Inside the New Age of Telecom & AI: Discuss Cyber Threats and Engineering Solutions from the Expert like Sridhar

LOS ANGELES, CA, UNITED STATES, September 1, 2025 /EINPresswire.com/ -- During a visit to a leading technology group, I observed rapid change in networking, telecommunications, cybersecurity, and AI-powered operations. Conversations around the table swirled with urgency—new threats, cross-platform convergence, and the evolving rules of enterprise defense.

What made this meeting particularly engaging was the participation of Sridhar Sriharsha Rachakonda, a Principal Staff Engineer and industry veteran with over 9 years of experience. His expertise and candor elevated the discussion as he shared real-world examples of innovation and threat defense in the telecom and collaboration sector.

“I think what’s really changed in the past 24 months,” said Sridhar, “is the volume and velocity of cyber threats targeting unified communications platforms. Migration from legacy UC and collaboration infrastructure to cloud-based UCaaS became critical—not just for scalability but to adapt to the changing landscape of security threats in the age of AI. I redesigned and overhauled our global infrastructure, retiring obsolete systems and closing crucial security gaps to achieve constant operational uptime.

He highlighted, “While migration addressed part of the challenge, meeting rooms and collaboration endpoints remained vulnerable. Credential management was a critical concern—static admin passwords proved to be prime targets for attackers. To combat this, we developed an automated access management solution that rotates passwords, enforces strong authentication, and streamlines bulk device onboarding with self-healing processes. This significantly improved data privacy and operational resilience.”

He continued, “AI is now integral to our device operations. We were the first to implement generative AI for large-scale provisioning in Microsoft Teams Rooms, leveraging advanced vision

models to automate logins, multi-factor authentication, and setup. This innovation enabled secure, robot-driven onboarding and immediate validation globally, eliminating password exposure.”

He affirmed that observability is essential for collaboration security, explaining that a comprehensive analytics engine should unify data across platforms to provide complete visibility. He concluded by emphasizing the necessity of predictive monitoring, automated alerting, and seamless integration with business workflows, all of which are vital for multinational enterprises to stay ahead of emerging threats.”

The discussion echoed a common sentiment in the industry: security and innovation can no longer be separate efforts. As cyber threats become more sophisticated, the collaborative mindset and technical depth displayed by engineers like Sridhar are setting new standards for enterprise protection in the digital age.

Colin Adams
Indigo Software
email us here
