Podcast Transcript

Risk Never Sleeps
Episode 51
Sam Stevens

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people that are on the front lines, delivering and protecting patient care. I'm Ed Gaudet, your host today, and I'm joined by Sam Stevens. Sam, welcome.

Sam Stevens: Thank you so much for having me, Ed.

Ed **Gaudet:** And Sam, you're the director of information security at Essentia.

Sam Stevens: That is correct. Yep, and I've been with the center for about five months.

Ed Gaudet: All right, cool. Tell us about your current role and the current organization.

Sam Stevens: Essentia Health is a healthcare provider based out of Duluth, Minnesota, ranges between North Dakota, northern Minnesota, and northern Wisconsin. So it's mostly rural, but we provide healthcare to folks in multiple different towns and cities up north. We also just opened a new hospital. Saint Mary's out of Duluth kind of dominates the skyline up there, so it's pretty nice. As far as my role, I am the information security director, as I said. I oversee cybersecurity for the organization, essentially. We have a CISO above me, he's a VP and a board member, so I handle more of the operational day-to-day cybersecurity, anything from vulnerability management to risk management to really incident response compliance stuff, yeah.

Ed Gaudet: So you're pretty busy.

Sam Stevens: A little bit, yeah, a little bit, yeah.

Ed Gaudet: And I see in your background you were in the Navy. Thank you for your service.

Sam Stevens: Thank you, yeah, I actually just got out in 2020, so a few years ago.

Ed Gaudet: Oh wow. During the pandemic of all times. Oof!

Sam Stevens: Yeah, my last deployment was actually a pandemic deployment, which was which was pretty rough. It was, yeah, luckily, I got off for the rest of my shipmates out there, but it was about four months at sea, not allowed off the ship at all, so.

Ed Gaudet: Oh, geez.

Sam Stevens: That was good times.

Ed Gaudet: And where was that? Where were you?

Sam Stevens: Yokosuka, Japan. Oh, yeah, the USS Ronald Reagan. I actually, it's funny, we had to go into quarantine around April 2020, so I spent about two weeks in a barracks room with tape on the door, you couldn't even. So if the tape broke, they would know that you had to restart. And we pulled out for this kind of training that you do prior to deployment for about five days, pulled back in, and then I wasn't allowed off the ship. My wife and I had our anniversary in May, so we had, I had to stand on the fantail and wave at her from the pier.

Ed Gaudet: Oh geez, so terrible. But look at the memories you have.

Sam Stevens: Yeah, yeah. Won't lose those anytime soon.

Ed Gaudet: Yeah, exactly. And I know you have done some ethical hacking. So you've been trained as an ethical hacker. So tell us about that and what that means to you in your role.

Sam Stevens: That was a little bit, that was a few years back, I think it was 2016 when I got my certified ethical hacker. At the time, I was in between commands, or I was about to leave my first command in the Navy, and I wanted to really advance my career and have a better technical understanding on the security side. Because, for my first few years of my career, I was mostly on the sysadmin helpdesk kind of side, but I had some secondary duties that were more on the identity and access management side of security, so I wasn't a very well-rounded security professional at that point. Like I had my ... plus. So I went for my CEH, and the reason I went for it was basically that I wanted to understand a little bit more from the offensive standpoint, what are the bad guys doing? Because, I mean, in order to stop them, you have to be able to think like them.

Ed Gaudet: Exactly.

Sam Stevens: That was early on. So since then, my priorities have been shifted around quite a bit. But I think in my role now, I still have that same mindset of I like to think like an attacker thinks, even though I'm not nearly as smart as they are. But I think that understanding in general what areas we need to focus on and how to prioritize risk and cost and all that and communicate to the business at all, it all folds together.

Ed Gaudet: Yeah. Which gives you a unique perspective, obviously, as you're building out your plans and managing the operations, and must come in handy, I'm sure. How did you get into healthcare?

Sam Stevens: When I left the Navy, my first job was, I was a business information security officer for the state of Minnesota. So I oversaw the departments of Public Safety, corrections, and Veterans Affairs. Veterans Affairs, as you probably know, is a healthcare organization, more or less. I mean, it's a little different than Essentia, obviously, because it's government and it's a little bit more pigeonholed, but it is healthcare. We had to deal with Biomed devices and just different type of data sets that we had to at public safety, like at public safety.

