Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host Brian Contos and we've got a very special guest today. Joining me is Ed Amoroso. Welcome to the podcast, Ed.

Hey Brian, thanks for inviting me. I'm glad to be here.

So Ed, we've crossed paths several times over the years as you have with most people I think in the cybersecurity profession. You're what I would consider one of the thought leaders in our space and have been so for quite some time. Perhaps you could give our listeners a bit of background on kind of where you came from and some of the roles you've had and what you're doing today.

Well, I'd be happy to. So I've been doing cybersecurity now almost four decades. I've kind of got into it at Bell Labs doing unit security and I never looked back. I eventually sort of mid-career got into the CSO role/Chief Security Officer for the combined AT&T, SBC, Cingular, DirecTV company. So that was a big responsibility. I've been an academic through that whole time, been teaching graduate and undergraduate students cybersecurity for three decades now. So I retired about three years ago and I started TAG Cyber. We're an analysis firm. So we do research and analysis and generate content kind of in that space where Gartner and Forrester and others compete. So thanks for inviting me and that's me.

Yeah. Thanks for doing that. Sometimes I forget that we are both at Bell Labs at very different times and locations, but of course I ran into you when you were running security over there at AT&T, which was just a massive, massive undertaking. I remember some of the key initiatives you put together there. Let's just really jump into it, y'know. Let's talk about security validation. Is it possible to validate security within an organization?

It's a tough thing because most types of functionality in computing, you and I can call the boss into a room and do a demo, right? If somebody says, "Hey, I need you to build a network that connects this to that." Pretty easy to demonstrate that, right? You have "validation" that the thing works. But now do the same thing and convince me that it can't be hacked. What do you do? You demonstrate the absence of hacking somehow? So it's really challenged. So what happens is we end up with all this compliance stuff, which for the most part is only there because you feel like you got to measure something. I think it's
a poor substitute for real validation at the operational, functional, technical level. But that's one of the challenges you have in computing, which are very easy to demonstrate the existence of a problem. It's very difficult to demonstrate the absence, which is what you need to do to validate security.

Ed Amoroso: So I would say we all do our best. I know there are a lot of really fine companies that build tools, Verodin being one of them, that help you do that sort of thing and I applaud that because it is one of the challenges. But the problem, I suspect you'd probably agree, is when you slide into this kind of compliance malaise where you're demonstrating and validating security by showing your ISO certification, that's not acceptable.

Brian Contos: Sure. Yeah. I hear a little bit of the New York background there coming through the windows. The thing that I wanted to ask you, you having run security from one of the largest organizations in the world. Where do you start? What's really the most important? Is it network? Is it cloud? Is it something else? Where do you decide to really focus your effort perhaps just even initially?

Ed Amoroso: Most people do start by thinking, right, it should be network, endpoint, cloud, blah blah blah. But I think it's more foundational, right? I think you set a culture in an organization. You try and build the basic kind of the building blocks, right, on which to do security. So I would say you think of it more ground up, bottom up, and get that foundational piece correct. That means having processes that are simple, that are documented properly, that people understand. Having computing systems that are open with clean interfaces that are not too complicated. Having team members that understand their roles and responsibilities that work well together. These have nothing to do with security architecture. But if you do any of those types of things wrong, you're going to have some trouble.

Ed Amoroso: So I think you start with these foundational things and then you build up from that. You build protection. I think if there's one sort of design concept that I think plays better than most in cybersecurity, it's that defense in depth concept, right? It's not enough to say, "Hey, I have a control in place. We're good." Yeah, that is a sentence that you hope nobody ever says of what we do. You'd prefer, "I have this control in place and I have these two others in case that control is bypassed or broken or so." So kind of on top of that foundation, you build the sensible defense in depth approaches that apply to a network and apply to endpoint and apply to cloud and apply to your apps and so on. You really do have to build a taxonomy of what makes sense.

Ed Amoroso: For example, if you're an industrial control company running a bunch of physical plant with SCADA and OT infrastructure, then you are going to have a different set of concerns than if you're an accounting firm, right, where everybody's doing white collar work with numbers and files sitting on servers in the cloud. So this
will be different but the foundations could be the same, right? You'd have the same kind of considerations around that basic building blocks on which you build your security. So I would say that that's how I would go about doing it. I'd start with the foundation.

