0:00
We have our partners with us today, Sunrise Labs. Thank you so much for joining us. We have great content for you today. We're going to be talking about cybersecurity in 2024 and beyond.
0:10
There's there's a lot to cover. We have an hour for today's discussion and we are going to be saving some time for Q&A.
0:17
So please make sure to put that in the Q&A function in the bottom air screen at any time questions arise to you.
0:24
Before I turn it over to our panel just want to introduce myself quickly. I'm Nicole Owens from Mathematic.
0:31
If you're not familiar with our organization, we are a medical device trade association for companies primarily in the New England area and we work to bolster the ecosystem through education and connection, events like this, efficacy and awareness.
0:47
All right, as I mentioned, we have an awesome panel for you today. Our moderator is Dave Hibbert.
0:54
He's the vice president of engineering for Sunrise Ls and he's joined by an ulcer panel including Shiv Sebastian.
1:02
He is the CTO of Sorellis Biosystems and then his team as well from Sunrise Labs, Christine Mason, Director of Software, and Nick Daniel, Senior Principal Software Engineer.
1:15
So I'm going to turn it over today for the conversation and enjoy. Take it away. Alright, thank you, Nicole, and thank you to Masmedic for hosting us today.
1:23
It's certainly not our to be here and be able to talk about cybersecurity and you know, just tell us. People, what we know. So again, my name is, my role at Sunrise Labs is the VP of engineering.
1:36
I'll just give it a brief overview of my background and then I'll let the rest of the team, give their background as well. But for me, I've been working in the medical device industry my whole career, so about 30 years now, a little bit more than that.
1:44
I've worked both on the industry side and the services side. And I've worked with, you know, large manufacturers such as Metronic and then services companies such as, and then as far as different types of technologies and products.
2:00

And then as far as different types of technologies and products that I worked on. So I've spent quite a bit of time in, as far as different types of technologies and products that I've worked on.
2:06
So I've spent quite a bit of time in, I've spent quite a bit of time in, in, and kind of combining those 2 aspects together for positioning and for radiation delivery. I spent a fair amount of time working on caratingal dialysis and then fair amount of time, also on insulin delivery, looking at different types of pumps and the companion apps do along with those pumps.
2:22
So I'd like each one of the panel to introduce themselves as well. So, should maybe you can go next.
2:28
Yeah, thanks David. Thanks, Nicole and mass medic for, hosting us today.
2:34
My name is Shifa Basin. I'm a CTO of, it's a startup Boston based startup.
2:41
It's a hard engine at spin-off. What we do is, remove skin in a scarless fashion.
2:47
And believe it or not, it requires a lot of data driven decision-making and therefore there is a role for cybersecurity even in our application. As far as I'm concerned, before that, before this startup, I've been in the medical device industry for 20 plus years.
2:58
I had my own startups. I sold one. I tanked one and then I had large company experiences with Matronic, Livenova, Phillips.
3:13
And then I took a detour to Google. And Google was part of their machine learning team.
3:19
And at that time, we also started working really closely with the FDA on their cybersecurity guidance. So I've been kind of watching this journey of how cybersecurity guidance. So I've been kind of watching this journey of how cybersecurity has evolved over these years.
3:25
I'm very excited to be here.
3:32
Thank you. Christine, you want to go next? Happy to. So I'm Christine Mason, director of software at St. Louis Labs.
3:40
I have been developing medical devices for over 20 years. At various layers of the software stack. But primarily in the embedded space, the types of devices I worked on.
3:54
Yeah, range to class 2 classroom medical devices. With, you know, battery operated, technologies wireless and fluid moving, devices.

4:05
So in my current role, I work with this software group. To develop solutions for our clients and among them, cybersecurity, local devices, which we're gonna get more into today.
4:20
Thank you. Christine. Alright, Nick. Awesome. Thank you, Dave. So my name is Nicholas Daniel. I've been working primarily on medical devices, but not just only in the medical space for about the last 15 years.
4:34
My experience as it comes as a pertains to cybersecurity. I originally started working on devices early in my career that were some of the first generation medical devices to integrate network connectivity and that came with a whole host of challenges of understanding the cybersecurity space so that I could develop robust solutions to mitigate these risks, which took me kind of all over of discovering this since this is primarily before any FDA guidance.
5:00
So hoping today I can share some of my experience and how. That pertains to as in my current role where I'm architecting and designing. A secure and robust solutions for medical devices.
5:12
Alright, well thank you all for being here today. So why don't we go ahead and get started.
5:19
So just to give a little bit of background information, why we thought this was important. So. Cybersecurity, you know, every day, more visibility, you see ransomware attacks and other attacks.
5:31
You see just. Medical devices having issues problems again being attacked in various different ways and so more scrutiny and really the whole cyber security feel gets more and more complex with each passing day so The FDA originally drafted some guidance.
5:46
I think it's been almost about 8 years now, but that was sent out as draft.
5:53
There's lots of feedback and a couple of that went there, as well. And then finally it was brought into law, in CFR, About 1415 months ago, something like that, but the final draft didn't really come out into the middle of last year.
6:09
So the final graphs. Final release guidance document really has been out for a few months now, maybe 6 months or so.
6:16
And Interestingly, even yesterday as we were kind of talking preparing for this webinar, we saw that they another draft guidance came out and it's really just a supplement to the document that was released.
6:22

