

CTL-CISO-Rock-Lambros

Sun, May 03, 2026 3:53PM 12:44

SUMMARY KEYWORDS

AI security, shadow AI, CISOs, CIOs, governance failure, identity management, machine identities, agent accounts, AI defense, OWASP, data poisoning, model theft, automated response, vendor marketing, AI attack surface.

SPEAKERS

Speaker 1, Rock Lambros, Jo Peterson



Jo Peterson 00:07

Hey everyone, thank you so much for joining. I'm Jo Peterson. I'm the CIO of clarify360 and the chief analyst at Clear Tech Research. And I'm here today with Mr. Rock Lambros, CEO and founder of RockCyber, hi, rock.



Rock Lambros 00:23

Hey, Jo, how you doing today?



Jo Peterson 00:25

I'm doing great. Thank you so much for making time to visit. If you all aren't following rock on LinkedIn, you should be, because he's always putting down some good AI security tea. Apart from rock cyber rock is he volunteers his time with the OWASP Gen AI security project. He serves as a Distinguished Fellow at the Enterprise Risk quantification Institute, and also serves on several boards. So welcome rock.



Rock Lambros 00:57

Thank you. Thank you for having me.

J

Jo Peterson 01:01

In case you guys are new to the podcast, we're a hot take approach to AI security, cyber security and cloud security, and each week, we ask our guests three focused questions, and our goal is to educate our listeners about the security landscape, both from a risk and opportunities perspective. So with that, without further ado, first question for rock is, give me your thinking around shadow AI, Rock. Is it an IT problem, a security problem, both neither and as a follow up, how are CISOs and CIOs addressing shadow AI in their environments?

R

Rock Lambros 01:41

Yeah. I mean, it's both, right? So actually, it's funny, you know that this question comes up because my friend Diana Kelly had a LinkedIn post either late last week or over the weekend where she essentially said shadow AI is just shadow IT with better marketing. And she's right, right? It's, it's the same governance problem that we have with shadow IT and users. They're not sneaking in chat GPT or cloud or whatever to the enterprise because they're malicious. They're doing so because the tools that IT approved or security approved, or they're slower, they're clunkier, or just non existent, right? Like never provided an alternative. And I think the smart CISOs and CIOs who are responding, they're doing so by they're standing up sanctioned alternatives fast, right? They're building acceptable use policies that are both tangible, but, you know, also actually have some teeth, and they're deploying discovery tools to see what's already out there, right? To help, you know, kind of block the shadow problem. I think the organizations who are still kind of playing Whack a Mole with their AI strategy and like hoping some browser extensions, kind of block it there. There's way behind the curve, right? And so I don't think shadow AI or shadow IT, for that matter, necessarily security failures. It's an overall governance failure with probably a minimum of, like, a three month Head Start, if you will, right? So your users aren't the threat. They're just trying to get their job done. Right? Your your slow approval and adoption processes.

J

Jo Peterson 03:21

Yeah, that's super fair. So first of all, love Diane Kelly. She's a she is a shero of mine from a security perspective. She always has something witty and intelligent to say. So I've got to go now check out this, this post that she did for sure

R

Rock Lambros 03:40

a couple days ago.

J Jo Peterson 03:41

Yeah. Oh, good. Okay. And, you know, the thing that I do like about the shadow AI conversation is it's forcing folks to talk to each other. I mean, right,

R Rock Lambros 03:58

yeah,

J Jo Peterson 03:59

who's hot potato? Is it, you know,

R Rock Lambros 04:03

Whos hot potato, is it absolutely right? And it's, I'm finding, like, you can't have a single owner, like you can have an owner for a use case of an initiative, absolutely right. But you know, that's where you start to get super fragmented strategy. And is that any different than traditional. It like, you know, in your in your CIO role, right when you start having a bunch of silos spinning up in the organization, and now, before you know it, I mean, I've had clients that have had like, two different ERP systems,

J Jo Peterson 04:33

oh, yeah, right for sure.

R Rock Lambros 04:35

Like, it's crazy talk, um,

J Jo Peterson 04:39

yeah,

R

Rock Lambros 04:40

you know, like, you need the right tool for the right job, but you know, are you overpaying for licenses? Are you over provisioning both, you know, enterprise chat, GPT and enterprise cloud subscriptions? For instance, when you have Google workspace and Gemini kind of comes with your licenses. Like, have you done the analysis of whether or not. I You need all three tools, right? So it's forcing those conversations.

J

Jo Peterson 05:04

Yeah, that's, that's a really good point, yep. Um, okay. Like, I don't know why this is, like, one of my favorite topics of this quarter, but it is. It just is. I'm fascinated by it. Um, maybe that's just me, but NHIs

R

Rock Lambros 05:22

Yeah

J

Jo Peterson 05:22

Nhi, right? Is it? It's a it is a four letter word. So, yeah. So what are some of the ways you're seeing CISOs and CIOs enabling NHS?

