#237 - What Comes After the 11 Strategies of a World-Class SOC? (with Carson Zimmerman)

[00:00:00]

G Mark Hardy: Hey, it's been a few years since I read the seminal book on how to run a SOC, the 11 Strategies of a World-class cybersecurity operation center. But I've got the author of that book here today, and we're gonna talk about what comes next. Stick around.

G Mark Hardy: Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy, and today I have Carson Zimmerman with me. As I mentioned before, he is the author of the 11 Strategies of a World Class Cybersecurity Operations Center.

And it came out a few years back and I think it's still one of the best documents today. first of all, Carson, welcome to the show.

Carson Zimmerman: Pleasure to be here.

G Mark Hardy: So tell me a little bit about your background and, how'd you end up doing this, and maybe a little bit about your book and things. it's your [00:01:00] show here.

Carson Zimmerman: Absolutely. Thank you. I've been working in cybersecurity. And most notably, security operations for most of my career. And it's really exciting. I think that cybersecurity is a really exciting field and inside of that, I don't think it gets any cooler than either breaking into systems or chasing after people who are breaking into systems.

And it was those experiences that I had when I was at MITRE that led me to write the first edition, 10 strategies. After some time went past and I got to talking with my co-authors, Ingrid Parker and Katherine Knerler, we decided to do the second edition of the book 11 Strategies. And no, we didn't just add one strategy.

Actually there's about four new ones and we moved a bunch of pieces around on the chess board. And what we ended up with was the book that came out, a couple years ago. We made a very deliberate choice to make it free, and there were many reasons why. to [00:02:00] put a very long story short, we felt and still feel that it's more important that the knowledge of how to do security operations really well, is available to as many people as you can.

And the money book authors make on their books is, very minor, compared to their time investment.

G Mark Hardy: Yeah, that's a good point. And I think a lot of people think, oh, I'm getting a book out there. I'll make a fortune. it probably won't even cover minimum wage for the time you put into it, but. It is a chance to go ahead and contribute. And I do appreciate that because they said the 10 strategies is the one that I used to, point to when I was teaching at SANS for a number of years.

And they're like, so somebody says, Hey, I want your 11 strategies book. Where do they find that?

Carson Zimmerman: It is@mitre.org WAC 11. Strategies. Very easy.

G Mark Hardy: And probably also at Amazon or Kindle, do they, charge it for there it is just best to go directly to mire.

Carson Zimmerman: You can go to Mitre if you want the PDF for free. You can go to places [00:03:00] like Kindle and Amazon and some other books, sellers. You can do print on demand. you can get the Kindle version. And what we've done is deliberately set those prices to where it's cost neutral. I don't see a dime from it, and neither does Mitre or neither do my coauthors.

G Mark Hardy: We appreciate that and it's like doing this podcast. I'm, wow, it's hard to believe I'm 237 weeks into this, and yet the idea. Is to go ahead and create a body of knowledge that's gonna help those who are in our career and those who are following in our footsteps to go do other things.

But probably since that book came out, you've probably seen new things as well as we know things evolve, information changes, situations change. not that I'm trying to press you into it, but if you had to write a third edition after the 10 and the 11 strategies, what do you think topics, what would you cover?

What, would you be adding?

Carson Zimmerman: A number of things. I can talk about a handful. [00:04:00] the first I'll talk about is a phenomenon I've seen where anyone who's been in a SOC for long enough sees this constant struggle between turning the crank on the incident lifecycle. detect, investigate, respond, recover. And there's this huge tension between doing that and doing everything else that's necessary to be awesome in a SOC.

And what I've seen and experienced firsthand, is that sense of stagnation. You get. Where you're only paying attention to the incident funnel and you're not stepping out of that and investing the time you need to get better. And that feeling I've had, and then so many other people I've had in security operation have felt is what led me to do the talk.

