CTL-CISO-Evan-Kirstel

Tue, Dec 16, 2025 4:55AM 13:51

SUMMARY KEYWORDS

AI security, generative AI, cybersecurity, incident response, AI triage, Microsoft Security Co-Pilot, IBM Watson X, CrowdStrike, training and simulation, zero-day exploits, data privacy, automated compliance, CISO governance, deep fakes, AI governance framework.

SPEAKERS

Jo Peterson, evan kirstel

J **Jo Peterson** 00:07

Hey everyone, thank you so much for joining. I am Jo Peterson. I'm vice president of cloud and security for clarify 360 and the panelist at Clear Tech Research. And I am here with the man, the myth, the legend. Evan kirstell, tech influencer extraordinaire, hi, Evan.

E **evan kirstel** 00:26

Hey, Jo, great to see you again.

J **Jo Peterson** 00:29

Thank you so much for making time to visit always. Of course, guys, in case you somehow are not familiar with Evan, I don't know how that could be. Evan has over 600,000 followers in tech across multiple platforms, and is a go to voice for all things tech, including cybersecurity. So you know again, welcome Evan.

E **evan kirstel** 00:56

Thank you so much. Great to be here.

J Jo Peterson 00:59

So in keeping with the clear tech loop hot take approach, we're going to ask Evan three questions about AI security and get his take on things. So let's get right to it with the first one, how can cyber security 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.

E evan kirstel 01:30

Oh, gosh, where do I start? I mean, there's just so much opportunity. And of course, Gen AI is being baked into all the tools that we know and love, and they're, you know, brand new capabilities out there that are being invented for that are Gen AI or AI native platforms. So let's just, I'll just start with, you know, things that caught my eye. You know, certainly AI powered triage. We all know that time is of the essence in an attack, and the amount of time you spend on Incident Response matters down to the minute, the hour, the second and what have you. So I think triage is a big opportunity. Just call it like Microsoft Security co pilot, for example. I think you know their solution pretty well. They can cut incident response times from hours to minutes. So just like an emergency room, minutes matter. So that's a huge opportunity, not just in security co pilot, but really all the tools related to triage and speed. Speed is of the essence. So generating not just detection faster, but detecting more faster. Like I know that another company you probably know, IBM Watson X, use Jo to kind of write and validate new detection rules in real time. So you're not just detecting faster, you're actually analyzing faster as well. So it's changing everything about response. I think that's hugely important. And I think it's also enabling analysts to predict, not just react. So we're used to reacting in security, always in it. In general, we're very reactive, where I think AI will free up more capability and give us new superpowers to kind of be proactive and not just reactive. I know, like CrowdStrike, for example, is is training, it's Gen AI on billions of endpoint signals, and it will be able, is able to kind of flag ransomware precursors early in the process. So you're not just learning about new ransomware in in the, in the, you know, the rear view mirror, you're actually seeing what's happening and what's being created in real time. That's huge. Also, I think, you know, training and simulation. You know, we it's, it's the old, you know, train, train, prepare, prepare, prepare. You know that from your Air Force days, I think you're always training and preparing and doing drills and ahead of real world exploit exploits. I think a lot of these new models are enabling us to simulate attacks so we can stimulate our responses. And, you know, you know, prepare before the hackers do so that, I think that's super important. And education is kind of like discovery as well. I think you know, a dark trace is looking at ways to find those mythical zero day exploits that are so dangerous and rare but very dangerous, by spotting unusual behaviors that humans just just wouldn't catch right through. Sifting through, you know, billions of data points. So those are a few ways, but there are so many more. I just pulled some examples that I sort of read about in the news. But, you know, there's really no, no limit to the opportunity for Gen AI and security.

J Jo Peterson 05:17

That was, those are some really strong examples. And you make some points that are sort of layered in there that are important. I think that this gives us a chance to really up level, our more entry level SOC folks, right? And it gives them remediation paths. So it offers them options. It doesn't just find things, but it gives solutions to the problem, right? So that's kind of cool as well. So lots of good things. Second question, How can organizations embed security and privacy controls into their AI model development without slowing down innovation?

