinson. I am a member of Hurricane Labs, a tier one, or tier three SOC team. One of my works that I did while I was here was the book building virtual machine labs, a hands on guide. Um, so I've got about, Oh, I'd say about eight years experience in various information security roles.

Speaker 1: Great. [00:01:30] Thank you all for joining me today. Uh, you know, before we get started into some of those meatier SOC questions, one that I've frequently heard asked is how do you even get into a cyber security role? Uh, so Kurt, what has your career journey been like and how did you come to be part of a SOC team?

Speaker 2: Uh, so far mine will probably be on the shorter end compared to both Tony and Roxie, but, uh, I actually was out of college now two years ago. So I interned a year at hurricane. I was one of the lucky [00:02:00] ones that, uh, got into cybersecurity out of college. I did go like strictly like straight forward into, uh, cybersecurity itself. So like my bachelor's was in like network security. I think really what got me into it out of college was doing all of the extracurricular activities and being extremely involved.

Speaker 3: Um, I did not have a lot of experience in tech. Um, so I spent from 2011 to 2013 doing tech support [00:02:30] and also becoming very active in the local cybersecurity community. Um, I joined 2,600 and our local Def con group. And I also spent a lot of that time studying. I had to self study because I, I, wasn't going to college. There's a lot of resources online that are free, that has to do with cybersecurity. And I ended up getting a security plus certification, um, from, I [00:03:00] was a security engineer at a very large cloud hosting company, which gave me a lot of experience as well with different types of situations, besides just alerting and tuning. I ended up at Hurricane Labs actually, because I talked to Tony about working here. And so, um, Tony had great things to say about Hurricane Labs and I just ended up here, uh, a year [00:03:30] later. So I'm very, very glad to be here. And I've been here for three years.

Speaker 4: I have a crazy background. I've kind of gone all over the place. I got an associates degree at Henry Ford community college up here in Michigan. And then I went to school at university of Detroit mercy. I went through, um, network administration in comp info systems. So I was kind of dead set on being an it guy and being the CIS admin for most of my career. And I was pretty happy [00:04:00] with that. Then I, uh, went into a bookstore and I found a copy of this book called the 2,600, the hacker quarterly. And I was like, man, you can get paid to break computers. That's amazing. So I started reading up on that and I started ever so slightly changing my career path. You know, at first I wasn't aware of like any, uh, social gatherings, like hacker conferences or local meetups or anything like that.

Speaker 4: So I kind of just was drilling on security, the certifications [00:04:30] for a long time that, uh, I had an opportunity where I moved out of Michigan and went over to the East coast and I worked for a couple of security companies out there. Um, at one point I was, uh, working for the intelligence community and other point I was doing, um, intrusion detection work for a large power company. And then, you know, it was completely by chance, but, you know, thanks to the people that I had met and, um, the different security events that I had gone to, and, you [00:05:00] know, all the networking, I had a friend who was working at hurricane when I was looking for a job and that's kinda how I got here. Um, bill and Steve, you know, some of the, uh, the senior members on the hurricane team were saying, Hey, we could really use some of your talent.

Speaker 4: You know, why don't you come interview with us? And I said, absolutely. And you know, here I am about three years later and I'm still really happy here. What's been the most interesting part of being in SOC for you, uh, feel [00:05:30] from my perspective, like having come from a bunch of different security operations groups, it's, uh, you know, not really knowing whether or not alert is something that's going to be a major deal breaker, or if it's just, uh, I need the tune, this thing again, it's real interesting to have a large body of data to take a look at and poke and prod and be able to ask different questions and, you know, kind of state your curiosity. That's one of the more interesting to me is being able to, [00:06:00] um, you know, do the Sherlock Holmes thing, put on the thinking cap and, um, ask different questions of your data.

Speaker 1: Kurt, what have you enjoyed the most about working in Hurricane Labs, SOC department?

Speaker 2: Uh, so as far as working in the SOC, the things I probably enjoyed the most are, uh, first off I enjoy the people I work with. Um, I feel like we have some pretty good banter in the office. Uh, definitely keeps the spirits up, but not only is it an enjoyable, a good amount of the time, uh, if when I work with is pretty knowledgeable. [00:06:30] So as far as being in the office and even out of the office, as of recently with all that code stuff going on, um, it's nice to be able to bounce ideas off of people that are pretty intelligent with what we're working with, which is a spunk most of the time. That's one of the major things that I really do enjoy is the environment, the atmosphere. The other thing I really enjoy actually is how the company is kind of broken down. As far as management level, it gets pretty flat company. And I really enjoy the fact that everyone kind of gets heard.