Brian Contos: Well, and you know Ed, one of the things I've always enjoyed when I have conversations with you is your ability to bridge both the technical world and the business world and of course academia as well. Do people you think outside of security get this need and this sort of desire now for security teams to rationalize, to be able to measure, to be able to not just have to get away from expensive in depth if you will, and get over to actually real functional defense in depth and proving what's working or what's not? Is this an overarching theme that you're seeing? Are people embracing this at both a business and a technical level?

Ed Amoroso: It's been my... You mentioned sort of measuring and people looking at... Like you and I and asking for metrics and measurements and so on. A couple of comments on that. My observation is that there are three phases of need for metrics in a career. Maybe there's some sort of a weird maturity model. In the beginning, when you're just sort of getting started, the metrics are hard to interpret and use and understand, a small company, somebody new in their career, a modest size sort of system, the metrics are not as important. As you get a little bigger, the metrics become pretty essential, kind of mid-career. People might spend their whole time doing metrics and really digging in and being data-driven in the way they do things. You wouldn't be data-driven if you have one PC for your whole business. That's just silly.

Ed Amoroso: But let's say you have 50 people on a little network and suddenly there's some data to collect, right? So as things get bigger, it becomes important. The challenge is as you get really big or as you get really far along in a career, say at a board level where you're really been at it for a long time or you got a big system, there's this belief that people go by data, but it's a lot more at that point driven by instinct. So if you have three CEOs on a board and there's a finance issue that the board is dealing with, there might be a bunch of data on the table, but those CEOs are not going to bother with the data. They're going to use their instincts to decide what to do. Now, they've grown up learning from data. They were data-driven their whole career.

Ed Amoroso: This is also true for massive infrastructure. It's hard to collect data that's meaningful for systems that are so big that we don't really understand how they work. What does it mean to talk about cybersecurity in the context of the US economy, right? What does that even mean? It doesn't mean anything. You have to go on your instincts. You and I would say, "Hey listen, you better get the industrial control stuff right or it could affect our economy." If somebody says, "Show me data," you'd go, "I can make up some data, but it should be pretty
much evident that that's the case." So we do go through these phases and people get that very, very much wrong when they think about boards because they presume that a board is always data-driven and follows these things.

Ed Amoroso: When you get boards that are Luddites and don't know anything about cybersecurity, the reason they want data is because they've not gone through that learning process to have developed any type of instincts whatsoever. They have no instincts at all. So they're back sort of in that learning phase and many times you do get asked to provide data in it and a lot of times they don't understand that anyway. So that helps you understand why boards are often pretty inconsistent in the way they treat data. I've sat on boards. I've sat on a board of a Fortune 500 bank. When you get into the detailed financials, the books all close and you've got a bunch of experienced people talking on instinct.

Ed Amoroso: When you get the cybersecurity, the books all open and everybody's looking, still learning and trying to understand when the CSO says, "We got attacked one million times last week." They scratch their head because they go, "Wow, back in the company that I run, our CSO said we get attack three times a year. How come you're getting attacked a million times a minute and we get attacked once a year?" Then you have to do that weird metrics semantic translation. Once you've taught them that, then when they see that again, instinctively they understand that when you say a million times a minute, you're talking about indicators or Splunk records or something, right?

Ed Amoroso: Okay, they'll understand that. When someone else says, "We get attacked one time per year," that means there was a large incident that got escalated that had significant consequences once a year and you don't have to look at the numbers, you just get it because you have experienced. So that's kind of the situation we're in in cybersecurity. People are still outside of ... You and I do this every day, so it's easy for us. But people on the outside are still trying to figuring out what to ask us, what to make of our metrics and how to be intelligent in interpreting what we provide them.

Brian Contos: You made such a great point there talking about instincts and I've never thought about it that way. But where there's a lack of instinct, you do have to back it up with some type of data that you can look at and measure, whether it's an audit or something else and that just makes a lot of sense. Very well stated.

Ed Amoroso: Think how scary that would be for... Let's say you and I are asked to be independent directors for a company that makes some dangerous chemical. Now, I don't know if you have a chemistry background. I don't.

Brian Contos: I don't.
Ed Amoroso: So we don't. So we're sitting there as directors and somebody says, "Here's this chemical and here's its properties and here's its chemical formula." We think, by putting it in these types of containers, we should be just fine and it won't be a health risk. Then they say, "All right, Brian and Ed, you guys are board members. Any questions?" We'd looked at each other and go, "Geez, I don't know. Is it all right? Can you show me some data?" Whereas if we'd spent our entire career in chemical engineering, we'd say, "Wait a minute, what kind of container? Don't you know that that thing never works." Then we would say, I give a bunch of examples. They go, "I know, but we don't have the budget." Then you go to this, blah, blah, blah. You get the point. So that's why judgment and experience are so important. if you don't have that, then you have to be data-driven, I get it. But data, without the experience and judgment, can be pretty misleading.

