Speaker 1:

This is IT Visionaries, your number one source for actionable insights and exclusive interviews with CIOs, CTOs, and CSOs, and many more. I'm your host, Albert Chou, a former CIO, former sales VP, and now podcast host.

Welcome, everyone, to another episode of IT Visionaries. And today, we have a special guest. He is the VP of strategy at a company called Arctic Wolf, not to be confused with Arctic Cat, which in America's, they make snow mobiles, uh, Ian.

Speaker 2:

(laughs)

Speaker 1:

This is a cyber security company. Nothing to do with snow mobiles. VP of strategy, Arctic Wolf. Ian McShane. Ian, welcome to the show.

Speaker 2:

Hey, Albert, thanks for having me.

Speaker 1:

Hey, listen, we're pumped to have you. There are a lot of companies in your space. Uh, Arctic Wolf does play in cyber security, and you guys claim on your website to be the leader in security operations-

Speaker 2:

Mm-hmm.

Speaker 1:

... so let's start with a simple question. What is unique or what is different about Arctic Wolf than some of the other service providers out there in this industry?

Speaker 2:

Yeah, I mean, you that, right, there are hundreds, probably thousands of companies in cyber security-

Speaker 1:

[inaudible 00:01:05].

Speaker 2:

... all out to make a dollar and confuse everyone on the way. And so we're- we're here, and I like- I like to say it like this. We're here to say to take the [inaudible 00:01:12] out security operations, right? So, obviously, security's difficult. Everyone knows it's hard. We here to make it easy by removing the barriers to all of those tools. You know, making it very easy for your staff, the people that you already have to be successful with what you have.

Speaker 1:

Yeah, I mean, you guys hit at- hint at it right away on the website, which is that, and- and for anyone who wants to go check it out, arcticwolf.com. At the time of recording, this information's on the website. Of course, by the time you hear it, might be different. But they lead with the fact that they agree that cybersecurity has an effectiveness problem. They list that there's over 3,000 in the industry to choose from. That's hard to choose from. Um, that over $168 billion is spent on cybersecurity annually across the globe. And even with all that said, there were 5,200 breaches. Or more than 5,200 breaches in 2021 alone. These are all stats that you guys are willing to stand behind.

Speaker 2:

Mm-hmm.

Speaker 1:

What position is Arctic Wolf trying to take to be more effective? 'Cause you've identified, "Yes, we agree. There is an effectiveness problem." We all agree this is a problem. So what are the steps you're taking, I can take to make cybersecurity more effective?

Speaker 2:

Yeah, like, so that's the- that's the problem. Like, when it takes companies 20, 30, 40, 50-

Speaker 1:

(laughs)

Speaker 2:

... security tools to manage and protect their infrastructure, it's gonna be a challenge to do it. And so that's- that's where we kinda step in, and you know, rather than have you replace something one year with a new product, or add another three later acronym, like XDR, or SIMM, for four later acronym, or, I'm trying to think of a five letter acronym now-

Speaker 1:

(laughs)

Speaker 2:

... to keep the pattern going. I can't think of one. But if you wanna.. if you wanna lay them all crap on top of more crap, like, you can do that.

Speaker 1:

Yeah.

Speaker 2:

But it's really hard to manage it, and it's often a placebo. Like, the fact is that the more tools you have, the less secure you're gonna be, because you're gonna miss things. You're gonna have too much noise to be able to do anything with it. And so that's what we do, is that we collect all of the data, all of the telemetry that's making noise in your environment, and we turn that into actionable things. So we tell your security team, or your IT team, "Here's a problem. Go and fix it. Here's the exact steps you need to take to do it. Go and have a cup of coffee and celebrate, 'cause everything's great."

Speaker 1:

So it sounds like it's a mix of technology plus services, like, expertise, plus technology. Trying to advise my team on, "Hey, this is a potential threat. This is a potential opportunity." Give me-

Speaker 2:

Exactly.

Speaker 1:

I guess, give me an idea, give us an idea of how, uh, con- a customer of yours would experience this service.

Speaker 2:

Well, tha- you, like, again, you nailed it. Like, you're doing a great job for me here.

Speaker 1:

(laughs)

Speaker 2:

A lot of companies talk about AI and ML and trying to almost replace humans in all aspects o- of the world, really, whether it's IT, manufacturing. Whether it's, you know, um, yeah. All aspects of- of- of life. What we're saying is, "You can't remove the human from security." You need that, you know, the- the IQ, the EQ, to be able to understand, is that normal behavior? Is that normal pattern? Is that suspicious? Is that malicious? You know, a... It's not always a binary yes or no. So being able to fuse our technology platform with security experts, when we know a lot of our customers and a lot of your customers and your listeners are probably struggling to hire a people. It's really a boon. 'Cause, you know, we're layering that human element that you can't hire at the moment, on top of the technology platform that we have.

Speaker 1:

So what are you seeing, I guess? How are companies reacting to this service. 'Cause we did the homework on R12. We can see it's fast growing.

Speaker 2:

Mm-hmm.

Speaker 1:

We're talking about potential IPOs.

Speaker 2:

Yeah.

