CTL-CISO-Thomas-Bryant

Fri, Apr 10, 2026 5:58PM 13:25

SUMMARY KEYWORDS

Shadow AI, security problem, discovery tools, non-approved AI, machine identity management, naming standards, just-in-time access, super agents, AI defense, adversarial AI, resilient security, AI governance, data leakage, AI tools, IT management.

SPEAKERS

Thomas Bryant, Jo Peterson

J **Jo Peterson** 00:07

Hey'all. Thank you so much for joining us today. We're here with ClearTech Loop. I'm Jo Peterson. I am the CIO of Clarify360 and I'm here with Thomas Bryant, Hi Thomas.

T **Thomas Bryant** 00:22

Hey, Jo. It's great to be here. Thanks for having me on.

J **Jo Peterson** 00:25

Thanks for coming. So in case you are not following Thomas yet, you need to be Thomas is an independent analyst and consultant at THB3, but Thomas is also a respected member of the product marketing community, having spent many years in senior leadership roles at Commvault, VMware, Dell Quest Software. He's an engineer by trade, which makes me like him even more. And shout out for Thomas here, in case any of y'all at cybersecurity firms are looking for a top notch product manager, Thomas might be available for a chat. I'm just saying. So just saying, if you're joining us for the first time, on cleartech loop, we are a hot take approach to podcasting, and we're really focused on AI security and cloud security, and so we've got a soundbite approach, and we hit you hot and fast with three questions. And Thomas's great answers, of course, today. So let's just get going with it. Thomas, first question, give me your thinking around shadow. Ai, is it an IT problem, a security problem, both, neither.

T Thomas Bryant 01:39

I think it's both. You know, I like to think of it sort of like the person bringing this real story here, the person who brings the air fryer into the lunchroom and the enterprise. You know, think about it. They're like the people that own the kitchen. They secure everything, they make sure everything's there. But people bring in their own devices, their own gadgets, and maybe it fries the wiring. Is it safe? Maybe it burns things down? We don't know. So I think it's kind of both problems in that it is really they've been so focused and security too, right? Security has long been the Department of No, and now they're kind of turning into this department of why? But I think the stat that I saw was 80% of employees use non approved AI tools, and that's what scares me the most, is like, what data are you leaking? So it needs to standardize, and they need to help, but at the same time, security needs to be able to say, hey, here's what's approved. Here's what, what, where the guardrails are, because I think there's a lot of it happening, but we don't know what the the governance is.

J Jo Peterson 02:51

Yeah, it's happening, right? That's for sure. It is happening. But you've had a chance to talk to lots of CISOs and CIOs. How are you seeing them address shadow AI in their environments?

T Thomas Bryant 03:04

Well, I mean, a lot of it comes down to them having to bring in the right sort of discovery tools. I mean, we say this in almost every industry, but it you truly can't manage what you don't know about. So some of it is going out and figuring out what is everybody spending money on so they can find them, it's doing an inventory so that they can start to address it, and then building the proper kind of rigor around what is and is not acceptable for you to be able to share out. You know, recent news, there was a big engineering company, and they were trying to fix some buggy code. It was in the news, and they were putting some of their proprietary code into public llms. They're not trying to be shadowy, they're just trying to be productive, right? They're trying to fix some buggy code. They're trying to see what it can do. But then they leaked secrets, and so these, you know, the the CISOs, the CIOs, are trying to figure out, you know, all right, what tools can we standardize, but then what are the right ways of enabling our people so that they know? Because at the end of the day, a lot of things, you know, it's people process and technology. And so if you've got people, you need to teach them a process of how to use tech. And I think that's where a lot of time is being spent right now. And even at the last few companies I've been at, there was a lot of focus on here's what we're standardizing on, tools you don't use the unapproved ones, and then here's the training of what you need to know what kind of data is okay to put in and what kind of data is not okay.

J Jo Peterson 04:37

Right? And it's as much about the education as anything, right? Because folks just don't know. They're just trying to get their job done.

T Thomas Bryant 04:44

Yep, Yep, absolutely.

J Jo Peterson 04:47

So I'm kind of tickled by the second question, because I have seen some some quirky and yet some really creative ways of handling this. I'm curious to see what you're. Going to say, what are some ways you're seeing CISOs and CIOs enable NHIS or non human identities?

T Thomas Bryant 05:07

Well, I mean, I think we got to, we got to step back and talk about the humans actually first, because,

J Jo Peterson 05:13

okay,

T Thomas Bryant 05:14

we were really good. We've gotten, you know, 20 plus years in the tech space of how to onboard people, right? Background checks, get them their badge, get them their password. Here's all the things that you need to get access to. We're really good at that, and we may have 1000s or 10,000 100,000, employees. The reality is with NHIS, they outnumber us 50 100 to one. How do you manage and onboard bots, scripts, AI, agents, all these different things that are running around with keys to your kingdom. Do you even know who owns the bot? Right? Who owns that? Nhi, because if you don't know who owns it, you can't fire it when it starts acting up. And so what I see a lot of the the CISOs and CIOs that I've been talking to, especially the forward looking ones, they're starting to give NHIS kind of their own driver's license. They're using machine identity management. And they're also coming up with even simple things like just naming standards for how they're going to name the these NHIS. Because, I mean, I don't know if you've ever looked at an IP six address, it's kind of the same thing. Like, I don't know what any of that means. It's hard to understand. So even just having some standardization around, like how you name your NHIs can make a big difference. And so I think the other thing that we're, I'm seeing outside of the identity management is gone. Are the days of permanence. You don't just give you the keys away for ever. It's Hey, how can we give away the short lived tokens so that that NHI has access for, you know, whatever it is just in time. People like to use that JIT term a lot. You know, just in time access, you do what you need to do, and then the keys get revoked. Or how do we keep it to where it's a minimal amount of time? That way, if anything does get hijacked, it's a it can help minimize the damage.