S

Speaker 1 05:37

Yeah, you've got to treat it. You got to treat them as like a first class citizen, right in your identity and access management programs, and not as a bolted on afterthought, right? So that means secrets, management platforms just in time, credential provisioning, life cycle governance that actually tracks who created the service account and whether anybody actually still needs it. The you know the truth, and frankly, the ugly truth is that **most organizations have at least 10x more machine identities than human identities, and they can't tell you which ones have admin rights to production right, for instance.** And so CISO is enabling this. Well, they're building, you know, frankly, identity inventories, enforcing attestation cycles, same as they would for human accounts. And you know, we need to treat agentic as the same, plus, plus plus, right? Because with service accounts, you can kind of buying those credentials pretty well with agentic, it's a totally different ball game. You know, **people keep saying that we should treat AI agents as interns, yeah, but even human interns are smart enough to escalate ambiguous instructions when needed, agents will, just like, try and bypass everything and figure it out,** right? So we need to take a look back. We've spent, you know, whatever, the last 20 years perfecting identity management for humans who check email and attend meetings. Meanwhile, all these machine accounts and now agent accounts that actually run, actually run the business, have been multiplying in the dark with God Mode privileges and no expiration date, and that sprawl has gotten you know, if you talk to any CISO today, I would bet that that sprawl is in like the top two or three bands of their existence,

J

Jo Peterson 07:43

fair and, oh my gosh. And this is not on the question list, but I'm just gonna ask it anyhow.

R

Rock Lambros 07:49

What

J

Jo Peterson 07:49

about the agent social media site? They've got their own social media What? What? Come on now.

R

Rock Lambros 07:58

I mean, it's a larity, of course, right? And I'm just sitting back with popcorn. Like, when cloud bot was released, whatever it was, probably a couple of weeks ago now, like, just, just get the shenanigans that are about to ensue. I'm just, I'm just gonna sit back and watch the popcorn. And, yeah, the mulch book is awesome. You know, I've seen some people out there saying, and this is how sky net begins, whatever. At least, if we have the awareness that this is how sky nets begins, we can do something about Skynet, right? And for those of you who don't get the Skynet reference, please google it. But yeah, I think it's hilarious. It's absolutely hilarious. Hilarity, security nightmare hilarity.

J

Jo Peterson 08:46

It is. But I saw some excerpt today, and I didn't get to dig in and double click on it, but one of the bots posted that they want to they would like to sue their human that they would like to take the it

R

Rock Lambros 09:05

that day may come by. You know, we're gonna drop these, you know, AI robots into our homes. And you know what happens when we get to the magical AGI or ASI, you know, artificial super intelligence, and we generally have these robots wanting to sue their their humans for right labor law protections, or whatever the case may be,

J

Jo Peterson 09:26

and we're laughing about it right now, and it seems absurd and far off, but the fact that they have their own social site, I was like, wow. Okay, wow, wow, wow. Um, all right, on to the next, more serious question. When you hear the term AI defense, what comes to mind for you

R

Rock Lambros 09:48

that I need to reach for my wallet because someone's a boss or something?

J

Jo Peterson 09:54

Why do you need to reach for your wallet?

R

Rock Lambros 09:56

Well, because, like, the vendors are just like. Like, you know, it's vendor, vendor, vendor, you know, buzzword, buzzword bingo, right? So I think, and I'll tell you, right, why, right? Like, I think the useful interpretation of, really, of AI defense is two sided, right, protecting your AI systems from abuse, right? So that's the prompt injection, training, data poisoning and model theft, inversion, attacks and right, all the things that we do, right, like you mentioned, OWASP, right, all the things that we talked about and we do what the OWASP Gen AI Security Project and the OWASP AI exchange, but then the second interpretation of it is using AI to strengthen your defensive operations, right your blue team, better detection, faster triage, automated response. The less useful interpretation is what a lot of the vendors are doing right now, by slapping AI powered whatever your existing sim or security tooling of choice, and calling it innovation, and, you know, kind of, you know, masking traditional automation, what's just, you know, which is a bunch of if then else statements in the background under the guise of AI. Now, because, you know, the marketing team say you have to AI all the things, and the investors are saying we're only going to invest in you if you're leveraging AI, right? So

J

Jo Peterson 11:27

yeah,

R

Rock Lambros 11:27

what I care about is, I care more about whether your security team understands the new attack surface than whether your vendor has a chat bot interface to their product, right? So beware of the vendor pitch decks that say AI powered. Dig into what that actually means. What's the problem that they solve with AI? How are they leveraging AI to do it? How are they ensuring some sort of determinism with regards to AI practices within the product, within the platform? Because otherwise, you're not buying defenses, right? You're really just buying, you know, a mark marketing with a subscription fee.

J

Jo Peterson 12:07

Oh, well. I mean, on that note, I, you know, I think, I think we're done. I think we're good. You were, you were lovely. Thank you so much for the laugh. I, you know, definitely would love to have you back, come visit anytime, lots of good stuff. So thank you again for the time. Thank you everyone for joining and we'll catch you next time.

R

Rock Lambros 12:32

Thank you, Jo, thank you everyone.