Speaker 1:

We can see that there's a lot of growth there. So in general, you would often find success with that growth. Give us an idea of what you're seeing within the industry what are customers demanding? What are the threats that are currently, I guess, growing? Give us an idea of what you're seeing out there. 'Cause we kinda wanna... That's the one thing I'll say about cyber security, is no matter where you are, it's like, everything's a moment in time. Like, everything you say today, my- (laughs) my... By the time this podcast airs, maybe, like, it's not- it's not relevant.

Speaker 2:

Yeah.

Speaker 1:

So give us an idea of how, like, I guess I really want to know is how you're accommodating for that.

Speaker 2:

Well, I mean, there's- there's... there are a few things that are always gonna be an issue over the next, you know, two, three years. 'Cause frankly, as an industry, we suck at solving them. And that's, uh, ransomware.

Speaker 1:

Yeah.

Speaker 2:

Like, you hear about it all the time in the news. We hear about, you know, services, companies, breaches, that end up either being extortion and ransomware or just ransomware and taking the services offline. So that's- that's what's top of mind for our customers, is, like, asking, "How do we- how do we protect against ransomware?" And so being able to use our technology experts, Arctic Wolf, to help them understand, you know, what's their baseline for risk today? And what are the things they can do to reduce the risk going forward, is something else that helps bring them a- a layer of confidence into our service as well.

Speaker 1:

What is happening, I guess, in regards to, like, the increase and proliferation of the bad actors? Because we had a couple of different guests on talked about, well, they... And it's, I guess, it's more of an opinion than anything else. But they were saying how, like, "Listen, there are plenty of companies actually right now that are just paying out ransoms." Like, meaning, like, they know that the fast way to solve it's the rans-

Speaker 2:

Yeah.

Speaker 1:

So that of course, adds to it. Then you have people that are, like, there's new strategies being developed, which is, like, the, um, I guess, they're, like, laying low. Like, they're taking years to collect data before they ever do an account. So you don't even know you've been compromised. You... There's, like, suddenly compromising.

Speaker 2:

Mm-hmm.

Speaker 1:

Then we've heard people like nation states are now getting more involved. They want, you know, different nation- nation state actors are getting involved. When you see these threats from all this different dimensions, and you're in charge of strategy, how do you think about approaching solving these angles? Are they all using the same techniques? Are they all using different techniques? Like, giving us an idea.

Speaker 2:

Yeah.

Speaker 1:

'Cause the actors seem... The bad actors... eh- you went from just ransom people to, like, you know, whole nations trying to attack you. (laughs) Give us an idea-

Speaker 2:

Yeah. Like, the- the fact is that the barrier to entry has drastically lowered over the last few years. And one of the reasons for that is people get very smart about how to use built-in tools. You know, we think, you hear a lot about living off the land, or low bins, like living off the lands binaries. Like, making use, a- adversaries making use of tools that were designed for IT administration that were used, you know, designed to help the administrators. But once they get compromised, that admin access across the entire infrastructure becomes, you know, the downfall of that company.

So, you know, when you think about the kind of adversarial activity, it's very easy to see why some of them are able to stay quiet. You know, they're, you know, fairly advanced. Maybe they are just trying to make sure they don't get caught. And then we see others. They really want to do a smash and grab, right?

Speaker 1:

Mm-hmm.

Speaker 2:

Uber's a great example of that. Like, the... just judging by the news reports rather than the inside's information. But you saw that, you know, some potentially young kid from the UK managed to break in there. And they're very noisy. Went on Slack and started telling the company, "Hey, you know, I just poned your entire environment."

Speaker 1:

Yeah.

Speaker 2:

You know, and... (laughs) Then, but like you said, then there's the polar opposite, where we see organizations that can be compromised for, you know, 250 plus days, which is, like, if my maths is right, that's kinda, like, someone getting breached on January 1st, and then still being in someone's system in, like, September or October.

Speaker 1:

Yeah.

Speaker 2:

Like, that's a crazy amount of time.

Speaker 1:

Yeah, the, uh, the... We had a cybersecurity leader on our show not too long ago, talking about how the new hack or one of the new crimes that's being perpetrated is this idea of, and I forget what he said. But he says, like, "You act like someone inside the organization."

Speaker 2:

Mm-hmm.

Speaker 1:

So you get your- your breach point. You collect data. You learn that Albert Handel's finances-

Speaker 2:

Yep.

Speaker 1:

... for this vendor. Then you mask and create an instance that looks just like Albert, and you submit a request to finance, to say, "Hey, do you mind updating this account number?"

Speaker 2:

Yeah.

Speaker 1:

And no one's the wiser. And, like, that's how- that's how the new crimes are being done, like-

Speaker 2:

Exactly.

Speaker 1:

(laughs)

Speaker 2:

This, like, that's one up there. One angle is called, like, business email compromise, which is a- a term I don't really like, 'cause it doesn't really describe what's happening-

Speaker 1:

Yeah.

Speaker 2:

... but when someone's able... Maybe someone phishes your account, Albert-

Speaker 1:

Yeah.

Speaker 2:

... and [inaudible 00:08:34] you accidentally give away your credentials. They can log into, you know, Google or Office 365, whatever it is you use. And then just impersonate you. They can create something like, maybe they create a calendar entry.

Speaker 1:

Yeah.

Speaker 2:

You know, invite some people to a meeting, and then in the- in the body of that meeting is a URL. And as a user, you're gonna kinda implicitly trust a lot of this stuff 'cause you see it coming from valid tools. It's not- doesn't have that big external standpoint. It comes from Albert, who I spoke to over coffee last week.