Brian Contos: Yeah. Well stated. Well, let's talk a little bit about ... We'll take this notion and we'll automate it if you will. There's been a lot of communication lately about continuous testing of cybersecurity in this idea that I want to validate, but I want to validate in perpetuity. What are your thoughts on that?

Ed Amoroso: Well, it's certainly a wonderful goal, right? I mean, it's kind of dumb when you do some sort of validation, whatever it is. Let's say you collect some data on patch statistics around the company. That's pretty common sort of thing to collect and you've stuck it into an Excel spreadsheet. You drop it onto a PowerPoint and you go home on Friday afternoon and you're ready to give the talk next Tuesday to your boss. So the patch statistics were collected one week, they're put on a chart on a Friday. You give the talk next Tuesday. Well, the chances of it being accurate on Tuesday, not so good, right? I mean, it might be close and you'd have to say as of such and such, but wouldn't it be better if it's a dashboard and it's continuously updating so that you've got automation in place that gives you situational awareness.

Ed Amoroso: Then you pull up the live dashboard. You're not doing this sucking of data into a PowerPoint anymore. You just say, "All right, let's have a look and see what our statistics are. It looks like it's such and such," and it might be better, worse, or the same as it was last week, but at least you know that it's being continuously updated. So I think it's pretty essential to try to do that. Sometimes you got teams who can do it and sometimes you don't. I understand, I think Verodin does some continuous validation. I think you guys are pretty good at that, so...

Brian Contos: Yeah. It's not to say the periodic pen testing and red teaming and audits that come in don't add value. I absolutely think they do. When people say, "Well, it's just a snapshot in time." Snapshot in time is not bad. It just shouldn't be the only thing that you have to measure, I feel. I think we need some type of near real time of visibility into what's happening.

Ed Amoroso: I would agree. I think that's well stated.
Brian Contos: So Ed, here's a bit of a loaded question because of your background at AT&T previously. But what do you think of the cloud in general? More secure, less secure? You see security experts on both sides of this equation. So I'm really curious to see what you think.

Ed Amoroso: Well, it's good that you said more or less secure because everything is relative to who's asking the question. So if you're a small or midsize company, I think it's a total layup that you use the cloud, right? I mean, it doesn't make any sense in 2020 to be running a local area network if you're a small or mid-sized business. The economics are challenging. It's too hard to keep things up to date and it's just kind of not worth it when there's such a rich set of service capabilities that you can subscribe to. You do your payroll out on the cloud. You'd store your data on the cloud. You do your email in the cloud. Let's say you're doing development work, you do that in the cloud. It's kind of like what's left? I mean, tell me what kind of business you are. Let's say you're an app-oriented business and chances are the apps, it's on the cloud as well. So for those types of businesses, it's a total, not even a question whether you do it.

Ed Amoroso: Now, when you get to larger companies, say the Fortune 100 and up, you could make the case that there's some companies that are big enough and willing to put the investment and time in to do kind of "their own virtualized infrastructure." So they might rent infrastructure from one of the traditional cloud providers. But perfectly reasonable if they're willing to make the investment to do things on their own and do it better than the standard Amazon or Microsoft ecosystem, then that's perfectly fine. But recognize that that's not cheap and you want to make sure that the entire stakeholder group understand that it's not security that drives that. This idea that you push your data out to the cloud and that's now a wide open. That's such a silly thing. I mean, let's face it, you already did that with telecom, right? Everybody already lets Verizon and AT&T more or less have their data. I mean, everybody uses one or the other for data.