6 months or so ago. But the one thing that I found interesting in it, just giving it a quick read is there is some, items where it said the FDA recommends blank or the FDA recommends you submit this document.
6:40
And now there's some of those recommends for changes to must. So again, it's becoming more and more, visible and more and more crucial, I think, to.
6:48
The FDA submission and product development overall. So what that said, like to kind of start out and, maybe kind of start on.
6:59
You know how does one get started in cyber security and how does what's the best place to start and really about timing.
7:05
So Kristen, maybe you can talk about a little bit about where to start. The cybersecurity in the product development lifecycle.
7:13
What's important and when. Yeah, of course. So yeah, one of the key takeaways that. I got from the guidance is that the service security should really be integrated into the total product lifecycle.
7:28
So. When you ask about when we should start. As early as possible. Ideally even during product conceptualization So I think as medical device, manufacturers developers were used to.
7:44
Incorporating safety risk management into. The whole development process. And so security risk management.
7:50
Really is a form of. Real risk management. And so. Yeah, TIR, 57 has this great diagram where it shows security risk management paralleled with safety risk management and how they can affect each other.
8:06
And so. Just early in the process we want to be in corporate cybersecurity. So one of the first things you want to consider is your device.
8:17
Security risk profile. Now that can vary depending on the device. 4 8, for example.
8:27
If you have a device that's, let's say, in a secure area, a hospital, It's not network connected.
8:34
It's only going to be really accessed by doctors and nurses. That's gonna have a very different security risk profile than something that's a device that's in a patient home where you don't have.
8:45

Control over the house network or in a publicly access area. So those are things to consider. The types of security.
8:53
Requirements you want to think about early in the process. So you know. Some of these examples of security requirements.
9:03
Could be like, you know, do you need authentication? Is there patient data, private patient data that we need to keep confidential?
9:12
Do we want to use encryption in our communication particles? So it's always great to incorporate cybersecurity early on.
9:22
It creates a more cohesive solution. In architecture. And so one of the ways that we can do this is to incorporate.
9:33
Cybersecurity into your quality management system. So QMS. I think the FDA refers to, you know, the term secure product development framework, but it's really a set of processes.
9:46
That incorporates security management into your whole product life cycle. And that's gonna look different for every organization.
9:52
With the goal of, you know, you want to reduce vulnerabilities and make. Safer devices.
9:58
And so. If you incorporate, let's just say you incorporate. Cybersecurity after the fact.
10:05
There's a lot of downsides to that. So first of all, your your, you don't have a cohesive solution.
10:13
Your security measures are more like patches or you know both on's it's not gonna be.
10:19
As efficient. In addition. Let's say for example you discovered you need secure boot.
10:29
You do your analysis too late. Well, with secure boot. Typically you need encryption keys in your hardware.
10:37
So that could. Make you want, have to redesign your hardware. I mean, there's a lot of.
10:46
Yes, yeah, you've got your schedule, your budgets. And it's just.
10:53
Something you want to incorporate early on. So. To bring it back to your question. You want to incorporate security.
11:00

As early as possible. Okay, thank you. So should 1, one of the things that, Christine mentioned was the environment.
11:09
So maybe you want to talk about, some of the sort of environmental and maybe physical security.
11:15
Concerns and how that could affect your overall architecture. As you're starting to develop a product.
11:23
Yeah, sure. So the, you know, I think As Christine mentioned, I think there's a whole bunch of considerations from an architectural point of view.
11:30
I think as far as, you know, physical and environmental are concerned, I think, you know, it again comes down to fundamentally you know the issues around you know access control where you actually want to I mean of course everything depends on the type of your product right I think but at the end of the day you know you want to I mean this is more of an issue when you have you know essentially data coming out of your device
11:55
and you essentially have other third parties and other locations where you're actually storing. Your system where I think it kind of gets into a much more interesting conversation. As far as, you know, the actual device is concerned. I mean, you just have to make sure that you know, there's not.
12:10
You know, if somebody really wants to do something physically to your device, there's not much you can do to stop it. But I think you still want to make sure that you had the right kind of access control capabilities from a perspective if you have a software interface to have kind of multi-factor authentication, some kind of authentication system.
12:26
If you have a physical needs, then you have to have something like in on a K cards and biometric access be able to have some sort of surveillance capabilities, you know, some sort of visitor management in case of data centers and data that's kind of stored there.
12:35
When it comes to environmental, you know, controls, you have to, you know, I mean, in general when you think about architecture you have to think about you know disaster recovery as just as a as a global principle.
12:50
And I think so, I think whether it's related to power backups or whether it's related to climate control or any kind of fire related issues.
12:57
Fundamentally, it all translates back to how do you actually build resilience and redundancy in your system.
13:03

