Laurence Avent

Security Engineer | Founder, Arbiter Security

arbitersec.com
+44 7590 551165
Exeter, UK
laurence.avent@gmail.com
github.com/postrv
/in/laurence-avent

SUMMARY

Security engineer with 5+ years of operational experience across SIEM, incident response, detection engineering, and application security—embedded in product teams where I triaged real alerts, tuned real detection rules, and led response to real incidents including Log4Shell. Frustrated by the gap between what security teams need and what existing tools deliver, I founded Arbiter Security and built two AI-native security products from scratch in Rust, exposed as MCP servers for AI agent orchestration. One finding has been responsibly disclosed to Anthropic; another to Cloudflare. I ship code, I understand attacker behaviour, and I know what matters when a SOC is under pressure.

SKILLS

Languages	TypeScript, Node.js, Rust, Python, Elixir, Go, SQL, Shell scripting
Security	Detection Engineering, Incident Response, Threat Modeling, Pen Testing, Vulnerability Research, SAST/DAST
Platforms	Rapid7 InsightIDR, CrowdStrike, Drata, AWS Security Hub/GuardDuty, GCP SCC, DataDog
AI & Infra	MCP Protocol, Agent Orchestration, LLM Security, AWS, Terraform, CI/CD

PROFESSIONAL EXPERIENCE

Apr 2024 – Present

Information Security Engineer — Remote, UK

Edmentum

- Own SIEM operations (Rapid7 InsightIDR): build and tune custom detection rules, triage security alerts, and manage incident response workflows across the organisation
- Led response to active Storm-1811/Black Basta-style vishing campaign—identified attack pattern, coordinated cross-team containment, and implemented preventive controls
- Built internal MCP registry and led security evaluation for GitHub Copilot Enterprise rollout: threat modeling, access controls, policy development, and governance framework
- Embed with product teams to conduct security design reviews and implement secure coding practices
- Configure and manage AWS security services: GuardDuty, Security Hub, Lambda-based automated remediation
- Drive SOC 2 compliance programme through Drata; coordinate third-party penetration testing engagements

`SIEM` `Detection Engineering` `Incident Response` `AI/LLM Security` `AWS` `SOC 2`

Nov 2022 – Nov 2023

Security and Compliance Engineer — Remote, UK

Encord (YC 2021)

- Configured GCP Security Command Center and Cloud Armor WAF rules for OWASP Top 10 protection
- Collaborated with product teams to improve security of multi-cloud storage integrations (Azure, GCP, AWS)
- Managed inbound vulnerability disclosures; triaged reports from external security researchers
- Implemented secure SDLC practices: security requirements, design reviews, automated testing

`GCP Security` `Threat Modeling` `Penetration Testing` `Secure SDLC`

Feb 2021 – Nov 2022

Security Engineer (Support Engineering entry point) — London, UK

Kobalt Music

- Founded the Security Incident Response Team from scratch—identified the organisational gap, built the business case, recruited responders, and delivered an operational SIRT
- Led emergency incident response to Log4Shell (CVE-2021-44228), coordinating cross-team remediation under time pressure across production services
- Discovered and remediated a WAF bypass vulnerability through independent security testing
- Implemented OpsGenie alerting and DataDog monitoring; drove preventive improvements from root cause analysis

`Incident Response` `SIRT` `Vulnerability Discovery` `Security Monitoring`

Jul 2019 – Jan 2021

Support Engineer — Enterprise InfoSec GRC — Ljubljana, Slovenia

Reciprocity (now ZenGRC)

- Technical support for 250+ enterprise customers on GRC platform (comparable to Drata/Vanta)
- Influenced product roadmap through structured customer feedback on security workflow UX
- Debugged complex integration issues across REST APIs, SSO/SAML, and role-based access control

`Enterprise Security` `Product Feedback Loops` `SSO/SAML` `REST APIs`

ARBITER SECURITY — FOUNDER (EVENINGS & WEEKENDS)

Arbiter

AI-Native Offensive Security Platform

arbitersec.com/arbiter

MCP-driven vulnerability scanner built in Rust. Models web applications as state graphs and uses constraint inference to discover and verify vulnerabilities across 52 classes—from XSS and IDOR to HTTP smuggling, cache poisoning, and race conditions. Every finding is verified in a real browser with full evidence chains. **100% detection on Google's Firing Range** benchmark (85/85 endpoints). Real-world vulnerability finds responsibly disclosed to Anthropic and Cloudflare. 267 MCP tools, 468K lines of Rust, 7,800+ tests.

