Michael Roberts (00:09):

Welcome to the Health Connective Show. I'm your host Michael Roberts, joined by our COO Justin Bantuelle. Today we're talking to Christian Espinosa, the founder and CEO of Blue Goat Cyber. Blue Goat Cyber specializes in medical device cybersecurity for FDA compliance and patient safety, and Christian has over a decade of experience helping medtech innovators secure devices from design to market. We wanted to have Christian on to talk about the cybersecurity process in medtech, including what to expect when to bring in cybersecurity experts in long-term cybersecurity planning. Quick hint, you'll find that cybersecurity is not a one and done process. Christian, thanks so much for joining us today. We're excited to be able to dive into these topics with you.

Christian Espinosa (00:50):

Yeah, I'm excited as well. Looking forward to it.

Michael Roberts (00:51):

Awesome. And I've got Justin here so that any of the hard questions, any of the techy stuff, like I can get outta the way and let you guys dive into the weeds more. But let's just start at a very high level. At what point should during the whole like application development process, so our background is we are in more of the software side of things. So that's kind of like where we'll focus I guess to kind of overlap between what you do and what we do. But when there's this software development process happening, when should Blue Goat Cyber become a part of the process for these medtech?

Christian Espinosa (01:21):

The sooner the better. Unfortunately most of the companies come to us, like their RA says you need to do cybersecurity. And it's like two months before the submission date. So then they contact us and their software's never been tested before. So we come in there and find thousands of vulnerabilities and they're like, "oh no, we can't fix all this in two months." So it delays the submission greatly and it costs them a lot of money. So if they would come to us sooner, we could have done iterative testing or even consulted them on cybersecurity requirements and design, then it would make the whole process go a lot smoother and it would cost less overall. So the sooner the better is really the answer.

Michael Roberts (01:56):

And does that mean even before you even start writing code? It seems like every expert that we talk about when it comes to getting a device to market, getting some sort of process to market, the answer's always "The first thing you should do is talk to us." And it seems like there's like 50 companies and 50 processes that say something similar. In fairness, like what is the reality of software testing along those kinds of lines?

Christian Espinosa (02:16):

So it's not just software testing. That's a good question. We have a client that came to us two months before submission, typical timeframe, and they had made a decision on a micro controller a year prior. 'Cause it takes a long time to develop this product. And that microcontroller did not support Secure Boot. Secure Boot is one of the FDA's requirements. So what ended up happening is they had to basically remove all the functionality off of that device and make it standalone. Before they wanted to have it approved with a cellular connection, a Bluetooth connection, a mobile app. But they had to take all that off because of a choice made a year ago to choose a piece of hardware that wasn't secure. So it's not just the software. We also have to consider the hardware as well.

Michael Roberts (03:03):

Yeah, so how all these pieces play together, just that initial architecture, even the initial decisions that you make are going to impact everything along the way.

Christian Espinosa (03:12):

A hundred percent. And it's much easier and it's much more cost effective to design cybersecurity into a system than try to retrofit it and bolt it on at the end <laugh> and it's more secure as well.

Michael Roberts (03:22):

Yeah, absolutely. So along those kinds of lines, like I'd love to hear, I don't know if if you call 'em horror stories or, or sort of like what, what kinds of stories you are seeing. I mean we say like, "Hey, you're gonna have to redesign things, you're gonna have to change things." What are the tangible effects of this? What kinds of market delays are we talking about? What kinds of pain are companies actually going through because they aren't being forward thinking enough around this?

Christian Espinosa (03:44):

So the story I just mentioned about the microcontroller, that company had a roadmap for the product, and they had shared it with their board of directors. It's a publicly traded company with their shareholders. So they had to reframe the story, because they were saying this product is gonna be released by this time with all these features and it's gonna do X, Y, and Z and help patients. So they had to change that narrative politically, where the product is like this is the first iteration of the product now and the next iteration will have these features. As you can imagine, there's probably some pushback from leadership from the shareholders, from the board of directors, but that's one of the impacts for them. They're a year out from what they projected to get these features back in the product and get it approved. I think that's super tangible.

