

Katie Hemus

AI INFRASTRUCTURE & CLUSTER SECURITY

katie@sushiroll.io | linkedin.com/in/katiehemus | github.com/katie-hemus | sushiroll.io | Manchester, UK

12 years building and hardening production infrastructure. Philosophy background, self-taught engineer. Built an AI platform at a leading security vendor; now operating national-scale Kubernetes for the public sector. Comfortable from eBPF to IAM, from Helm charts to threat models.

WORK EXPERIENCE

Civica

2025 - Present

Senior Platform Engineer

- Part of a new platform team formed during a major post-acquisition digital transformation. Building a shared platform to replace fragmented legacy infrastructure across government digital services. Many products can't rewrite on short timelines, so the work is as much about meeting them where they are as building the new thing. Champion AI adoption across the company: included in experimental access projects, founded channels for sharing AI tooling discoveries, mentored colleagues exploring LLMs for their work
- Consistently assigned the hardest enablement tasks: pensions, housing, debt collection, and currently leading discovery and solution design for migrating the payments system (the company's cash cow, PCI DSS compliance-critical)
- Pioneering the IaC and deployment patterns all products will adopt: short-lived K8s Jobs for privileged database operations that terminate after execution, reducing attack surface by scoping elevated access to the lifetime of the task. Built ArgoCD parameter overrides to handle a split-state reality where products use both Terraform and ArgoCD to provision infra and apps during the transition
- When the core platform team lacks capacity or gets stuck, I step in: pushed the Ceph/Rook storage feature over the line, unblocking shared filesystem access for products needing read-write across pods. Ran a Kyverno/Gatekeeper PoC to lock down resource creation (blocking S3 CSI driver usage, restricting storage class claims and API calls per team), with a recorded demo to win buy-in. Feeding requirements back to core platform, guiding what they build next based on real product-team needs
- AWS security: GuardDuty, CloudTrail, Control Tower with SCPs, WAF on CloudFront with IP sets and OWASP managed rules. Evaluated and deployed WIZ for cluster vulnerability management. Platform compliance via SafeBase: SOC 2 and ISO 27001 audit readiness, KMS key rotation, least-privilege IAM, SBOMs for supply chain integrity. Coaching mid-level and senior engineers

PortSwigger

Mar 2023 - Jun 2025

Platform Engineer, Technical Lead

- **AI platform lead.** Architected the LLM Gateway (LiteLLM) for Burp Suite: secure model routing, rate limiting, multi-tenant isolation across OpenAI, Anthropic, and open-source models
- Built three production EKS clusters. Helm push-based deploys (--atomic --wait) for auditable rollback over automatic Git sync. Hardened with OPA/Gatekeeper, Kyverno, Cilium with Hubble for eBPF network observability, Karpenter for scaling
- Built MCP servers for agent-driven infrastructure operations: GitHub, Jira, internal tooling. Engineered a RAG pipeline with pgvector before RAG was a category. Presented on vector databases and AI infra to the company
- Embedded security into CI/CD: Semgrep, Trivy, ClamAV in GitHub Actions. OWASP Threat Dragon for threat modeling. Cut deploy cycles from 2 weeks to minutes
- Reverse-engineered Chinese-language Nuclei vulnerability templates into an automated serverless detection engine. Worked directly with Ollie Whitehouse (now CTO, NCSC/GCHQ) on threat analysis. Earned a seat on the AI research team, diving into foundational papers including *Attention Is All You Need*

Self-employed

Dec 2018 - Present

DevOps Consultant - sushiroil.io

- **The Co-operative Group (2018-2022):** selected for their New Ventures team as a contractor, renewed every six months for four years with increasing rates. Built a new online pharmacy product (AWS, Kubernetes, NHS Spine/EMIS/TPP integrations meeting NHS Digital security standards) that was subsequently acquired by a German healthtech company. Also delivered their community volunteering platform connecting vulnerable people with local support, member points and charity donation systems
- **ITV:** managed infrastructure for Love Island catch-up, serving video on demand to millions with extremely bursty traffic patterns. Supported the Hub's broader Kubernetes migration
- Short-term platform contract at Booking.com: integrated a major Chinese ride-hailing platform into their infrastructure using AWS SDK and CloudFormation

TECHNICAL SKILLS

Cloud & Governance

AWS (EKS, ECS, Fargate, Lambda, VPC, IAM, S3, Route53, CloudFront, SSM, GuardDuty, CloudTrail, Control Tower, SCPs, WAF, Graviton, Inferentia, Trainium), GCP, Terraform, CloudFormation, Crossplane

AI/ML Infrastructure

LLM Gateway (LiteLLM), MCP servers, RAG pipelines, pgvector, Pinecone, Qdrant, Nomic Embed, agent orchestration. Early SageMaker adopter. Discovery work with TensorFlow, PyTorch, Jupyter. Understanding of model weights, embeddings, chunking strategies, decision trees

Languages

Python, Go, Bash, TypeScript, SQL, HCL (Terraform)

Security

WIZ, GuardDuty, CloudTrail, Semgrep, Trivy, ClamAV, OWASP Threat Dragon, Hubble/Cilium (eBPF), OPA/Gatekeeper, Kyverno, OpenSSL, AWS KMS, SBOMs, SafeBase (SOC 2 / ISO 27001)

Kubernetes

Multi-cluster EKS, Helm (charts, template, push deploys), ArgoCD, Kargo, CRDs, XRD Composition, Karpenter, Cilium/Hubble (eBPF), OPA/Gatekeeper, Kyverno, NetworkPolicy, RBAC

CI/CD & Automation

GitHub Actions (custom workflows, 95% runtime reduction), Argo Workflows, Playwright

Observability

Prometheus, Grafana, Loki, Datadog, CloudWatch, PromptLayer (LLM observability)

Also

German (bilingual), MBCS, Linux package management (yum, apt-get, brew), Bruce Schneier's *Applied Cryptography*, Kate Crawford's *Atlas of AI*

EDUCATION

BA Analytical Philosophy, University of York (James College)

2008 - 2011

Dissertations on environmental ethics (natural habitat reconstruction and value) and the structure of the good (flourishing and diminishing). Bilingual German-English; attended Dom Gymnasium before relocating to the UK.

Graduate Diploma in Law

2011 - 2012