

# Aleksandr Liukov, Staff Product Security Engineer

+375 97 888 176 | liukov.aleksandr91@gmail.com | [LinkedIn](#)

PROFILE	Security engineer with 11 years of experience specializing in product security and secure SDLC. Architects enterprise security pipelines integrating SAST, SCA, and DAST into CI/CD workflows, enabling engineering teams to ship secure code faster. Conducts security design reviews, threat modeling, and penetration testing with risk-based prioritization. OSCP certified with hands-on exploit development experience. Strong Python automation skills for scalable security operations.
WORK RIGHTS	Based in Cyprus. Open to relocation. Require employer-sponsored visa.
CORE SKILLS & TECHNOLOGIES	<p><b>Application Security &amp; SDLC</b> Secure SDLC, SAST, SCA, DAST, OWASP ASVS, Burp Suite, OWASP ZAP, WAF, threat modeling, design reviews, code review</p> <p><b>Security Architecture &amp; Design</b> Defense-in-depth, zero-trust principles, STRIDE, MITRE ATT&amp;CK, risk assessment, security requirements</p> <p><b>Vulnerability Management</b> DefectDojo, identification, triage, remediation workflows, false-positive reduction, Qualys, Nessus</p> <p><b>Programming &amp; Automation</b> Python (advanced), Bash (advanced), PowerShell, security tooling development, exploit scripting</p> <p><b>Cloud &amp; Container Security</b> AWS, Kubernetes, Docker, Kyverno, Falco, Seccomp, CI/CD pipeline security, Terraform, Ansible</p> <p><b>Security Operations</b> SIEM (Splunk, Humio/CrowdStrike), incident response support, log analysis, alert correlation, security monitoring</p>

EMPLOYMENT HISTORY		
Aug 2024 — Present	<b>Lead Product Security Engineer</b> , Unlimit	Cyprus
	<ul style="list-style-type: none"><li>Architect and deploy enterprise-wide security pipeline integrating SAST, SCA, and secrets scanning into CI/CD workflows with automated findings ingestion for developer-actionable remediation</li><li>Engineer integrated vulnerability management system (DefectDojo + Python automation) consolidating findings from multiple scanners with automated triage and false-positive reduction</li><li>Perform security design reviews and threat modeling for product features across engineering teams throughout the SDLC</li><li>Conduct application penetration testing of web applications and APIs, identifying vulnerabilities and validating exploitability</li><li>Develop AI-assisted tooling for automated codebase security analysis and business logic vulnerability detection</li><li>Define and enforce application security requirements as security SME for in-house software products</li></ul>	
Apr 2023 — Aug 2024	<b>Information Security Architect</b> , Kaspersky Lab	Russia
	<ul style="list-style-type: none"><li>Defined and documented secure architecture principles for products and infrastructure, establishing security standards</li><li>Evaluated product and system designs to identify security flaws and recommended risk-based remediation strategies</li><li>Advised engineering teams on mitigating risks and embedding security controls into design decisions</li><li>Conducted targeted penetration testing of applications and services to validate security posture</li></ul>	

Sep 2021 — Apr 2023	<b>Senior Cyber Security Engineer</b> , TheSoul Publishing	Cyprus
	<ul style="list-style-type: none"> <li>Automated and maintained security controls including SAST, DAST, and Infrastructure as Code deployments</li> <li>Strengthened security of Kubernetes clusters and CI/CD pipelines with policy enforcement and container security controls</li> <li>Managed SIEM, IDS, and vulnerability scanners with focus on alert optimization and actionable security monitoring</li> </ul>	
Jan 2020 — Sep 2021	<b>Information Security Engineer</b> , Vkontakte	Russia
	<ul style="list-style-type: none"> <li>Developed and maintained internal security automation tools (Python) to streamline security operations and enforce controls</li> <li>Managed SIEM platform (Splunk), configured log collection infrastructure (sysmon, osquery), and developed correlation queries for threat detection</li> <li>Investigated security alerts through log analysis, identifying threats and tuning detection rules for false-positive reduction</li> </ul>	
Aug 2018 — Jan 2020	<b>System Integration Specialist</b> , Positive Technologies	Russia
	<ul style="list-style-type: none"> <li>Developed automated attack simulations and exploit scripts to validate detection capabilities of security products</li> <li>Created automation frameworks (Python, Bash) for repeatable deployment and integration of security solutions</li> </ul>	
Oct 2016 — Aug 2018	<b>IT Engineer</b> , GDC (Fujitsu)	Russia
	<ul style="list-style-type: none"> <li>Administered enterprise identity infrastructure (Active Directory, MFA) and managed access control lifecycle</li> <li>Investigated security alerts using Splunk and endpoint protection systems</li> </ul>	
Jun 2014 — Oct 2016	<b>System Administrator</b> , Atos IT Solutions & Services	Russia
	<ul style="list-style-type: none"> <li>Maintained enterprise Windows Server and VMware infrastructure with PowerShell automation</li> </ul>	

---

## CERTIFICATIONS

2022	CISSP (Certified Information Systems Security Professional) — (ISC) <sup>2</sup>
2020	OSCP (Offensive Security Certified Professional) — Offensive Security

---

## EDUCATION

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