So fundamentally that's kind of what you're trying to do with these condom and control. So, you know, that's so that's typically what you have to think about.
13:09
We are thinking about environmental controls is, you know, how do you set up for disaster recovery? How do you actually plan for backup and storage? How do you, so those are the things that you have to kind of keep in mind. When it comes to architectural elements as it pertains to physical and environmental safeguards.
13:28
Thank you. Alright, so Nick, kind of expanding on the architecture a little bit. So if you're starting to develop a system architecture and then break that down into a software architecture.
13:39
Hmm. Hmm. What are some of the key considerations that you're looking at there and You know, even in terms of operating systems and just the architecture as all.
13:47
Yeah, absolutely. I like to echo a couple points already made, which is understanding the use cases is a really big one.
13:54
Understanding the environments so that you can adequately build appropriate controls. Understanding use cases in the data flow and the purposes for all the data will let you better categorize your assets.
14:06
Doing so will let you better analyze your different attacks surfaces and threat vectors. Because the goal is the architectural phase is to design out security risks.
14:13
If we can design them out, then we don't have to come up with unique or novel solutions for mitigations.
14:22
This is why it's so powerful doing this security analysis early. Is that you can avoid problems holistically.
14:32
Which is a great empower of the architecture, which can't, those solutions often can't be bolted on later, those ones that really design out the problems.
14:41
But beyond that, the sometimes, based on the use cases of the device, you might not be able to design out those problems. You, that is where you start looking into these security mitigations looking at the different assets you're protecting, such as data, where the data at rest, motion, and in use and making sure you're taking all the appropriate steps to control that.
15:00
That might be choosing authentication techniques that meets with your use cases, encrypting the data at storage and hardening your software systems to prevent against these type of attacks.
15:14

Hey, thank you. So one of the other things that Christine, mentioned was, one of the FDA concepts of the secure framework.
15:22
Do you have any thoughts on how that's set up and, what, are some considerations in terms of that framework.
15:29
Yeah, so for as far as like the security risk management frameworks, there's a few out there.
15:35
I have my own preferences. The ones I typically stand to is TIR. 57. That was one that actually the Christine had brought up.
15:41
I really like the way they describe the risk management, especially as somebody who's very familiar with 14 9 71, which is generic medical device management.
15:53
It really puts it in the context of the risk management that we're very familiar with. But steps into the space of secure, cybersecurity where the probability of initiation is a little different and has to have different considerations.
16:10
So TIR. 57, I think is really good. When it comes to actually conducting your risk assessment, the one I draw is the NIST 830.
16:20
I think it's a nice starting point for diving into all of the uniqueness that cybersecurity has as it comes to risk assessment. So those are the ones that I typically draw on to conduct the secure process as well as conducting my risk assessments.
16:34
Though I will give honorable mentions to the ISO 27 K documents as well as Kobit and Nest 853.
16:47
There's lots of frameworks out there. I think that really to make your own process, you really should read them all and understand the pros and cons. That they all weigh and you can really make a very robust process of these documents. Explain not only how, but why.
17:01
So this is very good documents. Okay, fantastic. I think one of the things that we've kind of been hinting at here is jumping into one of the early phases, which is a threat analysis.
17:13
So, Christine, maybe you can kind of give a little bit of a review of, how we connect it through now. So, and maybe how we've incorporated. Like the new standard into that threat analysis and do some of us more.
17:27
Sure, so. So, for, First risk assessments for security, we use the NIST 800 h story that Nick mentioned.

17:38
So that's a guide for conducting risk assessments, as it pertains to security.
17:44
So this is a guy that's widely used in. Many interesting industries and one that's actually recommended by the FDA.
17:52
So this guy, it provides a structured, methodical approach to identified threats. Evaluate the risks and then determine what kind of control measures we can put in place to reduce risk.
18:06
I see a lot. It's a very analogous to the FMA process where the FME.
18:15
Is based on probability. And severity of harms and that determines your risk. And so for security risk.
18:24
It's really the exploitability. With the with the severity of impacts. Now those impacts could be safety harms.
18:32
Or business or reputation. And so. One of the inputs. Or the input into the risk assessment is understanding what are your attack surfaces.
18:45
And a good way to figure out. What that is, develop a threat model. So a threat model is Typically a diagram, that shows a system view of how that product.
18:58
What that looks like and it's like ecosystem of use so it's gonna describe you know what are your external interfaces, showing internal interfaces.
19:12
Where are they assets or you know, keys, are located in your system. And.
19:22
Part of that is defining where your trust boundary is and that's going to depend on. The risk profile the device but really What that's, threat model shows is your attack surfaces.
19:30
Where are the entry points into the system? And so that's the first step. Of your risk assessment.
19:40
So once you have your attack service, and I can just go to go overview of the kind of the different steps, but not gonna go into too much detail.
19:49
So once you have your tax office. The next thing is what are your threat sources? And so that's identifying.
19:59
Who are your adversaries? Are they outsiders? With moderate secure knowledge. Maybe they have like wire shark, you know, or Do you have to worry about insiders?
20:12

