VLADYSLAV MAIDANIUK

DevOps/SRE Engineer | AI Infrastructure Specialist

Prague, Czech Republic | vla.maidaniuk@gmail.com | +420 721 579 603
linkedin.com/in/maidaniuk | github.com/vlamay

PROFESSIONAL SUMMARY

DevOps/SRE Engineer with 4+ years of experience building and scaling cloud-native infrastructure and AI/ML systems. Reduced deployment times by 80% and maintained 99.9% uptime for production systems serving 10,000+ users. Expert in Kubernetes, AWS, Infrastructure as Code (Terraform, Ansible), CI/CD automation, and AI agent deployment. Strong background in Site Reliability Engineering practices, monitoring (Prometheus/Grafana), security compliance (ISO 27001, PCI DSS, SOC 2), and security testing methodologies.

Core expertise: Kubernetes orchestration • AWS/Azure cloud architecture • AI/ML infrastructure • CI/CD pipelines • SRE practices • Security hardening • Ansible automation (3+ years)

TECHNICAL SKILLS

Container Orchestration & Cloud:

Kubernetes (EKS, self-hosted), Docker, Helm | AWS (EC2, EKS, RDS, S3, VPC, IAM, Lambda, CloudWatch), Azure, GCP

Infrastructure as Code & Automation:

Terraform, Ansible (3+ years production experience), CloudFormation | GitHub Actions, GitLab CI/CD, Jenkins | Python, Bash, PowerShell

AI/ML Infrastructure:

AI agent deployment & orchestration | ML pipeline automation | Model serving infrastructure | LLM integration (OpenAI API, Claude API) | GPU resource management | AI workload optimization

Monitoring & Observability:

Prometheus, Grafana, Splunk, ELK Stack | SLO/SLI/SLA definition, Error Budgets, Alerting (PagerDuty) | AI model performance monitoring

Databases & Web Servers:

PostgreSQL, MySQL, Oracle Database | Nginx, Apache, Tomcat, HAProxy

Security & Compliance:

CIS Benchmarks, ISO 27001, PCI DSS, SOC 2 | HashiCorp Vault, Security Hardening, Vulnerability Management | Penetration Testing Tools: Nmap, Metasploit Framework, Burp Suite, OWASP ZAP, Wireshark | Security Scripting: Python, Ruby, Bash | Network Security: Packet analysis, Protocol exploitation, LAN/WAN testing

Operating Systems:

Linux (Ubuntu, CentOS, RHEL) - Advanced administration, Windows Server

PROFESSIONAL EXPERIENCE

DevOps/SRE Engineer

January 2025 – Present

Up Coop (UP Group) | Prague, Czech Republic

Tech Stack: AWS, Kubernetes (EKS), Docker, Terraform, Ansible, GitHub Actions, Prometheus, Grafana, Loki, HashiCorp Vault, Python, Bash

- **AI Infrastructure & Automation:** Implemented AI-powered monitoring and anomaly detection using machine learning models, reducing false alerts by 45% • Deployed automated AI agents for infrastructure optimization and cost analysis, saving 25% in cloud costs • Built CI/CD pipelines for AI/ML model deployment with automated testing and validation gates • Orchestrated containerized AI workloads on Kubernetes with GPU resource allocation and auto-scaling
- **Site Reliability Engineering:** Established SLO/SLI framework with Error Budgets, reducing unexpected downtime by 35% • Led incident management transformation, decreasing MTTR by 25% through enhanced observability (Prometheus/Grafana/Loki) • Implemented blameless postmortem process, improving team learning and system resilience • Achieved 99.9% uptime SLA through proactive monitoring and capacity planning
- **Infrastructure Automation:** Automated provisioning of 50+ cloud resources using Terraform and Ansible, reducing provisioning time by 60% • Built reusable Terraform modules for VPC, EKS, RDS, S3 with comprehensive documentation • Implemented GitOps workflows ensuring infrastructure version control and auditability • Reduced infrastructure costs by 25% through resource optimization and rightsizing
- **Ansible & Configuration Management:** Architected enterprise-wide Ansible automation framework managing 80+ servers across multiple environments • Created 40+ reusable Ansible playbooks and roles for system hardening, patch management, and security compliance • Implemented Ansible Tower/AWX for centralized automation orchestration with RBAC • Automated security baseline enforcement using Ansible with CIS Benchmarks compliance checks
- **CI/CD & Deployment:** Re-engineered CI/CD pipelines with GitHub Actions, slashing deployment time by 80% (40min → 8min) • Implemented canary deployment strategies and automated rollback mechanisms for zero-downtime releases • Reduced production incidents by 40% through automated testing and quality gates • Created reusable workflow templates reducing pipeline development time by 60%
- **Kubernetes & Container Management:** Deployed and managed production Kubernetes clusters on EKS (20+ nodes, 50+ pods) • Implemented Kubernetes security best practices: RBAC, Network Policies, Pod Security Standards • Configured HPA/VPA for auto-scaling, achieving 60% average node efficiency • Managed containerized applications using Helm with custom charts and version control
- **Security & Compliance:** Designed secure secrets management solution with HashiCorp Vault ensuring 100% vault-managed secrets • Hardened Kubernetes clusters with RBAC, Network Policies, and security scanning (Trivy, SAST) • Achieved 95%+ CIS Benchmarks compliance through automated security hardening • Ensured ISO 27001 compliance across international teams • Conducted internal security assessments using Nmap and Metasploit for infrastructure validation • Performed network packet analysis with Wireshark for troubleshooting and security investigation