Speaker 4: I love hurricane a, it's a very positive [00:07:00] environment. Um, and if you have anything to add any suggestions they're taken seriously, if you have any concerns are taken seriously, and I gotta say it, bill and Steve and everybody else, you know, a part of the senior team, they're really good at taking care of us. And you know, so long as you're doing your so long as you're doing your duties, they are very happy to reward you for doing a good job. And I just really appreciate the positive environment.

Speaker 3: Oh, absolutely. Because I've actually been in [00:07:30] the past at four different cybersecurity positions of four different companies. And that's because the environment was not good for me, but here at hurricane lamps, I never feel like I'm being taken advantage of, or I'm not being recognized from a newbs perspective. This has been a fantastic job.

Speaker 1: You know, I've mentioned before, I've only been here one year. I was an English teacher for about 10 years prior to this. And this is a very different world. It's [00:08:00] been like, you all have said, it's been a very positive environment, especially for someone who has had very limited experience working in technology. There's been a huge learning curve for me here, but everyone's been like incredibly supportive. It's really a really great environment. So like I mentioned earlier, we've received a number of questions from folks on social media, especially Twitter. And they are hoping that you all could help shed some light on some things. So first up, Roxy, I think you [00:08:30] expressed interest in this one. Uh, what does it mean to escalate an event to an incident and how do you determine whether or not to escalate an events? There, there are a few different things that can prompt you to escalate the event.

Speaker 3: Um, a lot of time it has to do with just the experience that you've had before. As you gain experience, you understand more, what is normal expected and what is a non anomalous behavior. If there's any sort of behavioral [00:09:00] anomaly then is something that you most likely want to escalate. If it looks like something that is harmless or something that your client does not qualify as important to them, because every client is going to have different expectations and different needs. So if it's a behavioral anomaly that looks suspicious, or it looks like something that needs to be investigated, or if it is something that the client has specified [00:09:30] as important for them to know, that would be a reason to escalate. And another reason to escalate is if you see something new that you think needs a little additional investigation, even if it might look like it's not going to be harmful, you may want to investigate further just to make sure because sometimes new threats and new new types of attacks come to light that could end up being completely harmless, but you have to investigate in [00:10:00] order to understand whether or not it is something that you need to escalate.

Speaker 4: Yeah. To add on what Roxy is said so far. Um, the way that I've always kind of looked at it as, um, when you're looking at an event, you know, uh, most of my background has an intrusion detection systems and, you know, um, having definitions for what is considered on unusual or anomalous traffic and having alerts triggered off of it. So a lot of my background is, well, this is anomalous, or at [00:10:30] least the IVs thinking, it thinks that is what other contextual data do I have to work with. And if I can't answer the question, are there appears on my team that I can bounce the information off of

like, Hey, I got this alert from this client. Do we have any contextual data that I can look at in Splunk or another data source to kind of say, you know, determine whether or not this is something that would involve escalating into an incident and, you know, getting the client more involved in

Speaker 2: One bit, I would like to add that's kind of different from our SOC compared [00:11:00] to others. And Roxy definitely brushed on this a bit, but it really does depend on what our customers and clients are asking for as well across one customer. You might have a specific alert that they really aren't too worried about. That might get turned into maybe even a report or something that's sent once a week, where you might have a separate client that might view the same alert is a higher critical event because they're having issues with that currently in their infrastructure. So please from Hurricane Labs kind of perspective, working with a bunch of different customers [00:11:30] and clients, severity of notable events that do come to us really do vary depending on the customer's wants and needs. So

Speaker 1: Tony, when you were triaging events, how do you avoid spiraling down the proverbial rabbit hole, so to speak and keep focused on the issues at hand? What, what tricks do you use to stay focused?

Speaker 4: Oh, well it's kinda for me because, um, you know, like I said, I'm kind of, uh, guided by my curiosity. I was like, I found this new piece of contextual [00:12:00] data. Uh, is it, or is it not related? I think one of the tricks that I use to kind of try and help guide me along is if I have a specific timeline for an event or an alert or some sort of an investigation that I'm doing, um, I'll stick to just that timeline before I start theorizing about, well, this might have gone on sooner or this event that's outside of that timeline might be related. So I try and stick to a specific timeline.