Sam Stevens (cont'd): We had a lot of sieges, and in corrections we had a lot of sieges, but at Veterans Affairs, it was mostly PHI that I had to worry about, and we had some PCI and a lot more personal, identifiable information to be concerned about versus somebody's arrest records. So that's kind of where I got my feet wet in healthcare a little bit. I spent a few years there, and actually, my boss, who was the state CISO at the time, left to be CISO at Essentia, so that's kind of where my transition started. And I loved working for the state, but I always kind of had the idea that it was more of a stepping stone, because I have been military, and going from military to another form of government is a good transition, but I want to do more things and see more things.

Ed Gaudet: And healthcare, I think where there are some parallels with the military is that shared mission. And what does that mean to you?

Sam Stevens: I think that it's purpose-driven in a way that I probably wouldn't see. I mean, I've never worked for a Fortune 500 company, and I can't speak to that. But I think the way I see it is so far my role has been kind of a kind of stepping stones, but still in the service direction. So obviously, it was military, it's the ultimate service because you're constantly serving and you're completely under the thumb of the government, and you do whatever they tell you to do all the time. So that's one extreme. And then I went to the state government, which is still amazing way to serve your community, your state, your. And then I went into healthcare, which is, to me, it's a little bit smaller scale, but at the same time, it's just as important, and it's also very service-oriented. It's about patient safety. It's about protecting people. It's not about the bottom line as much. And it's a nonprofit too, essentially, so.

Ed Gaudet: Well, it helps you build that servant leadership muscle too.

Sam Stevens: Exactly.

Ed Gaudet: As you develop, which is great and again sets you apart from others, certainly, that come out of a profit industry, if you will.

Sam Stevens: I've heard some bad things from colleagues about working in the profit industry. I don't know. That was at the state where most people have probably been there for a long time, and they're used to a certain way of life, but I don't know if it would fit me well. I mean, we'll see. I got some years left to go for.

Ed Gaudet: A couple anyway.

Sam Stevens: A couple of years left.

Ed Gaudet: So as you think about the next 12 to 24 months, what are your top 3 or 5 priorities?

Sam Stevens: So number one is ... Reason being, mainly I know everybody talks about AI until everybody's blue in the face, but I mean AI is really going to enhance the need for a zero trust architecture. It's going to need to, It's going to enhance the need for thorough identification, validation of who you are and, what your purpose is, and what you're accessing and when. My current organization, we're just starting to go through a zero trust, we're going through a third party, and we're going through a zero trust assessment, and then we're going to build out a roadmap, and that's going to be really our biggest priority. So that would be my number one focus. But I mean, from a secondary standpoint, from a broader standpoint, being new to this organization and coming in new to multiple organizations, really with the state government, my biggest thing is always, build the foundation first. So everything starts with policies. Right now, we're completely revamping our vulnerability management policy, right? I come in, and I look at all the policies. Are they good enough? Are they not good enough? Most of the time, you're probably going to say no if you're new, you know, right? You have your own idea the way things should go, but you build that foundation, and then that gives you some teeth to start to enforce things. And you can really start to track your risks and start to understand who's accepting those risks and get a better understanding of your environment.

Ed Gaudet: Great point, and those policies have to be obviously dynamic and reviewed on a regular basis, because everything changes. A couple of years ago, nobody knew what tracking software was, and now all of a sudden, we care about tracking software, right?

Ed Gaudet (cont'd): And we're just at the top of the first inning as it relates to AI. We got a long ways to go before that becomes fabric to the way we work.

Sam Stevens: Exactly. And something that I think is going to be really important to you, obviously, is third-party risk assessment. Yeah, that's something that I think everybody thinks in security. But it's extremely important because we have so many relationships with so many people, with access to our technology, access to our data, and it's so hard to just understand where our risks are in that arena. We have our set of questions that we ask every time we bring on a new vendor, but it's how in-depth is that really going? Are we really doing our due diligence in that area?