How to save your SOC from Stagnation a couple years ago, where the premise of my talk, to put a long story short, is treat those investment areas in the SOC as a first class citizen. During [00:05:00] normal times, as if there's ever normal, as you would the incident funnel. So for example, engaging with your service owners and major stakeholders in co hunt and co, detection, creation, or, Working on your SOPs, in your playbooks, or using every incident as a training venue and a PIR venue, meaning post-incident response, how to get better. So the point is. SOC leaders, we need to build the metrics and rhythm and business around the activities that help us get better and step out of the incident funnel.

And one of the cool things that does for us is it'll both builds engagement and investment by the workforce in the SOC. And when the really big incident hits of, course, we should have some breach mindset, but when the really big incident hits the [00:06:00] capacity you had. On those things can be paused, but critically you need to come back to them and don't just get stuck into the, we're doing all of our resources on incident funnel all the time.

G Mark Hardy: Yeah, because I would think in a SOC that one of the most difficult things, and particularly about burnout and stuff like that, is the always on nature of alerts, pouring in information. And of course, no matter how you filter them, there's still a triage. Function at your level one to say, Hey, is this thing actually bigger than a bread box?

Do we need to kick this thing up? Or can we handle it at this level? Or do we just disregard it? And it would seem to me that if you had to look at every single alert that came in and then make a manual determination at that first round, you would be totally overwhelmed. You'd feel like an air traffic controller working Newark airport all by yourself. Are there tool sets out there that, or configuration tips that allow us to go ahead and, make the input funnel from about this big down to about that big where it's now manageable. Does that help at all with our [00:07:00] burnout issue or are we really talking about something completely else? so completely, entirely different that would cause that factor?

Carson Zimmerman: I would say that is the number one investment area, meaning controlling the signal that comes into the SOC. That is probably the number one investment area to reduce burnout. I'm not gonna say eliminate it, and it's not the only one, but I would say it's either number one or top three. And this is an area where I see so many SOCs fail, and the failure modes include, yes, burnout.

Yes, you are bringing in bad signal, but it's, a matter of discipline. And a lot of people who are new to this field, they'll come in and they'll take an off the shelf product from a very well known vendor of security products. Could be any of them. I'm not gonna picking on anybody today. And they turn it on and they get the defaults and they're flooded with alerts.

This is, in fact, this is [00:08:00] cliche at this point, Every security vendor that I know is talking about reducing alarm fatigue and increasing situational awareness, and that's still a good goal. But the best place of the SOC for be it should be is where they have a disciplined approach to tuning, and it is a day over day, week over week investment.

G Mark Hardy: So with that tuning, then, it sounds and a lot of companies, it's hard to be, in the Navy we used to call it a pre-commissioning crew. If you're part of a brand new ship, they're gonna lay the keel. You get out there and then you say, Hey, we're gonna be part of that original crew.

that sounds great on paper, but in reality it means about 18 months. Being in a shipyard and there's dust and there's noise, and there is grit, and it's hot and it's miserable. And then when you finally get out to sea and settle in, maybe you join on the second crew out of however many years you're doing.[00:09:00]

But organizations today, we build out SOCs and then we run them. How often are these new SOCs coming online? Are they like Chinese coal plants or are putting 30 a month online? Or are major SOCs only happening every now and then? And then people who get involved in that build out is act, are actually going through a rare experience in 2025 and beyond.

Carson Zimmerman: I want to use the word plank holder, but I won't. I would say at this point in time, we've seen so much digital transformation. The part of almost every organization out there has some kind of digital, footprint digital estate. And it's not like when I got started in the field 20 years ago where people are like, what's cyber?

It's now a transformation. So rather than saying, oh, we're gonna create a SOC from nothing, usually it's. We're doing some kind of transformation where we had something and then we're doing something different. And [00:10:00] then I might be, we're doing, we're starting with some hodgepodge of stuff. It could be, we're starting with, some outsourcing and maybe we're insourcing.

