

# CTL-CISO--Zach-Lewis

Sun, Feb 08, 2026 2:55PM 10:38

## SUMMARY KEYWORDS

AI security, generative AI, tabletop exercises, data classification, vulnerability management, natural language queries, EDR, DSPM, CISO collaboration, organizational governance, AI adoption, ransomware story, security program, training, innovation.

## SPEAKERS

Jo Peterson, Zach Lewis

---



Jo Peterson 00:07

Hey everyone, thank you so much for joining this is clear tech loop. We're on the move and in the know. I'm Jo Peterson. I'm the vice president of cloud and security for clarify 360 and the chief analyst at Clear Tech Research. And I'm joined today by Zach Lewis, who is the CISO heading up Lewis cyber strategies. Hi, Zach.



Zach Lewis 00:26

Hi Jo. Thanks for having me. I'm real happy to be here. I'm so happy



Jo Peterson 00:30

you reached out. I was I'm thrilled to take a look at your profile and see some of the things that you're doing. You are CISO of University of Health Sciences and pharmacy, and you just got named to the 40 under 40 by the st louis journal. That's exciting.



Zach Lewis 00:45

Yeah. Thank you very much. I appreciate that.

J

Jo Peterson 00:47

Listen. If y'all aren't following Zach, you need to. It's Z, A, C, H, L, E, W, i, s, Jo, y'all get that? Okay, in case you're just joining clear take loop. The podcast is a hot tech hot take approach to cyber security, cloud security and AI security. And I say it's high tech because and hot take because we're only asking three questions of Zach, we want to get a feel of what's going on right now in the AI security space. So without further ado, first question Zach, how can cybersecurity professionals leverage generative AI to break out of that sort of traditional tools and tech mindset and drive more innovative thinking and execution in their security programs?

Z

Zach Lewis 01:36

Yeah, I'll give an example of one of the ways that we've been using generative AI and one of my first sort of forays into it was, was to use it for tabletop exercises, which I really love doing, because you could feed organizational context into the AI and sort of generate these unique scenarios that then could inject different real time twists and sort of prompts into them that completely change anything you're kind of used to from your scenario. So very agile, very, very quick and changing. And make your team, whether it's a leadership tabletop or a technical tabletop, really make your team think about the different things that can come in, and then you can feed your responses back into it and kind of get that analysis back, maybe some missed actions or improvement areas. That was one of the best use cases I found for it. And what I'm also saying right now is a lot of natural language sort of queries being injected or at least set up, sort of in different applications like EDR or dspm. I think that's a great place for it, where you can query these generative AI tools like, what's the best you know, vulnerability I should fix right now that's going to have the long stream, you know, benefits down the line and maybe really get more juice for the squeeze out of every sort of fix you're doing, every patch you're implementing, every everything you're tagging. So some really cool areas there that the Generate AI is helping in.

J

Jo Peterson 02:56

I love the idea of juice for the squeeze. You know, I think that part of as a young engineer having to go through log files thankless job, I love that AI is up leveling young engineers by presenting options. So it's not just the natural language query for me, it's the options that are being presented, and it's acting as a training tool in some environments. That's kind of cool, right? It is kind of cool. Yeah, absolutely.

Z

Zach Lewis 03:28

If you get one of those vulnerabilities you don't quite understand, or something you can literally query. Now, what is this? What does it do? What should I be looking at? Where can I find, like, really learn a whole lot about what that is, as opposed to just getting it in a report and trying to figure it out from there,

**J** Jo Peterson 03:44

or the ranking, right? Yeah, back in my day, we didn't get anything ranked. So you had, like, a billion alerts, and you're like, which one's important? I don't know. I don't I don't know. And this will actually, AI will actually rank. Like, hey, you've got a problem. You need to, like, this is a bread alert, fire kind of thing situation. Or you got these things going on, and they're just sort of, you know, normal fare for the day, right? So anyhow, it's good stuff. Second question, How can organizations embed security and privacy controls into AI models, and that development without sort of slowing down innovation.