Christian Espinosa (04:27):

Another client of ours came to us last minute and they had like 6,000 problems they had to fix. This is a pretty complex IVD system, and they still haven't fixed them. We identified all these things eight months ago. They were supposed to submit 10 months ago or six months ago, and they still haven't fixed these items. And now they're at the point where they're just gonna submit to the FDA and hope they don't get deficiencies. And we're telling them, the FDA's gonna come back and expect these things to be fixed, but they don't wanna continue way past our timeline. So they're so frustrated they're just gonna submit anyway. Which is not a good strategy because the FDA's gonna come back and say, you have to fix all this stuff before we're gonna approve it. That's a pretty common scenario. And we even worked with a client in the past that didn't think about cybersecurity the very last minute.

Christian Espinosa (05:13):

And then we found so many things. They talked to their software development team and they said it's gonna cost this amount of money to fix everything, that they just abandoned the project. They're like, "We don't have any more money. We can't do it." So imagine working four years on this product and then at the very end when you think you're about to get approved, have all these cybersecurity challenges come up. Our company feels guilty telling these innovators about all these problems because I know the position they're in. So I'm trying to like educate the industry to come talk to us earlier, right? So they can avoid these scenarios.

Michael Roberts (05:45):

Yeah. You've got publicly traded company, your stock prices for the year may not be what you hope they are. They could definitely have some very real impact there. This big innovation could feel like a very muted launch, could feel like a very unsuccessful, very unhappy kind of story. But then you talk about if you frame that in startup land, I mean that's the difference between a startup making it or not, is if they like actually got this stuff in their heads like early enough and were able to kind of figure this out. So definitely disappointing in a lot of different ways.

Christian Espinosa (06:15):

You brought the startup space, most of the startups in medtech, there's funding rounds of funding, so there's investors. And we've also noticed, and it's probably because all of these investors have been burned, that now they're expecting the startup to have cybersecurity on their roadmap versus think about it the very last minute or don't even think about it at all until the RA says you need to consider this.

Michael Roberts (06:35):

Yeah. Well that's good <laugh>, that's refreshing to see that there is a shift. And one of the things that I'm aware of in this industry is just how much those cybersecurity requirements have changed. I can't say exactly the depth of it or anything like that, but just that it has gotten even harder.

Justin Bantuelle (06:53):

Yeah, they've evolved and the FDA has become more stringent about it and rightfully so, right? They've updated their guidelines recently.

Michael Roberts (06:58):

Yeah, absolutely. So I'd love to hear, you know, are these updated guidelines still surprising people along the way? Have these updated guidelines made things drastically harder for people? How are you seeing it play out?

Christian Espinosa (07:10):

I think they're still surprising people, and they've definitely made things harder. Before the FDA guidance from September of 2023, people could just submit anything to the FDA and pretty much cybersecurity was ignored. So now we have all these legacy devices out there where cybersecurity was not even considered. Right? So that's a whole other issue. But some of the big companies we work with, they had gotten products through the FDA in the past before that new guidance, and they were just following the same process. They didn't really pay much attention to new guidance. And then all of a sudden they get all these deficiencies from the FDA, they contact us.

Justin Bantuelle (07:42):

Right. A new revision can't roll out because they won't accept.

Christian Espinosa (07:45):

Yeah, exactly. So then they contact us like, "we've got all these deficiencies, how do we address 'em?" And it's almost like we know what they need to do, but if it's a large organization, they're so, I guess bureaucratized, it's too hard to steer the ship in a different direction. They wanna keep doing things the

way they were doing because it worked in the past, and we're telling them that won't work today. So it's like this constant like education and trying to get them to change how they've done things for years and years and years. And it's, particularly with big companies, and it's a little bit frustrating for us because we know it will work and what won't work, but they're like arguing with us to some degree because what worked in the past they think is gonna work now, even though they have proof from the FDA and the deficiencies that it obviously doesn't work anymore today.