I mean, it depends on. The risk profile device again. It's gonna vary. Then you're gonna identify thread events.
20:21
So think, you know, examples of this could be like. Denial of service from jamming or So, sipping data to read critical data.
20:33
Man, I'm middle attacks. Things like that. And then. Another factor are identifying.
20:42
Predisposing conditions. Let's say you have to. Interface to a legacy system or a different another device.
20:50
And they only provide a certain interface to communicate. And that communication is unencrypted. Well, there's nothing you can do about that. That's just it's part of the system but it should be factored into risk. So once you have that information.
21:07
The next thing is determining the likelihood. Of these of these threat events occurring. And you know that.
21:19
That's, that's a difficult one to, that one requires a definitely. Someone with a lot of experience in this area and it can actually change over time.
21:29
Depending on. New exploits and, discovered. So with all that information. What comes out of that is risk, right?
21:41
You've got the exploitability. The impacts and your risk. And so at this point. Are the risks acceptable or unacceptable if they're unacceptable?
21:52
You've got to put in your security control measures. Medications and you know, some examples of that could be.
22:00
You know, adding encryption. Or doing integrity checks on critical data. Or adding passwords to.
22:09
A bios or a screen. Actually, one of the attack surfaces you may not think of.
22:17
Is a touch screen. Worked on products where the service interface is available on. And if you don't, if you can just go in there and.
22:29
Yeah, change critical parameters. That's definitely a huge concern. And so, what comes out of that is, is this, is it, do you have a password as a mitigation?
22:39
And ideally the password is unique to each device. So. At the end of it, you have your residual risk. After your mitigation and hopefully at that point they're all acceptable.
22:54

So that's just kind of an overview of the process. Though we use here at Sunrise.
23:00
Yep. Thank you. So Nick, one of the concepts that, Christine mentioned was the trust boundary. What, how do you define a trust boundary and identify that?
23:08
Yeah, trust boundaries are a little tricky. You have to, they're basically setting up a line.
23:15
Where you as a product have considered everything within this. Boundary as trusted. So this as an example, if you have a little box and you have external interfaces, maybe you draw those trust boundaries just around the internals of your box to the point where you We're no, we're not going to worry about the security.
23:32
Between one particular integrated circuit talking to another integrated circuit so we don't have to encrypt internal communication.
23:41
That might be a place where you draw the trust boundary, though you're environment in use cases could bury. The box it loan might not be the trust boundary or it could extend past the box. So if you have 2 systems that are communicating closely, maybe you're trust boundary includes both of those systems.
23:57
So it's mostly establishing a line where at this point anybody who crosses this line is considered trusted. Otherwise you will end up in this infinite loop of finding your way all the way down to the circuitry of trying to protect those and you'll lose you have basically diminishing returns after a certain amount.
24:18
Thank you. So should, you know, when you're creating a threat model and trying to identify, All the attack vectors, what are some of the difficulties that you've seen and, you know, are there advice that you have to try and make that a little bit easier and Gain consensus between all the members because that's in any risk management.
24:37
That's always the hardest part I think that's, I mean. I, I think the challenge of, I think just building a tech model, of course, I mean, I think, you have said multiple times.
24:50
Everything's use case dependent, but I think the few, I would say that 3 and over these years and across many different products.
24:57
I think there's fundamentally I would say 3 really critical things that cause difficulty in Craig, the robust track model.
25:09
The first one is just the Just the evolving cybersecurity threat landscape. You know, you cannot prevent what you can't predict.
25:18
And, and which means that your tech model is dynamic in nature. You know, so today you debate about what you have your product today and what it can do.

25:28
But you don't know what is out there in the in the wild when this product goes out. So there's The debate is around how much can we predict.
25:36
Today about what we're gonna expect tomorrow and that's never easy you know. Unless you live in Arizona and you can predict every other day as a sunny day.
25:45
I mean, you know, that's not the case in cybersecurity. So there's that issue. The second issue, which I All this fine is a is a point of debate and also a point of I think I would say difficulty is as medical device manufacturers as companies go.
26:02
No, we always makes a decision of or do we build and what do we? Let's say, by, so to speak.
26:09
And from that advantage point, I think the issue is around, you know, the complexity in your device and the ability to do interoperability.
26:17
So every time you actually so complexity are defined in terms of the different components inside your medical device system.
26:24
And every time you have an interface, as Christine mentioned, every time we have an interface, now it's an internal interface, whether you're Let's say whether you're actually incorporating a software of unknown provenance inside your product.
26:36
All of these things then create these vulnerability points. They create these attack surfaces that that you don't have full control on and you have to rely on your partners to provide the information.
26:43
Or have the same level of commitment toward security. So there's, so there is that issue of complexity, which is I think more about how the system is built.
26:57
And the other aspect of this is the interoperability with other external system. So if you're thinking about it in a healthcare provider setting where you actually have to deal with hospital IT.
27:06
Now, yes, we can. Ensure that a product is essentially secure, but then it still has your interface with an EHR and EMR system that the hospital IT controls.
27:16
So then having that interoperability again creates that vulnerability point. That I think becomes again a topic of discussion or how do we actually create a tech model where we have a product that's let's say has soup components inside the system has interoperability with external infrastructure.
27:35

