Ivan Oravec

Senior Security Engineer

e0sec@proton.me
linkedin.com/in/ivan-oravec
Bratislava / Trnava · Hybrid · SK/CZ + EN C1

Security professional with 15+ years of experience spanning cloud security engineering, offensive security, identity infrastructure, and compliance. Proven record designing and operating security controls in Azure and AWS environments at Swiss Re and Siemens Healthineers. Hands-on background in threat modelling, penetration testing, SAST, PKI/HSM operations, network AAA infrastructure, and DevSecOps. Translates complex security decisions into clear guidance for both technical teams and senior stakeholders. Dual Azure-certified (AZ-104 + AZ-500, renewed 2026). Burp Suite Certified Practitioner. Active CTF competitor — top 1% nationally in Cybergame 2026.

CORE COMPETENCIES

Security Engineering & Architecture

- Penetration testing (web, cloud, application)
- Threat modelling & secure-by-design review
- SAST / DevSecOps pipeline integration
- Cloud security architecture (Azure, AWS)
- Network security (AAA, TACACS+, RADIUS)
- IEC 62443, PCI-DSS, ISO 27001

Identity & Access Management

- OAuth 2.0 / OIDC / SAML
- Cloud IAM — AWS & Azure (RBAC, least-priv.)
- PKI / HSM lifecycle management
- Secrets management (AWS Secrets Manager)
- AAA infrastructure & service-to-service auth

Cloud & DevOps

- Azure (AZ-500 + AZ-104, renewed 2026)
- AWS — EC2, IAM, VPC, S3, GuardDuty, CloudTrail
- CI/CD pipelines — Azure DevOps
- Infrastructure as Code (IaC security linting)
- Python · Bash · PowerShell

Leadership & Communication

- Product ownership & roadmap definition
- PTaaS delivery management (Swiss Re)
- Executive risk reporting & stakeholder briefings
- Agile / Scrum squad experience
- Conference speaker — Openslava 2024 & 2025

COMPETITION RESULTS // ATTACKER'S PERSPECTIVE

#2	**BSides Bratislava CTF**	High-level offensive skills vs experienced regional practitioners	May 2026
#8	**Cybergame 2026 (NBU SR / SK-CERT) — top 1%**	8th / 921 participants — Slovakia's premier open cybersecurity competition	Mar–May 2026
#23	**Guardians Quals 2026 — blue team defence**	Captained team 'IO99627' to 23rd / 130 teams	Feb 2026
#31	**THEM CTF — captained team 'e0_'**	31st / 920 teams — 48-hour international competition	29–31 May 2026
#100	**GPN CTF 2026 — co-captained team 'e0_'**	100th / 1,138 teams	5–6 Jun 2026
#255	**DEF CON CTF Quals 2026**	Captained team 'e0_' to 255th / 686 teams	May 2026
#297	**0xfun CTF 2026**	Captained team 'knowitalls' to 297th / 1,351 teams	Feb 2026

PROFESSIONAL EXPERIENCE

Independent Security Researcher · *e0 Security* — Mar 2026 – Present — Remote

> Deep-dive research into application IAM attack surfaces: OAuth/OIDC flow abuse, token forgery, secrets vault misconfigs, and CI/CD credential leakage.

> Active CTF competitor and team captain across international competitions — see Competition Results above.

> Speaker at Openslava 2024 & 2025 — the leading Slovak open-source and technology conference — presenting on offensive security to technical and mixed audiences.

OAuth / OIDC Attack & Defence · Cloud Security Research · Secrets Exploitation · CTF · Python

Penetration Tester / Source Code Analyst · *Siemens* — Mar 2024 – Feb 2026 (2 yrs) — Bratislava · Hybrid

Healthineers

> Designed and executed comprehensive penetration tests across Azure-hosted healthcare platforms — application-to-application authentication, authorisation flows, privilege escalation, and secrets handling.
> Conducted SAST across healthcare software aligned to IEC 62443 — identity-related code paths, insecure direct object references, injection risks, and hardcoded credentials.
> Integrated security testing into CI/CD pipelines on Azure DevOps — automated secret detection and policy-as-code gates, blocking credential leakage early in the SDLC.
> Translated vulnerability findings into executive-level risk reports for non-technical stakeholders; advised on access control hardening and cloud security policy.
> Automated testing workflows and cloud resource interrogation using Python and Bash.

