LAURENCE AVENT

Security Engineer

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

SUMMARY

Security engineer who thrives embedded within product teams, helping design and build secure systems from the ground up. Proven track record in vulnerability discovery, threat modeling, and building pragmatic security tooling that strengthens defences without slowing delivery. Led incident response to critical vulnerabilities including Log4Shell, subsequently improving response processes with dedicated tooling. Active open-source contributor building security automation in Rust and TypeScript. Passionate about championing secure coding practices and raising security awareness across engineering organisations.

SKILLS

Languages:	TypeScript, Python, Rust, Go, SQL, Postgres, Node.js, Shell scripting
Security:	Threat Modeling, Code Review, Penetration Testing, SAST/DAST, Taint Analysis
Cloud & DevOps:	GCP (Security Command Center), AWS, Azure, Terraform, CI/CD Security
Tools:	BurpSuite, SonarQube, TruffleHog, Rapid7, OpsGenie, GitHub Advanced Security

SECURITY PROJECTS

Open Source

Narsil MCP: Code Intelligence & Security Analysis Server

GitHub

Built comprehensive Rust MCP server providing 76 tools for deep code intelligence and security analysis. Features include taint analysis for injection vulnerabilities (SQL, XSS, command injection), OWASP Top 10 and CWE Top 25 scanning, SBOM generation, dependency vulnerability checking via OSV database, and license compliance analysis. Supports 16 languages with tree-sitter parsing. Published on crates.io, homebrew, npm, and more.

Vulnerability Research

Arbiter: Custom AI-Driven Vulnerability Research Tool

Proprietary

Built out a web security automation tool in Rust, which uses a state graph to constrain searches to valid hypothesis space, achieving a perfect score on Google's Firing Range and showing promising returns in early testing on HackerOne Vulnerability Disclosure programs. Includes MCP server for automated testing and CLI tools for programmatic analysis of captured HAR files. Also supports behaviour-based tools such as Blind RCE analysis.

Security Automation

Automated Security Investigation Tool

Sandworm Security

Built and deployed a comprehensive set of web tools for analysing malicious and suspicious indicators. Runs on Cloudflare Workers and includes a Claude-powered Fly.io sandbox, where suspicious domains can be visited, analysed, screenshotted, and classified automatically.

Open Source

Additional Projects & Contributions

GitHub

TruffleHog MCP Server (Go fork adding MCP interface for secret scanning), HyperMNIST (hyperbolic neural network MNIST solver deployed via ONNX/WASM in browser), Liquid Neural Networks implementation in Rust, and civic tech projects including FixingBritain.com

EXPERIENCE

Apr/2024 – Present

Information Security Engineer — Remote, UK

Edmentum

- Provided security support for GitHub Copilot Enterprise rollout including threat modeling, access control configuration, and security policy development
- Built internal MCP registry hosted on CloudFront enabling controlled use of approved Model Context Protocol servers, reducing attack surface while enabling AI-assisted development
- Conduct security design reviews and embed with product teams to implement secure coding practices
- Build and maintain enterprise security monitoring with Rapid7 InsightIDR, creating custom detection rules for various indicators
- Coordinate penetration testing engagements and manage vulnerability remediation lifecycle
- Secure CI/CD pipelines in Azure DevOps with SAST/DAST integration and dependency scanning
- Configure AWS security services including GuardDuty, Security Hub, and Lambda-based automated remediation

`Application Security / AI/LLM Security / CI/CD Security / Threat Modeling / AWS`

Nov/2022 – Oct/2023

Security and Compliance Engineer — Remote, UK — Encord (YC 2021)

- Led application security initiatives including threat modeling for web applications and REST APIs
- Performed security assessments and testing on production applications
- Configured GCP Security Command Center and Cloud Armor WAF rules for OWASP Top 10 protection
- Implemented secure SDLC practices including security requirements, design reviews, and testing
- Collaborated with product teams to improve security of cloud storage integrations (Azure, GCP, AWS) including granular permission models
- Managed inbound vulnerability disclosures, triaging reports from security researchers

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

Feb/2021 – Nov/2022

Support Engineer - Security Focus — London, UK — Kobalt Music

- Founded Security Incident Response Team and led critical security improvements
- Led emergency incident response to Log4Shell vulnerability, coordinating cross-team remediation under pressure
- Implemented OpsGenie for improved incident response workflows following Log4Shell lessons learned
- Discovered and remediated WAF bypass vulnerability through security testing and code analysis
- Implemented security monitoring with DataDog, creating dashboards for anomaly detection
- Conducted root cause analysis on security incidents and drove preventive measures

`Incident Response` / `Vulnerability Discovery` / `OpsGenie` / `Security Monitoring`

Jul/2019 – Jan/2021

Support Engineer - Enterprise InfoSec GRC — Ljubljana, Slovenia — Reciprocity (now ZenGRC)

- Provided technical support to 250+ enterprise customers on information security GRC tool, ZenGRC (similar to Drata and Vanta)
- Collaborated with Product and Design teams on feature and security enhancements
- Influenced product improvements through customer feedback including import/export, password security, and access controls
- Debugged complex product issues and doggedly chased down fixes
- Created best practices documentation for Support team members and trained colleagues

`REST API Security` / `SSO/SAML` / `Product Security` / `Enterprise Security`

2011 – 2019

Early Career — Various Roles

Developed foundational skills across customer-facing and analytical roles: customer service and call handling, paralegal work requiring attention to detail and compliance awareness, data analysis and data management, and business intelligence reporting. These roles built strong communication skills, analytical thinking, and an understanding of enterprise operations that inform my security work today.

TECHNICAL ACHIEVEMENTS

- **Security Tooling** - Built narsil-mcp (Rust) with taint analysis, SBOM generation, and vulnerability scanning for 16 languages
- **Incident Response** - Led Log4Shell response, established SIRT, implemented OpsGenie workflows
- **Supply Chain Security** - Implemented dependency scanning, SBOM generation, and license compliance in CI/CD
- **Code Security** - Conducted hundreds of security code reviews across TypeScript, Python, and React applications
- **API Security** - Secured REST APIs with OAuth2, rate limiting, input validation, and API gateway configurations

EDUCATION

2007 – 2011

2:1 BSc (Hons), Marine Studies (Merchant Shipping) — University of Plymouth

Broad spectrum studies encompassing global positioning systems, problem-solving in the marine environment, maritime communications systems, and critical systems analysis