Freelance DevOps & Cloud Engineer

January 2022 – December 2024 (3 years)

Upwork | Remote (Prague, Czech Republic)

Tech Stack: AWS, Kubernetes, Docker, Terraform, Ansible, GitHub Actions, GitLab CI, Prometheus, Grafana, Linux, PostgreSQL, Oracle, Python, Bash, Nmap, Metasploit, Burp Suite

- **AI/ML Projects:** Deployed AI-powered chatbot infrastructure for banking client, serving 5,000+ daily users with 99.8% uptime • Built automated AI agent pipelines for document processing and data extraction, reducing processing time by 70% • Implemented monitoring and observability for ML model performance and inference latency • Created Python-based automation tools using AI APIs (OpenAI, Claude) for infrastructure management tasks
- **Cloud Infrastructure & DevOps:** Designed and implemented CI/CD pipelines for fintech applications using GitHub Actions and GitLab CI • Built and managed scalable AWS infrastructure (EC2, RDS, S3, VPC, IAM) using Terraform • Containerized 12+ legacy banking applications using Docker, creating standardized deployment artifacts • Reduced deployment time by 70% (4 hours → 45 minutes) through pipeline automation
- **Ansible Automation:** Designed and implemented Ansible-based automation solutions for 8+ clients, managing infrastructure across 200+ servers • Created custom Ansible roles for application deployment, system configuration, and security hardening • Automated Linux system administration tasks (user management, package updates, service configuration) using Ansible • Built Ansible playbooks for disaster recovery automation and backup orchestration • Implemented Ansible-driven compliance automation for PCI DSS and ISO 27001 requirements
- **System Reliability & Performance:** Maintained 99.9% uptime for critical banking applications serving 10,000+ daily users • Optimized Apache/Tomcat/Nginx web server performance improving response times by 35% • Enhanced PostgreSQL query performance by 20% through optimization and indexing • Established monitoring with Prometheus + Grafana stack with custom dashboards
- **Automation & Security:** Automated routine tasks (backups, monitoring, deployments) using Python and Bash, reducing manual work by 80% • Implemented security hardening following CIS Benchmarks and ISO 27001 guidelines • Ensured compliance with financial security standards (PCI DSS, SOC 2) • Completed advanced penetration testing training (Hack The Box Academy) • Performed security assessments for 3+ fintech clients using Metasploit, Burp Suite, and Nmap • Conducted network security audits across LAN/WAN environments with packet analysis using Wireshark • Delivered security reports with remediation roadmaps and provided knowledge transfer to client teams

Cybersecurity Analyst

June 2020 – January 2022 (1 yr 8 months)

Motorola Solutions | Prague, Czech Republic

Tech Stack: Splunk SIEM, Nessus, Endpoint Protection, Windows, Linux, Firewalls, IDS/IPS, Metasploit, Wireshark