Ed Gaudet: Yeah, we have to move from that point in time notion of an assessment to much more of a continual assessment across the life cycle of the relationship we have with the vendor and obviously the product or products or services that we have.

Sam Stevens: Revamped that every once in a while, you know, a spreadsheet somewhere. It's not really conducive to that.

Ed Gaudet: It's a great point. So you brought up a couple of things that keep you up at night, I'm sure. What are some of the other things that keep you up at night?

Sam Stevens: Oh, I mean, number one is always going to be ransomware. And the only reason I don't mention that necessarily, as my focus, is because ransomware is also broad, and you're trying to stop the kill chain, and I think zero trust is a big part of that. But as far as threats go, it's terrifying. They just continue to have additional get more funding. There's more threat actors that are popping up every day. I'm sure you know about what happened in California a couple months back with the Receita ransomware and hitting healthcare organizations and we're critical infrastructure. They understand that we have a need to maintain patient safety. So when you have that need, that drives the actors to want to target you a little bit harder.

Ed Gaudet: Yeah, and they follow the money.

Sam Stevens: They follow the government, and I saw it in the military.

Ed Gaudet: And they follow the money too. And they know that, again, if it's a, if we don't have our act together and we can't recover, which is really much more important now, I think these days than even protection, because it's not a matter of if, it's a matter of when and when it does happen. I always say that as long as you can recover in a reasonable period of time and continue operations, then maybe you don't have to pay the ransom, right?

Sam Stevens: I love that matter of if not matter of when, because I think that's still a really foreign concept to a lot of folks that you're trying to communicate with who aren't involved in this every day. And I think there's a misunderstanding sometimes, in the non-security world, where folks think that if something like this were to happen, it's a major fault on either IT or on security. And that could be the case, but I also think that we have to continue to push that there's no such thing as zero risk, and that we don't necessarily always know what the threat actors are doing. We can try to stay one step ahead, but at the end of the day, the good guys are always going to be a step behind the bad guys, because we're the ones conforming to what they're doing once we find out they're doing it.

Ed Gaudet: That's right. And the organization has to prioritize cybersecurity. It has to be a first-class citizen at the board level. It can't be part of another committee, and it can't be an afterthought. It has to be part of how the leaders actually think about the business because we are so reliant, like you said, on those third parties and technology, and it's no longer a matter of if it's a matter of when and can we recover in a timely fashion to keep the business running.

Sam Stevens: It's a multifaceted approach, right? You need to look at it from a, how often are you assessing your entire organization, looking at a framework for whatever you're using to look from beginning to end, from identify, detect, protect, respond, recover? Like from the entire thing, what are we looking at and what are we missing, and what do we need to improve on? I also just think that risk is such an interesting concept because everybody looks at it differently. It's essentially mean, not always, but it's essentially subjective, right? I mean, a lot of times, you're applying what you think, and you're assigning kind of a quantifiable metric to what you think.

Sam Stevens (cont'd): And there are metrics that are measurable, obviously, but when you're saying, okay, we're going to measure this area, and this area is a higher risk than this area, saying threat times vulnerability times consequence. But how are you assigning those, and how are you actually thinking about that?

Ed Gaudet: And how do you know your program works, right? You can have all these fancy calculations and data cubes running analysis for you in the background and lakes of data, etc. How do you know it works? I think that's such a critical question that people can't answer when you really probe.

Sam Stevens: Yeah, and I mean, what does works even really mean? You know, if you stop at 99,999, but there's one that gets through, and that's why obviously it's spoken to death, but the defense in depth and being able to understand the kill chain and where your biggest threats land and say somebody does click on that phishing email. There's some kind of Cobalt Strike. Something's going on in the background, right? How are we stopping that before it gets to a point where they can encrypt everything?

Ed Gaudet: Yeah, all these things are part of an ecosystem. And ultimately, if you don't have the training, if you're not enforcing that training with good behavior, because again, people will do what they're going to do, and we have to remind them, don't click on.

Sam Stevens: You can't control 15,000 people.

Ed Gaudet: Exactly.

Sam Stevens: I wish I could, that'd be nice, but yeah.