Justin Bantuelle (08:26):

Yeah. There's a lot of cost aversion. And then like you said, just they're used to operating in a certain way. So having to learn a new methodology, having to reorg, it's just a lot of headache, but there's no way around it. <laugh>, you either give up or you figure it out. Right? Like it's kinda your only two options.

Christian Espinosa (08:42):

It, it's pretty easy for a small company though to make that pivot. But if you've got 15,000 employees and 12 products lines with different developers, sure that's a big change across the entire organization.

Michael Roberts (08:53):

I was gonna pivot a little bit here because I'm interested in, are there some categories of things that you could kind of point out? Like what are some of the specifics that people are just not remembering to do or not really taking the time to plan out?

Christian Espinosa (09:06):

I was having a conversation the other day with somebody about this. I think cybersecurity is thought of as any other thing in a roadmap. You've got a biocompatibility study, you have a sterilization study, you have a wireless emission study. And on a roadmap, those are typically blocked off. Like okay, we're gonna do this part for two months. And so they think about cybersecurity the same way we're gonna do this study or this cybersecurity stuff for two months. And I think people need to look at it as cybersecurity is an iterative process. So the sooner we can check on things, then we can find stuff and it, the code can be fixed, and then we check on it again a quarter later in an iterative manner versus a two month window, which it seems like people are trying to do with cybersecurity like they do with everything else that incorporates the submission. So I think that's one of the biggest hurdles is getting the regulatory affairs people and other people in the industry educated that this really should be iterative. It's not a two month time block goal.

Justin Bantuelle (09:55):

Do you find that when companies have taken the steps for something like SOC 2 approval, when they're certified SOC 2, that they tend to have some better process in place around cybersecurity? Or do you find that that's often not really considered as part of it? I've definitely assisted customers in the past where that was tied in, but I don't know if they were more security minded than the average person or not.

Christian Espinosa (10:18):

We had a conversation uh, not too long ago with a client that wanted to get SOC 2 certified first for their medical device. But their medical device was a physical device that talked via Bluetooth to a mobile app, that talked via API to a cloud ,and that the cloud is what they wanted to get SOC 2 certified. Our advice

to them was don't worry about SOC two right now, focus on the FDA clearance because the guidance for FDA are much more stringent than SOC 2. Now we have had clients that have come to us that have already gotten SOC 2 certified. That certainly helps the cloud component. And some of these devices are software as a medical device that is just in the cloud. So that does make things easier. But our general stance is let's focus on the FDA or MDR requirements first because it is more stringent than SOC 2.

Justin Bantuelle (11:01):

Mm-hmm <affirmative>. That makes sense. Yeah. Certainly in our space, a lot of the software writing is not technically classified as medical device. It's adjacent to it, but it's more like non-product GXP software instead. But when they step through the SOC 2 processes, something that I found is we're integrating static code analysis tools, other kinds of security vulnerability scanning. And when they put that kind of thing forward, it's very easy for us as part of code deployment to integrate that into a pipeline where you can even lock the code from releasing if any critical vulnerabilities are found. So then this kind of feeds into what you're saying, right, about the more iterative approach to this that it's never really done. New vulnerabilities are found, new issues emerge. And if you don't have something that's kind of routinely doing this for you, you're gonna have a bad time <laugh>. And some of that can be integrated into your infrastructure and process as long as you have the expertise to know upfront, which is where I imagine some of the benefit of a company like yours is for the consulting upfront side of things. Because you guide somebody to the right steps upfront, you're not bit by it down the road.

Christian Espinosa (12:06):

That's a good point you bring up about a CI/CD pipeline that has security built into it. And gates, we are definitely an advocate of that and we can help clients set that up. From our experience, probably 97% of our clients do not have a CI/CD pipeline with security built into it.

