CTL-CISO-James-McQuiggan

Sun, May 17, 2026 10:19AM 15:46

SUMMARY KEYWORDS

AI security, shadow AI, cybersecurity, threat intelligence, education, non-human identities, API security, phishing emails, AI defense, large language models, data flow, policy implementation, human risk, cybersecurity training, predictive analysis.

SPEAKERS

James McQuiggan, Jo Peterson

J **Jo Peterson** 00:07

Hey y'all. Thank you so much for joining. We're here today with ClearTech Loop. We're on the move and in the know. I'm Jo Peterson. I am the CIO of Clarify360 and the chief analyst for ClearTech research, and I'm here today with James McQuiggan, founder and CISO of Apparent Security. Hi, James.

J **James McQuiggan** 00:27

Hey, Jo, how you doing?

J **Jo Peterson** 00:28

I'm doing great. So, a little bird told me that you had one, maybe two dad jokes that you were going to do with us today. Is that was that little bird right?

J **James McQuiggan** 00:41

Well, yeah, we.. oh, I have plenty more. I could do a whole 10 minutes on dad jokes, but we have other topics. But yeah, I can.. I can drop one or two, I think, into a little segment today. Oh yeah, bring it.

Jo Peterson 00:53

I can't wait to see the audience response on that. So, in case you're not following James, you should be, because he is a threat intelligence strategist and an educator, he's a course director for Full Sail University, he's part-time faculty for Valencia College, and he's the education director for the Florida Cyber Alliance. So, James is going to take you to school, that's what James is going to do. That's my dad joke for the day. I don't know, but James has been - he's spent the last 25 years translating cybersecurity risk into boardroom language and frontline action. He's built programs across critical infrastructure, he's led human risk initiatives at scale, and he's delivered 500 plus presentations, probably one or two, with a dad joke inside them, from the front desk to the executives and the boardroom. I love his approach. It's collaboration first, protect always, and never underestimate the power of making security human. So great resume. And again, thank you for the time today. And in case you're joining the podcast for the first time, we are a hot take approach. Means I'm going to ask James three questions, and they are of the moment, and they are all about AI security. So let me get going with the first one. James, give me your thinking around shadow AI. Is it an IT problem, a security problem? Both, neither. And how are CISOs and CIOs addressing shadow AI in their environments? What are you hearing?

J James McQuiggan 02:32

Yeah, well, first of all, thank you very much for having me on the show. Real excited, because this, these are important topics that I know a lot of folks are dealing with, but interestingly enough, I think we're seeing what is old is new again, you know, whether it's in approvals, whether it's implementations, whether it's the threats, but I'm thrilled to be here and have this conversation with you. So, Shadow AI is kind of the successor, we'll say, of shadow, it, you know, for years CISOs and IT folks and organizations have dealt with shadow IT of people using cloud services or whatever else. Now we've got folks utilizing shadow AI, where they're trying to be more efficient, people know or may not know if their organization has a policy, they may or may not have had any type of training from within their organization, because AI is moving at such a rapid pace. Even last year we were seeing that it was doubling every seven months, and with what we've seen already here in the first few months of 2026 the advancements and the changes are incredible with what we're seeing in the technology and the capabilities. The problem that we're seeing is you've got organizations that are trying to get policies implemented and the technology is moving a lot faster than they keep up. People are worried about AI, they're worried that AI is going to take their job, and there's the saying that's out there, as you know, AI is not going to take my job. Somebody that knows AI is going to take my job. So people are trying to either get familiar with it, or they're sticking their head in the sand, and so you've got organizations and people that are out there that are just trying to keep up and wanting to leverage using AI, whether it's, you know, generative AI or agentic AI, a large language model, you know, whatever it may be, but leveraging different tools, or even with developers leveraging things like cloud code and other capabilities to do the code, so they can be more efficient and get the work done, and so you've got all these organizations that, and people that are trying to use it, but now you've got the CISOs and the leadership inside the organization, and essentially it's both, it's it, it's security. Are having to deal with it. You've got information security, cybersecurity folks that are getting the policies and the governance out there, so they can manage it. But then there's the technology aspect where we're trying to implement tools or capabilities so that people can't access it, but it's like we've seen so many times when you try to stop a human from doing something, they're going to figure a way around it, and they're going to figure their way to get to it. So we have to work, you know, this cybersecurity is not the department of no. We needed to be the department of, okay, well, let's try to work on that and come up with different policies, come up with different programs, different ways that people can leverage, whether it's using an AI proxy to filter and look at what that those requests are that are going out, make sure that we're not sending sensitive information up to a large language model environment or whatever else we're needing to make sure that we have technology that can safely let our users gain access to those large language models or the AI tools that they want versus them just trying to be sneaky about it. Now all of the computers that are being used, I don't know if anybody's ever been curious to know what kind of music a computer likes to listen to. Well, that would be an algorithm.

Jo Peterson 06:17

Oh no, okay. Number one, number one, no joke. All right, guys, just give him a little room, because he'll give us some more. I know he will. I know he will. And, but, James, you made such an important point, and what I liked is that very clear to me, that you're an educator, because you're the only guest that I've had on the podcast talk about the fact that education is a key component of rolling out any sort of policy, and I'm sure everybody else knows that that's not new information, but you brought it right to the front, because I feel like if the CISO can't baseline the environment, he's not going to know what department is maybe ahead of the others. Like, so, for example, you know the marketing folks are going to be way ahead of the accounting folks, no offense to either group, but they just are right. And so he knows that he's got some folks that are really heavy AI users in marketing, what's the next step then? How do you, how does, how does he make sure that they continue safely on their journey? That's the thing.