Speaker 1:

Yeah.

Speaker 2:

And you know, he seems like a standup guy, so this must be an important meeting. And so you click on that link, and then maybe you, you know, that's how the polo gets delivered. And then like you said, you know, we see a lot of third... the kind of impersonation crime where they go to finance and say, "Hey, can you pay this invoice that hasn't been paid yet? Can you update this account number? Can you- can you send half a million dollars to this account?" And as- as far fetched as it sounds, that (beep) works.

Speaker 1:

Yeah. And for yourself, personally, you've had a... We looked you up on LinkedIn, not, we didn't go too deep into your past.

Speaker 2:

(laughs)

Speaker 1:

We didn't hack you. All right? But you've been in the cybersecurity game for quite a long time. Uh, you know, you had long runs at Symantec.

Speaker 2:

Yeah.

Speaker 1:

You've worked at CrowdStrike. You've worked at different companies in, kind of in the similar security verticals.

Speaker 2:

Mm-hmm.

Speaker 1:

Give us an idea, is the primary difference between what's happening today and the past just, like, I guess the rapid change the attackers are now taking? Or wha- what else would you say is vastly different from what it used to be?

Speaker 2:

When you say used to be, I cou- I'm so old. That could be, like, 20 years ago.

Speaker 1:

Yeah, 20 years. (laughs)

Speaker 2:

I mean, but- but- the... (laughs) The- the dras- the drastic change, I think, is just that-

Speaker 1:

Or- or- or it could be a year ago. (laughs)

Speaker 2:

But, yeah. In dog years, you're right. Like, I think the drastic change is that everyone's life is not digitally connected in one way or another, whereas, it never used to be.

Speaker 1:

Right.

Speaker 2:

Right? And so there's a lot of bleed over between your personal life and your business life. Whether that's using the same phone or the same laptop for home and work. And so that means the there's, you know, the- the threat landscape is a lot bigger. Then we can consider things like the... You know, this rapid forced adoption in some cases of, like, remote working, you know, during the pandemic-

Speaker 1:

Sure.

Speaker 2:

That's- that's been beaten to death. That story has, but again, that makes it more risky because organizations cannot use that tried and tested method of, you know, building a moat around the infrastructure.

Speaker 1:

On prem VPN. (laughs)

Speaker 2:

Exactly-

Speaker 1:

Yeah.

Speaker 2:

Like, that- that stuff just doesn't- doesn't fit the model anymore. And so that throws everything into disarray. And people, you know, there are a lot of organizations, through no fault of their own, just really didn't understand how to make that work, and they're kind of... Their risk factor just grew exponentially 'cause they had stuff everywhere that just wasn't secure properly.

Speaker 1:

So what does this mean for yourself? Because you run... You got a unique title of VP of Strategy, Arctic Wolf.

Speaker 2:

Mm-hmm.

Speaker 1:

We know you guys are trying to solve some of these problems for different customers. But you just kinda... you just kinda hinted at it. But the reality is, the threats are changing all the time. Right? The environmental, societal, economic factors, you name it, name whatever you want, but it's forcing more gateways. Like you said, like, the pandemic. Right? It opened more gateways into companies' business critical data. Uh, software today, as you know, is more layered than ever, where you're using multiple vendors that now pass data from point A to point B. You know, A to B doesn't even do it justice, really. Like, most companies use, I think, like, hundreds of tech stack. Hundreds of different third party software.

Speaker 2:

Exactly, yep.

Speaker 1:

To move a customer's data, you know, from- from wherever they're go- (laughs) wherever in the system. So it does feel like so many things are amplifying, and, uh, exponentially, of, like, gateways and threats. For when you're in strategy of a company like Arctic Wolf, what are you focused on? How are you, I guess, educating, guiding, give us an idea of how you're preparing your customers and your company for all of this proliferation. 'Cause that's- that's really what you're hinting at is, like, there's every day, there's a new gateway that's being opened.

Speaker 2:

Yeah. I mean, luckily there are- there are plenty of smarter people than me in this industry, and so there's a bunch of frameworks that you can think of aligning yourself to. The one- the one that we look at is NIS, and that's kind of a five step process, where you've got identify, protect, detective, respond, and recover. And so what we're- what we're doing at Arctic Wolf is aligning ourselves to providing outcomes across all of those things.

And that means, for example, in under identifies, really helping organizations understand what assets they have and where they are, because again, you can go to many organizations and ask them, you know, "How many- how many end point devices do you have?" And they're like, "Well, you know, on a good day it might be X number. Maybe it's this. It depends who's- who's connected and who's where." They don't have a, you know, a good baseline of that kind of foundation as to understand what they have and where it is.

Because without that, they can't really successfully do the next step, wis- pis- which is protection. And that's, you know, building the preventative layers around it, whether that is, you know, through routing everything old school style through a VPN to your, you know, your on-premise infrastructure. Or whether that's built around more of the- the identity centric prevention.

And if you can't identify or protect, then you're living in a world where you're detecting everything. And this is where a lot of organizations find themselves. With just noise everywhere.

Speaker 1:

(laughs)

Speaker 2:

They just get alerts from thi- 30, 40, 50 different, you know, applications saying, "This is suspicious."

