

# Ivan V.

## Expert Cybersecurity/Application Security Engineer

### SUMMARY

- Cybersecurity specialist with 10+ years of extensive experience in securing cloud environments, applications, and infrastructure. - Specializes in GCP and AWS security, including secure architecture design, vulnerability management, and compliance-driven implementation (SOC2, ISO 27001). - Proficient in Python, PHP, JavaScript, TypeScript, and various security tools and methodologies, including DevSecOps, Kubernetes, and OWASP standards. - Experienced in leading cybersecurity teams, managing security programs, and ensuring compliance with standards like ISO 27001, SOC2, PCI, and GDPR. - Extensive experience in securing applications through threat modeling, secure SDLC, and implementing security controls across diverse technology stacks. - Skilled in securing cloud environments, managing SIEM systems, and conducting infrastructure security testing. - Fluent in English (C1), with intermediate Polish (B1+). - Holds ISO27001 Lead Implementer, AWS Certified Security - Specialty, Google Certified Cloud Security Engineer, and eMAPT certifications.

### TECHNICAL SKILLS

<b>Main Technical Skills</b>	GCP Security, AWS Security
<b>Programming Languages</b>	JavaScript, PHP, Python, TypeScript
<b>Security</b>	AWS Security, GCP Security, OWASP, SIEM
<b>Databases &amp; Management Systems / ORM</b>	ELK stack (Elasticsearch, Logstash, Kibana)
<b>Amazon Web Services</b>	AWS Security
<b>Azure Cloud Services</b>	Azure DevOps
<b>Google Cloud Platform</b>	GCP Security
<b>Version Control</b>	GitLab
<b>Methodologies, Paradigms and Patterns</b>	IaC
<b>Deployment, CI/CD &amp; Administration</b>	Jenkins
<b>Virtualization, Containers and Orchestration</b>	Kubernetes, Terraform
<b>Operating Systems</b>	Linux, Windows
<b>Logging and Monitoring</b>	Splunk
<b>QA, Test Automation, Security</b>	Threat Modeling, Vulnerability Management



## Other Technical Skills

AlienVault, ASVS, Containers, DAST, MASVS, SAMM, SAST, SCA, Secure code review, Secure SDLC

## EXPERIENCE

### Head of Cybersecurity

Dec 2023 - now

#### Responsibilities:

- Design and maintenance of Information Security Management System
- Ensure ISMS compliance with ISO 27001:2002
- Planning, team management, metrics, and reporting to C-level management
- Consulting clients for cybersecurity and application security
- Presales and sales activities
- Application security practices consulting: security architecture, S-SDLC, definition of security requirements and controls, threat modeling, and security risks assessment
- Improvement of corporate infrastructure, clouds, and services
- Implementation of various compliance requirements (SOC2, ISO, PCI, GDPR)
- Security awareness program: planning, presentations, courses, workshops, articles in corporate media

#### Personal achievements:

- Security evangelization within the whole company: C-level, managers, contractors
- Hands-on experience building a security program from scratch

### Senior Application Security Engineer

Jan 2022 - Dec 2023

#### Responsibilities:

- Metrics, reporting, and governance for application security programs across multiple accounts.
- Secured pipelines with SAST/DAST/SCA tooling across diverse technology stacks
- Led threat modeling and risk assessments
- Security architecture, definition of security requirements, and controls
- Security reviews and hardening measures for clouds and technology
- Vulnerability research, management, and automation
- Managed WAFs, IDS/IPS from a security perspective
- Conducted security investigations and ensured compliance requirements (SOC2, ISO, PCI, GDPR)
- Development and delivery of security awareness: presentations, courses, workshops

#### Personal achievements:

- Application security strategy in an outsourcing development company from scratch
- Presales and sales activities
- eMAPT certification
- Google Cloud Security Engineer certification



## **AppSec/SOC Lead**

June 2021 - Jan 2022

### **Responsibilities:**

- Manage the SOC team, investigations, and SOC program development
- Secure CI/CD pipeline (SAST/SCA)
- Secure self-managed Kubernetes clusters
- Vulnerability management, monitoring, and automation
- Threat modeling and security risk assessments
- Definition of security requirements and controls for banking applications
- WAF management
- Support anti-fraud investigation and countermeasures for discovered attack scenarios
- SIEM integration with external IoC providers

### **Personal achievements:**

- "Dive Into Kubernetes Security": presentation + attack demo at OWASP Kyiv conference

## **Cybersecurity analyst**

Dec 2018 - June 2021

### **Responsibilities:**

- Vulnerability management and automation for on-prem servers and Kubernetes
- Web application testing
- SIEM and log management engineering (Splunk + managed ELK)
- "Advanced SOC" activities: development extensions for Splunk for anti-fraud, integration with external systems, threat sources, and APIs
- Management of CyberArk PAM and Symantec DLP solutions
- Incidents and alerts investigations
- Contribution to internal security awareness program: phishing awareness, phishing site demo, articles for corporate media, etc.

### **Personal achievements:**

- ISO27001 Lead Implementer certification
- Completed DevOps course (GCP/Terraform/Kubernetes)

## **CTO**

April 2010 - Dec 2018

### **Responsibilities:**

- Technical consulting, software development, and team leadership for IT solutions, including networking, security, and database management for corporate clients and government agencies in small local company

## **IT Support Lead**

Jan 2004 - April 2010



**Responsibilities:**

- Comprehensive IT support for bank branches, including systems administration, ATM service, and user support, while also developing software and progressing to a management role

**System Administrator**

Feb 2003 - Jan 2004

**Responsibilities:**

- Administering Windows and Linux servers, Lotus Domino, and LANs, as well as providing user support

**CERTIFICATIONS**

- ISO27001 Lead Implementer
- AWS Certified Security - Speciality
- Google Certified Cloud Security Engineer
- eMAPT (Mobile App Penetration Testing)

**EDUCATION****National Aviation University (Kyiv)**

Faculty: Information Security in Computer Systems

Master's degree: Computer Systems Engineer

Graduate work topic: Secure information from unpermitted access from the Internet

2002 – 2003

**National Aviation University, Kryvyi Rih aviation college**

Faculty: Computer Engineering

1998 – 2002