So that's, I would say, the second difficulty in actually creating current model. And I would say the third one, which I think is, you know, is I think is equally important is I would say the Also the diverse usage environments.
27:50
We talked about how, you know, you know, different usage environments impact. Malls and that's kind of the outside the third critical component because you know again as medical devices go you can use them in your home And if you're using it in your home, then you're connecting to an insecure.
28:03
Network, then I think that again creates a vulnerability similar to, you know, your requirements for the same thing connecting to an hospital IT network is different.
28:17
So different usage environments again create different kind of third models. But I would say that I think. Those 3 are I would say the top 3 issues that I've seen.
28:26
That people have debated and I think is there is there a right answer or wrong answer no it's just very specific to the product. Depending on which product you actually are trying to build and how much is your risk appetite and what is the true, you know, harm that you identified.
28:41
I think defines the path forward. But I would say that those would be in my mind, probably the 3 main.
28:48
Outside difficulties that are kind kind of summarized across all the products that I've built so far.
28:54
Yeah, I'm glad you mentioned, you know, looking at other systems that may be involved and connected to yours. Because that that really does make a much more complex system than when you're just putting a product out by yourself.
29:04
So if you're trying to talk to possible information system, it really, it really does complicate the issue.
29:10
One of the questions that came up while we were talking, off the list went out to Nick, but anyone can answer if they want to, which is what is mandated by the by the FDA.
29:17
So if you the particular question was around are there standards that are mandated but, we can mention some of the standards that are available now to help I do but is anything required and what is.
29:25
Required just from a general sort of submission into the FDA.
29:36
Yeah, so, the FDA doesn't call out a mandation to follow any particular standard, but they are looking for you to follow a process.

29:46
So the standards that I listed like Ti, 57 or ISO 27,001. These these are standards that kind of outline a a process that you could follow.
29:58
But I think as far as what the FDA is looking for is for you to document and describe your process to make sure you're meeting the intent to the guidance, but your process is kind of up to your own.
30:10
I think pulling the sources from all this information and making it complete story for your process to cover all your concerns is is the most important part.
30:19
Yeah, I think I'll just add to that is I think that I think something that we're working in a very closely with Sunrise as an example is I think you know, so our quality management system, essentially, I mean, like any other quality manual system, you know, has the phase for, you know, requirements definition, risk management right upfront.
30:38
But most of the risk, we're going to ask Christine who is alluding to is focused on its safety risk assessment.
30:44
And but I think having a very specific SOP that's targeting cyber security risk assessment. Specific requirements. On cybersecurity. Creating those standard operating policies and then following those policies through design through test.
30:58
Through documentation. Then kind of is what I think, Nick, alluding to by saying process.
31:05
So that's kind of the process that at least we have, as followed. This is kind of how is, what, you know, companies that are dealing with data that are dealing with cyber security issues that are doing is to incorporate SOPs because at the end of the day engineers follow you know design control processes.
31:22
If you want to create that attitude and that mindset of security by design. That has to be part of a policy.
31:33
Okay, and the other the other question that came out of this was kind of long question so I'll paraphrases a little bit but. This question is asking about non-medical software. So maybe it's like an DDS or something like that that's interacting with a medical device and would you have different considerations there.
31:50
So I think First thing that I would say is the whoever developed the medical device software is certainly responsible for the cybersecurity of that device.
31:59
But, I don't know, Christine, if you have a few thoughts on.
32:06

If you were developing something to interact with the medical device, you know, again, maybe it's like, MDS or something like that.
32:13
Would you follow the same process? And, you know, what would you see is maybe some negative differences or even maybe there's only minor differences.
32:23
That's a good question. Okay.
32:29
I can also jump in. One of the things that I think would be a little bit different maybe would be, the way you're doing the risk assessment, right?
32:35
So if it's not a medical device. Maybe you're not as concerned about patient safety, right? By definition. It shouldn't be, right? But I think the process may be similar.
32:46
Okay. Yeah, I think the outside the process has to be similar even if you're interfacing with a medical device.
32:55
And you're providing that software back end, for example, you know, that's what, the, many people about data systems are. And that's why they're class one typically. And the the thing though is that I think at the end of the day As I mentioned earlier, about interoperability.
33:22
You have to make sure that the data is coming into your MDDS system. Is somewhat encrypted, right? Because I think in a year because the data is getting shipped from a medical device to your MDS system.
33:33
So at least you have to ensure when the data is coming in, what kind of controls can you establish for integrity checks as an example.
33:39
So these are things I think you will have to kind of ensure happens when the data comes in. So I do not necessarily think that it's a different.
33:46
Approach to security assessment and security management security planning and security and corporation. But I think it's just the it becomes a shared responsibility model.
33:57
Where you are actually sharing the responsibility of cybersecurity with the devices that you're interfacing with.
34:05
And so an example here would be, you know, like it's the similar example of that I can give when I let's say if I build a SAS platform.
34:12
And I'm working, I'm developing it on a show I'm developing around AWS. Typically you have a business, you know, agreement addendums with these kind of companies, right?

34:20
And these addendums are essentially the idea of, hey, I'm using your infrastructure to build my application. So we have shared responsibility for security. And so that's kind of the idea that kind of that kind of goes along with, you know, any MDDS system.
34:35
Even though it's not medical software, but it's still a software that is supporting a medical application.
34:42
Alright, thank you. Maybe one last question before we kind of move into the, but if we kind of wrap up, talking about sort of developing the product on the development phase that you would go through normally.
34:55
Maybe you can talk a little bit about how often you sort of go back and revisit your threat model. We visit. Any like known vulnerabilities, that type of thing as you go through the development process.
35:09
Yeah, absolutely. So some of the things for me that triggers me to revisit my risk assessment is kind of 2 different factors.
35:17
One is presumed use cases and features. Any changes to the product landscape or definition really should cause you to reevaluate your risks.
35:28
You could have really changed your risk landscape by modifying the use case or the features of the product. So that would be stuff if I was making a new alpha beta where we or a version 2 we would re-review and go back through the process.
35:43
The other thing that really informs that is in there's one of the recommendations of the FDA is to integrate.
35:51
Your monitoring of your software if I know the provenance or soup. During your development life cycle.
35:58
And some of the benefits of that is when you start seeing new CVEs or common vulnerability enumerations, which are basically just reports of different vulnerabilities that exist in different software systems that if you are ingressing those in analyzing those the development phase, they're better adequately describing the landscape of your software.
36:18
So if you see that, you might see that that is a higher risk than you originally assumed and has different types of impacts.
36:25
So continuously monitoring for different phone abilities or different. That might exist, those can continuously feed back into your risk assessment. So ideally, this is a continuous process that you're evolving as you get new information. As you go.

