Nazar Lysyk

Junior SOC Analyst

nazarlysyk.official@gmail.com

+48578772930

Warsaw

siteportfolio.info

www.linkedin.com/in/nazar-lysyk

github

LANGUAGES

Polski (C1)

English (B1)

Ukrainian Native

CERTIFICATES

- AWS Cloud Practitioner, 2025
- AWS Certified Solutions Architect - Associate 2025
- SoftServe Academy 2026

SUMMARY

Junior SOC Analyst passionate about blue team security. Built a threat detection platform on AWS — real honeypot that attracted attackers from 8 countries, integrated with Splunk SIEM, MITRE ATT&CK mapping and IR playbooks.
AWS Certified | Strong Linux & cloud background.

PROFESSIONAL EXPERIENCE

DevOps Training Program – SoftServe Academy
12/2025 – 02/2026
- Hardened Linux environments for secure deployment
- Applied AWS IAM least privilege and network isolation
- Containerized applications using Docker and Compose
- Monitored infrastructure with Prometheus and Grafana
- Deployed AWS EC2 infrastructure using Terraform

PROJECTS

GitHub nazarlx

- ***Threat Detection Platform***

- Deployed Cowrie SSH honeypot on AWS EC2 (Terraform) — real attacks from 8 countries in 24h
- Splunk SIEM via HEC — 500+ events, 6-panel dashboard with geo map and MITRE ATT&CK mapping
- Detected Docker escape attempt T1611 — confirmed malicious by 11/94 VirusTotal vendors
- Tailscale ACL, UFW, SSH hardening, CloudTrail → Splunk
- 3 IR Playbooks: SSH brute force, command execution, suspicious country access

- ***CI/CD Automation Project***

- Monitoring stack: Prometheus, Grafana, Loki
- CI/CD automation with GitLab Runner

- ***Cloud Portfolio (own)*** – siteportfolio.info

- AWS S3, CloudFront, Route 53 — managed with Terraform

SKILLS

SIEM: Splunk Enterprise (SPL, dashboards, alerts, HEC)

Security: MITRE ATT&CK, incident response, threat hunting

Network Security: TCP/IP, DNS, HTTP/S, VPN, IDS/IPS, Firewall (UFW, AWS Security Groups), SSH hardening, packet analysis (Wireshark)

Cloud: AWS (EC2, S3, IAM, CloudTrail, VPC)

OS: Linux (Ubuntu, Amazon Linux), Windows

Containers: Docker

Scripting: Bash, Python