Aletheia

Binary Analysis with Concolic Falsification

arbitersec.com/aletheia

Reverse engineering platform that disassembles PE/ELF/Mach-O binaries across four architectures, lifts to a 43-opcode IR, constructs SSA form, and decompiles to typed C. Novel concolic falsification architecture: runs binaries concretely through an emulator while maintaining a sparse symbolic shadow over tainted variables, then uses SMT solving to construct concrete exploit witnesses—eliminating false positives architecturally. Hybrid fuzzing, taint analysis, and vulnerability scanning across 14 CWE classes with CVSS scoring, MITRE ATT&CK mapping, and SARIF output. 140 MCP tools, 2,800+ tests.

OPEN SOURCE & CIVIC TECHNOLOGY

- **Tightrope Tracker** — Live civic dashboard tracking UK fiscal constraint across four pillars (market stability, fiscal headroom, labour resilience, growth delivery) with a composite score derived from OBR, ONS, BoE, and DMO data. Features interactive what-if simulator, embeddable widgets, public JSON API, and automated OG image generation. Featured on ITV's *Peston* alongside Robert Peston and Jeremy Hunt. Built for Looking For Growth UK tightropetracker.uk
- **Forgemax** — Open-source V8 sandbox for secure LLM-to-MCP tool execution; up to 99% token reduction, scaling to ∼5000 tool connections without context pollution GitHub
- **Narsil MCP** — 90-tool Rust code intelligence server. Published on crates.io, Homebrew, npm. Taint analysis, SBOM generation, 32-language support GitHub
- **Krait** — Self-evolving AI agent (Elixir/OTP + Rust) with AST-based security validation and cryptographic mutation auditingkraitbot.com
- **FixingBritain.com** — Open-source platform analysing UK structural policy challenges; part of the civic tech ecosystem alongside Tightrope Tracker fixingbritain.com

VULNERABILITY RESEARCH & RESPONSIBLE DISCLOSURE

- **Anthropic** (2026) — Discovered vulnerability in Anthropic's open-source MCP tooling. Responsibly disclosed and acknowledged by their security team
- **Cloudflare Pingora** (2026) — Identified security issue in Cloudflare's open-source HTTP proxy framework, used across their global infrastructure. Reported via their responsible disclosure programme
- **SecureDrop** — Security finding in the open-source whistleblower submission system used by major news organisations worldwide

EDUCATION & EARLY CAREER

2007 – 2011

2:1 BSc (Hons), Marine Studies (Merchant Shipping)

University of Plymouth

Critical systems analysis, high-stakes decision-making under uncertainty, GPS/positioning systems, maritime communications. The operational discipline and systems thinking from safety-critical environments directly informs my approach to security engineering.

2011 – 2019

Early Career

Customer-facing and analytical roles across paralegal work (compliance awareness, regulatory detail), data analysis and business intelligence (SQL, reporting, stakeholder communication), and enterprise customer operations. Built the communication skills, commercial awareness, and understanding of enterprise workflows that inform both security work and product thinking.

COMMUNITY & LEADERSHIP

- **South West Chapter Lead** — Looking For Growth UK, a cross-party grassroots movement for UK economic growth
- **Open Source** — Maintainer of multiple published packages across crates.io, npm, and Homebrew

INTERESTS

Surfing the Cornish coast · Trail running on Dartmoor · Filipino Martial Arts · Open-source development · CrossFit