36:43
Alright, Christine, you should have any last minute comments on the development phase before we kind of hop over to.
36:50
Some of the more vulnerable analysis and soup and things like that. No, I think, I think we covered this place well.
36:59
You can move to the next section. Okay. No, alright, so if we now jump into V and V, right? So you have your, product.
37:08
Process develops you know you go through the implementation phase and now you're kind of getting into how you're gonna test this so you know it's a bunch of things that are gonna be required as part of your submission including an S bomb and vulnerability analysis.
37:24
So Nick maybe you can talk a little bit about. You know, how do you evaluate soup? How do you find vulnerabilities that maybe in, components that you've incorporated in, but that's an operating system or, you know, drivers or whatever that is, how you do vulnerability.
37:44
Yeah, absolutely. So one of the very first steps is in order for to investigate and determine what kind of vulnerabilities is to really build a catalog of what you got.
37:50
Because without having an adequate understanding of the composition of your software components, it really won't be able to do a really in-depth analysis.
38:06
So kind of very first steps is looking at your systems. And determining all the different software that's ever under concern.
38:14
That doesn't necessarily mean software that you've written if you're using off-the-shelf parts off-the-shelf hardware and you're just configuring it, those are still points of concern. So that we've been calling that the security bomb or a software bomb. So building that S bomb is a really important first step.
38:32
How you do that is going to be a little bit different per system. Different types of systems such as interpreted languages have really nice package managers that will output you a complete manifest of all the packages you're using.
38:46
Other systems are a little bit more difficult where they don't use package managers and we have to use something called software composition. Analysis where we do, we do almost open source fingerprinting of binary images to find all the different types of soup that are in a system.
39:02

You'd be surprised. Often sometimes you'll have multiple of the same library embedded in different parts of your systems, all with different vulnerabilities. So it's really important to get an accurate understanding of as what is in your system. Once you have that accurate list, one of the important thing of continuous monitoring is taking that list and looking to what are the reported, vulnerabilities and anomalies with those different libraries.
39:24
Those will greatly inform how those impact your system. You really will have to go through it and in the first time it might be kind of a big list of vulnerabilities to analyze but you need to go through those one by one and understand the impact to your system of every vulnerability.
39:46
After you've made that initial pass, it may it gets a little easier because you're only looking at changes. As they accrue over time. But you need to do that first initial vulnerability scanning. Once you have that S bomb, my preference way is there are a lot of great tools out there, especially if you generate your S-bom into a format that is interoperable with other systems.
40:06
One example example is Cyclone DX. That's a really nice format that allows you to feed your S bomb into different systems that can do vulnerability analysis by going to different databases.
40:20
Of reported anomalies and ingressing all those data to give you a list of different vulnerabilities.
40:28
Which you can then take and do a security analysis of how that impact your system, which is a Probably the most important part because while you might have a CVSS or a condom and vulnerability, score of that is very high.
40:43
That may not impact your system at all and have no relationship. Or you might have one that's very low that does directly impact your software and its safety profile.
40:52
So it's very important to go through an enumerate. And look into each one of these vulnerabilities.
40:59
Good. Oh no, as on top of that, there's other types of testing options that you might want to employ to interpret during development such as continuous vulnerability scanning of your software through static analysis.
41:09
Testing of the inner, other interfaces, and even potentially fuzz testing to try to catch boundary conditions.
41:20
So. Okay, thank you. So Christine, I don't know if you've, have you seen tools for or techniques for storing the S?

41:31
As part of the cyber security. Work that you can. Yeah, but one consideration on, storing. You know, that is part of your configuration management.
41:46
So if you've got us a configuration management plan, that should be. Discussed as how you are controlling that.
41:56
And, BS bomb is. Really, a blueprint to your software. So. It's really important to store the S.
42:02
Mom and a high integrity secure location with limited access. Because we You don't want this kind of information getting to the hands of your adversaries.
42:18
And so I think that's an important consideration on storing SM. Yeah, another aspect.
42:26
Making sure your S. It's obvious that libraries and packages are. Should be listed but you know, Docker images, drivers, firmware loaded on ships.
42:43
It's, It's important to think about all the software that's comprising your system.
42:50
Alright, I don't know if you can talk a little bit about just when you find some of the vulnerabilities that Nick was talking about. How do you evaluate them? How do you store them? How do you how do you decide if it's something you need to address or something you can live with?
43:04
Yeah, it's a great question. I think, you know, there's as Nick mentioned, so there is the process of I think, you know, identifying these, you know, these vulnerabilities and scoring them and then the other aspect of this is to how do you assess based on the severity and the score, how does it impact your system?
43:22
I mean, that is something that I think we've discussed a few times in a few different ways. Is I think it comes down to, you know, your system security risk. So if you have a very well-defined security risk plan and risk management and you know what And if you've done that homework in your initial phase of your design.
43:40
Then this is just a mapping exercise. This you just look at, you know, the, the scores that you received because again, you know, as Nick mentioned, you know, these databases exist, you know, these tools exist, you know, these tools run through.
43:53
Existing vulnerabilities and assess if your system is exposed to it or not and gives you a score. And you know you are the best.
44:00
Person for your application. You know exactly how it's gonna impact your system. So if you have your risk document, you have this one member, it's a comparison exercise.