Maybe it's the reverse. Maybe it's a mix. So the point is, that relative to tuning or anything? Rarely do I see organizations starting from nothing, but rather they're like, there's something that happens. Usually it's a major incident, and then it causes a change in investment or investment events strategy.

G Mark Hardy: Got it. Now, one of the things that you had mentioned, we talked about is 14 questions are all you need. but what do you mean by that? what's the thought behind that?

Carson Zimmerman: I had a dream, that was more of a delusion right around the time I did the second edition of the book 11 Strategies with Catherine and Ingrid. And one of the next things that I wanted to do, I said I wanted to build a maturity and capability framework for SOCs and I didn't [00:11:00] have the time. And, because real life and.

In that time, there were a couple other frameworks that came out. Most notably SOCs, CMM, in the E-N-I-S-A. SOC, or C cert maturity model. You can go look them up on Google, you'll find them quickly. And I said, these are relatively comprehensive models. I have some things and some commentary about each of them, but I said, I'm not gonna do another one because I'm just, I'm crowding the space.

So instead, I thought about it for a long time and talked to a bunch of people and thought, what are the most important questions that a SOC needs to ask itself? Pertaining to what's getting in its way of success, and I thought about it a lot more and said, I bet I could get this. Answered this question in 20 questions.

I actually got down to 14 and this was about a year and a half ago. And the [00:12:00] whole LLM transformer thing was just coming out. I said, I'm gonna make fun of some people. attention is all you need, and I'm gonna do 14 questions are all you need. So the premise of this talk in my argument is there's a very small number of questions that we should make sure we're focusing on because those are the questions that are indicate we're getting in trouble.

So for example. We can talk about things like how long has a given group of people or a given role in a SOC done the same thing In the same way, if the answer is years, you probably have a problem because you are not evolving what you do and how you do it fast enough, or let me give you another example.

Many secret operations centers struggle to get what they need when they need it from their engineering resources. In fact, some SOCs have engineering not at all in the SOC, which I think is a terrible idea and is n I've never seen work. But anyways, one of the questions you should ask yourself is, from the time I say to myself, I need something to the time that I get it [00:13:00] satisfied, actually satisfied.

And I don't mean fake satisfied like we deliver to you a project. No. Like how long has it taken you to actually achieve ops impact? Is something worth measuring? And my argument also is it can feel very draining to build a very large and robust metrics program. And part of my argument is a lot of times anecdata is just as good because when you say that ec, when you collect that anecdata and then tell executives about it, they're like, whoa, I had no idea.

We totally need to go change X, Y, Z, and it's just as good if you spent six months building some crazy complicated set of dashboards.

G Mark Hardy: And we say anecdata, I'm figuring that's a portmanteau of anecdote and data

Carson Zimmerman: That's right

G Mark Hardy: and just try to make sure if, people are driving in their car, what did he say? And where do I find that?

Carson Zimmerman: It's ated. It's those stories, it's those vignettes when you say, Hey, today it takes me, I'm gonna make something outrageous up. It takes me three hours to triage every alert, and we [00:14:00] have 10,000 of them a day. I can do that based on an informed opinion about what's going in ops without actually having to go into my SIEM and my case management system and actually measure click times and, all of that stuff.

G Mark Hardy: Yeah. Now there's gonna be some people you need to convince. That will say, I get it. I got that. And other people that are gonna be showing me the data. And in a way, there's really no one solution that fits everybody. It's really understanding how does your management team that allocates budget, allocates resources, make their decisions?

And if you have that insight. It's almost, that's almost more at the political layer here, being able to communicate to people who are decision makers, power brokers in the language that they prefer. And if you tend to be a left brain by the book, hear the numbers and show up with a ton of data, and you're dealing with somebody who makes major multimillion dollar decisions on a golf course based upon.

oh, hey, okay. If I, make this [00:15:00] putt, you get the deal. If you make the putt, I get the deal. Whatever. Then you need to readjust. And that's what I think a lot of us who are in management to leadership roles, it should be people running SOCs. Alright? You've progressed past the technical level, you're doing a shift management or something like that.

