CTL-CISO-Mark-Lynd

Mon, Sep 01, 2025 12:54PM 18:07

SUMMARY KEYWORDS

Cybersecurity, generative AI, copilot layer, threat hunting, hypothesis-driven, time to decision, AI strategy, security controls, privacy controls, AI adoption, SOC augmentation, AI threat modeling, deep fakes, organizational governance.

SPEAKERS

Mark Lynd, Jo Peterson

J **Jo Peterson** 00:07

Hi. We're here today with clear tech loop on the move in the know. Thank you so much for joining. I'm Jo Peterson. I am the vice president of cloud and security for clarify 360 and the chief analyst at Clear Tech Research. And I've got an amazing special guest and long term friend of mine, Mr. Mark Lynn, Hi Mark.

M **Mark Lynd** 00:29

Hi Jo. Thank you for having me.

J **Jo Peterson** 00:31

Thank you for coming. In case you don't know him, and you should. He is head of Executive Advisory and strategy for netsync, and Mark leverages his extensive experience in cybersecurity, artificial intelligence, data center and IoT to provide strategic guidance for C level interactions. In addition to his role at netsync, he holds executive board roles, and the gentleman rocks the CISSP ISS AP and ISS MP, so in case you were looking for something to do in your free time, Mark has any free time, I'm fairly sure he doesn't. He's a girl dad, too. So keeps busy, keeps busy. So let's get down to our questions,

M **Mark Lynd** 01:21

okay,

J **Jo Peterson** 01:21

how can cybersecurity professionals leverage generative AI to break out traditional sort of that

how can cybersecurity professionals leverage generative AI to break out traditional sort of that tool and tech mindset and drive more innovative thinking and execution in their security programs?

M Mark Lynd 01:37

Yeah, you know, I really love this question because spending, I spent a lot of time with C level customers. And one of the things that they're, you know, they often do, is, should we approach how do we approach it? And I'm like, Look, you cannot approach us like you approached things you did before with it, and that it's just, it's a completely different animal. And so some of the things that talk to him about is make AI a copilot layer. Think of it as a layer, right? Because if you look at what Microsoft's doing, if you look at what Cisco is doing all these others, what they're doing is they're they're offering copilots for all of their products, right? And as part of that. So that's a great way to get some early wins. Because they asked me, you know, if your board's asking you, what's your AI strategy? How are you going to do this? If you're getting questions from your employees, leadership customers, it's a great way to get in there thinking about this copilot layer to make your people more effective, more efficient, and start to augment them, because that's really what we're talking about, right? It's kind of the it's kind of the piece you see with Jensen, the CEO for an NVIDIA he says, You're not going to be replaced by AI. You're going to be replaced by somebody who's really good at AI. So So you know, you think about that from a copilot layer, you can make your employees better at what they're doing, make them more effective, more efficient. And that's a good, solid early wins. Doesn't require huge investments and all that. And then, you know, one of the things also is you've got to think about putting in a framework, right? How are we going to do this so we can make better decisions, better buying decisions, right? But this isn't about better controls, like a lot of the previous products, are just about better decisions, because this augments and enhances your decision for your employees, for you, for you know, your peers, etc, and it has great benefit to your customers. So maybe an example, Jo of that would be is hypothesis driven threat hunting. So in the past threat hunting, you had to dig through the details, right? And they you may have a product that bubbles it up a couple. Maybe they look at 100,000 and they bubble up 10 or 15 for you to look at. But wouldn't it, where we're going to is you'll be able to ask questions, which one is the most you know, a problematic for us, which one might skirt around our security controls, things like that, and then let it auto materialize using these queries and levers. So you move from alert chasing to question asking, and I and we talk about this with our customers all times we sell a lot of security and do a lot of security for a lot of customers. So if you truly believe, and I do that, llms and, you know, generative AI, in this predictive part of the of AI is that piece, then that move from alert chasing to question asking is a really wonderful example on how this can really benefit, right? Because if you're more secure, that means your customers data is more secure. If your people are able to work on other projects, because you made them more efficient and effective, you know you're getting that. So those are some really good ones. And you also then the last element of that is measure time to decision not. Tool count, which directly goes against what you asked me right before it was like, Well, you know, nobody ever got fired for buying Cisco, right? Or, you know, we have 17 security products and that are done five integrations, etc. Now measure time to decision, right? Because a lot of times going and having to look at six or seven consoles, trying to figure out where, what information is where, and then trying to make those align with each other, so that you can make a good, informed decision. So difficult, but with llms, you can look at a wide variety of data sets in a data lake, or even even outside of that, by loading it, or using and using, you know, a rag, you can do that. And so now you can measure your time to decision,

not how many tools I had to go to to collect all this information and get all this even though there is a verification element of that that some may appreciate. If you do it right in the LLM, you can get that as well.