44:10
So I think it's, no different than the way people assess safety. It's the same process.
44:18
So, at least that's, I would say that's the simplest answer here. Like. So it comes down to again. You know, doing your homework upfront and knowing your security vulnerabilities upfront so that when something shows up that sounds bad but it's like hey doesn't impact my system for one reason or the other.
44:38
So we're not we're not doing any we're not storing any patient data so we're not worried about this.
44:44
Encryption issue on the device. For example, so it's a function of the thing the application.
45:00
Hmm. Okay. So We've got about 15 min left, but before we kind of move on to post market, I did have one more question for Nick, which was In terms of, you mentioned fuzz testing, so you know, fuzz testing, penetration testing, so maybe you can define those a little bit and and kind of say what the goal are and is there a particular time where you think those are more important
45:14
to do than others or is there times where you can do a lighter version of that testing.
45:20
Yeah, absolutely. There's since. Security is such a ever moving and evolving topic. More and more different testing strategies and testing tools are constantly coming out to help you evaluate the security risk of your product.
45:35
So like I've mentioned fuzz testing is it's a great testing tool for interfaces to just produce random entropy of data to see how your system responds.
45:46
That doesn't necessarily mean it's it's an exploitable event, but you might catch instances where you're software and misbehaves.
45:54
So the fuzz testing will take external interfaces and really just through them through a bunch of variability.
46:00
And make sure that a robust. That is something that can start very early. It has really no pre.
46:07
Pre conditions other than you have the interface present in order to fuzz test it and it's one I'd recommend doing early.
46:14
The other types of testing, security road, obviously when you're making your risk analysis, you're going to have a bunch of mitigations that you're going to generate.
46:23

Those are all going to be security level requirements and they need to be tested and verified as well as any of the other requirements in your system.
46:30
So testing those security ones to show that if you have a risk of denial of service which might have additional risk of your product such as delay of therapy or any any other types of risk that those are tested and shown to be implemented.
46:46
Other types of testing I like to do on my products in order to get kind of ahead of the game is to do my own vulnerability scanning. So there's open source tools out there such as Nessus or a Metisploit that allows you to point at interfaces and those CVEs that I was mentioning, they also have a great database in these tools along with Python scripts or any other types of scripts that actually will exploit them.
47:09
So you can point these. Scanning tools at your product. And look for the vulnerabilities yourself. Try to find them. You might, you might be surprised to what you find. But finally, when you're getting to the later stages of your product, I always recommend going through a third party to do penetration testing.
47:27
That can be an engagement in varying levels. You can go everywhere from what I call white box testing all the way to black box testing and even with gray box testing in the middle.
47:38
And what I mean by those box metaphors is that you provide the penetration testers with varying amounts of information for your system.
47:46
The goal is to get back as much actionable information as you can. So going complete black box testing has some downsides of where it will take a lot longer, but they are equipped with the same knowledge as most people would externally.
47:59
So you might get a more accurate representation, but it takes longer. Providing clear box or gray box testing, you give them requirements, design details, libraries, which allows them to be more actionable and be more targeted in their testing.
48:13
That's usually something I save and will probably engage periodically. Through the post of the device, but.
48:20
There's a kind of the varying, there's probably more in there that I miss, but those are kind of the high levels.
48:27
Alright, thank you. So I one question came in while we were talking up just kinda throw this out to whoever wants to jump in but The question was, do you have to do threat modeling?
48:38
Funds testing or other types of testing. If you don't store patient data on your device.

48:44
So I would recommend. If your device balls into the cyber device category of the medical devices, then yes, I think that those do apply.
48:56
And I also think that fuzz testing, even for a non-medical device, is a great tool for testing robustness of interfaces to make sure there's a lot of unforeseen circumstances in the world and with analog systems that you You can't always consider for so I think they are good robust strategies regardless of the different types of devices.
49:17
So I would implore to use them, they make a better product anyways, even outside the cybersecurity space.
49:25
Alright, awesome. Alright, well we have a few minutes left so I did wanna, you know, one last topic that I thought would be beneficial to talk about today's, post market.
49:35
So, should maybe you can define, you know, what, do we mean when we say post market? Obviously you've gone through development, down to your testing. Now you just put the put it out there.
49:43
What activities are you doing in the post market to try and keep the device secure? As it gets more and more acceptance in the field.
49:52
Yeah, so, you know, post market is. You know, in this world of as we discuss evolving threat landscape, right?
50:01
I think, you know, post market is about, you know, looking at many different aspects of how you, you know, ensure that the safe views of your device.
50:09
And secure user for device when it's in the wild. And that entails a whole bunch of things. It starts by, I think, our ability to, you know, continuously monitor. You know, this, the product.
50:22
And continuously be up to date with threat intelligence. And being able to know exactly, you know, there's a new threat that has come up to be able to have the ability to scan for those, understand those.
50:35
And then react to those. Through updates and patches. So which is essentially kind of the aspect of. Condition monitoring and that's about the thing vulnerability modeling and monitoring as well as you know making updates and patches, to actually, you know, against them or protect against them.
50:54
Despite our best efforts, you know, there's always a situation and that can arise. And therefore post-market, surveillance is also about how do you actually respond to incidents and how do you respond and manage those incidents?