Speaker 4: Like if I found [00:12:30] an alert or event, I try to stick to no more than like maybe five to 10 minutes beforehand. You know, if I find evidence that indicates that there's more activity outside of that timeline, then I'll deal with it. Then, um, the other thing is, you know, just like I said before, I also rely heavily on my peers. You know, I'll ask them questions, uh, say, what else do you think I should be looking at? What other angles should I approach this from? Because everybody has a different perspective or a different way, they consider investigating things. So having [00:13:00] somebody else's feedback on what you're doing and whether or not you're going in the right direction or what direction they would take it in is invaluable. In my opinion,

Speaker 2: Totally agree with what Tony said and just add on to it. Uh, I take very, maybe I don't even think about it sometimes when I am working alerts, but I'm always kind of looped back when I'm doing the larger investigation thing. Who, what, where, when and why. And that that'll kind of keep me on paced and not go down per, like you said, a different rabbit hole or to kind of get away from what I'm looking at. And Tony mentioned like staying maybe 10 minutes before and after the incident [00:13:30] took place, which is good to kind of stay focused on the event, but sometimes you might dig down a while and realize that, okay, you come to a user or an IP address or an IOC of some sort that might've been taking place for a while, and then you might actually have to change up

your timeframe. So as far as the prevent yourself from going down rabbit holes, it really does kind of matter the investigation that you're looking at. If it's really broad, if it's over a large timeframe or if it's something specific like an IDs event where you're looking at a specific thing of network traffic, [00:14:00] that's the, those are two separate investigations. And in my view,

Speaker 3: No, for me, something that I do. And in addition to what, um, Kurt and Tony had mentioned is that I keep in mind the appropriate times that I should be spending on each type of event. So it's very, very easy to go down a rabbit hole on a low priority event, just because you're curious. And so what I'll do is I will stop myself and work on some of the higher [00:14:30] priority items first. And then if I have time, I'll go back and put more, more into that lower priority item. But if I can close it out a lot faster with the appropriate amount of information for that type of event, then I will do so. And I'll tell myself if I have time, I can go back later and I can look at it. And I can maybe some additional information that I can add on later, or I can send in an email or I can, I can just keep in mind for next time.

Speaker 1: [00:15:00] Do any of you have experienced mitigating specific zero day exploits? And if so, how did you address it?

Speaker 3: I have had some experience there and I think the number one thing to consider is that when it comes to zero day exploits, there's often a, a panic that can set in because there's so little information, but it's important to take some time to sit down and come up with an action plan or to already have an incident response playbook, or some [00:15:30] sort of documentation that helps you work through certain incident. From my perspective, when it comes

Speaker 3: To dealing with a zero day exploits, obviously, you know, one of the most important things you can do is patch, but you know, when it comes to certain organizations, they have a lot of sensitive operations and they require change controls there's rules for these sorts of things, there might be changed freezes. You might have to roll out patches over time and to induce some sort of a rolling release program, [00:16:00] or one group gets the patch and then the other, then the other, and you find out problems along the way. The most important thing you can be doing is keeping an ear to the industry, experts like paying attention to us, cert or paying attention to your vendor when they're telling you that they're, there are these vulnerabilities out and about, and there's no patch yet. Typically they're also going to have some sort of a mitigation in place.

Speaker 3: Like, uh, I'll give you a great example from the beginning of this year, when we were dealing with the, uh, remote desktop gateway vulnerabilities, [00:16:30] one of them was for, or one of the issues was with Citrix. The other one was remote desktop gateway and the remote desktop gateway vulnerability. It was exploitable specifically over UDP. One of uh, was one of the issues. And it came out after a little bit of analysis that basically all you had to do is a plug before over a UDP for the desktop gateway application. Then that was a valid mitigation. You know, it's just paying attention to different researchers, paying attention to the vendor. [00:17:00] And what they're

saying, mitigations are, and or if there are methods for detecting it, I'm ensuring that you have those in place as well. You know, are, are there any tells them the logs? Are there any tells in the network traffic until the past can be deployed and tested successfully for your environment? So, you know, much like Roxie said, there are playbooks that are typically developed for this sort of thing, and you should be definitely following those. And if your playbooks don't involve, you know, reading what the [00:17:30] vendor's saying about the vulnerability they need, they definitely need to be updated.