E evan kirstel 05:59

Yeah, that's key. You know, we've got to make security sort of baked in from the beginning. It's, it's so often still an afterthought on a lot of the model training. And there's some interesting work being done by startups whose name escapes me, but they're, they're training models with differentiated privacy from the beginning, so they can kind of shield sensitive data from exposure right at the front end and turn it versus leaking it out the back end. So it's sort of, you know, built in data controls. I think open AI actually has enterprise ais that ensures zero retention of data, because you don't want the model to hang on to your data. If you're in healthcare, you're in finance, you're in a lot of industries, that's an absolute no no. So I think even the big players are waking up, have woken up to this, this problem. So I think it really is, you know, secure frameworks, and I think that can actually mean faster launches, because you don't need all that verification and testing SQA on the back end to discover and fix all the problems that you've created on the front end. I think like Salesforce, for example, they have automated security reviews into agent force releases, so it's, it's just sort of integrated automatically into the process. There's a lot of, like, automated compliance happening now too. That's, that's pretty cool, like compliance, again, is like one of these things a lot of engineers, you know, data scientists, kind of don't necessarily think about at the beginning. So something like an Amazon bedrock will auto enforce certain policies and practices during model training, like HIPAA and GDPR and other SOC two for, you know, other other frameworks, which, you know, is a big help. I think that will be a big deal. Just putting it out of out of not something you don't have to worry about, it sort of becomes a checkbox. And also testing, amazing work being done with testing cycles. And you know, how do you help developers not just develop code, but flag security vulnerabilities as they code? So it's not like one of those typical, you know, develop test cycles, but it's, it's, it's sort of happening in real time. It's like GitHub copilots doing that, so that that's kind of cool as well. So again, so many opportunities, and it just, it's just going to require a brand new rethinking of embedded security and how you develop and test software. And tell you, it's just amazing what's happening there with automated code Gen and I think the security around it is as important as the tools that are being rolled out, right?

J Jo Peterson 08:51

And that's those are such great points. And, you know, I like that we're seeing sort of collaboration between teams. You know, five years ago, there wasn't a network security engineer. The title didn't exist, really. I mean, maybe isolated here and there, but it wasn't sort of a norm title. And the same thing happens with developer security, right? So now you've got a dev security person that maybe sits between the security team and the dev team, and that can sort of help and coordinate and provide a bridge. So that's all good stuff that's occurring. Last question, how should the CISO be thinking about AI adoption, not only in terms of its use to secure emerging threats, because we kind of talked about that a bit, but more from the organizational governance perspective, like, how do they find balance?

E evan kirstel 09:47

Yeah, I don't think CISOs have much balance these days. What a job. I wouldn't want that job. Yeah, tough job. Even tougher job, kind of overwhelming. And you know what I'm hearing, you know, I'm sure you're hearing the same on your show. But from my show is, you know, using AI to secure AI, you know, is the big theme. I think even about things like deep fakes and and fake IDs. And, I mean, they're like 30 Evan curstells on social media, you know, crazy stuff. And that's only going to get one. Going to get work worse, worse, with deep fakes, voice and video deep fakes. So I think some of like, what Deep Mind is doing around synth ID to secure images and videos with watermarks is really cool. And I think we're going to need more on that so you don't have these, you know, investor calls that are completely faked. You can kind of differentiate between what's real and what's not. I think, you know, systems are putting up more guardrails that will keep everyone on a certain path, and that provides governance. They can, they can fast track deployment without, you know, going off the rails. Pun intended. So like JP, Morgan has an whole AI governance framework that they use internally to develop new chat bot applications, and everyone's on the same page, so no one's sort of going rogue and has to worry about compliance problems after the fact. So that's kind of cool. And again, AI, you know, AI as a enabler we talked about, but also as a as a kind of a threat Hunter. It's out there doing work that you can't do. You cannot spend all your days on twitter and reddit forums looking for, you know, following new challenges. You only have so many time, so much time of the day. Of course, AI is an infinite amount of time to find new threats, identify those you can kind of outpace adversaries that might be targeting your organization, or organizations like yours. So I think, I think that's really interesting, and I really like the work that, you know, companies are doing to go on the offense, you know, like with Palo Alto Networks, they're using Gen AI to sort of automate red teaming and stress testing and pen testing so you don't just have to wait to be attacked and respond, but you can think more proactively and offensively about threats. And you know, the whole like communication and collaboration dynamic is probably changing. It has to change faster, like how the CISO reports to the board on security risks, and, you know, engages with the wider team on customer trust and brand teams that have to deal with reputation. So it's not just like you're sitting in your siloed office and you're just talking to your IT and security people all the time that sort of wider communication. I know Walmart is breaking down a lot of those barriers across the CISO to the board, and so, yeah, all this is, is necessary good.

Jo Peterson 13:06

I think you make a great point. And maybe, you know, we're all growing and learning as we go here. But it seems to me that maybe the big thing will be that this is going so quickly that it's going to force some of those silos to come to fall down, and it's going to force communications right quicker, which is which are good things. So as always, it's a joy to talk to you. Thank you so much for the time and everyone. Thank you for turning for tuning in, and we'll see you next time. Thanks so much you.