Eduard Sh.
Expert DEVSECOPS ENGINEER

SUMMARY

DevSecOps Engineer with over a decade of expertise, specializing in compliance automation and cloud security hardening, underscored by a solid foundation in Computer Science and Software Engineering. Their technical prowess spans CSPM tools, security suite deployment, and vast experience with CI/CD pipelines and major cloud service providers (AWS, Azure, GCP). With proficiency in key programming/scripting languages such as Python, Bash, and PowerShell, they have effectively contributed to various domains, including Healthcare, Business, and EdTech, holding certifications like Azure Security and MS 365 Security. Their track record demonstrates implementing secure solutions, from SIEM enhancements to fortifying high-load NFT trading platforms. The engineer's ability to transform security practices, ensuring robustness and business continuity in fintech and healthcare, positions them as a competitive candidate poised for contributing significantly to prospective projects.

TECHNICAL SKILLS

Main Technical Skills	AWS CloudTrail (6 yr.), Azure (3 yr.), IaC (6 yr.), Ansible (8 yr.)
.NET Platform	Azure (3 yr.), Identity Server (1 yr.)
Security	Nessus (6 yr.)
Databases & Management Systems / ORM	MySQL (3 yr.), PostgreSQL (3 yr.)
Cloud Platforms, Services & Computing	Azure (3 yr.), GCP (2 yr.)
Amazon Web Services	AWS CloudTrail (6 yr.), AWS Security Groups (8 yr.)
Azure Cloud Services	Azure Kubernetes (3 yr.)
Deployment, CI/CD & Administration	Ansible (8 yr.)
QA, Test Automation, Security	Checkmarx (1 yr.), CSP, Nessus (6 yr.)
Platforms	CloudCheckr Finance Manager (6 yr.)

Virtualization, Containers and Orchestration	Docker Compose (6 yr.)
Version Control	Github Actions (1 yr.)
Methodologies, Paradigms and Patterns	IaC (6 yr.)
Soft Skills	Mentor Aptitude
Scripting and Command Line Interfaces	Shell Scripts
Other Technical Skills	ACF (3 yr.), Content Security Policy, Palo Alto (3 yr.), Snyk (2 yr.), Sonarcloud (1 yr.), XDR (1 yr.)

WORK EXPERIENCE

DevSecOps Engineer, SIEM Configuration Tuning and Service Onboarding

Duration: 08.2024 – till now
Summary: SIEM CONFIGURATION TUNING AND SERVICE ONBOARDING
Responsibilities: Investigated and onboarded services into Google SecOps SIEM to enhance organizational security; Engaged with service owners to gather requirements, understand security needs, and define SIEM coverage scope; Developed a tailored set of security rules; Conducted thorough testing and validation of security rules; Collaborated with cross-functional teams; Contributed to improving the organization’s security posture.
Technologies: Google SecOps

DevSecOps Engineer, NFT Trading Hub

Duration: 02.2024 – 08.2024
Summary: NFT TRADING HUB
Responsibilities: Communicated security strategies, policies, and procedures to stakeholders; Designed and implemented security measures; Configured and managed network security; Analyzed security (SAST and DAST); Installed and maintained the ELK stack; Hardened Azure Cloud infrastructure; Ensured high availability and disaster recovery; Implemented data protection strategies; Developed a vulnerability remediation plan; Developed Security Policies; Wrote Python scripts for key management; Provided Information Security Audit.
Technologies: Azure, Terraform, Docker, Linux, Bash, Python, IIS, ELK, One Identity, Snyk, SonarCloud, Git

DevSecOps Engineer, Fintech Project in Real Estate Business

Duration: 01.2022 – 01.2024
Summary: FINTECH PROJECT IN REAL ESTATE BUSINESS
Responsibilities: Analyzed SAST security; Performed security scanning with Qualys; Launched AWS resources via Terraform; Hardened security via benchmarks; Developed Security Policies; Managed vendor risk; Wrote scripts with Python and Bash; Implemented the ELK stack; Ensured high availability and disaster recovery; Developed documentation on vulnerability assessments.

Technologies: AWS, Ansible, Bash, GitLab CI, Python, IIS, Git, Linux, Terraform, MySQL, Qualys, Checkpoint, Docker, ELK

DevSecOps Engineer, Remote Patient Monitoring Project

Duration: 12.2020 – 01.2022
Summary: REMOTE PATIENT MONITORING PROJECT
Responsibilities: Deployed, configured, and managed Sentinel One; Analyzed security (Checkmarx, Snyk); Supported IaC (Terraform) and GitHub Actions pipelines; Automated application deployment via Docker; Monitored Reapsaw automated continuous security; Tweaked Security Suites with Checkpoint; Provided Information Security Audit and compliance control; Hardened security via AWS benchmarks; Managed CyberArk Vault; Implemented NIST security standards.
Technologies: AWS, Sentinel One, Kubernetes, Docker, Bash, Terraform, CyberArk Vault, Git, GitHub Actions, Reapsaw, Checkpoint, Checkmarx, Snyk, MySQL

Team Lead / DevSecOps Engineer, Business Application

Duration: 03.2018 – 11.2020
Summary: BUSINESS APPLICATION
Responsibilities: Developed Cloud Security Posture Management Product; Provided security control coverage for clouds; Researched and developed security rules; Developed business logic; Hardened security via benchmarks; Developed remediation plan; Validated security controls; Provided cloud security infrastructure audit; Managed vulnerability; Presented product features; Implemented security best practices.
Technologies: AWS, GCP, Azure, Terraform, Bash, Docker Compose, Linux, Git, Nginx, PostgreSQL, Kubernetes, HALO, Checkpoint, CloudCheckr, Prisma Palo Alto, AQUA, Prowler, Cloud Custodian, PowerShell, Windows Server, CLI

Security Engineer, Banking Project

Duration: 01.2012 – 02.2018
Summary: BANKING PROJECT
Responsibilities: Deployed Vulnerability Management System; Implemented security measures; Created backup and disaster recovery processes; Collaborated with development team; Wrote documentation; Supported infrastructure; Troubleshot and resolved issues; Scanned images for vulnerabilities; Monitored logs; Implemented ISO2700x; Wrote scripts for automation; Implemented SIEM; Prevented malware; Hardened security; Developed Security Policies.
Technologies: Linux, Bash, Windows Server 2012, ELK, Qualys and Nessus, Manage Engine, QlikView, Ansible, Qlik Sense, Graylog, New Relic

EDUCATION

- **Computer Science and Software Engineering**

CERTIFICATION

- **Azure Security (AZ-500)**
- **MS 365 Security (MS-500)**