- Deployed and maintained endpoint protection across 200+ Windows and Linux workstations
- Monitored security events in Splunk SIEM, performing triage and escalating validated incidents
- Performed malware analysis (static/dynamic) to identify threats and develop containment strategies
- Conducted vulnerability scanning using Nessus and documented remediation procedures
- Practiced penetration testing techniques in isolated lab environments using Metasploit and Nmap
- Analyzed network traffic using Wireshark for security incident investigation and protocol analysis
- Collaborated with network team to optimize firewall and IDS rules, reducing false positives by 30%

Oracle Database Administrator

April 2019 – June 2020 (1 yr 3 months)

N-iX | Krakow, Poland

Tech Stack: Oracle Database (11g/12c), RMAN, Oracle Enterprise Manager, SQL, PL/SQL, Linux

- Administered Oracle Database instances achieving 99.9%+ availability
- Optimized database performance through tuning and indexing, improving throughput by 25%
- Implemented backup/recovery using RMAN with regular disaster recovery testing
- Managed database security with RBAC, privilege management, and audit logging
- Proactive monitoring using OEM and custom scripts ensuring performance baselines

System Administrator

May 2016 – January 2019 (2 yrs 9 months)

PESA Bydgoszcz S.A. | Bydgoszcz, Poland

Tech Stack: VMware vSphere, Hyper-V, Docker, Kubernetes, Ansible, Windows Server, CentOS, PowerShell, Bash, Azure AD

- Architected VMware vSphere cluster (20 ESXi hosts, 400+ VMs), improving consolidation by 40%
- Deployed Docker and Kubernetes platform for development teams, accelerating delivery by 50%
- Implemented Ansible for automated system configuration and patch management across 100+ servers
- Implemented security hardening aligned with CIS Benchmarks, reducing audit findings by 60%
- Automated maintenance tasks using PowerShell and Bash, reducing manual workload by 40%
- Led disaster recovery planning, reducing RTO by 30% (8 hours → 5 hours)
- Integrated on-premises infrastructure with Azure AD and Azure Site Recovery

EDUCATION

Master's Degree in Information Systems Security

2017 – 2019

Jagiellonian University, Krakow, Poland

Bachelor's Degree in Computer Science

2014 – 2017

Jagiellonian University, Krakow, Poland

CERTIFICATIONS

Active Certifications:

• Certified Ethical Hacker (CEH v12) – EC-Council | Issued: 2024

• DevSecOps Certificate – TryHackMe | Issued: August 2025

• Palo Alto Networks Cybersecurity Professional Certificate | Issued: 2025

• Google IT Automation with Python Professional Certificate | Issued: 2024

• EF SET English Certificate (B2 Upper Intermediate) | Issued: 2025

In Progress:

• AWS Certified Solutions Architect – Associate (Planned: Q2 2025)

• Certified Kubernetes Administrator (CKA) – CNCF (Currently studying)

LANGUAGES

Ukrainian: Native Proficiency **Russian:** Native Proficiency **Czech:** Professional Working Proficiency (B2)

English: Professional Working Proficiency (B2) **Polish:** Intermediate (B1)

ADDITIONAL INFORMATION

Work Authorization: EU Citizen – Authorized to work in Czech Republic and European Union | Valid Canada Work Permit until 2029

Current Location: Prague, Czech Republic

Relocation: Open to relocation worldwide

Work Arrangement: Open to on-site, hybrid, or fully remote roles (3+ years remote work experience)

Availability: 2-week notice period

Security Clearance: Eligible for security clearance

RELEVANT SKILLS FOR PENETRATION TESTING ROLES

3+ years hands-on Ansible experience for automation and security hardening • Deep Linux expertise with advanced system administration across Ubuntu, CentOS, RHEL • Network security skills: packet analysis (Wireshark), LAN/WAN testing, protocol understanding • Penetration testing tools: Nmap, Metasploit Framework, Burp Suite, vulnerability assessment • Web server administration: Nginx, Apache, Tomcat configuration and optimization • Security scripting: Python, Bash, Ruby for automation and custom exploit development • Team collaboration: Knowledge transfer experience, security training, mentoring • Remote work: 3+ years successfully delivering complex projects remotely with strong communication • CEH certified with continuous learning through Hack The Box Academy and TryHackMe