Ed Amoroso: So it's not like we haven't done that already. Now we just complete the connection out to a workload hosted virtually and in cloud infrastructure. So the fact that you're parking it there as opposed to parking it back in your enterprise after it traverses Verizon's MPLS network, it's not like the most gigantic change from what you're doing now. So it's not, you know what I mean? It's like people go, "Oh, my God, I would never let my data leave the enterprise." You just kind of roll your eyes and say, "Dude, you totally already are." Even if you're buying MPLS VPN services, that's shared infrastructure. What do you think that is? That's not a rope that goes from your building A to building B. That's just not how it works. So I think it really matters who you are. But any small or medium sized business, forget it. It's a total. At larger companies, it depends. It really does come down to what you're willing to invest.
Brian Contos: Yeah. I always think back to my very first startup, which was Riptech with Grant Geyer and Amit Yoran and those guys and Grant and I were in our office in San Jose and we had a PBX box that we had in our room for our telephone systems. We didn't know anything about PBXs, physical PBXs. This was before there was voice over IP and all these other solutions you can use. I remember I had all these cards and we're trying to figure it out and it was very cryptic and just the interface was very clunky. I remember when we sold the company to Symantec, we said, "Hey, who's going to take this PBX box home with them so he can use it for the next company?" Thank God we never had to build up our own PBX infrastructure again because then everything got pushed into the cloud and it was great. Like email, right? I don't think I would ... For a small company, why would you ever set up your own email exchange, right? So just make sense.

Ed Amoroso: Riptech was a good company. It was a cool, cool product.

Brian Contos: Yeah, that was a fun time. Well, let's talk about threat intel as well. I know you've got some perspectives on that. Where do you land on threat intelligence?

Ed Amoroso: Well, again, it's who's asking. You pour all kinds of threat intelligence into your infrastructure, but if you have no means for processing or interpreting it or acting on it, then don't bother. You know what I mean? People get all these feeds that come in and they push them into some data store and maybe they do something, maybe they don't with it. It really depends, so.

Brian Contos: Yeah, it's like somebody handing you a file cabinet and saying, "Here's a bunch of bad stuff, IPs and domains and TTPs," and five seconds later, "Here's another one and here's another one." Sometimes it's like, "Hey, what do I do?"

Ed Amoroso: I had this neighbor who for years subscribed to the Wall Street Journal and I'd see at the foot of his driveway one after another after another, just sitting there all rain soaked and unread and it's that kind of thing. It's like I subscribe to the Wall Street Journal, but every day it sits unread and wet at the base of my driveway. So threat intelligence is kind of like that. Now, if you're pouring threat intel into your proxies, like if you're trying to determine appropriateness of outbound web browsing and you're using the threat intelligence service to determine categorized versus uncategorized, appropriate versus ... Then you don't need to be looking. That's going to go into the proxy, your web security gateway and determine in an automated way whether something's appropriate. So yes, I totally get that. Or if you're buying the threat feed that powers the signatures in a next generation firewall. Again, that's great. When it lubes an automated system then that's not a big consideration where they have humans curating.
Ed Amoroso: But this concept of threat intelligence, all sorts threat intel coming and being made available to a SOC team, well, that's great if you've got a SOC team. If you don't, you don't have hunters then why are you buying based threat intelligence. So you got to think that through and make sure that if you're making the investment to pull that stuff and it's not automated into a tool, then make sure you have the ability to do something about what you're given. If not, don't waste your time. Again, if it's automated, different story. But if it's not, then you really ought to think that through.

Brian Contos: Yeah. I think the the lever there is automation. Because when I think about, we'll just take TTPs and IOCs that are in your environment. If you can automate the process of--we'll go back to validation, validating that, "Hey, if one of these IOCs was in my environment and there's some beaconing or some command and control or whatever the case is, are my systems stopping it or they alerting on it?" Right? Or if there's some type of TTP that has to do with lateral movement and scanning for open ports and then trying to do whatever, the same thing. How am I prepared for this if it was inside my environment? I really like that. I think by combining that level of automation with threat intelligence, it's not just operationalized, but I like to say it's personalized and I think that's what people need. anything less than that, honestly, I think it's just that term paralysis of analysis. I think we're just drowning in data and we just never get out of our own way. It almost becomes just like a good idea as opposed to something that actually makes us more secure.

Ed Amoroso: Yeah, you got it right.

Brian Contos: So, Ed, as we wrap up here, there's a question I like to ask every one of our guests. It's probably the most important question today, which is who's your favorite superhero or super villain and why?

Ed Amoroso: Batman totally for the car. When I grew up in the 60s and 70s-

Brian Contos: Oh, the original Batman car. There you go.

Ed Amoroso: Yeah, it was the coolest show ever. So even the more modern ones are cool. But yeah, that original car was pretty cool.

Brian Contos: Right, right? That was the first, really ... Every kid wanted that matchbox car, right? That's awesome. So, Ed, thanks so much. Again, thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.