Hayden Williams

Software Engineer in Cyber Security and AI

hayden@haydenwilliams.dev haydenwilliams.dev

linkedin.com/in/hayden-williams-uk github.com/hayden-uk

PROFILE

Software engineer and consultant with a strong foundation in artificial intelligence, cyber security, and systems programming. Experienced in building secure architectures and scalable data pipelines using languages like Python, C/C++, and Java. Combines technical problem-solving with strategic leadership to deliver reliable and effective technology solutions.

EXPERIENCE

September 2025 – Present

Associate in AI, *Oxford Capital*

- Engineering AI agents and Azure data pipelines to improve competitiveness and improve productivity
- Lead secure Generative AI and automation strategy within a regulated venture capital environment.

June 2025 – September 2025

Consultant in AI (Summer Internship), *Oxford Capital*

- Consulted on and explored effective generative-AI deployment in venture capital.

October 2024 – April 2025

Peer Assisted Learning (PAL) Leader, *Oxford Brookes University*

- Led weekly Python and Java support sessions for first-year students; handpicked by the Department as a top-performing second-year.

June 2024 – March 2025

IT & Data Protection Officer, *TEDxOxford*

- Managed all IT infrastructure (ticketing, mail, web) for the 2025 conference at the Sheldonian Theatre, University of Oxford; audited and strengthened GDPR compliance.

July 2024 – August 2024

Technology Tutor, *FunTech*

- Taught Python to UK and international students aged 9–15 in groups of 1–6, adapting methods to diverse learners and earning top student feedback.

EDUCATION

2023 – 2026

BSc (Hons) Computer Science for Cyber Security, *Oxford Brookes University*

- Dissertation - Project Earworm: an agent-based audio prompt-injection evaluation framework for assessing Large Audio Language Models (LALMs).

2021 – 2023

A Levels — Computer Science, Geography, Business Studies, *Esher Sixth Form College*

2016 – 2021

GCSEs — 8 including English & Mathematics, *The Hollyfield School*

TECHNICAL SKILLS

Languages
Python, Java, C, C++, C# (.NET MAUI), JavaScript, Assembly, SQL, HTML/CSS

Frameworks & Tools
FastAPI, LangChain/LangGraph, .NET MAUI, Docker, PostgreSQL, REST APIs, Git/GitHub, Claude Code, Microsoft Azure Cloud, Google Cloud

Specialisms
LLM Security, Prompt Injection, AI Agents, Generative AI, UNIX/MINIX Systems Programming, CISCO Networking (CCNA)

QUALIFICATIONS AND AWARDS

April 1st, 2026 — **Shortlisted, TechShow 2026 Project Exhibitor,** *School of Engineering, Computer Science & Mathematics, Oxford Brookes University*

December 1st, 2023 — **CCNA: Introduction to Networks,** *Cisco*

December 1st, 2018 — **Sir Jack Petchey Award (Robotics)**

NICAS Rock Climbing Certifications Levels 1-4, *NICAS*

CyberFirst Advanced, Futures, Defenders Awards, *National Cyber Security Centre (UK)*

HIGHLIGHTED PROJECTS

Project Earworm, *Python, FastAPI, LangChain, Docker, PostgreSQL (Final-year dissertation)*
- An agent-based audio prompt-injection evaluation framework for assessing the security of Large Audio Language Models (LALMs), built on a custom ReAct agent architecture.
- Systematically evaluates how adversarial audio can manipulate voice-enabled LLM agents into unauthorised actions.

SecureBlockShare, *C, UNIX/MINIX, POSIX IPC*
- A daemon-based data sharing and storage system for UNIX, built around local inter-process communication.
- Designed with a security focus throughout, covering privilege handling and controlled access to shared data.

Blog System CGI, *C++, CGI, Apache, MariaDB*
- A secure, multi-user blog platform built as CGI executables in C++ for a Secure Programming module, following OWASP guidance.
- Implements email-based two-factor authentication, bcrypt password hashing, expiring session tokens, and defences against SQL injection (prepared statements) and cross-site scripting (output escaping).

Badgering About Assembly, *x86-64 Assembly (NASM), Linux*
- A command-line CRUD inventory-management system written entirely in hand-written x86-64 assembly (1,150+ lines) for a Malware Analysis module.
- Demonstrates manual memory management, System V AMD64 ABI compliance, and low-level data-structure and algorithm design.

Eligere (EligereAI & EligereManage), *C# (.NET MAUI), LLMs, PostgreSQL, REST API*
- A multi-platform suite for music-library management: EligereAI converts natural-language questions into PostgreSQL searches using LLMs, while EligereManage provides graphical library management.
- Engineered with a security focus, applying prompt-engineering safeguards against injection.

LEADERSHIP AND ACTIVITIES

December 2025 – Present — **The Oxford Union Society,** *Director of Strategy*
- Renegotiated the Shigeru Kawai piano partnership, successfully securing continued sponsorship valued in the thousands of pounds
- Working with alumni and internal stakeholders on long-term fundraising strategy
- Directed the flagship 'Artificial General Intelligence' debate, securing high-profile speakers including Prof. Michael Wooldridge and Dr Roman Yampolskiy
- Trusted technical adviser to senior staff and the President

May 2025 – Present — **Lincoln College Chapel Choir, University of Oxford,** *Tenor*
- Sing weekly collegiate services from a wide variety of English Choral Music repertoire

June 2024 – April 2025 — **The Debating Society, Oxford Brookes University,** *President*
- Led my four-person committee to deliver two successful termcards of debates and social events