J Jo Peterson 06:01

I love that answer because it was so layered. And one of the things I heard you say is, you know, we need to teach our newer security folks to ask better questions.

M Mark Lynd 06:02

Yeah,

J Jo Peterson 06:03

we have to teach them to ask better questions, because we're going to, you know somebody, some system somewhere, is buying some fancy tool, and it expects you to ask it questions.

M Mark Lynd 06:27

Most I do an AI table top, right? And we do that for the C suite. You have to put it in very measurable or simple terms, right? So I say, Stop buying Blinky boxes. Start buying better questions. And that is an actual sound bite from our quote from, from the AI table top.

J Jo Peterson 06:50

That's so good. That is, that is so good, right? It's, and I you know, but it's a different way of thinking. It is like the part of the different way of thinking is, you know, your next military guy, cybersecurity is very rule bound, right? If this, then that right? Ai doesn't behave that way.

M Mark Lynd 07:11

No, it does.

J Jo Peterson 07:12

So it's a different way to look at, you know, is rolling crazy ball in some instances, right? And you have to think differently to lock down those attack vectors.So,

M Mark Lynd 07:26

you know, to that point you think about this, one of the ways to augment that and to do that

and think that different way is like, if you're thinking about purple teams, right?

J Jo Peterson 07:36

Yeah.

M Mark Lynd 07:37

So Purple Team loops. How about AI? AI augmented Purple Team loops. So if you use LLM agents, and agentic AI is the big rage right now, right? But if you're able to do that to script, you know, adversary behaviors like fishing lures, prompt, injection strings, you know, data poisoning, cetera, et cetera, so that every, every exercise hardens both systems and staff, right? And then maybe you, I don't know, maybe you anchor that to minor Atlas tactics to model how attackers target. AI, that's a that's a really great way you know how you and I are talking about using questions and and using it in a different taking a different approach to an age old problem.

J Jo Peterson 08:23

Are you listening venture capital people? You need to call this man, because he's got a great idea here. Just call him.

M Mark Lynd 08:33

Remember, Purple Team loose.

J Jo Peterson 08:37

It's such a good idea, though, because you're using AI to outsmart itself?

M Mark Lynd 08:42

Yeah. I mean, you think about it, you and I both spend a lot of time with customers, and one of the ones that we always hear is we need to do more with less, right? I may not have the exact budget, I may not have the head count, I may not be able get great people, enough of them, right? And you're always in this struggle where you're trying to make get one or the other. So a way to do that is to truly take what the LLM provides you, this augmentation, right, and then, you know, apply it to given problems that purple team loop. I've heard that issue. They didn't call it a loop, but I've heard it sounds like a circle to me. I hear all the time when you get down there with engineers, with their leadership, and you start to talk about, maybe it's an incident response table top, maybe you're talking about, you know, purchasing a new product or tool, or whatever it may be. And these questions come up, and I've heard the purple team one a bunch of times. I've still not seeing anybody solve it.

J Jo Peterson 09:41

That's a great one. It really is. And speaking about, you know, sort of balancing things. How can organizations embed security and privacy controls into AI model development without slowing down innovation?

M Mark Lynd 09:57

Yeah, you know, I. Love this one too, because I have it kind of take a weird angle on this one. I always think, you know, having been this guy on CISO several times, and you know, it was me on the line, and my, my, my team, I like to give teams a fast, paved road with guard rails. That's my angle, right? And what I mean by that is, you know, governance that ships maybe. So don't go out and try to create some governance on your own. There's so much out there, right? You got NIST, you have ISO. Microsoft has their own, Google has their own. I mean, just go down the list. I think there's 11 or 12. The last time I heard,

M Mark Lynd 10:41

yeah, and you know, if you're, if you're just purely Microsoft, and there's a lot of shops out there that do a lot of Microsoft, or lean heavy on Microsoft, and maybe you want to get the early wins without 365 and their copilot. That's a reasonable strategy, right? Then you may want to adopt theirs. And then maybe, you know, position yourself towards NIST further down the path, right as you start to expand and broaden your horizons around you know, generative, AI, etc, and then you know security by default. We're back to that security baked in is always better than bolted on, and we've been saying that for years, right? Well, security by default, may think of it as a golden path with this. LLM, right. You need to look at the model. You need to understand the data sets, the data lake. You and I've talked about DLP in the past, injections. You know, there's a lot of pieces to this. It didn't just simply, and that's why people are so fearful of shadow AI. It's not just simple bring something up and start loading PDFs and asking questions and giving access to data that may or may not be sensitive. There's a lot of effort to that. So you know, in my mind, it's going to have to be done early. You're going to have to have a good AI strategy. You're gonna have to ensure that your base based on some kind of governance and model that pre exists, don't try to build your own. I've seen too many customers go down that, that that lane, and it just, it's fraught with, with, you know, all kinds of potholes and and damaging issues. And, you know, do that, and then last but not least, make sure that for your environment, when you give it access to your information, your data, and that you let your the employees know and share with them, right? But bring them along for the ride that you know sensitive information going in there will be trained on and will become public information more than likely,