Speaker 1:

(laughs)

Speaker 2:

Or, "This doesn't look right," or I'm just a really terrible application and I'm just gonna fire all these alerts off. And so people were just drowning. So that's what we're trying to do, is take people on that journey, on that security journey of, like, deploying the fundamentals, reducing the risk, and then helping them improve all the way along so that when something bad happens, and you know, it's like a mathematical certainty that at some point, an organization is gonna be breached, that recovery phase is easy because number one, they know what they need to do. They've got trusted partners like Arctic Wolf that can help them.

And number three, it's not the first time they've done it, because every organization should be, you know, in the same way you do fire alarm tests every quarter, every six months, or every year at least, I hope, you should be doing the same thing for IT incidents. You should be having, you know, fire drills for your security. And so when something bad does happen, you've got the muscle memory to be able to respond and recover.

Speaker 1:

I- I gotta ask, how do you teach people to, like, I guess, focus in on that- that signal to noise ratio? 'Cause I use this exa- 'cause, like, for example, I'm like, the G Suite administrator for Mission, right? And I get the spam alerts of, like, suspicious activity.

Speaker 2:

Mm-hmm.

Speaker 1:

And I also get, "Hey, this email has been identified as spam from these users." But I'm a human being. After a while of not a problem, I definitely have paid a little less attention to it, and I think that's how most people are.

Speaker 2:

Yep.

Speaker 1:

If nothing happens-

Speaker 2:

Yep.

Speaker 1:

They'll just kinda-

Speaker 2:

Exactly.

Speaker 1:

... stop. So that's a human nature problem, how do you go about educating companies or customers or do you handle that side of it for them because of the fact that it does, over time, kinda become, let's say, possibly less effective? (laughs)

Speaker 2:

Yeah, I mean, that's the thing. Like, keeping people vigilant is really important. And you know, I say it's... few moments ago that one of the challenges is that everyone's kind of digital life has bled into their business life, where the person nowhere ends in business. But that's a good thing, I think. If you- if you start to talk about security in the context of, just is not just for, like, a- a boring business seminar that you need to go through just to tick a box and have that, you know, I've completed my security training. This actually have benefits for you in your, you know, day to day life. Because it bleeds over.

Things like using unique passwords. That's not something that just protects organizations. That protects you with your banking, or your, you know, Venmo or PayPal. So making sure that you can link security, not just as a business, boring, hey, protect the company, but to something that actually has tangible impact to a human really helps to keep people vigilant.

Speaker 1:

Yeah, yeah. No doubt about it. For yourself, what are some of the things, I guess, that excite you, uh, innovation wise or on the operational side that you see coming down the pipe, or you've seen implemented in its infancy that you say, "Hey, this- this looks really promising."

Speaker 2:

Yeah, I mean, people talk about machine learning and AI in ways that they're, um, detrimental in a lot of cases. But certainly, it's- it's really impressive to see how an engineering team can build patterns and algorithms that can start to predict whether something is going to be bad before it's even got to it. So that whole, you know, what's the Tom Cruise movie from, like, 20 years ago that had, like, the pre-cogs-

Speaker 1:

Minority Report.

Speaker 2:

There you go. That one, where they can predict where something bad's gonna happen-

Speaker 1:

Yeah.

Speaker 2:

... based on usual, you know, usual behavior or unusual behavior, maybe, like, when we get to that point, they're starting to be able to be more proactive and start to really think about, "Do you know what? These five things I've just noticed on Ian's laptop are unusual. So let's take, you know, let's increase the level of security around his account. Let's maybe lock him out, so that he has to reauthenticate before something bad happens." So that- that kind of prediction thing is really- really interesting to me when you see all of this noise and actually being, you know, used for good, rather than just being a collection of S3 buckets of data crap in the cloud somewhere, right?

Speaker 1:

(laughs) I guess, how far away are we before those predictive, uh, let's say, those predictive warnings are-

Speaker 2:

Well-

Speaker 1:

Super accurate. I don't- I don't, and I don't even know what you think super accurate is. But I'd love to say, like, 90... if 90% of my alerts were accurate, I'd be like, "Yeah, this is phenomenal." (laughs)

Speaker 2:

I mean, frankly, like, the- the kind of the file based ML, the, a lot of security companies have been doing for 10, 15 years is exactly the same thing, right? If they... a file they never seen before has some suspicious capabilities or some things that look and resemble suspicious capabilities, they give it a score. They predict whether it's gonna be good or bad. Now, it's not always 100% and so, you know, to take the Minority Report thing, you know, I don't think we would be making life or death decisions based on (laughs) algorithms that may be trying to predict things. I think that's a little bit far- farther away.

But we certainly see a lot of that in- in cybersecurity today, where we can make pretty accurate predictions about whether something is good or bad.

Speaker 1:

There you go. Well, I mean, within that, also opens the doorway, which is, like, no matter what, even if it's 99.9% accurate, there's that .01 if it does slip by, could potentially be, uh, you know, we see these, like, $100 million dollar mistake. Hund- like, $100 million dollar incident-

Speaker 2:

Yep.

Speaker 1:

Uh, or something like that. Do you e- do you ever see a... I mean, 'cause I don't. I don't ever see one where it's, like, infallible. Like, it just- it just always feel like the bad actors are always gonna find a way.

Speaker 2:

There's no way. This, I mean, think about it. The- the bad actors aren't always outside of the organization, right?

