

W. Mouton

Independent Security Researcher & AI Architect

github.com/wmouton | gitlab.com/wmouton | www.linkedin.com/in/wmouton

Summary

Independent security researcher and AI architect specialising in reproducible, isolated and security-boundary systems, plus web and AI security. Founder of Souverain Labs and Chief AI Architect at Plank Designs. Background in networking, offensive security, software engineering and AI architecture, with hands-on experience in identity and access management and security operations. Every finding is documented with a threat model, a disclosure timeline and a mitigation.

Experience

Souverain Labs

Founder & Security Researcher

Dec 2025 – Present

- Architecting the next generation of Bio-Synthetic Nervous Systems to advance human longevity through the deep convergence of Artificial Intelligence and biological frameworks.

Plank Designs

Northern Cape, SA

Co-Founder, Chief AI Architect & IAM Analyst

Dec 2024 – Present

- Co-founded the agency and led its AI architecture, engineering strategy, and intelligent automation initiatives.

Origin Wellness

Freelance Senior Software Engineer

Aug 2023 – Sep 2024

- Co-developed and engineered key areas of the company website, including primary navigation, information architecture, responsive layouts, and interactive UI systems.

Random Access Media Productions

CTO

Jan 2023 – Aug 2023

- Led the company's technical architecture and AI strategy, architecting scalable systems that quadrupled revenue and transformed core business operations.

Random Access Media Productions

Software Engineer III

Nov 2022 – Jan 2023

- Architected and deployed a robust internal CRM using Python and Django, featuring seamless integrations with Google Workspace APIs and a high-performance PostgreSQL backend.

Random Access Media Productions

Software Engineer II

Jan 2020 – Oct 2020

- Engineered high-performance full-stack applications using Next.js and TailwindCSS, bridging the gap between responsive front-end interfaces and robust SQL-backend data architectures.

Varidian

Freelance Software Engineer

Apr 2019 – Jan 2020

- Built modern, responsive websites and web applications using React.js, Next.js, TypeScript, JavaScript, HTML, and CSS.

NightOwlSystems

Private Offensive Security Consultant

Feb 2014 – Jan 2017

- Conducted authorized offensive security assessments across Windows, Linux, wireless networks, and identity infrastructure, identifying vulnerabilities, misconfigurations, privilege-escalation paths, and attack vectors.

Nodeworks

IT & Network Freelancer

Feb 2012 – Jan 2014

- Providing independent IT and networking support for individuals and small businesses, with a focus on reliable infrastructure, troubleshooting, security, and system administration.

Projects

SOC Incident Response

DFIR · Detection · Reproducible

Evidence-driven investigation of a synthetic intrusion: environment and attack design, generated telemetry, a verifiable evidence chain, detection engineering and a validated response.

Reprobe

Nix · Go · Reproducible builds

Reproducible-build verifier that rebuilds an artifact from pinned source in independent, hermetic environments and reports where the outputs diverge.

KeyTUI

Rust · TUI · SQLite

Terminal token vault for rapid credential access, with Vim-style navigation and a persistent SQLite backend.

BioFly

Python · Evo2 · Next.js

Genomic analysis tool using Evo2 to predict disease likelihood from DNA mutations.

Skills

Security: Web & API security | AI security | Threat modelling | Detection engineering | Sigma | Splunk SPL | Microsoft Sentinel KQL | MITRE ATT&CK | Incident response | SOC triage | Identity & access management | Coordinated disclosure

Engineering: Rust | Go | Python | Zig | Nix | Lua | Next.js | SQL | React | Wayland (Smithay)

AI & Data: Machine Learning | Deep Learning | LLMs & RAG | LLM evaluation & red-teaming | Vector search / embeddings | PyTorch | TensorFlow | Hugging Face | ONNX Runtime | MLflow | Scikit-Learn | Pandas | NumPy | Polars

Systems & Cloud: NixOS (reproducible, declarative) | Void Linux | FreeBSD | KVM/QEMU | nftables | LUKS2 | Docker | Git | AWS | GCP | Azure

Education

MIT

Online

Computer Systems Security (OpenCourseWare)

2026 – Present

- Coursework: OS security, capabilities, information flow control, language security, network protocols, hardware security and web application security

Harvard University

Online

CS50: Cybersecurity

2023 – 2025

- Coursework: Securing Accounts and Data, Threats and Defences, Cryptography, and Security Ethics

Harvard University

Online

CS50: Artificial Intelligence with Python

2021 – 2023

- Coursework: Search, Knowledge, Uncertainty, Optimization, Learning, Neural Networks, Language

Harvard University

Online

CS50: Computer Science

2018 – 2020

- Coursework: Algorithms, Data Structures, Abstraction, Memory, and Web Development

Bugcrowd University

Online

Ethical Hacking & Cybersecurity

2018 – 2019

- Coursework: Web Application Security, Vulnerability Discovery, and Responsible Disclosure

Certifications

Codecademy: Google Associate Cloud Engineer: Identity & Access Management (IAM)

freeCodeCamp: Scientific Computing with Python | Data Analysis with Python | Machine Learning with Python

HackerRank: Go (Basic) | React (Basic) | Python (Basic)

Pluralsight: HTML, CSS, and JavaScript

Selected case studies

OAuth consent phishing to cloud data access

IAM Analyst at a web design company

SOC Analyst at a web design agency

Incident: leaked CI token and tampered build artifact