

Zulia Shavaeva

AI Security Leader at AWS
Generative AI Innovation Center, EMEA

Summary

I lead security for the AWS Generative AI Innovation Center in EMEA. I work with delivery teams on security reviews of AI applications, including data protection and agent permissions. My experience spans more than eight years in software engineering, DevOps and security, across more than 100 engagements. My work includes threat modelling, data residency and retention reviews, and security guidance for regulated deployments.

Selected work

Co-authored a proposed security operating model for forward-deployed AI engineering teams in AWS Professional Services. It covers security reviews of agent actions and the access engineers need during delivery.

Author of a GenAI security capture-the-flag spanning prompt injection chains, guardrail bypass and data exfiltration via tool-use, selected for AWS re:Invent 2026 GameDay. I built LLM guardrails tooling hands-on, including a prompt-safety gate and a programmatic PII sanitiser.

Featured in BBC News coverage of women in computing, and winner of the Professor Sue Black Award for Technology Evangelism.

Experience

- 

Security Leader, Generative AI Innovation Center, EMEA

Amazon Web Services, Professional Services

Dec 2025 to present

- Own the security review function for GenAI engagements across EMEA end to end, and lead security design for AWS's forward-deployed AI engineering model.
 - Advise regulated customers on frontier-model deployment security, including Claude via the AWS and Anthropic partnership: data retention and Zero Data Retention, EU data residency and cross-region inference boundaries, encryption, guardrails and audit logging. Review processing locations and retention settings against the deployment's data-protection requirements.

- Resolved security blockers in pre-sales for European banks, automotive groups and Middle East enterprises, which led to multi-year follow-on contracts: risk-based exceptions with compensating controls, synthetic-data strategies and security architectures that passed customer risk review first time.
- Approver for prohibited and high-risk AI use-case assessments across EMEA under EU AI Act-aligned risk triage. I help develop the organisation's EU AI Act guidance and lead the region's GDPR and DPIA-aligned data classification and risk-acceptance process, escalating to Director and VP level.
- Built the organisation's security operations dashboard, and a security onboarding knowledgebase. I run standing EMEA security office hours and deliver security workshops to customer-facing teams.

● Senior Security Consultant, Generative AI Innovation Center

2024 to Dec 2025

Amazon Web Services, Professional Services

- Led enterprise security reviews of AI deployments, covering model risk and data protection. Reviewed operational-resilience evidence, including recovery objectives and service commitments.
- Agentic AI security: security reviews of MCP-based and autonomous-agent systems, including Amazon Bedrock AgentCore applications and agent frameworks. Reviewed access controls and the handling of personal data. Required teams to address critical findings before approval.

● Security, Risk & Compliance Consultant

2022 to 2024

Amazon Web Services

- Led security workstreams on large EMEA programmes for banks, exchanges, airlines and consumer brands: secure migrations, regulatory alignment and resilience uplift.
- Designed enterprise AWS security frameworks and reference architectures, including IAM baselines, KMS and encryption strategy, secure landing zones, monitoring standards and incident response playbooks passing ISO 27001, NIST CSF and PCI DSS audits first time.
- Implemented Zero Trust architectures with least-privilege IAM, just-in-time access and elimination of standing privilege. Hardened EKS estates with image scanning, admission control and runtime monitoring for regulated workloads, plus SIEM and SOAR integration and tabletop exercises.

● Earlier roles

2018 to 2022

- DevOps Consultant, AWS (2020 to 2022): CI/CD and infrastructure automation with Lambda, Terraform and CDK, then promoted into the security specialism.
- Algorithms and Data Structures Instructor, Durham University.
- Software Engineer, Nissan Trading Corporation, building a manufacturing scheduling optimisation that saved over £1 million within six months, and secure REST APIs with OAuth 2.0 and JWT.

Expertise

- Frontier-model deployment security
- Zero Data Retention
- EU AI Act readiness
- Agentic AI and MCP security
- Bedrock Guardrails
- GDPR and DPIA data classification
- EU data residency
- IAM and Zero Trust
- KMS and encryption
- EKS and container security
- SIEM and SOAR
- ISO 27001, NIST CSF, PCI DSS
- DORA and NIS2 readiness
- CISO and board advisory

Education

BSc Computer Science, Durham University

Languages

English, fluent

Russian, native

Community

Community lead, AWS Cloud Women Manchester