Ed Gaudet: Never going to happen, especially in healthcare. All right, that's great. The last couple of years have been difficult. We went through a pandemic. Obviously, you went through a job change, a couple job changes. So you've had an interesting last couple of years. What are you most proud of personally and professionally?

Sam Stevens: Oh, that's a good one. Honestly, I would say my transition from the military was not easy for obvious reasons. I went from being on a ship during the pandemic, and I came over to the US again, and I was, I had to quarantine again in Washington, and meanwhile, my wife was in Minnesota and trying to get settled. And I, while I was in Washington, I started my master's program, and then I also moved into my apartment and started doing all these different things with my new job at the state at the same time, and then all the while, trying to go through getting my master's in security technologies from the University of Minnesota. So shout out to ... for that. But, and then, once I was finally done with my master's degree, I moved again. I got to, finally got my own house. So that's a big milestone. But I think, long story short, I think that the thing I'm most proud of is just all those things in succession and meanwhile trying to wrap my head around the transition from military life to civilian life because it's just such a culture shock. You just, you think you're prepared for it. But until it really happens, you're not really, I don't know. I know a lot of guys got it harder than I had because I was lucky enough to have landed a job before I got out. But just that, going from, especially during the pandemic, right? I went from a job where they wouldn't let me go home to a job where they wouldn't let me go to work. So it was extremely shocking.

Ed Gaudet: That's shocking, exactly. You have a lot to be proud of, it sounds like. That's excellent.

Sam Stevens: Thank you.

Ed Gaudet: So I imagine you have other hobbies and passions outside of healthcare and outside of cyber. What are they?

Sam Stevens: Passionate about?

Ed Gaudet: Yeah. Yeah.

Sam Stevens: So I'm a musician. I actually, before I joined the Navy, I went to music school, which is part of the reason I had to join the Navy because it was a bad financial decision. But I've been playing guitar since I was a teenager, and now I have actually behind me. I've got like a whole whole studio in here, and I'm trying to write an album and I've got one song up on Spotify now.

Ed Gaudet: Oh my gosh, Holy Cow, that's cool.

Sam Stevens: Thank you. Thanks. That's one of the greatest things too about.

Ed Gaudet: What genre?

Sam Stevens: My own, I guess indie rock and ... in general.

Ed Gaudet: No, I love indie rock. Okay, let's go to this question then. So you can see my, this is my first love right here. Probably ... You're a Meyer fan? You must be a Meyer fan if you're a guitarist, right? Personality aside, guys in the, virtuoso, right? He's ...

Sam Stevens: Yeah, he's a beast. He's a beast. He's a beast. He is. Yeah. There's there's no question.

Ed Gaudet: All right. So you're on a desert island. What. Top five albums. No, no greatest hits now, would you bring with you?

Sam Stevens: Oh, five albums? I would say number one would be Red Hot Chili Peppers, Stadium Arcadium. Just because it's a double album. I don't know if that's necessarily my favorite album of theirs, but it's.

Ed Gaudet: I love the double album. That's a good call, by the way.

Sam Stevens: Yeah, it's like cheating the system, right? You know.

Ed Gaudet: Greatest album, but you get two albums in one. Yeah, yeah. That's why like LED Zeppelin, Physical Graffiti is my double album.

Sam Stevens: Was about to say Zeppelin 4 would have been my.

Ed Gaudet: Four is great, yeah, four is good. Yeah.

Sam Stevens: And Physical Graffiti would have been smarter though because it's a double album.

Ed Gaudet: Yeah.

Sam Stevens: Let's see, after that would probably be the Beatles' Abbey Road.

Ed Gaudet: Some just.

Sam Stevens: I love Abbey Road.

Ed Gaudet: Awesome album. Yes.

Sam Stevens: It is, and then let's see.

Ed Gaudet: You're an old soul, Sam. That's good stuff, man. Nobody says the Beatles anymore.

Sam Stevens: Yeah, my parents are, were a little bit older when they have me not, but they introduced me to a lot of the, their boomers and the truest sense of boomers. And then I would say The Strokes, Is This It? That's, that would be one of my favorite albums ever. And then, one more? I shouldn't overthink this, right? Like it really matters. I'm not in a desert island.

