Aleksandr Liukov, Security Engineer

+375 97 888 176 | liukov.aleksandr91@gmail.com | LinkedIn

PROFILE

Security engineer with 11 years of experience spanning system administration, infrastructure security, and application security. Established enterprise-wide monitoring systems including SIEM deployment (Splunk, Humio), log collection pipelines, and detection rules that transform raw telemetry into actionable intelligence. Pioneered AI-driven security tooling for vulnerability analysis and findings triage. Strong advocate for automation-first approach with proven ability to bridge security operations and engineering. CISSP and OSCP certified.

WORK RIGHTS

Based in Cyprus. Open to relocation with visa sponsorship.

CORE SKILLS & TECHNOLOGIES

Detection & Response

Splunk, Humio/CrowdStrike, Logstash, log analytics, detection rules development, alert correlation and tuning, endpoint monitoring (winlogbeat, sysmon, osquery), security alert investigation

Security Automation

Python (advanced), Bash, PowerShell, AI-assisted security analysis, Infrastructure as Code (Terraform, Ansible)

Cloud & Identity

Microsoft Azure, AWS, Active Directory, IAM, MFA, device management, Group Policy

Application Security

SAST, SCA, DAST, penetration testing, threat modeling, vulnerability management, DefectDojo, Burp Suite

Infrastructure & Containers

Kubernetes security (Kyverno, Falco), Docker, CI/CD pipeline security, OS hardening

Frameworks

MITRE ATT&CK, defense-in-depth, zero-trust, CIS Controls, OWASP ASVS

EMPLOYMENT HISTORY

Aug 2024 — Present

Lead Product Security Engineer, Unlimit — Cyprus

- Develop AI-driven tools leveraging LLMs to examine codebases for business logic vulnerabilities and automate security findings triage
- Engineer integrated vulnerability management system (DefectDojo + Python automation + Jira) consolidating findings from multiple scanners with automated lifecycle management
- Architect and deploy enterprise-wide security pipeline integrating SAST, SCA, and secrets scanning into CI/CD workflows
- Conduct internal penetration testing and security assessments of web applications, APIs, and infrastructure
- Perform security design reviews and develop application security requirements for software products

Apr 2023 — Aug 2024

Information Security Architect, Kaspersky Lab — Russia

- Defined and documented secure architecture principles for products and infrastructure
- Evaluated product and system designs to identify security flaws and recommend remediation strategies
- Conducted targeted penetration testing of applications and services

Sep 2021 — Apr 2023

Senior Cyber Security Engineer, TheSoul Publishing — Cyprus

- Managed SIEM, IDS, vulnerability scanners, and security alerting infrastructure
- Strengthened security of Kubernetes clusters and CI/CD pipelines with policy enforcement
- Automated security controls deployment using SAST, DAST, and Infrastructure as Code
- Developed secure remote access solution with automated access controls, routing, and monitoring

Jan 2020 — Sep 2021 **Information Security Engineer,** VKontakte Russia

- Configured enterprise SIEM platforms (Splunk, Humio) and log processing pipelines (Logstash) for security monitoring
- Developed complex correlation queries transforming raw log data into actionable security alerts with optimized false-positive rates
- Deployed log collection agents (winlogbeat, sysmon, osquery) across corporate endpoint fleet and initiated mass rollout
- Investigated security alerts through log analysis, identifying legitimate threats and tuning detection rules
- Developed and maintained security automation tools and scripts (Python) to streamline security operations
- Designed and executed security awareness program including phishing simulation campaigns

Aug 2018 — Jan 2020 **System Integration Specialist,** Positive Technologies Russia

- Developed automated attack simulations to test and validate detection capabilities of security solutions
- Deployed and configured security products across customer environments including OS hardening and network encryption
- Created automation scripts (Python, Bash) for repeatable security solution deployment and integration
- Configured servers and network infrastructure for enterprise security deployments

Oct 2016 — Aug 2018 **IT Engineer,** GDC (Fujitsu) Russia

- Administered enterprise identity infrastructure (Active Directory, MFA, Microsoft Identity Manager) and access control lifecycle
- Investigated security alerts using Splunk and endpoint protection systems
- Managed Microsoft AD Domain Services, DNS, DHCP with PowerShell automation

Jun 2014 — Oct 2016 **System Administrator,** Atos IT Solutions Russia

- Maintained enterprise Windows Server infrastructure with system monitoring and patching
- Automated administrative tasks using PowerShell for identity management workflows

CERTIFICATIONS

2022	CISSP — Certified Information Systems Security Professional, (ISC)²
2020	OSCP — Offensive Security Certified Professional
2017	Microsoft Azure Infrastructure Solutions (Exam 533)
2017	MCSE — Cloud Platform and Infrastructure, Microsoft

EDUCATION

2014 **Voronezh State Technical University** Russia

Bachelor's Degree in Computer Systems & Networks