Speaker 3: And if a zero day is out there and there's no patch by the time everybody finds out about it, there's typically some sort of work around or some sort of way of dealing with it. There's rarely an instance where you simply cannot do anything. It, so usually it will be something like this only affects this certain type of situation. So if you close this port or if you [00:18:00] don't need this service and you shut it down, then that's a work around or a way of decreasing the risk. If not eliminating the risk until a patch can come out.

Speaker 1: So we're gonna change gears a little bit. Um, you know, a lot of what we've been talking about today deals with staying focused while handling a lot of different tasks and details, and one issue facing many InfoSec professionals is burnout. Uh, Kurt, what are some of the things [00:18:30] you do to avoid this problem?

Speaker 2: Probably the best way that I've coped with it has been, have been a few things. First off hobbies are huge. And as much as it might sound odd, but outside of work, I feel like that's your recoup time to completely get away from the computer and it can kind of get your sanity back a little bit. So I really make sure that outside of work, that I have hobbies, I'm big into music. Teddy, try to go outside as much as I can when it's sunny, try not to have much screen time after work. [00:19:00] I feel like that's one huge, huge step into preventing like crew burnout out from not wanting to go to work the next day. That that definitely helps me a ton is as far as during the day when I'm actually working at alerts, there definitely were times where I would get extremely burnt out and I'd go get a coffee or talk to someone, obviously though this isn't always going to be an acceptable thing to just walk away from your computer. If something critical is taking place. And actually probably the best way I battled burnout when I wasn't able to take a physical break or walk walk around [00:19:30] the building a few times was actually a probably with humor, cracking jokes with my coworkers and trying to keep the mood up actually probably really was the biggest benefit and helped me the most with actually keeping on task while it might sound counterproductive, sometimes smiling and laughing and having some jokes thrown left and right actually can keep the mood up

Speaker 3: For me. Any type of burnout that I have experienced personally has been a result of poor leadership. And I'm not saying that that's the case [00:20:00] every single time, but just in my experience, I have seen management place, too many projects and too many expectations on one member of the team and that person will get burned out. So it's very important. If you feel like you have too many projects or you have too much work that is being piled onto you to either delegate it or address that with management and let them know that this is too much for me, there's nothing wrong with [00:20:30] being

human and being incapable of being a superhuman. And I've noticed that a lot of people that end up getting burned out are doing things such as putting Slack or HipChat on their personal phones, answering work emails after hours. The way I think of it is that if, if the company can't survive without me for, for one night or without me being able [00:21:00] to take my vacation, then that is a staffing issue. And that is potentially a training issue as well. It's all about finding a balance and understanding what your limitations are.

Speaker 2: I, I, I just want to touch base on the fact Roxy, if you brought up the phones and emails and everything after work, um, I think that's huge. I think it's extremely important to make sure that there's a, there's a split between work and your, your home life and everything else. And I couldn't agree more with that. I just wanted the second day, cause [00:21:30] I truly do feel it's important.

Speaker 4: And you know, it shouldn't be more than just words that are sent from the human resources team or from your management. They need to support your need to take a break and recharge. I mean, a good example prior to the pandemic, of course, and you know, maybe once a year, once everything goes back to some semblance of normal, I used to love taking a trip to Northern Michigan with my family, um, in the summer, like late June, early July. And it's an area where there's not even cell [00:22:00] reception for the cell carrier that we have. And it's the best time I could ever have is like I don't have cell coverage. And then I just throw my phone back in my backpack. I was like, I have no idea. I don't even care. So just to echo, if they said good work life balance is extremely important.

Speaker 4: Time, something I've seen among, uh, security analysts and security professionals out there is they have a lot of passion projects outside of their workplace as well. I'm not saying that you shouldn't have those, but keep those in mind when [00:22:30] you're dealing with burnout as well. Sometimes you just got to, you got to shell them for a little bit and enjoy the things that you enjoy the most, you know, just enjoy life once in awhile, get away from the screen, play video games. If you want to be at the screen still, you know, the root of it is to have a good work life balance in there and not just don't let those be words. And when it's the end of your shift and you're not on call, you know, log out, don't be afraid to log out. You're getting paid to be there for a certain number of hours. You [00:23:00] know, you can love your job. You can love your coworkers, but don't work for free. That's all I've really got to add to it.

