ANDREW DANNENBERGER

AI Security Standards & Enablement Lead | Technical Product Support | MCP Security | Secure AI Adoption

Chicago Area / Remote | (206) 898-7637 | drewdannenberger@gmail.com | andrewdannenberger.com
LinkedIn: linkedin.com/in/andrew-dannenberger-0b23a7216

SUMMARY

AI security standards and enablement professional helping organizations adopt AI safely by translating LLM, agentic AI, MCP, and RAG risks into practical guidance, benchmarks, tools, and learning programs. Principal co-author of the CIS Controls v8.1 Model Context Protocol (MCP) Companion Guide and collaborator on the AI/LLM and AI Agents Companion Guides. Leads CIS AI Benchmarks Community work, MCP Benchmark development, AI Office Hours, internal advisory efforts, customer-facing MCP enablement, and AI assistant initiatives at the Center for Internet Security. Combines standards expertise, hands-on AI implementation, CLI-heavy technical product support, customer engagement, and prior international defense-training leadership.

AI SECURITY, STANDARDS & ENABLEMENT SNAPSHOT

- AI security portfolio combines standards development, public guidance, community leadership, internal enablement, customer-facing platform concepts, and hands-on AI assistant work.
- Principal co-author of the CIS Controls v8.1 MCP Companion Guide and collaborator on the AI/LLM and AI Agents Companion Guides; focuses on making emerging AI risks understandable and actionable for practitioners.
- Lead CIS AI Benchmarks Community efforts, including external member recruitment, cross-organization participation, scope framing, feedback cycles, and practical guidance development.
- Lead scheduled CIS MCP Benchmark development, connecting MCP clients, servers, tools, resources, prompts, authorization, least privilege, auditability, and confused-deputy concerns to benchmark-style guidance.
- Run secure AI enablement efforts including AI Office Hours, leadership briefings, and practical learning sessions that help technical and non-technical teams adopt AI responsibly.
- Bridge standards and implementation through CLI-heavy technical product support, MCP server concepts for SecureSuite Platform, chatbot/knowledge-base initiatives, support escalations, and customer engagement across diverse technologies.

CORE COMPETENCIES

Secure AI Enablement: AI Office Hours, enterprise AI adoption, prompt/workflow design, customer education, practical use-case development, responsible AI usage, secure adoption programs

AI Security & Standards: LLM security, agentic AI risk, MCP security, prompt injection, RAG/knowledge grounding, tool governance, least privilege, human approval, AI risk management

Frameworks & Guidance: CIS Controls, CIS Benchmarks, CIS WorkBench/community processes, NIST AI RMF concepts, OWASP LLM Top 10 concepts, MITRE ATT&CK, MITRE ATLAS, audit/remediation guidance

Implementation & Technical Product Support: Bash/CLI, Linux, Python, PowerShell, SQL, AWS, Azure, APIs, logs, configuration files, test environments, chatbot architecture, knowledge-base automation, technical troubleshooting, escalation

PROFESSIONAL EXPERIENCE

Center for Internet Security (CIS) - CIS AI Benchmarks Lead / Technical Product Support Specialist, Security Best Practices | Remote | Oct 2021-Present

Functional scope: AI security standards, secure AI enablement, benchmark leadership, technical product support, customer engagement, and practical AI adoption

- Lead secure AI enablement and standards work related to CIS Controls, CIS Benchmarks, AI/LLM systems, AI agents, and MCP.
- Principal co-author of the CIS Controls v8.1 Model Context Protocol (MCP) Companion Guide and collaborator on the AI/LLM and AI Agents Companion Guides.
- Lead CIS AI Benchmarks Community work to advance practical guidance for emerging AI technologies, including external member recruitment, community coordination, scope definition, feedback cycles, and publication strategy.
- Lead development of a scheduled CIS MCP Benchmark, translating protocol and implementation risks into actionable benchmark-style recommendations, audit concepts, and control-aligned guidance.
- Lead AI Office Hours and employee enablement sessions for beginner and advanced groups, turning complex AI security topics into practical workflows, exercises, and adoption guidance.
- Develop MCP server concepts for SecureSuite Platform and engage with customers and technical stakeholders on integration, governance, supportability, and secure adoption considerations.
- Serve as an internal AI advisor to leadership and cross-functional teams on emerging AI risks, adoption patterns, use cases, and practical implementation tradeoffs.
- Developed a documentation-focused AI chatbot and led its transition from proof of concept toward minimum viable product, gaining product management, project management, and secure deployment experience.
- Created an internal customized chatbot for CIS Knowledge Base articles and maintained AI research resources tracking emerging AI advances, risks, and organizational implications.

- Provide technical product support across diverse CIS SecureSuite products, frequently using Bash/CLI workflows, logs, test environments, product documentation, and cross-team troubleshooting; created 30+ Knowledge Base articles and Quick Start Guides.

Center for Internet Security (CIS) - Benchmarks Development Intern | Remote | Jul 2021-Oct 2021

- Mapped Windows 10 CIS Benchmark recommendations to MITRE ATT&CK techniques and sub-techniques in collaboration with Benchmark Development engineers.
- Researched and documented recommendation justifications for Windows 10, Windows Server 2016, and Microsoft Edge Benchmark content.
- Built practical knowledge of secure configuration concepts across Windows, Linux, macOS, AIX, and other technologies.

EARLIER LEADERSHIP, TRAINING & INTERNATIONAL EXPERIENCE

Raytheon Intelligence and Information Services - Site Lead / Principal and Senior Training & Development Specialist, Kabul, Afghanistan

- Developed and led English Language Training programs at the Afghan Presidential Palace and NATO Resolute Support HQ in coordination with the Afghan National Security Council and U.S. Department of Defense stakeholders.
- Launched a new training program at the Afghan Air Force Academy and managed up to 27 instructors in a high-ambiguity, high-pressure operational environment.
- Designed customized instruction for senior military and government stakeholders, including high-ranking Afghan generals and the Deputy National Security Advisor of Afghanistan.
- Held a U.S. Secret security clearance (inactive).

International and Domestic Education Roles - ESL, Business English, Military English, Test-Prep, Cultural Orientation, and Job Readiness Instructor

- Delivered training and curriculum programs across the United States, Afghanistan, Taiwan, Hungary, and refugee resettlement contexts, including NATO-related military audiences and classes of 30-50 students.
- Translated complex material for diverse adult learners, building the communication foundation now used in AI enablement, customer engagement, and security guidance work.

U.S. Agency for International Development, Indochina Department - Intern

- Supported Indonesian development program work, including preparation for congressional committee hearings.

EDUCATION & CERTIFICATIONS

- Highline College - BAS, Cybersecurity & Forensics, 4.0 GPA; AAS, Network Security Engineer, 4.0 GPA; Cyber Competition Club
- Virginia Military Institute - BA, International Studies & Political Science; minors in History and German; exchange student, Universität der Bundeswehr München
- Certifications / Training: GIAC GCIA; GIAC GCLD; AWS Certified AI Practitioner; Cisco CCNA; CompTIA Security+; Harvard Kennedy School Executive Education, Leading in Artificial Intelligence