Dr. Donnie Wendt

Cybersecurity Educator | AI Security Researcher | Industry Practitioner

Cybersecurity educator, researcher, and industry practitioner specializing in secure and responsible artificial intelligence adoption, adversarial machine learning, and security automation. Author, lecturer, and recognized thought leader focused on advancing AI governance, AI risk management, and defensive innovation.

Contributed to industry initiatives including co-authoring the AI Adoption & Management Framework and leading the FS-ISAC Working Group on combating AI threats. Experience with major frameworks and regulations including NIST CSF, NIST RMF, NIST AI RMF, ISO 27001, ISO 42001, GDPR, EU AI Act, and PCI-DSS.

Certifications include Certified Information Systems Security Professional (CISSP) and AI Governance Professional (AIGP).

Areas of Expertise

- Adversarial Machine Learning and AI Security
- Secure and Responsible AI Adoption
- AI Governance and Risk Management
- Security Automation and Active Cyber Defense
- Detection Engineering and Security Operations
- AI Strategy and Organizational Transformation
- Workforce Development in Cybersecurity and AI

Academic Appointments

Cybersecurity Lecturer - Columbus State University
Teach applied cybersecurity courses within CSU's Nexus program, preparing students for careers in cyber defense and security operations. Mentor students pursuing cybersecurity certifications and industry pathways while supporting regional workforce development initiatives aligned with Georgia's growing cyber ecosystem.

Developing courses focused on Securing AI, integrating hands-on labs, adversarial AI exercises, and real-world scenarios to bridge academic learning with industry practice.

Utica University - Adjunct Professor of Cybersecurity | 2016–2025

Developed and taught graduate-level cybersecurity courses, including Security Automation and Active Cyber Defense and Securing and Defending Networks. Additional instruction included Cyber Intelligence, Critical Infrastructure Protection, and the Master's Capstone.

Courses emphasized applied security engineering, machine learning in cybersecurity, and operational defense strategies.

Industry Experience

Mastercard (Retired) - Principal Security Researcher | 2004–2024

Researched emerging cybersecurity threats and future defensive capabilities, with a focus on adversarial generative AI, extended detection and response, securing machine learning systems, deception technologies, browser isolation, and continuous controls monitoring.

Recognized as a frequent speaker and thought leader in machine learning security, generative AI risk, and security automation. Led the FS-ISAC Working Group on combating AI threats and contributed to industry guidance on generative AI vendor risk management.

Earlier Roles at Mastercard – Engineering & Program Leadership

Served in multiple technical and leadership roles including product owner, vendor manager, and security engineer responsible for designing and implementing enterprise security controls such as intrusion prevention, endpoint protection (EDR), data loss prevention, database monitoring, and file integrity monitoring.

- Technical lead for Security Orchestration, Automation, and Response (SOAR) within the Security Operations Center
- Lead engineer for enterprise data loss prevention initiatives
- Program manager for access management infrastructure modernization
- Project manager for cryptography-as-a-service API development supporting secure key management and encryption services

---

Professional Leadership & Industry Contributions

- Co-author, **AI Adoption & Management Framework (AI-AMF)**
- Lead, **FS-ISAC Working Group on Combating AI Threats**
- Contributor, **Generative AI Vendor Risk Management Guidance (FS-ISAC)**
- Developer, **Adversarial Machine Learning: Understanding and Defense**, EC-Council Learning

---

Publications

- *AI Strategy and Security: A Roadmap for Secure, Responsible, and Resilient AI Adoption.* Apress, 2025.
- Adversarial Machine Learning: Understanding and Defense. EC-Council Learning, 2025.
- *The Cybersecurity Trinity: Artificial Intelligence, Automation, and Active Cyber Defense.* Apress, 2024.
- The AI Adoption and Management Framework (co-author), 2025, aiamf.ai.
- Secure AI Integration: Supercharging Your Business, 2025, The Cyber Security Tribe.
- Combating Threats and Reducing Risks Posed by AI (co-author), 2024, FS-ISAC.
- Generative AI Vendor Risk Assessment Guide (co-author), 2024, FS-ISAC.
- Addressing Both Sides of the Cybersecurity Equation. *Journal of Cyber Security and Information Systems,* 7(5), 22-29, 2019.

Selected Media, Interviews & Recognition

- “10 Most Expert Cybersecurity Leaders,” CIO Business World, January 2025.
- “Adversaries May Be Poisoning Your Machine Learning Engine,” Interview by B. Barth, SC Magazine, September 29, 2022.
- “The Reality of Deception for Cyber Resilience,” Interview by R. Hegde, KuppingerCole, March 21, 2022.
- “Banks Cautiously Consider Expanding Automation’s Role in Incident Response,” SC Magazine, October 10, 2021.

Education

Doctor of Science in Computer Science, Information Security — Colorado Technical University
M.S. in Cybersecurity (Intelligence Concentration) — Utica College
B.A. in Business Administration — Webster University

Certifications

Certified Information Systems Security Professional (CISSP) — (ISC)²
AI Governance Professional (AIGP) — IAPP