

CTL-CISO-Lori-MacVittie

Mon, Sep 01, 2025 12:51PM 16:24

SUMMARY KEYWORDS

AI security, generative AI, cybersecurity professionals, pattern recognition, network issues, IoT devices, DevOps, architectural controls, technical debt, MCP servers, AI threat surface, semantic patterns, secure coding, organizational governance, AI adoption.

SPEAKERS

Lori MacVittie, Jo Peterson

J Jo Peterson 00:07

Hey everyone, thanks so much for joining clear tech loop. 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 here today with Lori McVitie, five, Distinguished Engineer and chief evangelist for Fi hi. Lori,

L Lori MacVittie 00:26

hi, hi, it's me. I'm here.

J Jo Peterson 00:28

I'm loving the pink headphones,

L Lori MacVittie 00:31

my gaming headphones. Well, this is actually my backup gaming headphones, so, but

J Jo Peterson 00:36

you got swagger,

L Lori MacVittie 00:38

yeah,

J Jo Peterson 00:39

In case you guys don't know Lori, because she should. She's a distinguished engineer in f5 office of the CTO with an emphasis on emerging architectures and technologies, including cloud and edge computing, digital transformation and application delivery. Lori has over 25 years of industry experience, and it spans app dev, IT architecture and network and systems operations. So, yeah, right. I mean, hard. How did that all happen? Lori,

L Lori MacVittie 01:17

oh, that's, that's a long story, but I get bored easily? Well, I used to, I used to get bored easily. So I would jump to different industries, and then the next thing you know, you're playing with networks, running tests, and then working for a tech company for almost 19 years. So, yeah, yeah, I've been here a long time, probably because emerging technology keeps changing everything, so there's always something new to learn. It's it's really hard to get bored today. I think you have to try today with AI to get bored.

J Jo Peterson 01:51

Yeah, you do. That's a really good point. I also understand that you have strong opinions about cheese and gaming systems.

L Lori MacVittie 02:01

Absolutely. I mean, I am from Wisconsin. There is a cheese head back there, right? And it's cheddar, cheddar, like American, is not acceptable cheese that should not be used at all. It should be a nice cheddar. The more aged, the better, a 15 year aged cheddar from, you know, a local, oh, it's, it's absolutely brilliant. Yes, perfect, perfect.

J Jo Peterson 02:28


I had never, I have a customer in Wisconsin, and, you know, I'm not a spring chicken. I know that surprised everyone, but I had my first cheese curds. I Right. I was like, What's a cheese curd? And they all started laughing at me. And yeah, but they were delicious, and they went so well with beer, I can see people like them.


L Lori MacVittie 02:54


Oh yeah. Were they deep fried or were they fresh?


J Jo Peterson 02:58


Well, I had both.


 Lori MacVittie 02:59
Oh, excellent.


 Jo Peterson 03:00
They said that I had a sample both, in order to get the full kind of effect of things,


 Lori MacVittie 03:05
yes.


 Jo Peterson 03:06
So y'all, this was not what you were expecting from an AI Security Podcast, huh? Well, I mean, y'all, but you know, it's, it's good stuff. Everybody should know something about cheese curds, right?

 Lori MacVittie 03:18
Absolutely, absolutely cheese curds. You must try, right? You go to Wisconsin, you must try cheese curds, deep fried and fresh, and they got to be fresh, never refrigerated, never

 Jo Peterson 03:31
okay,

 Lori MacVittie 03:31
never be cold.

 Jo Peterson 03:33
That's so I think you may want to change your profile to say you have strong feelings about cheese curds too. I'm just saying

 Lori MacVittie 03:39
that's Yeah, that's true, because they're not exactly cheese. So

J Jo Peterson 03:42
cheese, right? It's not exactly cheap. I mean, so I've learned,

L Lori MacVittie 03:46
yeah, no, they're not, yeah. All right,

J Jo Peterson 03:49
we're gonna, we're gonna turn the tables a little bit and talk about, and talk about some AI and security and AI security together. Okay, all right. Questions for you. Here's the first one. 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 the security programs?