Speaker 1:

Oh, yeah.

Speaker 2:

Sometimes you have-

Speaker 1:

They might be internal. (laughs)

Speaker 2:

... the term malicious insider.

Speaker 1:

Yeah.

Speaker 2:

And you know, and honestly, it's... if you think about the kind of economic state of the entire planet, like, how long is it gonna be before someone is desperate enough to say, "Hey, I'm gonna get in touch, or I'm gonna try to get in touch with a ransomware gang and say, 'You know, if you can give me half a million dollars, I'll give you my log-in.'" Like, it's not outside the realms of possibility that kind of stuff could happen, right?

Speaker 1:

That's pretty crazy to think about. Yeah, like-

Speaker 2:

Like, what's- what's your pri- what's your price, Albert? Like, how much would it cost... how much would I have to pay you to give me your log-in right now? Like, $10 million dollars?

Speaker 1:

Yes, a number- a number that I would-

Speaker 2:

$20 million dollars?

Speaker 1:

... know that I was-

Speaker 2:

Like, [inaudible 00:19:12]-

Speaker 1:

I wouldn't have to work. Yeah. (laughs)

Speaker 2:

You... Exactly, but that's the... The answer's irrelevant. The fact that there was a number-

Speaker 1:

Yeah, yeah.

Speaker 2:

... is, like, is the problem, right?

Speaker 1:

Right, right. If the bal- if I deem, if I'm the bad actor, and I deem your number worth the bounty in front of it, then I pay.

Speaker 2:

Mm-hmm.

Speaker 1:

I mean, this is exactly what... how criminal enterprises work.

Speaker 2:

So, like you say, there's no infallible way of doing it because there's the human element everywhere, right?

Speaker 1:

So how... I guess that, well, that brings us back to, like, full circle, is, like, the... (laughs) I- I forgot who it was in our, one of our cybersecurity guests. They're like, "People are the problem, and they always be the problem. And technology can't solve people." And I- and I was like [inaudible 00:19:48]-

Speaker 2:

(laughs)

Speaker 1:

(laughs)

Speaker 2:

I think- I think that's a bit- I think that's a bit more aggressive than I would say. I don't know. I don't know about calling them, everyone the problem.

Speaker 1:

No, no, but the-

Speaker 2:

I think-

Speaker 1:

... problem... (laughs)

Speaker 2:

... maybe problems are linked to end users, yeah.

Speaker 1:

Yeah, problems are linked to end users.

Speaker 2:

Yeah, yeah. I get ya.

Speaker 1:

When you think about that, though, you know, this is like a... It's such an inexact science. And you know, it's also... So I feel like this- this industry you're in is very much like a, um, I guess sports is a good analogy. It's like, you're only as good as your last season, or last at bat, or whatever the case may be.

Speaker 2:

Mm-hmm.

Speaker 1:

You know, 'cause you're in an interesting position where you're trying to help plan out the strategy for... Did you focus mostly on customers or more internal team? Like, this is how we're going to solve these problems?

Speaker 2:

it's- it's internal. Yeah, internal.

Speaker 1:

So you have that ta- duty, to say, like, "This is how we're gonna do this," right? But you're in an ever changing landscape, and you're always gonna have... Really, that's the reality of the industry you're in. You're always gonna be judged based on what the last incident was.

Speaker 2:

Mm-hmm.

Speaker 1:

If you have no incident, you're judged more higher.

Speaker 2:

Yeah.

Speaker 1:

If you have a lot of incidents in a year, Ian, I'm not gonna... it's not gonna be hard to figure out. It's not gonna be a good year.

Speaker 2:

(laughs)

Speaker 1:

Right?

Speaker 2:

Well, I don't know. I- I mean, hold on, let me- let me interject because I would rather have... I- I would rather have more incidents than none because if I'm having no incidents, that tells me I'm not looking in the right places.

Speaker 1:

Ah.

Speaker 2:

If I'm having more incidents, I'm detecting more things-

Speaker 1:

Gotcha.

Speaker 2:

... and I'm like, "Cool, we can do something about that. We can fix it."

Speaker 1:

Okay.

Speaker 2:

So it's... Again, it's not an exact science, you know?

Speaker 1:

Yeah, it's not an exact science. So when do you think about, how do you- how do you build, I guess, an organization the is gonna continue to be at the forefront of this type- this industry because of the fact that it's always changing?

Speaker 2:

Well, I mean, that's the thing that keeps everyone in our industry employed, is that there's no- there's no destination for cybersecurity, right? It's not something you buy. It's not something you turn on. It's not something you forgot to do on a Monday morning, all right? It's there.

Speaker 1:

And you can't really fix it. You can't even fix it. It's like, it's like a process.

Speaker 2:

Right. It's proc- it's a journey, that's the thing, right? 'Cause it's a continual journey, and you improve it every single week. And the only way you can improve it is being honest with where you are. Like, do we see as much as we need to? You know, is, you know, understanding what's normal and what's abnormal can really help you understand whether you're not... you're missing things. So it's this whole kind of journey that you need to take people on, and that's, again, that's something, if you go to arcticwolf.com, we talk about a lot. It's like, helping our customers along that security journey, no matter where everyone is. Because there's no one size fits all, but there are some foundations that everyone needs to adhere to.