But at some point, if you're leading a SOC, which means in addition to delivering on time, on budget and making sure that all that stuff happens in the. fashion you meet your SLAs, that you take. Responsibility for the wellbeing of your people. And that's what I say is the unwritten rule in a lot of leadership positions.

They don't say that it's not in the job description, it's not in the performance review. It's really what differentiates you from a manager is that beyond just getting the job done, you're growing and developing your people. And some of the things that we're talking about here about being able to say, Hey, I've gotta deal with stagnation.

I'm trying to deal with burnout and stuff like that, go a long way to being able to address the. Taking care, if you will, or understanding and developing your people. But one thing [00:16:00] that's the elephant in the room for a lot of us is our people. And the nature of what we do in cybersecurity doesn't necessarily lend itself well to the average person that's out there.

And so what we find out is we look at labels, and I hate labels because it automatically causes you to pre classify and pre-judge people. But the reality is, let's face it, the idea of neurodiversity, however we wanted, define that. But typically, is that people approach problems in life a little bit differently.

Then the mainstream. So if you look at the bell curve Yeah. A lot here. Okay. And, maybe over here, but what do we see in the SOC world and things like that about, neurodiversity and in the security operations world in general? And is that a strength of ours? Is that a weakness? Are we coming a na where we're attracting people that can't get a job anywhere else?

Or is this is where people with these special skills, because they're innate in their personalities, can come and shine?[00:17:00]

Carson Zimmerman: This is a fascinating topic and I'll make a couple comments, G mark that actually probably go back to the experiences you and I have had at security conferences 20 years ago when I went to Defcon in the early aughts. and I looked at the crowd. I saw a lot of young white males, and it was a very unilateral, one dimensional audience.

And in that time when I was learning cybersecurity, it was generally possible to know and have your mind wrapped around. Most of what you needed to know to be a cybersecurity professional. And in that last 20 years, we've branched out so much. You've got people who are total nerds about GRC.

You've got people who are total nerds about just cloud authentication. You've got people who are total nerds [00:18:00] about certain areas of mal analysis or penetration testing, et cetera. One of the things I wanna highlight is the diversification of experience and background. When I now walk around Defcon, which has gotten absolutely huge, I see a more diverse crowd and I see a more diverse set of experiences and expertise.

So we need to harness that and inside a SOC, when people think SOC, they think someone who's staring at alerts. That's true, but that's actually one of only about 10 or 12 different personas. So we think about in that context, how do we think about those different personas of leadership management types, hunters, triage people, investigators, incident response coordinators, malware analysts, data scientists, et cetera.

So let's think about that for a second. Is the persona and background for someone who's running an incident call and herding 50 [00:19:00] cats. Along the way, the same person you want doing PE header analysis. And the answer today is absolutely not. Can one person go from one role to the other role that I described?

Yeah, I've seen it happen and in fact, sometimes it's really awesome. But here's a piece of anecdata for you. I have stood in front of crowds at conferences as you do, and I've asked for a show of hands that in the room I said, how many people here are neurodiverse? And what happened next? Blew me away. Half the hands in the room went up.

In fact, probably more than half. In fact, because we know at conferences GA, you've probably done this many times, you ask for audience participation. It doesn't matter if you ask who's here, not all hands will go up. And I'm like, whoa. Now this is not a scientific study that I've just done, but think about that for the moment.

Half the people in the audience or more have just [00:20:00] asserted their neurodiverse. And I would further conjecture, some of the most predominant areas of neurodiversity are probably ADHD, Autism spectrum, and anxiety, and yes, there's a comorbidity between them. By the way, I'm not a health professional, but I read a lot. So my argument here is when we look at a security operation center, number one, we need to think about those different personas and for the people who are bringing neurodiversity as a superpower. That superpower of being able to focus on a problem to hyperfocus or that superpower of being able to see a bunch of different connections and bring together different perspectives or different pieces of data that a neurotypical person wouldn't.