Speaker 2: Uh, last thing I'm going to throw in there, cause Tony, you mentioned the, uh, at home projects and I find that funny, you brought that up. Cause, cause I mean, I have a server at home. I have a couple of different things, set up some VMs and I mean the it's the backend to my network at my house. So I do have to keep the things running. I admitted it a bit and uh, I laugh cause occasionally I'll have the power go out and I'll have to go and log in and turn all the VMs [00:23:30] on out of the SXI and it's sort of, so it's like, it's always at the worst times too, so I'll have the power go off occasionally and the power supply, I have backing everything up will won't last long enough and it'll beep it to me, things will turn off and I find myself getting really frustrated, like, and those are projects that like I enjoyed setting up, but then I find myself getting annoyed,

maintaining them sometimes. And I mean, well, it's a great learning resource. It definitely can be annoying sometimes to instill rope you back [00:24:00] into work when you don't realize it.

Speaker 4: Yeah. I'll bring up the funny story of my own. It was like I've got a ESX server in the basement up until I started, uh, right. Like doing a lot of writing recently, it sat down there and it was powered on for about a hundred days with nothing running on it. I was just like, Oh, well I got this thing here. I need to do something with it. You know, then I just, after a while I get the burnout just kinda subsided and I found my passion again and then started working on various side projects, you know? So I totally get ya.

Speaker 2: Yeah, no I've yeah. I've alternated. [00:24:30] There's times where all I'll go through and set up a whole Splunk instance to go through, set up free NASSCO through and get a whole windows environment set up and I might spend two weeks doing it. I'm loving it outside of work. And then I won't touch it for a year. So anyhow, any last quick pieces of advice that you would offer someone who is considering a career in InfoSec,

Speaker 3: The biggest and best piece of advice I can get is find your specialty. Because if you spend your time trying to learn everything, it's never going [00:25:00] to happen. Find something that you truly enjoy and specialized in it.

Speaker 4: Roxy just said there now don't, uh, don't look down at the certifications, use them as a way to kind of get a, a mile wide view of the different aspects and areas of information security, take advantage of that. You know, look at the different certification material out there and kind of use it as a springboard to see what interests you the most. Once you found your niche, be sure to network with your peers because they all have [00:25:30] different specializations and things that interest them. You can learn to rely on their, uh, their expertise and their specialization in the area that interests them the most in order to help support your career and you know, vice versa. Don't be afraid to offer your advice when they ask for it. And don't be afraid to ask, ask of it when it's something that's outside of your wheelhouse.

Speaker 3: And just to add to what Tony said, when you find out what other people's niches are, you can create a CTF [00:26:00] team, which is capture the flag and these are cybersecurity competitions. And when everybody has their own thing that they're good at, it makes a good team and you all can work together and learn together. And I've learned a lot from CTS. I actually learned more from CPS now than I do from reading with CTS. It's more like a game and it forces me to like actually learn something.

Speaker 2: Uh, last thing I'm gonna throw in all of this is, uh, I really feel like it's extremely [00:26:30] important to recognize that, uh, you're, you're not always going to be right. Um, there's going to be times where you're, you're think you're right and you're wrong. I think it's really important to accept the fact that when you make a mistake or can accept the fact when you are wrong, asking questions, when you don't know something and admitting that you don't know something is important as well, the it sec, community's huge. It's never ending things, constantly change. We could be getting hit with an exploit two weeks prior to this, and then a month later it's totally separate across all of

our customers. It's just important to note [00:27:00] and recognize that not everyone knows everything and the, the whole everything's changing 24 seven. So no, one's always, no, one's going to be on top of all of it as a group though. You can hopefully accomplish more than you could single individual.

Speaker 1: All right. Well great. Thank you all so very much for joining me today and for contributing and I really appreciate it.

Speaker 2: Yeah, you're welcome. Awesome.

Speaker 3: It's nice talking to you!

Speaker 1: If you're looking for more ways we can support each other to fend off burnout, be [00:27:30] sure to check out our links for Meredith Kasper's blog. We also have some exciting updates about our use of the MITRE attack framework. So be sure to see our links, to find out more that's all for today. Thank you for listening and I will catch you soon. Bye.