Beyond the Firewall:
Evolving Cyber Skills for the Age of AI and Automation

VetSecCon 2025

Ron Woerner

Session Summary:

As the cybersecurity landscape undergoes rapid transformation driven by artificial intelligence, automation, and increasingly sophisticated threats, the skill sets required of today's cyber professionals are evolving at an unprecedented pace. This interactive session delves into the shifting demands of the field, highlighting the transition from traditional technical expertise to a more holistic blend of strategic thinking, adaptive learning, and interdisciplinary collaboration.

Contents

Presentation & Contact

Content:

- LinkedIn – Ron Woerner
- Linktree – CyberRon
- GitHub – Slide Deck PDF

Cybersecurity Awareness & Fundamentals

Content:

- Stay Safe Online – Cybersecurity Awareness Month
- Saltzer & Schroeder Design Principles (1975)
- NIST Cybersecurity Framework (CSF)
- Threat Modeling Manifesto
- Shostack Threat Modeling Resources
- CISA – Secure by Design
- CISA – AI and Secure Software

AI, Agents & Agentic Systems

Content:

- NIST AI Risk Management Framework 1.0
- Forrester – Agentic AI Guardrails (AEGIS Model)
- AI Multiple – Agentic AI Overview
- AI Multiple – AI Agent Tools
- Google AI Studio
- IAPP – Key Terms for AI Governance
- The Hacker News – Secure Vibe Coding Guide

🧠 AI Learning Platforms

Content:

- MIT Open Learning – AI Courses
- DeepLearning.AI (Andrew Ng)
- Google Cloud Skills Boost – Generative AI Track
- Microsoft Learn – AI Fundamentals
- Hugging Face Learn
- Fast.ai

🧪 Adversarial AI & Threats

Content:

- NCSC & CISA – Guidelines for Secure AI Development
- Microsoft – ML Failure Modes
- MITRE ATLAS – Adversarial Threat Landscape
- Adversarial Robustness Toolbox (ART)
- Kali-GPT

🛡 OWASP AI Security Projects

Content:

- OWASP AI Main Site
- AI Security Overview
- AI Security Matrix
- Periodic Table of AI Threats
- GenAI OWASP Project

Career Development & Community

Content:

- CyberSeek Heatmap
- CyberSeek Career Pathway
- NICCS Cyber Career Pathways Tool
- Cybersecurity Guide
- Cyber Canon – Book Recommendations
- CyberSN – Red Flags in Job Postings
- CISO MindMap 2025
- TEDx Talk – Hackers Wanted