Hanna Nyzhnia

+34 637953524 | hanna@nyzhnia.com | linkedin.com/in/hanna-nyzhnia | github.com/grepxz | nyzhnia.com |
Barcelona, Spain

PROFESSIONAL SUMMARY

Security-first DevSecOps engineer with an offensive and governance origin - OWASP/pentesting, an M.S. in Cybersecurity, and ISO 27001/NIST bank audits at KPMG. I take infrastructure solutions and make them real: I built out and hardened a DevSecOps stack on AWS EKS with Terraform IaC, ArgoCD GitOps, container and IaC scanning (Trivy, tfsec), Kyverno admission policies, and keyless CI/CD via GitHub Actions + AWS OIDC. Secure by default - I first learned how systems break. Fluent in English and Russian.

CORE COMPETENCIES

Kubernetes (AWS EKS) | Infrastructure as Code (Terraform) | GitOps (ArgoCD) | CI/CD - GitLab, GitHub Actions, Jenkins | Scanning & Policy-as-Code (Trivy, tfsec, Kyverno) | Application Security (OWASP, pentest)

WORK EXPERIENCE

Archilabs

Sep 2024 - Feb 2025

Full Stack Developer - Houston, TX (remote)

- Built and deployed automation across a multi-tool pipeline, cutting processing time from 5 minutes to 30 seconds.
- Maintained and optimized backend infrastructure for browser-based rendering, sustaining 200+ concurrent users with lower latency.

Mission Zero

May 2023 - Dec 2023

Full Stack Developer - Houston, TX (remote)

- Implemented scalable backend infrastructure serving up to 5,000 concurrent users; integrated RESTful APIs and third-party services, improving data-sync efficiency by 35%.

KPMG

Dec 2021 - Dec 2022

Cybersecurity Consultant - Kyiv, Ukraine

- Audited bank security policies against ISO 27001/27002, NIST, and VAIT across a 5-client portfolio, lifting compliance by ~40%.
- Delivered remediation plans and technical documentation that removed identified vulnerabilities for banking-sector clients.

PROJECTS

Project-Ramus - DevSecOps on AWS EKS

Kubernetes | IaC | GitOps

Built out and hardened a three-tier microservices app on self-managed AWS EKS (Kubernetes v1.30): provisioned the VPC, subnets, IAM and cluster in Terraform, delivered via ArgoCD GitOps, added container + IaC scanning (Trivy, tfsec) and Kyverno admission policies (audit-first), managed secrets with External Secrets Operator + AWS Secrets Manager, and ran keyless GitHub Actions CI/CD via AWS OIDC.
github.com/grepxz/Project-Ramus

AI-Powered SIEM - Splunk-style clone

Incident Response | Detection | Python

Reverse-engineered a Splunk-style SIEM - core log ingestion, search, and alerting - to understand SIEM internals, then built an AI layer for automated alert analysis and triage.

EDUCATION

M.S., Cybersecurity – Kyiv National University of Construction and Architecture — Jan 2023

CERTIFICATIONS

Azure Fundamentals (AZ-900) | ISC2 Certified in Cybersecurity (CC) — Microsoft | ISC2
CompTIA A+ & Network+ | Google Cybersecurity & IT Support Certificates — CompTIA | Google

SKILLS

Cloud & Containers: AWS (EC2, EKS, IAM, Secrets Manager, OIDC), Azure (AZ-900), Docker, Kubernetes, Istio (service mesh)

IaC & CI/CD: Terraform, ArgoCD (GitOps), GitLab CI, GitHub Actions, Jenkins

Security: Trivy, tfsec, Semgrep (SAST), OWASP ZAP (DAST), Kyverno, OWASP Top 10, ISO 27001, NIST, GDPR, vulnerability assessment, OSINT

Scripting: Python, Bash, PowerShell, SQL

Languages: Ukrainian (native), English (fluent), Russian (fluent), Spanish (A1)