Those are superpowers, number one. Not everyone in the audience or in the SOC knows that they have that, and they may just be over-functioning. Or a high functioning person who doesn't [00:21:00] realize, they're neurodiverse, but really good at it, or they are. And the point is, how do we as leaders, as managers, as leaders, et cetera of the SOC and other parts of the cybersecurity apparatus, recognize those superpowers and embrace them and make those people super effective people who are gonna find the next major incident or pre prevent the next major incident.

G Mark Hardy: And that's a real challenge of leadership. I think any of us who have had that privilege. to lead. Others find that often there are some, maybe one, maybe several people that, for better or worse, they just don't quite fit in. They're not in the correct role, they're not in that, but you don't necessarily have a chance to change that.

But if you have the perceptiveness to be able to say he or she could do this, and you assign them some type of role where they could shine, not only is there a great deal of job satisfaction in that because people said, wow, [00:22:00] I'm doing, I'm loving this. But then other people who look at the scans you know this guy.

Wow, this person is becoming a rock star. And I have seen that myself by being able to find people like this, give them specialized assignments, and they do extraordinarily well. And the benefit is significantly beyond what an individual contributor might normally do because this is a role that you wouldn't give to a typical individual contributor.

And One of the things that we have to be sure of as leaders is to look across the people that we have now, of course, there's a lot of pressure going on in political, and we don't get into politics here about identity and things such as that. People are who they are. And I don't think a lot of people wake up one day and say, you know what?

I wanna get beat up a lot. I wanna get bullied. I want people to screw with me and make my life miserable. So I'm gonna declare this. rather, it's the opposite, is that here is who I am. I've figured out, thyself like the oracle at [00:23:00] Delphi. And then people say, I don't like the fact that you know yourself because you know yourself as this of.

Looking at stocks, cybersecurity, neurodiversity. I tell people that is actually, as you had said, the same term, a superpower. It allows us to go ahead and look at things and either absolutely focus in laser focused and just go over and over and wait a minute, There and nobody else could see that.

Or you've got such a huge range of inputs and a little bit like a beautiful mind with Russell Crowe. You see all these numbers and everything patterns and all of a sudden that's it. And it's okay. The average person doesn't do that, and we don't need everybody to be able to do that. But it does bring up an interesting point, and as we talk about boredom and the like before, is that. Career progression and career rotation. I'm gonna fall back into my Navy example because in the Navy we had a couple things for our military. In the office or community. [00:24:00] First of all, it's upper out. So every six years you get another look at you to say, are you progressing correctly? Have you moved from ma technical to management?

Have you moved from management to leadership? Have you moved from leadership, political work? And at the end of six years, they say, yeah, you're not gonna promote lieutenant commander or captain or rear Admiral or whatever. And that's a normal progression. And it necks it down and it gets it smaller.

Similar things happen in the corporate world, although maybe not. In such a structured fashion. But we used to talk about the fact that the Army had a lot of gray haired majors. They were brilliant at their technical role, and the Army didn't force 'em out of it. They said, look, you're a rockstar. Be a rockstar now.

Title ten's gonna catch up with you, and at the end of 20 years as a major, you gotta go home. But that's still a long run for a technical expert. The Navy's you're really good at that. Okay, good. Let's switch you over here. you're really good at that. Okay. And waiting for the Peter principle.

You get promoted to your own level of incompetence. You're good here. We'll promote you. You're good here. We'll promote you. You're not good. we can't promote you. We're gonna leave you where you're not [00:25:00] good. the solution to that, by the way. Is what we did, and we said someone needs to be fully qualified for the next level.

So when we say, Hey, I'm gonna put you into the next level, it's, I'm not really gambling that maybe you'll figure it out. You've already demonstrated by, if you will, overclocking your performance at one level that yeah, you can do this. And I've seen glimpses of, yeah, she's gonna do all right there. So let's give her the full title, give her the paycheck and the responsibility and run with it.