Speaker 1:

Yeah. Our lead sponsor, Salesforce, eh, was partnering with the World Economic Forum, and one of the things they're doing is the cybersecurity learning hub.

Speaker 2:

Mm-hmm.

Speaker 1:

Which is, they're trying to teach and upskill or reskill.

Speaker 2:

Mm-hmm.

Speaker 1:

They said there's a shortage of millions. Millions of people in the cybersecurity industry. And they were on a previous show, episode, talking about how, listen, "There's a massive shortage." This is the first... I wanna say it's the first. But it's one of the few endeavors where it's, like, across private companies, across government entities. Everyone is pushing for more people to get disciplined in this field. How about for yourself? 'Cause you're- you're- you're more on the front lines of recruiting and retaining and trying to hire people that have these skillsets. Where do you see, or how do you see a way to get more people interested in this domain and field? Because if there's such a skills gap, and we all agree that this is a necessary thing, like, that's now part of our future-

Speaker 2:

Mm-hmm.

Speaker 1:

... our future economy for- for the foreseeable future, I think that's fair to say, how do you get more people interested in this field?

Speaker 2:

That's something that's really interesting, 'cause there are so many different perspectives on what skills gap or skills shortage means.

Speaker 1:

Yeah.

Speaker 2:

Because, you know, I can assu- I can assure you that there are plenty of people that would be happy to walk into, you know, a relatively high paying job like cybersecurity, like, say, when people say, "We just don't have the applicants for it," I start to wonder if people are looking for the wrong kind of people. And it's, you know, I've written about this before is that, and there's a lot- been a lot of commentary, and you know, I'm sure I'm paraphrasing, uh, other folks this as well. But you'll see people using words like, "Hey, we're looking for a rockstar or a unicorn that can do everything." And so they set their benchmark really high.

Speaker 1:

Yeah.

Speaker 2:

And wonder why they don't get, you know, they don't find that perfect person. And then you can also think about it, like, if there are a lot of people willing to get into cybersecurity, is it really basic skills that we're missing, or is it actually the folks that are already there, that are looking to level themselves up to being, you know, three to five years of experience, and they can't find the roles there. So there's this whole different kind of, like, facet of things that- that can really play into this. And as an industry, I think everyone's- everyone's different. There are some people that are looking for people that are, you know, first timers or trying to hire that junior role. Whether that's because it's a junior role truly, or whether it's because they've got a junior salary to go with it-

Speaker 1:

Yeah.

Speaker 2:

Or not, is you know, a different- a different question as well. So some of it might just be, you know, kind of self-inflicted for some organizations.

Speaker 1:

What about for yourself? What would you recommend, or how would you recommend others, maybe reapproach the recruiting and talent problem? What are some of the things you look for? What are some of the things that you think as a company, maybe I should provide, so that I can get more people interested in working in cybersecurity for me. Give us this idea of this ideal- ideal person, fit, company, culture.

Speaker 2:

The ideal person I look for when I'm hiring someone is gonna be someone that's got IT operations experience. Someone that's done help desk support. And not just because that's kind of some of my background. But you have people that understand what it's like to have screaming end users at you.

Speaker 1:

(laughs)

Speaker 2:

So you know, they've got- they- they've got used to, you know, disappointing people on the- on the regular. You've got people that understand, especially if you're hiring internally, the IT folks understand your network, and so they've got a better understanding, again, like I said earlier, of what's normal and what's not normal. So it helps them to be more, you know, in tune to suspicious activity. So really trying to recruit maybe, from IT, and maybe from help desk, is a- a place I would start. Because again, I think you could probably back fill those roles, um, a little bit easier. 'Cause those roles tend to be more structured than cybersecurity is for a beginner.

Speaker 1:

How about for a company? If I'm trying to attract someone to my organization. Because this is something that everyone is battling for as well. 'Cause we already said, there's a huge, uh, skills gap.

Speaker 2:

Yeah.

Speaker 1:

Or that people say there's a skills gap. I liked how you-

Speaker 2:

There's a demand. There's a demand for people. Yeah.

Speaker 1:

Yeah, there's definitely demand for people, right? I like how you framed it. It's like, maybe you're looking in the wrong place. (laughs) Because... (laughs) I like how you framed that. But there's a- there's a demand. There's a demand. Yeah, there's jobs, there's people going into the jobs. So what, if I- if I don't have someone applying to work with me or for me, what should I be doing, maybe culturally, maybe it's... Is it a culture thing that I have to offer?

Speaker 2:

Yeah. (laughs) Like, ask yourself, why- why people are not coming here? Does everyone hate working here? 'Cause-

Speaker 1:

Yeah, yeah, that's- that- well, I don't have... we don't have a cybersecurity role here at Mission.

Speaker 2:

(laughs)

Speaker 1:

I can tell you that, but, like, but if I did, what- what do I need to offer? Like, what are the best people in your industry, I guess, attracted to?

Speaker 2:

I mean, frankly, like, the way we solved a lot of this, um, at Arctic Wolf is we've got some pretty ties with the- the US military, and so veterans that are coming out. We've got some close ties with local, uh, with some of the universities that are local to our offices. So we get folks that, you know, going through courses and looking for internships, looking for, uh, their first role. So we have the- the ability to tap in there. And so maybe that's a good place to start for some organizations, is, like, what's around? Where are the, you know, where are the folks coming from? Where are the schools that are nearby to you? What can you do to, you know, increase your- your outreach? Because just posting stuff on LinkedIn, especially if you're using ridiculous terms like rockstar and unicorn-

Speaker 1:

(laughs)

Speaker 2:

... and you know, you're- you wanna pay a- a McDonald's salary for a, you know, a C-level, um, security expert, you're probably not gonna have much luck.

