

JOHN M. WALLER, CISSP

AI SECURITY & GOVERNANCE | CYBERSECURITY CONSULTING LEADER

Mystic, CT | 860.861.0283 | john@johnmwaller.com | linkedin.com/in/johnmwaller | site: johnmwaller.com

PROFESSIONAL SUMMARY

AI security and governance consulting leader with 25+ years across software engineering, cloud architecture, cybersecurity, and technology delivery. CISSP with an M.S. in Artificial Intelligence who developed UltraViolet Cyber's AI Governance practice. Experience spans AI threat modeling, adversarial testing, NIST AI RMF maturity assessments, AI-SPM, and enterprise governance engagements. Proven leader skilled in developing teams, managing complex engagements, and earning the trust of executive and technical stakeholders. Author of *The Unconstrained Machine* (pending publication), examining how technical and governance constraints can preserve human control over AI, as well as articles in multiple industry publications.

CORE EXPERTISE

AI Threat Modeling & Adversarial Testing | NIST AI RMF Maturity Assessments | AI-SPM
AI Governance Practice Development | Client Engagement Leadership | Executive Advisory
Cloud Security & Architecture | NIST CSF & NIST 800-53 | OWASP Top 10 for LLMs
Secure SDLC / DevSecOps | Consultant Development | Proposal & Methodology Development

PROFESSIONAL EXPERIENCE

ULTRAVIOLET CYBER | BLACK DUCK | SYNOPSYS

Risk Advisory Practice Lead | May 2022–Present

Continuous employment through corporate transitions | McLean, VA / Remote

- Developed UltraViolet Cyber's AI Governance practice, creating service offerings, reusable assessment methodologies, technical content, and client deliverables to support business development and consistent engagement delivery.
- Lead NIST AI RMF maturity assessments and AI governance engagements, evaluating accountability, risk management, lifecycle controls, and oversight; translate findings into roadmaps and executive recommendations.
- Direct a five-consultant team delivering NIST 800-53 Security Control Assessments and continuous monitoring for a federal financial agency; coordinate evidence, validate control effectiveness, oversee quality, and guide remediation.
- Perform threat modeling and adversarial testing of AI systems to identify security risks and inform control recommendations; bring AI Security Posture Management (AI-SPM) experience through Cyera to AI security advisory work.
- Lead AWS, Azure, and GCP cloud and application security reviews spanning IAM, infrastructure as code, API security, and vulnerability management; advise enterprise and federal stakeholders on architecture and remediation priorities.
- Conduct NIST CSF and other cybersecurity assessments that frequently generate follow-on business; manage scope, proposals, statements of work, delivery quality, executive reporting, and consultant development.
- Author thought leadership articles for industry publications and speak at conferences, translating complex security and governance issues into practical guidance for executives, technical teams, and broader audiences.

DOCXELLENT, INC. | Norwich, CT

Director of Information Security & Cloud Services | March 2014–May 2022

Led cybersecurity, cloud operations, and software engineering for a SaaS document control and quality management provider.

- Established and led the enterprise security program protecting corporate, product, and cloud environments, including security architecture, policies, risk management, vulnerability management, and incident readiness.
- Advanced NIST CSF, ISO 27001, and GDPR readiness efforts, translating security and privacy requirements into practical controls and operating processes.
- Architected, deployed, monitored, and maintained AWS and Azure environments supporting customer and internal workloads; managed the team responsible for DocXellent's cloud services.
- Integrated security into the software development lifecycle and Azure DevOps CI/CD processes, combining hands-on engineering with technical leadership and project management.
- Designed, developed, tested, and delivered security-focused product enhancements, connecting customer requirements with application design and cloud infrastructure.

PREVIOUS EXPERIENCE

edX / UNIVERSITY CYBERSECURITY BOOTCAMPS **Cybersecurity Instructor | July 2021–January 2025**

Part-time, concurrent with primary employment

- Taught the University of Connecticut School of Engineering’s Cybersecurity Bootcamp, delivering hands-on instruction in offensive and defensive security, networking, systems, web technologies, and databases.
- Previously taught the program for Case Western Reserve University and substituted for Columbia, Penn, and Vanderbilt.

IMARK GROUP | Bowie, MD **Senior Software Developer | June 2011–March 2014**

Owned full-SDLC delivery of ASP.NET applications supporting sales, invoicing, communications, document generation, and credit analysis. Introduced .NET, object-oriented practices, test and staging environments, and mobile capabilities.

PFIZER | Contract through Sunrise Systems | Groton, CT **Application Developer / Support Team Lead | January 2010–June 2014**

Developed SharePoint solutions for compliance and critical business functions in a regulated pharmaceutical environment. Transitioned from full-time development to concurrent part-time leadership of offshore support and development teams in June 2011.

CCS ONLINE | LEGRAND | DOLAN MEDIA | SCHNEIDER ELECTRIC **Progressive Software Development Roles | June 2000–June 2011**

Built enterprise web applications, databases, and integrations through increasingly responsible software development and client delivery positions.

EDUCATION

M.S., Artificial Intelligence & Machine Learning | Colorado State University Global, 2025
4.0 GPA; deep learning, NLP, LLMs, generative AI, computer vision, and neural networks.

M.S., Information Technology | University of Massachusetts Lowell, 2018
Focus: cloud computing, cybersecurity, and DevOps.

B.S., Individualized Studies | Charter Oak State College, 2010
Focus: technology and management | Honors in General Scholarship

A.S., Computer Science | Three Rivers Community College, 2003 | Magna cum laude

CERTIFICATIONS & PROFESSIONAL CREDENTIALS

Certified Information Systems Security Professional (CISSP), ISC2
Cyera: AI Security Practitioner | AI Governance Practitioner | Agentic Security Practitioner
Certificate of Cloud Security Knowledge (CCSK), Cloud Security Alliance
Microsoft Security, Compliance & Identity Fundamentals
Previous: AWS Certified Security – Specialty | AWS Solutions Architect – Associate | HashiCorp Terraform Associate

TECHNOLOGY & FRAMEWORKS

AI Security & Governance: AI threat modeling, adversarial testing, NIST AI RMF maturity assessments, lifecycle controls, model security evaluations; ISO/IEC 42001, OWASP Top 10 for LLMs, EU AI Act, MITRE ATLAS; Cyera AI-SPM.

Security & Federal Frameworks: NIST 800-53, FedRAMP, NIST CSF, ISO 27001, HIPAA, PCI-DSS, GDPR, CIS Controls; security control assessments, continuous monitoring, threat modeling, vulnerability management.

Cloud & Identity: AWS, AWS GovCloud, Azure, GCP, Terraform, Checkov, Okta, SSO, OAuth, SAML; cloud infrastructure, IAM, networking, and monitoring.

Security Tooling: Cyera AI-SPM, Qualys, Splunk, Sumo Logic, Scout Suite, Burp, Kali Linux, OWASP ZAP, Wireshark, SonicWall.

Engineering & Delivery: Python, C#/.NET, JavaScript, databases, APIs and web services, GitHub, Azure DevOps, SAST/DAST/SCA; Agile, Scrum, Jira, Microsoft Project, Asana.

THOUGHT LEADERSHIP

Author, *The Unconstrained Machine* (pending publication). Articles in leading industry publications and company blogs. Speaker at TechEx North America; OWASP Conference, Boston; ISACA Raleigh; AI Community Conference, Boston (Nov. 2026).