Ed Gaudet: No, you're not. But if you are, know your five albums.

Sam Stevens: Yeah. That's true. I'd say Streetlight Manifesto, the Ska Band. I don't know if you ever, ever heard of them, but.

Ed Gaudet: Don't know them.

Sam Stevens: And now I'm blanking on what the album is, but it's their third.

Ed Gaudet: Streetlight Manifesto, cool name. I'll have to check them out.

Sam Stevens: Oh. They're amazing. I mean, ska is kind of an acquired taste.

Ed Gaudet: I love ska, I love ska.

Sam Stevens: There you go.

Ed Gaudet: Yeah, no, I love.

Sam Stevens: Well, then you'll like Streetlight. I will tell you, they are the purest form of.

Ed Gaudet: Mirror In The Bathroom? Do you know that song?

Sam Stevens: I do not.

Ed Gaudet: Oh, okay. I'm trying to remember the, I knew I was going to blank on the band. I've seen them too. Sorry, right?

Sam Stevens: I'm blanking on the album, and I'm saying I'd bring it to a desert island.

Ed Gaudet: It'll come to me. Are you a Jam? Do you know the Jam? You ever hear the Jam?

Sam Stevens: Jam? I don't think so.

Ed Gaudet: No? Oh, man. Wow. Really?

Sam Stevens: Is that another ska band?

Ed Gaudet: Oh, no. Early, almost like punkish early 70s, out of England, I think they're out of Manchester, but I'm not sure, but.

Sam Stevens: Cool name.

Ed Gaudet: Yeah, The Jam. Yeah. Great, by the way, great band. Check them out.

Sam Stevens: I definitely will.

Ed Gaudet: Yeah. So I'll have to check out that ska band too. And I'm trying to think of the band, I've seen them too, in concert too. It's going to drive me crazy. I'll email to you later, because it'll come to me tonight.

Sam Stevens: Appreciate it.

Ed Gaudet: So I'll check them out and you'll have to send me your Spotify link. I want to hear your, if you don't mind, I'd love to hear.

Sam Stevens: Absolutely not.

Ed Gaudet: Is it under Sam Stevens or?

Sam Stevens: No. I'm actually, I have a kind of a stage name I just came up with randomly. It's Mondegreen. M O N D E G R E E N. It's a word that means when you hear lyrics, but you mistake them for something else.

Ed Gaudet: Oh, yeah. Like eyes without a face, Billy Idol, and how's about a date? I think is what we thought it used to be, right?

Sam Stevens: Yeah, but I've only got one, I've only got one song up so far, and it's.

Ed Gaudet: That's okay.

Sam Stevens: First song I've ever really tried to release that way, but it's not just on Spotify. It's on all the streaming services. I went through the whole thing, but hoping to have an actual album together sometime over the next year.

Ed Gaudet: Awesome, that's great.

Sam Stevens: If I find the time for it.

Ed Gaudet: I did a recording when I was in high school. I'll have to send you that and get your thoughts on it too.

Sam Stevens: Yeah, that'd be awesome.

Ed Gaudet: Yeah, I wrote the lyrics and the music with a friend, and we actually went to a four-track studio and recorded it.

Sam Stevens: Oh, that's awesome.

Ed Gaudet: Yeah, yeah, it's pretty cool. Yeah, four tracks, exactly. All right. Riskiest thing you've ever done? I've got to ask it. Risk Never Sleeps Podcast. Of course. You've done a lot, sounds like. Navy, come on.

Sam Stevens: Oh, boy. I would say, you know, what's funny is I'm over here racking my brain, even though I read the questions before, but I just never came up with an answer, so now I'm still on the spot. Let me see. I would say the riskiest thing was probably honestly just joining the Navy in the first place, just because I kind of went in a little bit blind, like it wasn't, not blind necessarily, I have a lot of family in the military. My dad was in the Navy in Vietnam, so I had a lot of exposure to what to expect. But at the same time, it just came on very suddenly because I was gonna go back to school, keep studying music, and then I just found out I didn't qualify for federal loans anymore for whatever reason.

