

CTL-CISO-Stefano-Righi

Sun, Feb 08, 2026 2:54PM 12:21

SPEAKERS

Jo Peterson, stefano righi

J Jo Peterson 00:07

Hey everyone, thank you so much for joining. I'm Jo Peterson. I'm the vice president of cloud and security for clarify 360 and the chief analyst at Clear tech loop. And I'm here today with Stefano Righi, chief security architect, American mega trends. Hi Stefano,

S stefano righi 00:26

Hi Jo. How are you doing

J Jo Peterson 00:27

good. Thank you so much for taking time to visit today. Very nice of you. And if you all are new to the podcast, we are a hot take approach. We're talking about, we're going to do three questions with Stefano on AI security and give you an of the moment, sort of feeling of what's going on from Stefanos perspective. So let me get busy with the first one, nano fanoteStefano. How can cybersecurity professionals leverage generative AI to sort of break out of that traditional tools and tech mindset and drive more innovative thinking and execution in their security programs.

S stefano righi 01:12

Thank you, Jo. Thank you Jo, for having me part of this conversation. I'm very glad to be here. Generative AI empowers cyber security teams to move beyond the reactive and tool centric approach and embrace proactive and adaptive strategies instead of relying on static rules and malware workflows. Gen AI enabled innovation through automation, predictive analytics and intelligent orchestration. We should take this opportunity to move beyond reactive security posture, while traditional security focuses on detection and response after incidents, Gen AI enable, anticipate, anticipatory defenses. Let me give you a couple of examples. Gen AI could provide predictive threat modeling, that is the ability to forecast attack patterns before they occur. Or another example could be dynamic risk assessment, which means to continuously evaluate vulnerabilities and adjust defenses in real time. We should treat Gen AI as a strategic

enabler to drive innovation, embed Gen AI into our security programs, and not as a bolt on tools, as you are saying, but as part of the design. From the very start, we need to pursue secure by design for AI model, that means to build privacy and adversarial resiliency into AI life cycles to mitigate risk like prompt injection and data poisoning without slowing innovation. It is also necessary to have a governance framework, we should adopt AI specific standards, like they are proposed by organization like NIST and OWASP, and extend zero trust principle to AI system to counter identity fraud and modern manipulation. We should cultivate a culture of innovation, because breaking out of the how you call it, tool and tech mindset is really cultural issue. For example, **prompt engineering training is necessary because prompt, a poor prompt, lead to poor outputs training team in domain specific prompt design, improve Gen AI effectiveness and security outcomes.** In our DevOps, we adopt AI native workflows. How we can achieve this, just moving beyond the static scanners, adopting AI driven orchestration layer, connecting detection, remediation and prioritization. I also want to touch something that is very close to my heart, meaning that **we need to combine AI with human oversight, because then AI can surely accelerate processes, but human validation ensure compliance and prevent misuse.** We all know that Gen AI is still subject to hallucination. Anyway, I believe that the right check and balances, the right human oversight is required for every sort of automation I want to touch also, if you allow me a little bit on a firmer perspective in this conversation, because I have personally worked in firmware my entire career of over four years, and firmware security has always been in the last 10 years, my focus point and firmware. Is unique challenges because it is a very complex environment with multiple layers that go from micro code to BIOS to BMC to Root of Trust. The complexity of the platform is constantly escalating, and we are in front of evolving threats like boot loader malware and AI driven exploits. So I also want to mention that for firmware specifically, there is a real global talent shortage in general for firmware, but is specific for firmware security. So firmware security is very basic. Is a very basic need, because firmware run under the operating system, and any attack that could happen at such layer could may go undetected by any antivirus solution running in the operating system. And at AMI, we are addressing these challenges, including AI into our development processes and solutions for our customer, introducing dynamic and adaptive capability. Let me give you a few examples. For example, we provide automated firmware debugging so the capability of identifying problem root causes and proposed fixes using AI models that has been trained with historical back and fixes data and all of this can be integrated into bless you, reflected into CICD pipeline for continuous validation. We provide also threat identification and vulnerability discovered to our customer with AI driven tools to identify female vulnerabilities in providing the necessary mitigation. We have also started intelligent code generation using AI power tools we can provide. We have also included predictive threat intelligence on some of our solution that analyze telemetry of fewer logs, detecting anomalies and anticipating emerging threats. So in conclusion, **generative AI transform cyber security in every space from reactive defense to proactive innovation. This can be achieved by embedding AI into workflows, fostering a culture of innovation and applying strong governance in this way professionals like us can secure organization from emerging threats, especially in complex area like like firmware that, but at the same time, accelerate agility and resiliency,**

J Jo Peterson 07:51

gotcha. And you sort of answered the second question when you talked about, you know, putting security into the start of the process, which is very spot on. So I'm going to go right to the third question. How should the CISO be thinking about AI adoption in terms of its use to securing emerging threats, and then the other side of that coin from an organizational governance perspective?

J Jo Peterson 08:17

Sure, sure. Yes. Very, very pointed question. CISO should approach AI adoption as a security force multipliers and the governance imperative. The goal is to harness the AI speed and press and prediction power to counter emerging threats and at the same time embed Accountability and Compliance into every stage of the deployment. AI is a security force multiplier. AI has the potential to accelerate threat detection of response. This because AI driven analytics may process massive telemetry data in real time, spotting anomalies and novel attack patterns that traditionally, that traditionally system, like signature based system, could not be able to identify. This is because the AI power attack have the potential to shrink the compromised window time to a very short time. But beside the technical may you also predict and enable predictive defense, and most of all, AI has the potential to provide automation at scale because they enable automated incident reagent, triage and orchestration, reducing alert fatigue and aligning response speed with machine Against The Machine. Broad attacks. So the governance, governance may act as a catalyst, catalyst, not as a break to innovation, enabling innovation while ensuring trust. We need to align with industry standard that are coming from recognized organization like ISO NIST, and we need to comply also with regulation that are growing constantly, like the Europe acts, both the AI Act and the cyber resiliency act, because at the end, all these AI system are also required to be compliant with both acts at the end, because AI system have the digital elements into them, so they this governance cannot Be silhouette into security. But the season needed to create these cross functional committees in order to ensure that policies are applied company wide, and not only for specific specific incidents.

J Jo Peterson 11:19

He makes such a good point, because I'm starting to see these cross functional conversations now that I really wasn't seeing before, because people are trying to figure out, hey, if I'm going to do an AI governance framework, for example, I want to make sure that I include the other, you know, technical leadership and get their thinking, because AI is touching everything.

S stefano righi 11:46

Yep,



Jo Peterson 11:47

it touches everything, right? So, So anyhow, very lovely conversation. Thank you for the great points that you made and taking your time to visit with us. And we'll have to have you back again to talk about MCP servers and those sorts of things, sure, absolutely, it will be my pleasure. Thank you so much. Bye. Thank you.