Mohamed Aly Amin

Ankara, Turkey — open to Istanbul / relocation | contact@mohamedalyamin.com | 0552 554 86 60
mohamedalyamin.com | linkedin.com/in/mohamedalyamin | github.com/skylight74

Summary

Security and fintech-infrastructure engineer with a DevSecOps, Go streaming, and applied-security-ML core. Formed and technically led a 6-engineer DevSecOps team, sole-built a real-time Go detection engine sustaining ~400k events/sec, and first-authored a peer-reviewed intrusion-detection paper (98.11% accuracy, AINA 2024). Strong across cloud-native security (Kubernetes, Terraform, SIEM/SOAR) and high-throughput backends (Kafka, ClickHouse). Native Arabic; Turkish (B2) and English (C1).

Skills

Security & DevSecOps: DevSecOps, secure SDLC, SAST/DAST/SCA, SIEM/SOAR (ELK, Wazuh, TheHive, Cortex, MISP, Suricata, Microsoft Sentinel), detection engineering, MITRE ATT&CK, threat hunting, vulnerability management, red/blue team, penetration-testing tooling (Burp Suite, OWASP ZAP, Nmap, Metasploit), FortiGate (NGFW), ISO 27001, GDPR & CIS Controls (familiarity)

Cloud & Infrastructure: Kubernetes (Helm, Skaffold, Istio, Kind, MetalLB), Docker, Terraform, Ansible, AWS (EC2, Lightsail, RDS, S3, IAM), CI/CD, GitOps, OpenTelemetry, Prometheus, Grafana, Proxmox

Backend & Streaming: Go, Python, C#, TypeScript, Bash, Kafka, ClickHouse, Redis, PostgreSQL, MongoDB, gRPC, REST, microservices, event-driven architecture, high-throughput pipelines

Applied ML & Data: PyTorch, TensorFlow, scikit-learn, OpenCV, MLOps (GPU Kubernetes, training pipelines), anomaly detection, LSTM, InfluxDB

Fintech & DLT: Technical due diligence (crypto/fintech ventures), Hyperledger Fabric (permissioned chaincode), transaction-grade streaming pipelines, PCI DSS & SOC 2 (familiarity)

Certifications: Planned for 2026: AWS Solutions Architect – Associate, then Certified Kubernetes Administrator (CKA)

Languages: Arabic (native), Turkish (B2 – professional), English (C1 – full professional)

Experience

Security & Software Engineer, Independent / Freelance (project-based) – Remote — Turkey — Jan 2023 – present

- Sole-built the 10-microservice PHP/Laravel rebuild of a live housing-listings platform (270k registered users, 360k+ cumulative listings) on AWS (EC2, RDS, S3); rebuild currently in staging.
- Built protocol adapters — OCPP for EV chargers, SunSpec/Modbus for solar inverters, and IEC 62056 for smart meters — to normalize multi-vendor energy-device data for a smart-grid monitoring stack (InfluxDB, Grafana).
- Assessed 15+ crypto/fintech ventures' codebases, architecture, and technical risk to inform venture-capital investment decisions.

R&D Engineer — Cybersecurity, Dolusoft – Ankara, Turkey — Aug 2024 – May 2025

- Sustained ~400k events/sec by sole-designing and building a modular real-time filtering engine in Go, ingesting security events from 80+ sources (Kafka → filter/aggregate → ClickHouse, Redis-backed state, full OpenTelemetry tracing).
- Designed chained, first-seen, and z-score anomaly-detection rules in a configurable detection engine to cut false-positive noise.
- Built a Go multi-channel alerting service (Slack, email, webhook) with rate limiting and policy-based routing for faster incident response.

Research Assistant (part-time, TÜBİTAK-funded), Middle East Technical University (METU) – Ankara, Turkey — Jan 2022 – Apr 2025

- Reached 98.11% intrusion-detection accuracy by developing an SGD one-class SVM model for containerized microservices — first-author publication at AINA 2024 (Springer).
- Built the end-to-end GPU training pipeline (GPU-enabled Kubernetes cluster, dataset curation, evaluation) for the DIONA graduation project, shared with the AINA intrusion-detection research.

Cyber Security Specialist (Tech Lead — OSSArch), Interprobe Bilgi Teknolojileri – Ankara, Turkey — July 2021 – May 2022

- Shipped an MVP SIEM/SOAR platform (OSSArch) in 3 months — against the company's 6–12 month norm — by forming and technically leading a 6-engineer DevSecOps team with TDD, DDD, and daily agile.
- Automated threat enrichment by integrating ELK, Wazuh, TheHive, Cortex, MISP, and Suricata with OSINT feeds (VirusTotal, AlienVault OTX).
- Trained 4 engineers and ASELSAN partners; taught Introduction to Cybersecurity as visiting lecturer at Istanbul Aydın University; ran pre-sales demos/POCs at GISEC Dubai.

Projects

SmartGridLedger — Permissioned Blockchain (Hyperledger Fabric) — Jan 2024

- Authored original multi-org Fabric chaincode (TypeScript) on a Kubernetes + Istio network for secure energy-distribution settlement; published at MedPower 2024 (TÜBİTAK-funded).

Real-Time Detection Engine (Go) — 2024 – 2025

- Kafka → ClickHouse stream-processing engine at ∼400k events/sec with Redis state, OpenTelemetry observability, and a configurable detection + alerting rule engine.

DIONA — LSTM Intrusion-Detection System — 2022 – 2025

- Graduation project (BSc, METU): built the end-to-end MLOps/GPU training pipeline (GPU-enabled Kubernetes cluster, dataset curation, evaluation); enterprise pilot at Koç Sistem (Azure Sentinel/Defender integration phase).

Publications

Misuse Detection and Response for Orchestrated Microservices Based Software — Apr 2024
Mohamed Aly Amin, Adnan Harun Dogan, Elif Sena Kuru, Yigit Sever, Pelin Angin
link.springer.com/chapter/10.1007/978-3-031-57942-4_22 (AINA 2024, Springer — presented in Japan; TÜBİTAK Grant #120E537, TÜBA GEBİP Program)

Permissioned Blockchain-Based Monitoring Framework for DER-Integrated Distribution Networks (MedPower 2024) — 2024
Pelin Angin, et al. (incl. Mohamed Aly Amin)
(MedPower 2024 — TÜBİTAK Grant #120E537)

Education

Middle East Technical University (METU), BSc in Computer Engineering — Cyber Security specialization — June 2023

- Türkiye Bursları (Turkish Government Scholarship) recipient.
- Graduation project: DIONA — built the end-to-end MLOps/GPU training pipeline (GPU-enabled Kubernetes cluster, dataset curation, evaluation) for an LSTM intrusion-detection system; enterprise pilot at Koç Sistem (Azure Sentinel/Defender integration phase).