Justin Bantuelle (12:22):

Yeah. I'd imagine a lot of them don't even have a pipeline at all <laugh> or any kinda timeline, right? And then like it's a subset of those that even have security as a component for sure.

Christian Espinosa (12:31):

Some of it's maturity from the organization, but I think a lot of it also is, everyone starts off with their best intentions for a product from a software development perspective, but then all of a sudden there's deadline keeps getting moved forward. So they're like okay, we have to cut corners on certain things and just get it done. And I think that worked in the past before the new guidance, but now because of all this rigor, the FDA requires, those corners you cut are gonna be found out, and that's what's causing a all of the problems.

Justin Bantuelle (12:55):

Absolutely. It is one of those things where retrofitting, it's gonna be very expensive. Like you said, at the end of the line, there's gonna be everything you could have found and considered along the way and it's a nightmare of like, oh this package or whatever this library you depended on is just inherently abandoned and unsupported and 20 vulnerabilities. Like you can have pretty significant rewrites as a result of having made bad decisions pretty far in the past <laugh>.

Christian Espinosa (13:20):

Yeah. And that with the uh, software bill materials and like the third party libraries. It's not so much just like, okay, this library has a vulnerability and we have to do something with it. It's also, and we're starting to see more of this, some third party libraries are open source code. If you use it in a specific manner, the open source development organization can tell you you have to disclose of your source code. So from a legal licensing perspective, it opens up another can of worms because a lot of these medtech innovators, that bread and butter's their intellectual property on their algorithm or their software and if you have inadvertently included a third party library where they could ask you to make your closed source code open source, that's a big problem obviously. I don't think people are thinking about that too much.

Justin Bantuelle (14:02):

Is that something that you guys also provide as a component of this analysis of the software that's included for license review?

Christian Espinosa (14:10):

Yeah, a hundred percent. We look at all the software bill of materials, we look at it for vulnerability and licensing challenges. The FDA or regulatory authority doesn't care about the licensing challenges, but the organization should care about it.

Justin Bantuelle (14:22):

Absolutely. That's awesome that you have that as well as component of your offerings. 'Cause yeah, that's one that's like so easily overlooked and then you're in very hot water. And it only takes one person, one developer pulling it with no oversight or structure in place and then you can end up in some pretty hot water. <laugh>

Christian Espinosa (14:38):

For sure.

Michael Roberts (14:38):

There's some interesting stuff here where we're talking about like the actual code, and there's some very clearly defined things. This is allowed, this isn't allowed. There's sort of that very clear-cut black and white. But there also are these softer skills that you've already kind of touched on just a little bit, feeling like you're disappointing the innovators, feeling like people are gonna be sad when they hear this kind of news. Like you have to play the bad guy I guess sometimes <laugh>. But one of the things that Justin and I have actually discussed on the show before is sort of like even the hostility that can get directed towards security teams because "hey, my code's fine" or "hey, whatever it is I built is right." And so there's clear evidence that hey this isn't gonna work. But how do you kind of navigate that softer side of things beyond just "See I told you!" <Laugh> What's, what's the process that you take there?

Christian Espinosa (15:27):

I have a book here I wrote on this topic called "The Smartest Person in the Room." I, I think one of the biggest challenges in cybersecurity is most teams lack emotional intelligence. If you're telling somebody something pretty bad, you need to be able to see the world through their lens, how they're receiving it and have that emotional intelligence. So that book is really about adding emotional intelligence to highly rationally intelligent individuals which are typically in high-tech industries. So my team has the emotional intelligence and I make sure in my culture they have that intelligence because you're telling

someone some really bad news. The client that has 6,000 vulnerabilities, that is not the thing they want to hear two months before submission because they know they don't have the budget to fix it, they don't have the resources, they don't have the time <laugh>. So it's not an easy thing to hear.