51:10
So having a good insurance response plan and having the ability to collaborate with stakeholders and notify them about breaches, about security issues. Is the importance of having incident response plan and management? That's one other aspect of this. We talked about these databases in response plan and management. That's one other aspect of this. We talked about these databases on vulnerability.
51:31
How did they come up? Well, because when different companies and different folks faced. These kind of cybersecurity threats they had to report.
51:40
Right, so there's a requirement around regulatory reporting and maintaining compliance. So when you actually face this, over together issue.
51:46
We have to have procedures in place to be able to report these things to the regular bodies so that again that adds to the database but also is important for us to be aware of these things.
51:56
And then, and that thing goes, it also is about, I think training and education, around these things that I think is also making people aware that, you know, that, you know, there is you know, we will have to do software updates, you know, walking to hospital every 3 months and asking them, Hey, I need your system to update the software is not something that anybody likes.
52:11
But that's the reality of the situation, but can you do that remotely? If you want to do it remotely, then how do you want to do it?
52:22
So. Capabilities like that and things like that is what I would kind of consider as. As post-market surveillance in a broad scheme. I mean, there's many things that have to be considered, but I would kind of summarize it in that way.
52:37
Alright, thank you. So Christine, she's talked a lot about the patches. So I don't know. You know maybe you can just talk a little bit about the process of how you would go about You know, to verifying a pat, right?
52:51
So you're, you identify a vulnerability, you have maybe an incident, and then you need to get a patch out there. So what's, sort of. Activities would you revisit as you're preparing that?
53:04
Well, certainly if you're changing the software, you've got to make sure. That you're not introducing any additional safety risk associated with that.
53:13
And of course there's going to be a regression testing too. So that's where we have the systems approach, right?
53:22

With security and safety. Actually Nick, I remember the story you told about good example of where that could be.
53:30
What is, you decide you want to add encryption. To our communication. Interface. Yeah, it uses more processing power and.
53:44
If you're on a battery upper device you're life of the device is now reduced. And that could be a safety risk.
53:51
So it's definitely part to think about. What kind of safety risk or maybe even other security risks that.
53:58
Could be there. You know, automated testing is recommended so that when you're doing your regression it's Not a huge lift.
54:08
And looking at the vulnerabilities themselves sometimes. The vulnerability is not. Related to your use case.
54:22
So if you have a library, library does a bunch of things, but you're only using this small intended use that's not affected by the vulnerability in that case to do that analysis.
54:32
To not necessarily have to do it Patrick, cause there's always a risk. So.
54:40
Those are some. Considerations and so. Touching on what shit said, it's very important to have a plan about how you're going to do.
54:48
The patch. And talking about how often you should be doing. These monitoring. Ideally it's a venture event.
54:57
So because. Yeah, very important point is. You're a security effectiveness.
55:05
Is really correlated with how fast you can fix it. So the longer the vulnerability is out there. The more likely there could be an exploit. So being responsive is really important.
55:17
Alright, thank you. Well, we're starting to get a little bit tight in time, so I'll just kind of open it up and see if anyone has me last thoughts.
55:26
It's other say otherwise. Nicole, there was a question about, can we provide a list of Sanders that we mentioned in the air?
55:32
So if we can maybe email that out afterward, that would be good. But does anyone have any, final thoughts?
55:39
Yeah And if not, well, we'll probably end up wrapping up. I think we've gone through a lot.

55:48
There's a lot of areas we didn't touch on today either. Series of post-market things and, submissions to the FDA, which we didn't really get into.
55:55
But I hopefully you guys found this. Informational and if you do have questions you can always try and reach back out to sunrise and we can help you with that.
56:03
But I think I'll turn it back over to, Nicole and we'll wrap up so we can finish up by one.
56:12
Alright, thank you so much. What an awesome conversation. Dave, is there a good email for folks to reach out to Sunrise? If they have any questions.
56:22
Bark, do you have a generic email that or an email that would be best?
56:28
Okay. Or do you have a slide you want to flip to? Maybe it has the contact information. Regardless. Awesome. Yeah, there's this there's a slide. Yep. There we go.
56:34
Thank you. So much everyone for joining us today. Thank you to our panel. Really appreciate your expertise. Just want to say thank you to Sunrise Labs for sponsoring today's content. We can't put on these expert panels without support of members like you.
56:46
So really appreciate that. Please make sure to check out mathematic.com and go to our events tab and see all of the great events we have coming up.
56:57
And we'll see you next time. Thanks so much. Take care. Hi guys