

# Aleksandr Liukov, Software Security Engineer

+357 97 888 176 | liukov.aleksandr91@gmail.com | [LinkedIn](#)

## PROFILE

Security engineer with 11 years of experience spanning IT infrastructure, DevSecOps, and platform security. Advocate for Infrastructure as Code, automating security controls across CI/CD pipelines and Kubernetes environments. Expertise in cloud security architecture, identity management, and container hardening. CISSP and OSCP certified. Builds AI-driven security tools for code analysis and vulnerability triage. Foundation in system administration enables practical understanding of how complex systems are built, deployed, and secured at scale.

## WORK RIGHTS

Based in Cyprus. Open to relocation to London. Require employer-sponsored visa.

## CORE SKILLS & TECHNOLOGIES

**Cloud & Platform Security:** AWS, Microsoft Azure, multi-cloud architecture, IAM, network segmentation, encryption controls, cloud security posture

**Container Security:** Kubernetes, Docker, Kyverno, Falco, Seccomp, kubebench, container orchestration, security policy enforcement

**DevSecOps & CI/CD Security:** Pipeline security, SAST, SCA, secrets scanning, GitOps workflows, secure SDLC, supply chain security

**Infrastructure as Code:** Terraform, Ansible, automated configuration management, policy enforcement, infrastructure automation

**Security Architecture:** Threat modeling, STRIDE, MITRE ATT&CK, defense-in-depth, zero-trust principles, risk assessment

**Identity & Access Management:** Active Directory, MFA, Microsoft Identity Manager, access control lifecycle, enterprise identity infrastructure

**Automation & Development:** Python (advanced), Bash, PowerShell, Go, AI-assisted code analysis (Claude Code), security tooling development

**Security Operations:** Splunk, Humio/CrowdStrike, log analytics, alert correlation, DefectDojo, vulnerability management

## EMPLOYMENT HISTORY

Aug 2024 — Present

**Lead Product Security Engineer**, Unlimit

Cyprus

- Architect and deploy enterprise-wide security pipeline integrating SAST, SCA, and secrets scanning into CI/CD with automated findings ingestion and developer dashboards
- Engineer integrated vulnerability management system (DefectDojo + Python automation + Jira) consolidating findings from multiple scanners and automating remediation lifecycle
- Develop AI-driven tools using Claude Code to examine codebases for business logic vulnerabilities and automate triage of security scanner findings
- Conduct internal penetration testing and security assessments of web applications, APIs, and cloud infrastructure
- Perform security design reviews of software products and infrastructure architecture, advising engineering teams on risk mitigation
- Provide security subject matter expertise to product teams throughout the SDLC, embedding security into design decisions

Apr 2023 — Aug 2024

**Information Security Architect**, Kaspersky Lab

Russia

- Define and document secure architecture principles for products and infrastructure, establishing security-by-design standards
- Evaluate product and system designs to identify security flaws and recommend remediation strategies
- Develop and implement Secure Software Development Lifecycle (SSDLC) processes across engineering teams
- Advise and guide engineering teams on mitigating risks and embedding security controls into architecture decisions
- Conduct targeted penetration testing of applications and services to validate security posture

Sep 2021 — Apr 2023	<b>Senior Cyber Security Engineer</b> , TheSoul Publishing	Cyprus
	<ul style="list-style-type: none"> <li>• Strengthen security of Kubernetes clusters and CI/CD pipelines, implementing container security policies and runtime protection</li> <li>• Automate and maintain security controls through Infrastructure as Code: SAST, DAST deployments using Terraform and Ansible</li> <li>• Develop secure remote access solution for corporate infrastructure with automated access controls, routing, and monitoring</li> <li>• Manage SIEM platform, IDS, and vulnerability scanners with focus on alert optimization and actionable security intelligence</li> <li>• Deploy container security tooling including Kyverno for policy enforcement and Falco for runtime threat detection</li> </ul>	
Jan 2020 — Sep 2021	<b>Information Security Engineer</b> , Vkontakte	Russia
	<ul style="list-style-type: none"> <li>• Develop and maintain internal security tools and automation scripts (Python) to streamline operations and enforce controls at scale</li> <li>• Manage SIEM platforms (Splunk, Humio) and configure log processing pipelines (Logstash) for enterprise monitoring</li> <li>• Prepare and deploy log collection agents (winlogbeat, sysmon, osquery) across corporate infrastructure</li> <li>• Develop complex correlation queries transforming high-volume raw log data into actionable security alerts</li> </ul>	
Aug 2018 — Jan 2020	<b>System Integration Specialist</b> , Positive Technologies	Russia
	<ul style="list-style-type: none"> <li>• Deploy and configure security products across customer environments including OS hardening and network encryption appliances</li> <li>• Create automation scripts (Python, Bash) for repeatable installation, configuration, and integration of security solutions</li> <li>• Develop automated attack simulations to test and validate detection capabilities during integration projects</li> </ul>	
Nov 2016 — Jul 2018	<b>Security Engineer / IT Engineer</b> , GDC (Fujitsu preferred supplier)	Russia
	<ul style="list-style-type: none"> <li>• Administer enterprise identity infrastructure (Active Directory, MFA, Microsoft Identity Manager) and manage access control lifecycle</li> <li>• Investigate security alerts using Splunk and endpoint protection systems, assess change requests for security impact</li> </ul>	
Jan 2015 — Oct 2016	<b>System Administrator</b> , Atos IT Solutions & Services	Russia
	<ul style="list-style-type: none"> <li>• Maintain enterprise Windows Server infrastructure, VMware vCenter, and IBM WebSphere with system monitoring and patching</li> <li>• Automate identity management workflows and maintenance tasks using PowerShell</li> </ul>	

---

#### CERTIFICATIONS

2022	CISSP (Certified Information Systems Security Professional) — (ISC) <sup>2</sup>
2020	OSCP (Offensive Security Certified Professional) — Offensive Security
2017	MCSE: Cloud Platform and Infrastructure — Microsoft
2021	Splunk Certified User — Splunk

---

#### EDUCATION

2014	<b>Voronezh State Technical University</b>	Russia
	Computer Systems & Networks: Bachelor's Degree (5-year Specialist program)	