Christian Espinosa (16:10):

So my team is well versed on how to position these things in as soft a manner or as positive as manner as possible. But there is some hostility there. That organization, one of their developers tried to fix a bunch of things, but what he did was just change some data in a staging server. So it looked like he fixed it, but he didn't actually fix it. So we looked at a different record, the same vulnerability was there. So now we have to have a way to navigate, well this guy basically lied to us. He's trying to trick us and say if you just look here, it's fixed. But if you look anywhere else in the code, it's not or any other record is not fixed. So we have to navigate that as well. And from my perspective, I am definitely not comfortable as a company owner or founder sign off on something unless we have fully done our due diligence, and our testing is very complete and accurate, because we're basically at testing that this device at the time we tested it is secure. And if it's fielded, hacked into, and somebody dies because of it or a patient is harmed or injured, obviously it doesn't look good for my organization.

Justin Bantuelle (17:09):

Absolutely. Yeah. And adding to I guess maybe where I observe a lot of friction, it's often with an internal organization's security team where somebody submits their code, somebody submits for a release and then the security audit comes in and they just sort of say rejected, and they're very oblique about what's wrong. They're not really trying to provide enough detail on the specific issues and what appropriate remediations might be. They are maybe unwilling to have conversations about something that maybe is a false positive. And where I think like that dialogue is really important. And like you said, that meeting the team where they are and I've worked with some amazing security people within an organization that view themselves as a partner where it's like we're trying to get this out and the security team is facilitating like I want you to be able to release this too and here's how I'm helping partner with you on it. I'd imagine an organization like yours coming in from outside brings a lot more of that holistic view. Whereas somebody who's maybe is like, "oh, my job is just security at this position so if I just reject everything then it's uh, <laugh>, no vulnerabilities will ever occur." But I don't know how much you've seen that kind of friction occur where a security group maybe ends up feeling more oppositional because they view their role as just rejecting and not facilitating <laugh>.

Christian Espinosa (18:32):

That's the common challenge in cybersecurity in the industry as a whole. We partner with an organization and our goal is to help them get their device cleared. So we work with them until it's cleared. And we don't just point out problems without a solution. We'll tell 'em, here's the vulnerability we found, here's exactly how to fix it. If you need help fixing it, we're happy to get on a zoom call with you and walk you through it. We're very collaborative versus just "here's all the things wrong and you have to go fix them." In a principle, I don't believe in telling somebody there's a problem without offering a solution, right?

Justin Bantuelle (19:04):

Right, right.

Christian Espinosa (19:05):

But I think a lot of cybersecurity people do that.

Justin Bantuelle (19:07):

Yeah. And that's very much where that reputation occurs from. And I'm in a similar boat where they do a lot of software and like as a result of releasing software, we support that software and it has a terrible reputation. Right. Because there's so many bad IT organizations out there. And while we don't really function that way, we are functioning as support for our own software. And that's something I'm always coaching my team on how to like navigate that to not be like those nightmare IT scenarios where you contact people and just have a terrible time and it's just, I've got a problem, I just need help solving it <laugh>. And you feel like you're not getting anywhere, spinning your wheels. So I'm very sympathetic to having a bad industry wide perspective and trying to navigate that and be somebody who stands out by just doing the right thing and collaborating with people to help them solve their problems. It's wild that that's not the norm. But <laugh> here we are.

Michael Roberts (19:59):

Let me ask you guys both a question around this 'cause you're both managing teams that have to think through this. Is this something that you recognize on hire and this candidate is gonna be able to do this well? Or is this something that requires just a whole lot of training after getting the candidate, regardless of who they are coming in? How much of this is something that the candidate brings versus something that they can learn?

Christian Espinosa (20:21):

Blue Goat Cyber is my second cybersecurity business. My first cybersecurity business, I hired people based on their certifications, their degrees and their credentials. That was what I looked at first. I didn't look at their people skills or emotional intelligence. And when I looked at my company, like I zoomed out and looked at it, 99.9% of the problems I had were because my staff lacked emotional intelligence. So then I changed the culture and flipped the script and I looked at core value alignment, cultural fit people skills first. Only if they pass those things, did I bother looking at their technical skills. And to be honest, if they had those things and they had a decent aptitude, I feel like they could learn the technical side because I feel like the technical skills are easy to learn for most people than the people skills. 'Cause there's an aversion people in high-tech to learning people skills. They think that it's not necessary. But to me those skills like people skills have an infinite shelf life versus tech skills which have a finite shelf life. So why not learn the people skills?

