Michael Morey Presentation on Red Teaming and AI

Chadwick Bennett
February 18, 2026
CYSE 200T
Professor Duvall

BLUF (Bottom Line Up Front)

Michael Morey, Senior Principal Cybersecurity Engineer at Frontier Technology Inc., delivered a focused and practical discussion on Red Teaming and AI. Three key takeaways resonated most with me:

1. The importance of "The Village" culture in cybersecurity teams
2. The strategic value of penetration testing and security awareness
3. The professional development insights shared during the Q&A

These themes reinforced how technical skill, teamwork, and continuous learning strengthen cybersecurity operations.

1. The Village

"The Village" describes a tightly connected cybersecurity team where each member supports a specialized function while contributing to a shared mission. Rather than operating in isolation, team members collaborate to strengthen defensive and offensive capabilities.

This stood out to me because it emphasizes:

- Cross-functional team support
- Trust and communication within teams
- Passion for continuous learning and skill development

The Village is not simply a technical unit; it is a professional community. Members actively improve their penetration testing skills while mentoring and supporting one another. What Morey described was a high-performance environment where individuals are motivated not just by compensation, but by intellectual challenge and mission impact. They get paid for what they love to do.

This reinforced the idea that cybersecurity success depends as much on team cooperation and bonding as it does on technical knowledge.

2. Penetration Testing

Morey distinguished between security awareness testing and adversarial penetration testing..

Security Awareness Testing

- Focuses on educating employees
- Tests phishing recognition and reporting procedures
- Reduces human error, the most common vulnerability

Adversarial Penetration Testing (Red Teaming)

- Simulates real-world attackers
- Attempts credential theft, malware deployment, and network compromise
- Evaluates detection and responses

More and more businesses are hiring companies to provide Security Awareness testing with limited access to parts of their systems. It's normally held during non-operational hours over the weekends to avoid disrupting the business. The final reports are targeted to different levels of leadership:

- **Executives (CEO, COO, CIO/CTO):** Financial and operational impact
- **Management:** Process improvements and training strategies
- **Technical Teams:** Specific vulnerabilities and steps to improve weaknesses

This shows that it is important to communicate differently with various company management and staff, versus just providing a technical report and findings.

3. Q&A: Career Development and Practical Insight

The Q&A session was an added-value part of the presentation, because it allowed us to ask questions that weren't necessarily discussed during the presentation. It provided valuable information on Capture the Flag, security systems, offensive and defensive strategies, and how each team player had different roles or parts they played.

I was particularly interested in the certifications and training topics that were discussed, including TryHackMe and DEF CON.

These topics talked about the value of hands-on experience and the cybersecurity community. The discussion reinforced the importance that certifications and continued education have for professional growth.

Conclusion

Michael Morey's presentation was informational and very stimulating. It provided information on Red Teaming, security awareness, and how the team spirit and bonding make a difference. Although I didn't go into depth about Zero Trust, I found its philosophy about "don't trust anything" and "verify everything" to be guiding principles. People are the weakest link in cybersecurity and protection, and the Zero Trust subject is important for everyone to understand.