Now does this suggest. That for we, if we're gonna be wise, leaders have to be able to have enough insight to craft career patterns for our people to know that someone to say, Hey, in this world of neurodiversity, they're gonna, if you will eventually become a gray haired major, which is absolutely okay, or this is somebody who is going to be moving around in different levels, how do we gain that?

Wisdom number one. And then number two, how do we fight against the machine? That is to say [00:26:00] the human resources department that might have an up or out out thing to say, this person really hasn't progressed and they only met the same goals they met last year. They met the same goals they met the last year and the year before.

So why do we wanna give them raises? It's because they are doing absolutely essential stuff. So it's a big dilemma for a lot of people running teams. But any thoughts on all that?

Carson Zimmerman: I have many. I'll offer just a couple. The first is from my own experience. One of the reasons why I've loved serving in management and leadership roles is that moment where you see a problem the business needs to solve. Someone who has talent in that area and may not recognize that they can do it, but that you believe in them and then you're ready to take your hand behind their back and push them into the deep end and watch them succeed.

And it is so cool to see and to see them grow. So that's a big piece of it is [00:27:00] recognizing and making those connections. one of the things that I think about in this context is security operations is such a dynamic field. I'm sorry for the cliche, but it's true. And as a consequence that we enables us to have career progression and skills progression built into the SOC as a necessary and more prominent aspect of the job expectations than I think exist in many other fields.

Sure all fields are progressing, but like right now, think about how differently we're doing things today than we were 10 years ago or 10 years before that. Like when we wrote the first edition of the book, when I wrote it, I spent a long time on network sensing and it's still in there in the second edition.

It might be there in the third. We'll talk about that in a second. But like how many people have I talked to recently who have gotten [00:28:00] fired up about Snort? And the answer is no one.

G Mark Hardy: Marty Rush. he's, but

Carson Zimmerman: should we still have network sensing and network telemetry and our portfolio of tools? Of course we should. Do I still think Suricata and Snort are premier tools?

Of course I do, but there's so many other things we have to bring to the table now that we weren't thinking about as hard before. part of the moral of the story here is again, going back to save your SOC from stagnation. Make sure that all the roles in the SOC are progressing and that people are having that prog career progression inside the SOC, or maybe in and out of it.

Some of the best people in the SOC I've seen are people who used to do red penetration testing and red teaming.

G Mark Hardy: And so it's interesting. Yeah, because we do have. That ability to flow in and out of a SOC. You don't have to sign up and then say, okay, there's gonna be my career for 20 years. A lot going on out here. And we look at [00:29:00] all the additions and the expansions of technology and the roles and the tools and everything else.

but to use what almost became a meme that the talk I had last weekend up at the THOTCON, but AI.

Carson Zimmerman: Ugh.

G Mark Hardy: We did a pattern that's, this is, for those who are watching on YouTube, I got the longest beard I've ever had and we did a talk called Grey is the New Black, Why You Should Listen to the Old Person in the Room and the panel that we had up there, it back and forth and we discussed things, but it really came around a lot to, that almost became silly in a way because we're talking about it, but not so silly when it comes to a SOC.

When we look at the constraints that we have in terms of available people. Possibly being able to get additional resources for those people, the running of a SOC itself, versus outsourcing to an MSSP, depending on your size, of course. And now with the advent of artificial intelligence, which adds up on both sides, it provides attackers, it democratizes some [00:30:00] of the capabilities that were only heretofore available to nation states and really smart and clever and perhaps evil people, but also on the defensive side.

It may allow us to go ahead and do a lot more without having to have human intervention, allowing us to almost make decisions at line speed. So a lot of stuff there, but I wanna just sit back and listen to you talk about what are your thoughts about what AI is gonna be doing for us going forward.

