Timofei Mihhailov

Cyber Security Specialist

Cybersecurity analyst with a background in full-stack development, skilled in log analysis, threat detection, and vulnerability assessment. Experienced in supporting SOC workflows, analyzing suspicious activity, and strengthening system security through secure coding and structured investigations.

timofeimih@gmail.com | +37254824711 | Tallinn, Estonia | linkedin.com/in/timofeimih

WORK EXPERIENCE

Security Focused Full-Stack Developer
LLC "UBK Business Dialogue"

11/2011 - 10/2022

LLC "UBK Business Dialogue", a network of offices of legal and accounting support for small and medium-sized businesses.

Achievements/Tasks

- Investigated and responded to real security incidents involving brute-force attempts, suspicious logins, and website compromises.
- Conducted regular vulnerability scans and manual pentests. Reported findings to leadership and worked closely with engineering teams to remediate vulnerabilities.
- Responsible for web application security, covering web application vulnerability scanning, application security and WAF.
- Analyzed logs (web, server, auth) to detect intrusion attempts, extract IOCs, and validate incidents.

Security Focused Full-Stack Developer
LLC “CANAPECLUB”

11/2019 - 10/2022

LLC "CANAPECLUB" is a catering company in Moscow.

Achievements/Tasks

- Built interfaces inline with industry UI/UX standards, while adhering to OWASP ASVS Security Standard.
- Integrated external APIs (Foodpicaso, Yandex Market) with proper validation to maintain data integrity.
- Supported troubleshooting by reviewing logs and identifying abnormal behavior affecting availability.
- Applied secure development principles across the platform to enhance resiliency.

EDUCATION

Cybersecurity
TalTech Tallinn & Tartu University

09/2022 - 06/2025 *Master's degree, Estonia*

Thesis/Courses

- Development of Cybersecurity Learning Material for Future and Current School Teachers in Ida-Virumaa (thesis).
- Information Systems Attacks and Defense.
- IT Infrastructure Services.
- Privacy-Preserving Technologies.

Information Technology Systems Development
University of Tartu

09/2016 - 06/2020 *Bachelor of Applied Science, Estonia*

SKILLS

Incident Response | Log Analysis | Threat Detection | SIEM | Python | JavaScript | SQL | Bash | Network Security | Application Security | Penetration Testing | Wireshark | Metasploit | NMap | Linux | Digital Forensics

PROJECTS

"Players Casino" Incident Management Plan (09/2023 - 12/2023)

- Developed an incident response plan for a multi-venue casino, covering threat classification, detection workflows, escalation procedures, and coordinated response actions based on the SANS IR model.
- Built playbooks for phishing, ransomware, and credential-theft scenarios, defining containment, recovery, and post-incident processes to improve overall SOC readiness.

"PowerAB Smart Home" Security Risk Analysis (01/2024 - 05/2024)

- Identified and assessed security risks in smart-home IoT systems, focusing on replay attacks, weak encryption, and data exposure.
- Developed SOC-aligned countermeasures such as secure transmission, anomaly detection, and improved access control.

COMPETITIONS & EXCERSISES

SANS Nordics Cyber Tournament 2024 (11/2024 - 12/2024)

*Placed **69th out of 500** competitors. Solved challenges in forensics, web exploitation, reverse engineering, and infrastructure attacks.*

Locked Shields 2024 (02/2024 - 03/2024)

White Team Member (supporting world’s largest cyber defense exercise).

LANGUAGES

English ●●●●●

Russian ●●●●●

Estonian ●●●○○

INTERESTS

Technology | Volleyball | Swimming | Cross-Country Skiing | Hiking | Crab Fishing