Justin Bantuelle (21:17):

Absolutely. Yeah. I couldn't agree more with that. I very much feel like you need to look for people who are aligned to that core philosophy of helping people and having passion for solving those problems. The things that I work on now, like the things that our team builds are so wildly different from when I came into this field 18 years ago. There's almost no technologies that I worked on then that are exactly the same today. Many of 'em are like completely new pieces of software and things like that. So you have to adapt, you have to learn constantly. So I think there is an aspect of looking for somebody who would be a good fit. And then I think you reinforce it through the culture. So you're constantly identifying areas where maybe somebody missed the mark in a communication or you're starting by being present with them and then giving them advice afterwards. But you very much shape the company you are and the culture that you've defined through constant interfacing and leading by example as well, by allowing them to see how you tackle problems, talking out why you approach something a certain way. And

when you hire the right people, they're receptive to that and they absorb that and then reflect it without you having to micromanage everything.

Michael Roberts (22:21):

Let me ask one last question here as we're wrapping up. Christian. Who is it that you and that Blue Goat Cyber sells to? If there's a person in either a large company or in the startups, who is the key target that needs to recognize, shoot, we need to be thinking about cybersecurity right now?

Justin Bantuelle (22:37):

Are you asking like specifically just like title department, those kinds of things. Like who are the right audiences to care?

Christian Espinosa (22:42):

There's three main buckets. If it's a startup, it's typically the CEO founder or the CTO, those two. And they're very early on in their phase and we do consulting with them for the design and then do the pre-market submission package later on. If it's a mid-sized company, it's often a regulatory affairs or RAQA person. They've been assigned to handle the 510k submission or PMA submission and they're going through their checklist. They're like, okay, what are we doing about cybersecurity? Oh, the company doesn't have anybody. So then they reach out and find us. So that's the other one. If it's a really large organization, it's often the product owner that will reach out to us or search for somebody to help them with cybersecurity. So those are like the three main buckets for us.

Michael Roberts (23:23):

Okay. And if you were gonna like leave them with some advice for how they should be thinking about things going forward, besides "contact us immediately," <laugh>, what, what, what sort of advice would you give them to kind of be thinking through these kinds of things going forward?

Christian Espinosa (23:37):

I think it goes back to what I said earlier on a project timeline. Cybersecurity is more of an iterative approach versus having a block of time to work on it for two months. And I think this is the shift that needs to happen because most people, as I mentioned, if you're doing your biocompatibility study, you block off two months of time in your entire three year timeframe as an example. So people have to understand like cybersecurity is not the same as those 'cause the applications being developed, the software's being developed, and just like that's an iterative process, the cybersecurity should align with it as an iterative process. So it's not just starting early, it's thinking about it a little from a different mindset, not just a a block of time, but an iterative approach throughout the entire roadmap, really.

Michael Roberts (24:17):

Awesome. Awesome. That's perfect. Yeah, I think that that's great advice to leave with everybody. Christian, thanks so much for joining us. We really, really appreciate it and love to get the chance to nerd out on this stuff and really dig into it some. So thanks so much for joining us.

Christian Espinosa (24:29):

Yeah, thanks so much for having me on. Appreciate it.

Michael Roberts (24:31):

In our interview, Christian shared insights into cybersecurity for medtech and how it is very much an iterative and ongoing process. To learn more about what Christian and Blue Goat Cyber do, check out bluegoatcyber.com. Thank you to our viewers and listeners for joining us for this episode. For more on the Health Connective show, please visit hc.show for previous episodes and Health Connective as a company.