Speaker 1:

Yeah, yeah, no doubt about it. I like how you framed it. It's like, "Hey, you could do this, this, this, this, and this. And here's the wage." I mean, we say in all industries, though, that's a- that's always a big challenge. You know, that's- that's another thing that you kinda hinted at, which is, there's a lot of vendors- there's a lot of vendors and terms being pitched all the time. And so for someone who maybe is not as versed in this domain, they're sitting there thinking, "Hey, I run a software company or something like that. I wanna protect my data information, my customers. What am I supposed to invest in?" Want type of skill, what other skills should I invest in because, you know, there's MI, there's, you know, machine learning based cybersecurity. There's AI... You'll hear every buzzword, if there's a buzzword, there's some cybersecurity company-

Speaker 2:

(laughs)

Speaker 1:

... out there saying that they have that.

Speaker 2:

Yeah.

Speaker 1:

And so it's really touch to even know what you actually need. If you were to say, "Hey, what should I inve- you should invest in this." What are some of the, like, I guess, the fundamental building blocks you think, hey, Mr. or Mrs. New software startup, fast growth company. You now need to get secure- secure systems. What should I be investing in?

Speaker 2:

In terms of technology, do you mean, sorry?

Speaker 1:

That's right, technology and skills.

Speaker 2:

Yeah, I mean, like, there's- there's a whole foundational, like, level of- of capabilities that you need to be able to do, and I can, you know, I touched on the- the NIS framework, so that's something that's open. It's an open standard that organizations can go and look at and see, "Hey, do we have the capabilities in all of these areas?"

I think also, uh, CISA in the US, so, um, cisa.gov has got some really good guidance on what you should be doing from an organizational perspective for- for cybersecurity, and there's also, you know, the UK equivalent, and I'm sure, uh, around the world, governments are doing the same thing. So there's- there's a lot of guidance you can give there. You, or you can get, sorry, that's this freely available.

I think where it comes down to, again, is, like, really working with your IT team to understand what it is you have and what it is you need to secure. 'Cause they're gonna... They're gonna really understand it. There's no, like I said earlier, in, um, terms of cybersecurity, but there is no one size fits all. So when someone says to me, "What should I go and learn, 'cause I want to get into cybersecurity?" There's, you know, this is a domain that is, like, 10 miles wide, right?

Speaker 1:

Yeah.

Speaker 2:

Just, you know, even taking some of the- even taking some of the certifications. Like, you, uh, you learn a small amount about an entirely, like, vast bunch of topics.

Speaker 1:

Yeah.

Speaker 2:

And then you can start to focus in on those. And it's- it's really hard to say, "You should go and do this, or you should go and do that," because every role is kind of different.

Speaker 1:

There you go. Well, if you've listened to this podcast, and you wanna learn a little bit more about Arctic Wolf and want a company like Ian's can do for you, go check them out. It is arcticwolf.com. Ian, I wanna say thank you for joining us today on IT Visionaries. But before you go, it is time for the lightning round. The lightning round is brought to us by Salesforce platform, the number one cloud platform for digital transformation and [inaudible 00:29:37] experience. Ian, this is where we ask you questions outside of the realm of work. So our audience can get to know you a little bit better. You ready.

Speaker 2:

Hit me.

Speaker 1:

All right, listen. What are you holding in your LinkedIn? Is that a coffee or a Guinness? What is that?

Speaker 2:

(laughs) That is- that is a coffee.

Speaker 1:

(laughs)

Speaker 2:

I wish it was Guinness, but yeah, it's a coffee. That's actually a fre- frequently asked question. Thank you.

Speaker 1:

Are you a big coffee drinker?

Speaker 2:

Yeah, I would die.

Speaker 1:

(laughs)

Speaker 2:

Without it.

Speaker 1:

All right, I always ask. How many- how much coffee, excuse me, do you drink in a day?

Speaker 2:

It can- it can very. And so, you know, the coffee snobs on that are listening are probably gonna frown when I say I go through, like, maybe a sleeve of Nespresso slee- uh, capsules a day.

Speaker 1:

(laughs)

Speaker 2:

Becau- I mean, I... (laughs) I cover a lot of time zones, so my work day can be pretty long. And so, you know, going through 10 Nespresso capsules isn't unheard of.

Speaker 1:

There you go. And what's- a Nespresso is for what, for how much? How much does one make?

Speaker 2:

Uh, one of them is usually an espresso. So, you know, maybe I'll two of those at a time. So-

Speaker 1:

Okay. You know, 10- 10 espressos a day. That's- (laughs) that's a great- that's a-

Speaker 2:

Yeah, I mean, it's spaced- it's spaced out now.

Speaker 1:

(laughs)

Speaker 2:

It's all good. (laughs)

Speaker 1:

(laughs) Now, one of the things I made a comment on before you even joined the show is, like, "Man, you've got one of the most rocking looks I've had on IT visionaries." And I'm a big fan.