J Jo Peterson 10:41

wow. Okay,

J Jo Peterson 12:43

right? And and we all have heard the horror stories about people not locking stuff down and the crown jewels getting into the public domain, and it's sad. So last question, how should the CISO be thinking about AI adoption in terms of its use to both secure emerging threats and then from an organizational governance perspective.

M Mark Lynd 13:07

Yeah, this is one that I, you know, I think about this in kind of a interesting way. It's really, I got to give all the credit to the customer, and it's a variation of what we just talked about, it's move fast on a paved, well lit road, right? If you're, if you're going to look at some kind of analogy to think about this is, don't go off on your own trying to figure this out. You know, to really think about what you're trying to do, bring others in. You might want to bring third parties in that have done this for others, to help them with that. And some of the things you can think about, you know, from a CISO perspective, SOC augmentation, that's a big win, a really big win, right? Use LLM To summarize, alerts, enrich your Ico, generate IR drafts, you know, but keep the human in the loop. That's the big thing now, or you're we're hearing that from a lot of big even the even the AI manufacturers themselves are saying, keep the human in the loop. We're hearing that over and over and over again. And then, you know, another good one is AI threat modeling. We kind of touched on that, you know, it kind of aligns with with minor Atlas, with NIST ai 100 dash two, some of those, and then, as we move into the future, think about it as deep fakes and fraud resonance, right? Is resilience. You've got to create a way to battle what AI is going to be bringing at you. I don't know what you're hearing from your customers, but I'm hearing a lot of fear in certain customers about because they're starting to see this, these AI driven and power attacks happen, and they don't have the personnel, they don't have the cadence, and they don't have the determination and capabilities to offset that right now. So they're they're leaning on some of their manufacturers are leaning on their their partners and and it's really, you know, you're going to have to make investments. You're gonna have to invest in your team, you're gonna have to invest in your organization, you're gonna have to invest in yourself. And you've really got to come up with kind of this, a way to treat AI as both a control surface and a risk surface, right?

J Jo Peterson 15:24

Good. I love that way of thinking, control service and a risk service, because

M Mark Lynd 15:29

it is. It is the only difference. The only difference is the blast radius could be infinitely larger, neutral, nuclear, potentially. I mean, it is. It's like, you know, in my new book that I have, I that's what I covered. It's, I used a it's AI, it's aI powered cyber threats. And that's, that's what people truly fear, and there's a reason to fear it. But it's not, you know, it's not uncapped. It's just, you're gonna have to make those investments. You're gonna have to learn how to augment yourself, your team, your organization, with AI, and use it to manage both that control surface and that risk surface.

Jo Peterson 16:12

Love that. And what is the name of your new book? And where can people find it?

Jo Peterson 16:16

Oh, I'm sorry, yeah, it's called Cyber it's called cyber war one scenario. And it's kind of a mix of Annie Jacobson, who's a very famous author who I love, who did nuclear war and area 51 and she does narrative nonfiction and fiction in the form of Tom Clancy. So if you, if you smash those two together, and some of the early reviews have even commented on that. It's a narrative fiction, and it's about a cyber attack that's AI powered that leads towards impacting our critical infrastructure, both here and abroad, and then turns and starts hitting everybody, and they assume they have to join together to do that. And it's it was fun writing it. It's a long read, fairly it's like 307, pages, but a lot of research went into it, and a lot of good customer information went into it.

Jo Peterson 17:16

Wow, that sounds cool. I'm gonna need to check that out, so you'll have to send me the link so I can add it in the podcast notes, when we send, when we post the podcast.

Mark Lynd 17:25

Yeah, it's on Amazon, Barnes and Noble Koto, Apple books. I think it's on like 93 platforms.

Jo Peterson 17:33

93

Mark Lynd 17:34

yeah, there's, believe it or not, there's over 300 platforms.

Jo Peterson 17:39

These so many things I don't know, just so it's just a lot. Well, it was a pleasure seeing your face. It was a pleasure hearing your thoughts. Thank you so much for making time out of your day to visit, and thank you guys all for joining and we'll see you next time.

Mark Lynd 17:56

Thank you, Jo