L Lori MacVittie 04:16
Wow, that was really a leap from cheese curds. So one of the, the first things is that traditional security, and we're calling it traditional now, or classic. It's not quite vintage, but we're, we're getting there, but security has been kind of based on rules. There are rules we implement everything, you know, IP tables. It's rules. We have firewall rules. We have WAF rules that say this, you know, if this, then that they're very simple. And what AI brings to the table, both classic and generative, is really the ability to find patterns rather than look at, you know, did this break a rule? And this is. Is this is one of the ways we can break out. I had a network problem at home last week. I was getting terrible ping spikes in my game, very frustrating. So I did a packet capture, of course, because that's what we do. But instead of looking through it, I fed it into chat GPT, and I said, you know, find the patterns here, and it immediately identified an IoT device that was just way more chatty than it should have been. Like, absolute discovery storms on the network that were overwhelming the router, causing some lag. So, you know, I turned that off, I'm like, I don't need that anyway. So let's get rid of that guy and fix the problem. That would have taken a lot longer had I not had AI just kind of find the patterns in there, right? It was able to very quickly identify, look, there's a pattern of this kind of traffic right here that let me then go back and identify, right, which device, where was it, what's going on. So I think using those kind of tools to do faster discovery and find the patterns is a lot better than who's breaking a rule, because that's going to get very tedious, and we know that right. Traditionally, it's it's a long process. We have to build the rules, we have to check the rules, we have to see who violated the rules and the logs. It's just, you know, looking for patterns a little easier. I think so, thinking of new ways to use generative AI, basically, is one of the ways to break out of that. Instead of defaulting to, I'm going to go here and here and here, because that's our standard process, where would it make sense to apply AI or leverage it or ask it questions explore the data faster? So I think that's really where that helps break out of that loop and starts accelerating the security process and a better understanding of what's going on in the network.

J Jo Peterson 07:01

That's a great answer. And what you really what I heard, one of the things I heard you say in subtext was it's, it's about the money too. Like, think about it. We've been engineers for a long time. Think about mean time to repair, right? And imagine by just doing something simple like you did, and getting outside of the rules and looking at the patterns, maybe you compress that cycle, and maybe the business gets back up and running.

L Lori MacVittie 07:31

Absolutely, absolutely. I mean, we went through this with DevOps, right? Part of the DevOps process was not just about the tools and the build pipelines. That was the implementation. Actually putting it into practice meant you had to step back and say, what is our workflow? What is step one? Step two, step three. Find the value chain, find the delays and try to compress them. That's how you make things more efficient. That's how you make them faster. And that's true in business processes. It's true in DevOps. It's true in security processes. And right now, security is very by its nature, right, very rule based, both in its processes and in the way that it's implemented. So we've got to look at the process and say, Where, where, what takes the most time. And can AI help me with this? Is there something it can do to accelerate that and reduce that wait time?

J Jo Peterson 08:27

Yeah, I like that. And thank you going, thank you for going to the dev part of the equation. Because, you know, one of the questions that sometimes we hear, and it's getting better from development folks, is you're slowing me down. You're slowing me down. Right? How can organizations embed security and privacy controls into AI model development without slowing down that innovation that everybody wants to see?

L Lori MacVittie 09:02

So I'm going to be contentious and controversial and say something, don't build it in. It should be in the infrastructure, in your architecture, if your security is built into the applications, your APIs, your your AI, your models, your servers, you are, you are binding yourself to a point in time that is almost certainly, thanks to AI, not going to be relevant in perhaps six months, and certainly not in 12 months. And you're going to have to go through that process. We talk all the time about technical debt and architectural debt. How about, you know, security debt building it in. If it's in the architecture where it's more dynamic and it's more able to apply policy or enforce policy in real time, in that architecture, you don't have to hold back the development, because once it gets in. Into the environment, you are applying the correct security at the time it's relevant to that process. So I think you know, building insecurity is there's secure code, of course, right? Come on, right? That's like default. Every developer should be doing that period secure coding by design, but when it comes to policy and enforcement, checks balances governance, that is an architectural question that needs to be, you know, implemented in the infrastructure and by the infrastructure, not by developers. These these two shouldn't be clashing like that,

J Jo Peterson 10:39

and you make a good point, because we're starting to see the evolution of MCP servers, which is architecture, right? And it is to me, and maybe I'm just thinking about it wrong, but to me, it feels like not only a proxy server, but a firewall of sorts.