**Z** Zach Lewis 04:25

Yeah, so, you know, strong AI security, I think, I think with everything, kind of starts with doing the basics well. So we really need to look at data classification, early categorization, early kind of identify what's that confidential data, what's regulated with public and get that, you know, properly labeled before we're injecting it into these models. I think that helps a lot with sort of the output later on. And again, more basic stuff is, are these models internet accessible? If they are, maybe critical data shouldn't belong there. I think we should probably segment that these models that you're making for internal like. At your companies, you know, do you have the right access controls on it? Do people have access to the right information that goes back to your data classification stuff, some of these foundational things that in security we've known for a long time sort of get forgotten and muddled when you're playing with the latest and newest technologies. And I think we need to bring that back into, you know, front of mind, that that is what helps make things secure in the long term. Other than that, document your everything you know, track your prompts. What data sources are you using? What are your model versions? Are we are we test? Are we patching regularly? Are we testing input validation? Just your basic least privilege access? That's another one. Just basic foundational controls still apply here in the age of AI,

**J** Jo Peterson 05:43

and you know, before we started recording you and I were talking about the collaboration that's taking place now between the CIO and CISO. Not that they weren't collaborating before, but it's even more important with areas that intersect, like data classification, for those two executives to really have a conversation about how they can help one another?

Z

Zach Lewis 06:07

Yeah, I mean, those two are gonna have to work together. When you're talking data classification too, and really tagging and who has access to what and how critical it is, you're gonna have to reach out to a lot of your business partners, a lot of your department heads too. There's gonna be data owners you have to work with. And that's why the CISO role, the security roles, actually sort of a networking role to where you have to make these partnerships with people in your organizations. You want them to think of you when they think of projects. Because we want security embedded there at the beginning, and not not wait till later on, where we're trying to patch things up, to fix things after the fact, but get that in at the get go,

J

Jo Peterson 06:42

look at you the AI cheerleader, AI security cheerleader. That's great. I love it. Last question, how should the CISO be thinking about AI adoption in terms of its use to secure emerging threats, but then also from an organizational governance perspective. So two sides of the same coin.

Z

Zach Lewis 07:04

You know, I read a lot of reports lately that say, you know, 80, 90% of these AI initiatives are failing. And I think that's interesting, because then you see other companies, like Google, Amazon, Microsoft, these big players that are, you know, laying off 1014, 25,000 people at a time and integrating AI. And I kind of contrast the two, because I think in these other organizations where we're seeing failure rates, we're trying to take AI and give it to the people. And maybe there's not proper training, maybe there's not proper incentive, but a lot of people don't want to change from their process. You know, they have a process it's worked for years. Why would I change that now? Maybe there's even some fear there that, hey, if I put AI in and it does my job for me, do I still have a role? There may be some fear there. So there's resistance to that change, and it's causing these AI initiatives to fail, whereas these big tech companies, they're getting rid of people, and they're like, Hey, we're going to backfill with AI. You don't have these 25,000 people anymore. You're going to figure out how AI is going to work and fill that role, or else, you're gonna have to pick up all the slack for everyone who's not here. So they're almost like forcing that line. So I think we really need to sort of create that environment that's without fear, show how AI arguments, rather than, you know, replaces people. I think good training. We've seen success, you know, getting a work group stood up and using looking at use cases that our teams are using, and sharing those with different people. Here's where I say an hour, here's where I say five hours last week, like, these are the things working for me, and we can make those people more efficient, and they'll be probably happier in their job and be able to get some more done and hopefully find some more satisfaction and not be worried about AI taking their job over.

**J** Jo Peterson 08:43

I love your approach. You know, so many times in security we get the a bad label. We get told we're the Department of no right? But your approach is so collaborative, and that is refreshing. It's kind of what we need to see at the executive level, how can we all work together and make AI work for us? So that's really cool.

**Z** Zach Lewis 09:09

Yeah, there's just a lot of unknowns around AI right now, in the best use even though the big providers of AI open AI and meta and Google, they they don't even know the best use cases every now, we're all sort of figuring that out. So I think just really documenting and defining, defining what that is, what success looks like, and encouraging our teams to try it out and figure it out, makes makes the most sense right now.

**J** Jo Peterson 09:32

It's great advice. Thank you, and thank you for joining me today. This was lovely. Y'all follow Zach if you haven't already, he's got a book coming out in January. Do you want to take a minute and talk about that book before we leave?

**Z** Zach Lewis 09:44

Zach, sure, yeah, real quick. The book is called locked up, and it's a real world ransomware story that I kind of worked through and we survived at the university, just giving all the pros, the cons, the decisions, sort of everything that goes on in it to help guide, you know, future practitioners and. And building a good security program and surviving ransomware attacks as they continue to increase throughout year after year, basically. So it'll be out January 6, lovely.

**J** Jo Peterson 10:09

So we'll have to have you come back and talk about some of the real world lessons that you learn from the book, because that's going to be super important to a lot of people listening.

**Z** Zach Lewis 10:19

Yeah, absolutely. I would love to do that show. Thank you.



Jo Peterson 10:21

Okay, great. Well, thank you again, and thank you everyone for joining and back at you next week. You.