J Jo Peterson 07:18

And I love the naming convention thing. And I really hadn't thought about that, but it makes all the sense in the world. The thing that strikes me when I start thinking and hearing about Super agents, and I don't know what your thoughts are on this, is, super agents, if I'm getting this right, are going to be able to create other agents to do tasks. You're smiling already, because, you know, I think you know where I'm driving the bus, right? So how do we how are those permissions granted, and how long do they last? Are they ephemeral? Like, yeah, right. That becomes a whole thing.

T Thomas Bryant 07:55

It does. I mean, as soon as you have agents creating other agents and doing things, you really have to have solid governance, and you have to have traceability, more than anything.

J Jo Peterson 08:04

Yeah,

T Thomas Bryant 08:04

you know, we don't have to look far in any news article. I don't remember the company name, but they had their AI agent, and it wiped out their entire database because they gave it the keys. It had the ability to do things. And just because you can give it access doesn't mean you should. And so I think for me, it's you have to be pragmatic and responsible with it. Yes, the business wants to move fast, but you can't just go full bore and go, Hey, we're going to give it the keys to do everything. It's a stair stepped approach. You know, you got to you got to crawl before you can walk, and you got to walk before you can run. And I think that's what we're going to see with the the super agents is people should step in slowly and find success. Don't just go all in and, you know, wind up the next news article.

J Jo Peterson 08:57

I know, and trust me, I'm excited because I understand that they're going to be released on the consumer side before the enterprise side, which is probably a really smart thing to do, but I'm kind of interested, yet nervous about using one myself. I don't know,

T Thomas Bryant 09:17

yeah, I mean, I take a pretty tepid approach. I mean, I was very was a naysayer, I would say, in AI, and I've come to realize how much it can help augment what I do. So I think for like the super agents and agents creating agents, I think it, for me, it's how can I use it. It's not no again. It's not about no anymore. It's, How can I use it? How can it make my life better? What things could I use and find success? And once I find that, then it'll kind of grow from there. But I think the other thing too is, at least I find this in other areas. You need a community that's talking about that and finding these you. Space is to spur your ideas. And I still that one's still, at least, to me, a little early, and so I think people are still coming up with that, and they're keeping it kind of close to the chest, because some of it's IP,

J Jo Peterson 10:12

yeah, some of it is, I mean, personally, I keep thinking about a dream trip to Italy, you know, all laid out for me, perfect. So they don't have to figure anything out that, you know, probably thinking small, but it sounds good to me, so I'm just going to go,

T Thomas Bryant 10:27

Yeah, I like that. That's a really, that's a really good idea, actually, right? Just this is what I want come up with an itinerary. Now, book it for me. I think you got your

J Jo Peterson 10:37

hotel in the restaurants and the end the elephant, right?

T Thomas Bryant 10:40

Yeah, yeah, that, yeah. I think you just, you just cracked, like the whole travel industry, you got to make a travel AI now,

J Jo Peterson 10:47

code, yeah, all right, well, so been doing some reading, and I came across the term AI defense, and I thought, Oh, that's a nice, sort of ubiquitous term, but it might mean something different to me than it does to you. So when you hear the term AI defense, what comes to mind for you?

T Thomas Bryant 11:09

Well, to me, first, it's not a firewall, it's like an immune system. You know, when I think security, I always think like firewalls and radius and that kind of stuff, but I think in AI defense, a lot of it is now about adversarial AI like specifically inside of that, because one, we're inundated with data, and no human can look through, you know, the millions, billions of lines of logs and all the performance data that's coming in to be able to find the needle in the stack of needles, you have to have AI that can go through and pinpoint where to look and where to focus in. And that's to me, is like what AI defense is all about, like having these adversarial pieces that can go off and and find what's what bad things are happening, and then being able to act on it. Because, if I'm a malicious actor, what's the best time of day to do an attack? Weekend, probably 3am 4am when everybody's sleeping, right? You can't wait for me to wake up. I'm going to be groggy. Let me get a coffee in. Why is my phone blowing up? You need to have these kind of AI defensive tools that can go on the attack. Because the other, you know, in the industry I was just in, you know, it's not a matter of if you get hit, it's a matter of when and how bad is it. And I think that really has changed the idea of moving away from kind of this reactive world to being resilient. And I think resilient is the right word, because you need AI that can help stop the threat actors or the bad things that are happening in your AI model, but also can take you back to when it was a good known state.

J Jo Peterson 12:56

That's really good advice, solid, sound advice. So always fun chatting with you. Thank you for taking a few minutes with us today and giving your ideas, and I look forward to having a chance to chat with you again.

T Thomas Bryant 13:12

Thanks, Jo. It's great to see you.