L Lori MacVittie 11:05

It's, it's a Franken server, right?

J Jo Peterson 11:12

Yeah, and you know what? Let's have you come back and let's, let's talk about all things MCP servers, because that's a whole nother topic. But yeah, that's the thing I would get. Was trying to get to was agreeing with you that we're starting to see architectural controls pop up, whether they're fully formed or not. We're starting to see them pop up, right? So to in line with your thinking, let's build it in the architecture so the developers don't have to worry about it. Or we know the llms. People are going to be using the llms. What can we do to make it safer?

L Lori MacVittie 11:54

Right? Yes, yeah, it's, it's very reactive at the moment, yeah. What one of the things that I do right throughout the year is a lot of research digging into these different topics. And we just happen to be looking at AI security right now. And one of the themes that I'm seeing in the responses is really that evolution and adoption of AI and its technologies, MCP, agents, agentic AI, is that it's outpacing security at this for sure. It's absolutely terrifying. What's, you know, how fast that is really. It's just like over running. It. It's, you know, it's like the Road Runner and the coyote, that poor Coyote, is never going to catch up at this point. You know, we need to do something.

J Jo Peterson 12:40

There's a vast gap. And various and sundry sources cite that disparity between AI security and AI projects, right? So you're you're not wrong in your thinking. And, yeah, yeah,


L Lori MacVittie 12:57


what does AI security mean?


J Jo Peterson 13:01


Well, and that's another that's a whole nother thing, because I grapple with that myself. I think about, I think of it two ways. I think of it as part embedded, as part of a tool somewhere, right? And then I think about a stand up framework that balances against something like NIST, right?


So I think of it, and I don't know if I'm thinking about it right, but I think about it two different ways, so don't know it's evolving

 Lori MacVittie 13:33
absolutely all right,

 Jo Peterson 13:35
my last question how should a CISO be thinking about AI adoption in terms of its use to secure emerging threats, and also the other side of that from an organizational governance perspective.

 Lori MacVittie 13:49
Wow, yeah, it is a big one. I mean, you have to treat AI as both a capability and a threat surface, like they do different things. And it's, it's not just the API anymore. This the threat surface. It's also, it's also the AI. It's, it is right, the the context, the prompts, the responses, the completions, whatever we want to call them, all of that is a threat surface that is distinct from the API, that is distinct from the network stack that is distinct, distinct, distinct. So it is a threat, service unto itself that you have to think about, especially on the governance side. Because, I think, and this goes back to your first question, right? About rules? Right? Well, what words do we look for? Right? This problem is not going to be solved by a series of reg x, it's not we can't just keep looking for, you know, this little pattern, this little pattern, we have to look at AI as a capability to help us identify right semantic patterns that are saying this. This is trying to manipulate the model. This model. Model is giving bad answers. It's it's giving information that it shouldn't in a way that we don't recognize. Because there's no rules that say, you know, if these words are strung together, it's bad it because it could change how it strings those words together. What if I tell your model to answer only in pink Latin. Well, every one of your rules is good, right? It's that's an that is an easy, easy, you know, going back to the the days of IRC, right? You know, like rot 13 this, you know, your rules are going to be useless, so you have to think about using AI to combat AI, as well as the threat surface it presents.

 Jo Peterson 15:46
Okay, we've had cheese curds, Pig Latin. I mean, I hope that folks watching this have a hoot, and I have to have you come back and we'll talk, you know, model, context, protocol, security, and if it's a viable architecture and all the good stuff about that. So anyhow, thank you so much for joining today. You were awesome. Thank you guys for joining as well, and we'll see you next time you

 16:12
I'm