Speaker 2:

(laughs)

Speaker 1:

Listen-

Speaker 2:

Come on.

Speaker 1:

I listen to metal. I got a terrible haircut. I got a mullet. You know what I mean? So what kind of music do you listen to?

Speaker 2:

Man, I am digging pop punk at the moment. I'm having a real revival with pop punk.

Speaker 1:

(laughs)

Speaker 2:

Yeah, I've gone... If you'd have asked me a year ago, it was probably back in grunge. But at the moment, yeah, real, real pop punk. And there's this- there's a band I discovered called the Bomb Pops, and they are on-

Speaker 1:

The Bomb Pops. Yes, uh-

Speaker 2:

They're on Fat Mike's record label from NOFX, which is, um, Fat Records. And I just came across them when I was getting tattooed recently, one of the- the songs came on. I was like, "What is this? I've never heard it." And do you know what? I cannot stop listening to a record of theirs called, um, Death in Venice Beach.

Speaker 1:

Yeah.

Speaker 2:

It's amazing. So good.

Speaker 1:

Bomb Pops. That's a- it's a- female vocalist, right?

Speaker 2:

Yep, you got it. Yeah, yeah, it's great.

Speaker 1:

I wanna say I've seen them life. I think I have. I think I have.

Speaker 2:

No, get out.

Speaker 1:

Yeah, yeah, yeah.

Speaker 2:

Really?

Speaker 1:

I think I have.

Speaker 2:

Oh, man, I'm jealous.

Speaker 1:

Yeah. So you mentioned, you- you were getting tattooed. All right. Do you consider your sleeve a single tattoo? Or is it a bunch of small tattoos that have been put together?

Speaker 2:

Oh, it's...

Speaker 1:

(laughs)

Speaker 2:

It's a bunch of crazy crap. Man, I've got, like, I've got Agents of Shields. I've got a Nasir one right here. I've got Chris Cornell from Soundgarden. That one's a whole- a whole thing. This one is, like, my random arm. Like, I kid you not. Like, if I have a rare Saturday when I'm bored, like, one of the first things I'll do is text my tattooist friend to be like, "Do you got any openings and can I come and get something?" And then if they've got 30 minutes, maybe I'll get, um, like, the dumpster fire-

Speaker 1:

(laughs)

Speaker 2:

... you can't quite see it there. But I've got a burning dumpster fire one there which was a, you know, 45 minute tattoo because I was bored.

Speaker 1:

(laughs) Hey, listen, I've not heard, personally, of someone getting tattoos of that, um, that quickly. But I gotta respect it because-

Speaker 2:

(laughs)

Speaker 1:

I've got a bunch of tats. My whole chest is tatted up, and, uh-

Speaker 2:

Nice.

Speaker 1:

Someone once asked me, like, "Well, do you regret anything?" I'm like, "Not really." I mean... (laughs)

Speaker 2:

Nope.

Speaker 1:

And I- I actually tell people, like, "You should just actually get it done sooner." Like, there's no... Like, you- you might think that you have this, like, meaningful plan that you wanna put in place, but I'm telling you as someone who's been living with tattoos for 20 plus years, it doesn't matter. (laughs)

Speaker 2:

Some of my favorite tattoos have come out of the get what you get thing, which is, like, a gumball machine, you turn the handle-

Speaker 1:

(laughs)

Speaker 2:

... pops out a little ball with a picture in it, and you're like, "Okay, that's what you're getting." Or you can pay, you know, $100 bucks to go have another shot. So some of my best tattoos have come out that way.

Speaker 1:

There's another one, there's a cool tactic, which is you follow the artist. 'Cause every now and then the artist will, let's say, do a design that they just really like.

Speaker 2:

Yeah.

Speaker 1:

And they'll just kinda throw it out there. Like, "I wanna tattoo this-"

Speaker 2:

Yeah.

Speaker 1:

"... on somebody. Who wants to step up there and get it done?" And, uh, that's usually fun experience as well.

Speaker 2:

Yep.

Speaker 1:

(laughs)

Speaker 2:

Yeah, I've done that as well. And it's... There's a few on Instagram that I've- I've grabbed that way, yeah.

Speaker 1:

There you go. Well, Ian, it was awesome having you on the show. Thanks for sharing your perspectives on cybersecurity. I think the things that are happening in this industry, you did a great job just... you know, they're extremely complex, but it's like, you have to do foundational things, and you constantly have to be in this learning environment in order to have even a chance. I like how you're not afraid of even encountering an incident because that means it's a new thing to learn. And a new problem to solve. And now that you've changed my... you've changed my perspective. I would agree, like, if you're cybersecurity-

Speaker 2:

(laughs) I appreciate that.

Speaker 1:

Hey, listen, if you're out there, and you're trying to shop for a cybersecurity vendor or service provider, and they say they've had zero incidents in the last year, what Ian is saying is they're not looking hard enough. Like... (laughs) They- they-

Speaker 2:

Exactly.

Speaker 1:

... didn't know what happened. Which is another problem.

Speaker 2:

Exactly, there are incidents everywhere.

Speaker 1:

Yeah, exactly. If you don't have an incident, you just didn't spot it. It happened. (laughs)

Speaker 2:

Exactly. You got it.

Speaker 1:

(laughs) Ian, thanks for joining us today on IT Visionaries.

Speaker 2:

Thanks so much. This is great.