Sam Stevens (cont'd): And once that was determined, I looked at my, I looked at my life, and I said, I have no idea what the hell I'm going to do so, I don't know if we're allowed to curse on the podcast. I'm sorry.

Ed Gaudet: That's, I think, hell's a.

Sam Stevens: It's a pretty simple one.

Ed Gaudet: Hell's a borderline curse.

Sam Stevens: H-e-double hockey sticks.

Ed Gaudet: Yeah.

Sam Stevens: But so it was the leap of faith, I would say, which is pretty risky. It could have gone poorly. And then obviously throughout my time in the Navy, there was a multitude of of risky decisions depending on the situation. It was, it could have been risky for the job. It could have, you know, I was involved in a few NCIS investigations where I had to, I can't talk about them because of, you know, obviously, obvious reasons, but just being able to allow myself to, to agree to do that, I think was probably a pretty risky decision because you never really know what's going to come from that. And if you could be targeted because of the fact that you're part of that investigation or.

Ed Gaudet: That's a good point, yeah. So cool, all right. That's good. That's a good answer. Hardest lesson so far in your career?

Sam Stevens: I would say that the hardest lesson so far in my career was when I was on the ship. And to be honest, I was kind of a cocky little guy. I felt like everybody came to me for answers on everything, so I never really second-guessed myself that much toward the end of my time on the ship. You know, you spend weight, you spend 100 and something hours a week working. You're constantly working, so you're just an expert, absolute expert, and you can do this stuff in your sleep.

Sam Stevens (cont'd): And I was a security guy because I was in the security division, so I was kind of the security lead for the entire ship, and I prided myself on that, and then I took my CISSP and I failed it, and that was a major ego shot, yeah. Because I was trying to finish my bachelor's at the same time, and I was taking classes, and I was in port, and I remember my department head at the time had a ..., and I talked to him, and he was like, don't give yourself more than two weeks, because if you do that, you're going to overthink it. So I only gave myself two weeks after I finished my undergrad course, that was supposed to be a CISSP course, did not help me at all, by the way. And then I did two weeks of self study, went and took the test, didn't pass it, and it was just a huge shot to the gut. And I remember one of my buddies on the ship in my division, I went and I told him, and I was so upset, and he basically said, I don't, I can't exactly remember what he said, but I just remember it was something like, I guess, probably good for you to fail, because I was probably getting cocky. It's probably a good thing. It'll teach you some humility. Yeah, yeah, humility, I think.

Ed Gaudet: I've been through it. I've been through it. Absolutely, no, that's a, those are important lessons and those are the ones that last. Any parting advice to those folks that are getting ready to maybe join and jump into the cybersecurity profession or in healthcare, or maybe going to the Navy? Any last-minute advice for listeners?

Sam Stevens: In anything that you do, just make sure that you're taking a step back. If you get into a stressful situation, take a step back. Don't be reactionary. As much as you can, possibly, do not be reactionary. I mean, I speak to the Navy, and the Navy was, it was very easy to be reactionary. When you're under a lot of stress, you're not sleeping, you're just on edge all the time. And I'm not perfect in that at all. I was way too reactionary, way many more times than I even want to mention. So that's the biggest thing, is when you start to feel your blood pressure spike and you start to feel stressed, and it's going to happen in security, it's going to happen in IT. It's going to happen in any field you go into. Take a step back, breathe a little bit, and come at it as objectively as you possibly can, and people will respect that. Also, have some empathy. If you're going to be.

Ed Gaudet: Sprinkle a little empathy.

Sam Stevens: You got to have empathy. Otherwise, it's not the 1950s anymore. That's, unempathetic Leaders don't get anywhere.

Ed Gaudet: Exactly. No, great great advice. Thank you so much for joining us today. Sam.

Sam Stevens: Thank you so much for having me.

Ed Gaudet: Yeah, my pleasure. And for those of you on the front line delivering patient care and protecting patient safety, remember to stay vigilant because risk never sleeps.

CENSINET®

Censinet RiskOps™ Demo Request

Do you want to revolutionize the way your healthcare organization manages third-party and enterprise risk while also saving time, money, and increasing data security? It's time for RiskOps.

SCHEDULE DEMO

www.Censinet.com