WiCyS × Cisco: AI & Cybersecurity Event Transcript and Analysis

Location: Cisco–Splunk Offices, Santana Row, San Jose
Event: WiCyS Silicon Valley Chapter – AI and Cybersecurity Panel
Compiled by: Juan (Cybersecurity Student, CSU Monterey Bay)

This document provides a complete and organized transcript of the WiCyS × Cisco AI & Cybersecurity event, integrating the official panel discussions, Q&A; sessions, and networking conversations. It includes commentary from industry leaders including **Ramana Kompella** (Cisco Fellow, Head of Cisco Research), **Dr. Yu Fu** (Senior Principal Security Researcher, Palo Alto Networks), and **Neha Pattan** (Head of Cloud Networking - AI & Principal SWE, Google). The purpose of this transcript is to extract technical and professional insights relevant to students exploring AI, cybersecurity, and quantum computing intersections.

Panel Overview:
The panel explored the convergence of artificial intelligence and cybersecurity, covering topics such as trust in AI systems, agentic workflows, quantum computing's effect on cryptography, and the changing role of human oversight in autonomous systems. Panelists agreed that while AI significantly enhances detection, observability, and anomaly response, it also introduces novel vulnerabilities that require new frameworks of defense-in-depth and zero-trust approaches.

Ramana Kompella – Cisco Fellow and Head of Cisco Research
Ramana discussed the evolution of AI in cybersecurity, emphasizing layered protection and "agentic workflows." He introduced concepts such as **TPACK** and **T4PACK** for contextual access control. He also highlighted the future of quantum computing and the need for crypto-agility within enterprise security systems. His insight linked AI's speed in detection to the need for equally agile security systems and architectures. **Neha Pattan** – Head of Cloud Networking - AI & Principal SWE, Google
Neha described how AI contributes to cloud resilience through observability and anomaly detection in network systems. She recommended that students study both **supervised and unsupervised learning** within the context of packet analysis and network metrics. She emphasized continuous learning and endorsed Google's certification in AI and cybersecurity as a strong entry point for students. Her focus was on developing the technical depth through reading research papers and practical exposure. **Dr. Yu Fu** – Senior Principal Security Researcher, Palo Alto Networks
Dr. Fu discussed AI's role in both offensive and defensive cybersecurity. She described her academic journey and transition into industry, highlighting how AI can detect malware and malicious JavaScript through classification models. She cautioned about the evolving nature of threats, such as polymorphic attacks, and explained how AI must adapt to continuously changing attack vectors.

Key Takeaways:

1. **Defense-in-Depth for AI:** Security systems should integrate layered protections against prompt injection, data poisoning, and model misalignment.
2. **Quantum Readiness:** Enterprises must adopt post-quantum cryptography and maintain crypto-agility to evolve with new threats.
3. **Continuous Learning:** University education provides the foundation, but professionals must supplement it with certifications, online courses, and applied experimentation.
4. **Zero-Trust Mindset:** Both AI systems and professional practice must maintain skepticism and validation before trusting inputs or models.
5. **Human Oversight:** Even advanced AI requires human review and contextual judgment to ensure accuracy and ethics.

Personal Reflection and Application:

As a cybersecurity student at CSU Monterey Bay, this event reinforced the value of balancing theoretical study with industry-driven skill development. The discussions illuminated practical pathways for integrating AI in cybersecurity defense, as well as how to prepare for roles that blend technical analysis with ethical responsibility. Networking with industry leaders underscored the importance of curiosity, adaptability, and lifelong learning in an evolving landscape where AI, cloud, and quantum technologies converge.

Appendix: Transcript Highlights

Conversation with Neha Pattan (Google)
“Every hyperscaler has resources on AI and security. Google’s certification for AI and Cybersecurity is a great start. When I want to learn something new, I focus on books and papers. For students, reading research and experimenting on network datasets will teach you supervised vs. unsupervised learning better than any class.”

Conversation with Industry Mentor (Santana Row 12)
“You won’t get the latest AI tools at a university. That’s where Coursera, YouTube channels, and VC tech updates come in. Experiment safely, learn the tools firsthand, and understand both sides—how they’re used for good and bad. The best way to learn cybersecurity is by doing it, safely.”

Conclusion:
The WiCyS × Cisco event at Santana Row provided invaluable insights into how AI is reshaping cybersecurity. By engaging with experts from Cisco, Google, and Palo Alto Networks, attendees gained a multidimensional understanding of the field’s future—marked by interdisciplinary knowledge, ethical responsibility, and agile defense strategies.