Ivan Kuznetsov

Cybersecurity Engineer

ikuznetsov511@gmail.com

+37256237788

Tallinn, Estonia

Website

LinkedIn

Github

Profile

Cybersecurity Engineer specializing in SIEM/XDR, detection engineering, incident response, and security automation. Experienced in security operations, IAM, threat detection, and web security protection. Holds a BSc in Cyber Security Engineering and CompTIA CySA+ certification.

Education

BSc Cyber Security Engineering,
Tallinn University of Technology
09/2023 – 06/2026

Professional Experience

Cybersecurity Engineer (Full-time), *Admiral Markets AS* 01/2026 – Present
Promoted from Junior Cybersecurity Engineer after 6 months.

- Investigated and remediated security incidents via Cortex XDR
- Enhanced web application security through Akamai CDN, WAF tuning, rate limiting, and bot mitigation
- Managed identity and access using Microsoft Entra ID
- Developed a custom vulnerability remediation workflow using Python and Cortex XDR to streamline patch deployment for vulnerable software
- Conducted vendor risk assessments and security reviews aligned with internal policies

Cybersecurity Engineer (Project-based), *Cybertex Security OÜ* 12/2025 – Present

- Planned and conducted company-wide security awareness training and phishing simulation campaigns
- Performed email security hardening, security reviews, and technical support
- Supported implementation of security tooling and cybersecurity processes

Junior Software Developer, *Saule IT Services OÜ* 09/2025 – 01/2026

- Developed PHP-based backend with secure data validation
- Improved CAPTCHA implementation for security and UX

Cyber Security Intern, *Cybertex Security OÜ* 12/2024 – 11/2025

- Built SIEM/XDR infrastructure using Wazuh with automated incident response workflows and realistic attack simulation scenarios for client demonstrations

Certificates

- CompTIA CySA+ (2026)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals SC-900 (2025)
- EITCA/IS - Information Security (2025)
- Security for Blockchain and DApps - LearnQuest (2025)
- CCNA - Cisco (2025)
- Red Hat System Administration I & II (2024)

Skills

Security Operations
SIEM, XDR, Incident Response, Detection Engineering, Vulnerability Management

Platforms
Cortex XDR, Microsoft Defender XDR, Wazuh, ELK, Akamai

Identity & Infrastructure
Entra ID, GPO, Active Directory, Windows, Linux, CIS Benchmarks, IaC (Ansible)

Automation
Python, PowerShell, Bash, n8n, APIs, LLM Integration

Projects

CIS Benchmark-Based Endpoint Hardening, *Admiral Markets AS*
Implemented CIS Benchmark-aligned endpoint hardening for Windows and macOS, including audit controls and centralized patch management across systems

LLM-Enhanced SAST False Positive Reduction, *BSc Thesis Project*
Built an automated DevSecOps pipeline integrating SAST, local SLMs (including abliterated models), and cloud LLMs for vulnerability triage, false-positive reduction, and privacy-preserving source code security analysis.

AI Sales Assistant
Developed a RAG-based AI assistant with LLM integration, automated n8n workflows, and a full-stack web application.

Languages

English
Fluent

Estonian
Fluent

Russian
Native