Carson Zimmerman: So there's no question that there is a lot of hype and a lot of attention about AI right now. Now, to focus this for a little bit, when we talk about a ai, I'm going to infer on your prompt pun, doubly intended, that we're thinking about Ag agentic models, SLMs and LLMs, and other generative capabilities.

Yes, all of this AI stuff [00:31:00] I think is gonna transform the way SOCs operate. And I'm actually deliberately waiting for this field to develop before I write the third edition of the book. More on that in a little bit. So I further agree that, they're gonna help different parts of the SOC. And I think we're just getting started in understanding what that really looks like.

So first of all, if you haven't seen the fact that there's a million startups and all the big companies, who are putting resources towards this, if you're not seeing that, you're not paying attention to the industry. So let's get that out of the way and. I wanna also acknowledge that there's a lot of products coming to market now that have really great promise, and beyond that, there's a lot of vision around using these generative technologies to replace human tasks.

And I think we're [00:32:00] all there with the vision. The question is, how soon will we be able to depend upon them and in what capacity? I. So there's a couple things I wanna pull back from. I don't think we're gonna get our human body count down to zero for all of the things that we have these generative technologies take over for us.

We will probably have our humans doing other things. So the first misconception that I would offer is that a lot of people when they approach this, they think of what the work that the SOC has to do as a static and finite set of stuff. And I reject that, remodel that model. Instead, think of it as, Hey, I've never met a SOC that felt like they had enough people.

So the point is, that there's always more signal to consume, analyze, and respond to. So the name of the [00:33:00] game now is, what are the things that we can automate now and where are we gonna move our humans to moving forward? The first thing I think I see a lot of people spending a lot of calories on is, writing code summarization and alert triage.

there's, you go look at a, bunch of go to market strategies, lots of marketing around this, blah, blah, blah. Everybody's talking about it. where I think you and I have probably ourselves had success is like, Hey, whatever tool I like, Jim and I co-pilot whatever. Write me a code that does blank and you'll get results that look pretty good.

Are they perfect? No. And that's the first place I wanna stop and say. one of the ways I think about using LLMs right now is you've starting with a blank sheet of paper. What do I do? So that's one way is to think about it. The next way to think about it is we are applying LLMs and [00:34:00] technologies like that and using Agentic frameworks to automate a bunch of tasks together, and we immediately go to Analyst Triage, which is great.

But think about those different personas I mentioned before. Think about all those different personas in the SOC and how can we use generative AI to enable all of those personas and think about them across the incident lifecycle. And suddenly, we now have all kinds of ideas on how these technologies will help different parts of the SOC at different times.

And then the third way to think about this is I'm gonna take a page out of the old book and say, think back to the days of network intrusion prevention systems and think about SOAR meaning, SOC Orchestration, Automation, and Response automation. The mental models we used with those technologies still hold when I turn on an [00:35:00] IPS back in the days, back in 2005.

When I had more hair, people would turn on it in full auto straightaway and they'd be very disappointed at the results. And instead they learned that they needed to turn it on in alert only mode for a while and tune it. And so when we think about G Mark, to your point, are the adversaries going to use generative ai?

Yes, they are. Are they gonna use it to go a lot faster? Yes, they are. And before we go full auto. We need to manage our own expectations, tune our implementations, make sure that the underlying signal quality is good enough and that we have full transparency into how those models are working on our behalf.

I. So what is old is new again. Just like when cloud technology happened 10 years ago, there were a lot of people with this reaction. Like they, it's like they had an instant amnesia. I've forgotten everything I ever [00:36:00] knew about it and I'm gonna start over. And I say, no, actually, more than you think you know.

And what I'm saying is take the mental models we applied to anything that's in line, or prevention and any of the automation stuff, because all those same concepts and our approach still apply here. That's, my, that's my TED talk on the matter. I'm sure you have questions.

G Mark Hardy: Sounds good. one of the things that with the embracing of AI is I'm worried about people getting over the handlebars where they're, oh, they're gonna throw, let's just outsource this thing to ai. Let give it to it. Oh, who needs people when we have this? And of course they're gonna end up, with a difficult situation.