Azure DevOps · Web & Cloud Pentesting · SAST · Secrets Detection · IEC 62443 · Executive Reporting

Security Operations Engineer · *iptiQ by Swiss Re* Mar 2022 – Feb 2024 (2 yrs) Bratislava

> Administered AWS IAM across multiple accounts for an InsurTech platform — designing RBAC structures, enforcing least-privilege policies, and managing service account lifecycles.
> Owned secrets management using AWS Secrets Manager — rotation policies, access auditing, and eliminating hardcoded credentials across microservices.
> Implemented and monitored CloudTrail, GuardDuty, and S3 security policies; performed continuous threat hunting and incident response using AWS-native tooling and SIEM.
> Managed security backlog in an Agile squad; introduced IaC security linting and automated compliance scanning.

AWS Security · IAM/RBAC · Secrets Management · Incident Response · DevSecOps · Agile

Penetration Testing as a Service – Delivery Manager · *Swiss Re* Jun 2019 – Feb 2022 (2 yrs 9 mos) Bratislava

> Owned the full lifecycle of the internal PTaaS programme — scope, roadmap, and SLAs aligned to Swiss Re's cloud security strategy across Azure and AWS.
> Managed external ethical hacker teams and vendor relationships; coordinated testing of cloud-hosted auth and authorisation implementations.
> Built executive dashboards to track programme effectiveness and surface risk trends to senior leadership.
> Guided remediation workstreams for authentication and access control findings across technical and business stakeholders.

Product Ownership · PTaaS Delivery · Azure/AWS · Stakeholder Communication · Risk Reporting

***Career Break —** Professional Development* Jan 2019 – May 2019

Information Security Specialist · *VUB banka (Intesa Sanpaolo Group)* Sep 2016 – Dec 2018 (2 yrs 4 mos) Bratislava

> Managed PKI operations and HSM lifecycle for internet and mobile banking platforms — enterprise-grade cryptographic identity infrastructure serving millions of users.
> Maintained secret key material governance, certificate authority operations, and token issuance; ensured PCI-DSS compliance through regular audits.

PKI · HSM · Certificate Management · Secrets Governance · PCI-DSS · Banking Security

EMEA Security Devices Manager · *First Data Corporation* Mar 2014 – Aug 2016 (2 yrs 6 mos) EMEA

> Managed lifecycle of 200+ military-grade Secure Cryptographic Devices across EMEA Tier 3+ data centres; provided cryptographic infrastructure integration consulting.

Cryptographic Device Management · HSM · Enterprise Infrastructure · EMEA Operations

IT Security Consultant · *KPMG* Mar 2013 – Feb 2014 (1 yr) Bratislava

> Advised public and private sector clients on ISO 27000 compliance, risk analysis, and security governance; co-authored training curricula and delivered awareness sessions.

ISO 27001 · Risk Governance · Security Training · Stakeholder Advisory

***Career Break —** Travel* Aug 2012 – Jan 2013

Network Infrastructure Security Engineer · *Hewlett Packard Enterprise* Aug 2010 – Jul 2012 (2 yrs) Global Network Infrastructure

> Secured network access for ~20,000 devices and ~50,000 active users via AAA infrastructure (TACACS+, RADIUS, Cisco ACS) — core identity and network security at enterprise scale.

> Managed Juniper SSL gateways, Active Directory integrations, and host hardening across the global HPE network; deep Linux/Unix expertise established here.

AAA / TACACS+ / RADIUS · Active Directory · Network Security · Linux / RHCE

CERTIFICATIONS

AZ-500 Azure Security Engineer — Microsoft · Renewed 2026

AZ-104 Azure Administrator — Microsoft · Renewed 2026

Burp Suite Certified Practitioner — PortSwigger · Jul 2024–2029

RHCE / RHCSA — Red Hat · Jan 2011

EDUCATION

M.Eng. — Applied Informatics, specialisation Security Engineering 2005 – 2010
Slovak University of Technology in Bratislava (STU) · Diploma thesis (A): Methodologies for Examination of Information Systems Security

HOBBIES

Cycling · Competing in Alternate Reality Games · Fixing broken Apple products