James McQuiggan 07:34

yeah, and you know it's interesting, because as I, I started off with, you know, what's old is new again, we're still trying to get our hands around, you know, the technology. We're still trying to get our hands around what we have, that inventory, the fun saying of you can't protect what you don't know about. So we have to know about all the software, we have to know about all the hardware, have to know better users, we have to know about what AI tools are out there that our users want or are going to be using and going through and educating them first, because for me, anybody that has an email address in the organization has a key to the front door, can be susceptible to a social engineering attack, or using some an AI tool, or accessing a site inappropriately, and so it's a matter of not just hitting them once a year with training, it has to be frequent, it has to be continuous, it has to be almost be monthly, and I'm not talking about doing 45 minutes, but like micro learning, five minutes, you know, something in a newsletter, a video that goes out, or lunch and learn, or or something that you know, gets out in front of the user, so they go, "Oh, right, okay, the new AI tool or AI is doing this, okay? Got to be aware of that, and having that awareness is one part of it, but they've got to make sure that the behavior is there for them to make sure that they're taking the necessary steps to keep the organization secure from, you know, using unapproved AI tools, and so it's got to be education. It's got to be where they're kept up to date, and it's as I said, it's moving fast. So we're always going to be behind the eight ball, we're always going to be playing catch, catch up, but if we can at least have something out there, going out, you know, every couple weeks, letting folks know, and maybe even be letting them know about, here's how the different attacks are going. Here's what we need to do to make sure we don't fall victim to this kind of attack, and keep that education, keep that learning going.

Jo Peterson 09:34

That's so good. So, so much has come out about, I mean, I got to give it to Mouthbook, you know, AI agents having their own social platform, like, who knew, right? So, let's talk about these non-human identities, or NHIs minute. How are you as you talk to CISOs and CIOs? How are you? You seeing those folks enabling these NHIS.

James McQuiggan 10:05

yeah, I mean, your NHI is, you know, that non-human identity, it's got control, a lot of them are trying to get their hands around it, because when you, when you're putting out the service and the product, you're having to make sure that you're controlling its access, you don't part of it is you want it to be able to communicate or give back information like a large language model on you know resources and things that you have in your organization, so you have to give it access to, you know, if hopefully not, but I know folks are doing it with email, they're doing it with all the different directories, all the data that they've got in the organization, and what's happening is sometimes you have people that go in and ask it a question and it gains access to something that the person isn't supposed to know, and so you're now having to control the data flow for the users based on what their permissions are, because when the NHI has got full access to everything, it's going to give everything, and so we're again getting back to API security, we're getting back to authorization of what data can be shared with what people, and if that's not implemented, and it's just, you know, wide open. It's going to be a lot harder for organizations to be able to lock that down if they're not being fully aware of it and exposing data that to their users that they're not supposed to see.

Jo Peterson 11:37

Yeah, exactly. All right. Last question, but before we do that, the audience is begging for a second.

James McQuiggan 11:45

Well, I have to admit, Jo, I, you know, when it comes to security, you certainly are a true emphasis of a security-minded, and I'm going to say woman here, because this leads up, you are a security-minded person, plain and simple, but when it comes to women, I don't know if you know the name of the most secure woman in the world. Her name is Emma Emma Faye.

Jo Peterson 12:14

Okay, guys, we're on to the last question, when you hear the term AI defense, what comes to mind for you?

James McQuiggan 12:27

When I, yeah, AI defense, you know, kind of the first thing we think of is our own defense, you know, what are we doing defending our organization with AI? And there's actually three ways that I look at this, and the first one is defense, and I'm not going to go into a lot of detail, because we've already been doing AI predictive analysis or machine learning in our security products for the last 10 plus years. I remember going to RSA 10 years ago, and AI was everywhere then with security products, so we know we've got that capability, and now we're leveraging AI with large language models with regards to, you know, doing knowledge-based questions, help desk, that kind of stuff, but what we're looking at now is AI defending the fact that cyber criminals are in scammers and nation states are out there using AI to generate phishing emails, you know, create for years we always said, you know, check the spelling, check the grammar, because that's because cyber criminals from nation states and other parts of the world, English wasn't their first language, and so, you know, you were able to get a easily spot that, well, now that goes away, and they can do it, not only in English, but Spanish and Portuguese and Russian and Japanese, and all the other languages that aren't exactly easy to learn quickly for a large language model, that's no problem. And so essentially now on the AI defend, we've now got to make sure that we're defending against the AI attacks that cyber criminals are leveraging, whether that's agentic type attacks, which we are hearing about, we're starting to see that, and essentially then looking to move forward with the AI defend of our own organization, but also securing the AI systems themselves, you know, we've got all of our AI systems that we're using inside of organizations. We have to make sure we defend those, because if a cyber criminal gets in and they gain access into that AI environment, AI environment, that's it, game over. They're going to have access through, you know, the agentic AI to all your data, all your systems, and so we have to make sure that we're defending that, so it's AI defend of the attacks coming in, AI defend of us defending, and then also defending our own AI tools, products, and services as well.

Jo Peterson 14:51

I think that's a very good holistic answer. So, thank you for that. But before we leave, I know you have one more dad joke for us.

James McQuiggan 15:00

Yes, one more dad joke. Okay, do you know what a computer and an air conditioner have in common? They're both useless when you open windows.

Jo Peterson 15:12

Oh my, okay, all right. For more dad jokes, but more importantly, for great virtual cybersecurity support. Get hold of James, he's on LinkedIn, so get hold of him, and he'd love to help you. James, thank you for taking time today. It was lovely visiting with you. Bye, everyone.

J James McQuiggan 15:35

Bye.