They're gonna say that's not helpful. that is not gonna give us what we need. And as a result. What comes out of that is that we say, okay, you've now created this function in your organization because whether it's hallucination or lack of being able to understand how this thing is gonna interact, it's just not gonna work.

And then okay, [00:37:00] fine. How do we get the people back? I'm sorry you fire me because you wanna have ai. I'm not coming back. And, so people can. Disassemble a well performing team by misunderstanding the capabilities of ai. Absolutely agree. You wanna walk before you run. You wanna put it in audit mode, if you will, or monitor mode before you let it go and do actions.

But at some point in time, we need to go ahead and say, yeah, it's a competitive advantage, if not, just in terms of using it in our business model to be able to keep up with the threat actors who are incorporating. These types of generative tools in increasing the intensity, the capability, the breadth of what we're facing.

I don't know. I, you're right. It's something to observe and watch and find out. I think, as you had said, your third edition, which I'm guessing if you're gonna do in the oceans 11 and 12, that this is gonna be the 12, tips that you can use for your SOC and you progress from there, will encompass, encompass ai.

But [00:38:00] anything else. It's never going to be fully ready. We can't say, yep, we're baked in. We're good to go. so at what point in time do we just jump in a little bit and start going, is now too early to start, putting in the AI tools in our SOC? And if so, are there. Anything we're seeing out there that we expect some big developments taking place in the vendor space in the next few months.

Kind of doing a little bit of prediction since we've been in our sac and, have black hat coming up. They always get to see those shows and see what's next.

Carson Zimmerman: My advice is if you haven't started, you really ought to and use the model of the different personas in the SOC, the different jobs to be done to help us understand where to achieve thoughtful insertion of AI technologies. and I also advise being very pragmatic and very thoughtful in application of lms.

Don't just say, [00:39:00] oh, an LLM was the answer. What was the question instead? in fact, there's a lot of, automation techniques that are not going away. rioting a Python script is still useful. in fact, predictability and repeatability and determinism are still important. having an LLM based agentic framework may not be the way you want to respond to every alert because there's some built in lack of determinism there.

That's part of the point. So the point is be thoughtful about which technology, you're applying to each of them. Cost, efficacy, efficiency, et cetera, being part of it. but absolutely my advice is get started. now be thoughtful about the different parts of your SOC and where you're using it, and be very thoughtful of what are the measurements of success?

can I rely on this? have I saved time or is this a, have I [00:40:00] gone off and chasing squirrels, because I've got a shiny technology.

G Mark Hardy: Sounds good. we're getting close to the end of the show here, so any final thoughts that you have that you'd like to leave our listeners with to, perhaps look forward to in the next few months or things that you just think are in general are important?

Carson Zimmerman: I would say at the risk of stating a worn out cliche, expect constant and continual improvement and innovation from your SOC. If your ops model and what you're asking your SOC to do or your resourcing, don't sustain that. I strongly urge you to reexamine what that is looking like for you. You either need to work with them to enable them to cut down the work that's of lower value or work with them to restructure and focus their resources on stuff that helps 'em get better.

G Mark Hardy: Sounds good. for everybody out there, thank you very much for [00:41:00] being part of our audience here at CISO Tradecraft Carson. I do appreciate having on the show. I always loved talking with you. You get me thinking about really great ideas. It's one of our latest, entrance into the career pattern.

This is my niece Zoia, so we're staying up at her house. Yay. So for folks out there, we do more than just podcasts. Go ahead and follow us on LinkedIn if you don't already. We have a Substack newsletter, we have shorts out, things like that. Also, go ahead and subscribe if you don't, and let everybody else know where you got your great information from.

So appreciate you being part of our audience. Thank you for taking the time to develop your career. This is your host, G Mark Hardy at CISO Tradecraft. Until next time. Stay safe out there.