

Samet Yılmaz Temel

Siber Güvenlik ve Yapay Zeka Mühendisi

sametyilmaztemel@outlook.com

[in](https://www.linkedin.com/in/sametyilmaztemel) [linkedin.com/in/sametyilmaztemel](https://www.linkedin.com/in/sametyilmaztemel)

blog.sametyilmaztemel.com/

github.com/sametyilmaztemel

+90 *** ** 07 30 Yenimahalle / Ankara / Türkiye



HAKKIMDA

Siber güvenlik ve yapay zekâ alanlarında uzmanlaşmaya odaklanan, yazılım geliştirme, uygulama güvenliği ve AI tabanlı sistemler üzerine deneyim sahibi bir mühendisim. Akademik çalışmalarımın yanı sıra çeşitli projelerde aktif rol alarak yapay zekâ entegrasyonu, güvenli yazılım geliştirme ve otomasyon sistemleri üzerine çalışmalar yürüttüm. Teknik bilgi birikimimi yenilikçi, güvenli ve ölçeklenebilir çözümler geliştirmek için kullanmayı hedefliyorum. 2024 yılında **TEKNOFEST** SorAI projesiyle **En İyi Sunum Ödülü** ve **HAVELSAN Trende Hackathon** MAIN Fikir ve Uygulama Kategorisi'nde **Üçüncülük ödülü** kazandım.

PROFESYONEL DENEYİM

ThinkBro Yapay Zeka Bilişim ve Danışmanlık | Yapay Zeka Mühendisi | Stajyer | Haziran 2026 – Eylül 2026

- Mevcut yazılım ürünlerine LLM ve AI servisleri entegre ederek yapay zekâ destekli özellikler ve uygulamalar geliştirdim.
- Multi-Agent Systems, LLM Orchestration, Tool Calling ve API entegrasyonlarıyla otonom AI iş akışları ve otomasyon sistemleri geliştirdim.
- Prompt Engineering, RAG ve Agentic AI yaklaşımlarıyla model etkileşimi, görev yönetimi ve çoklu ajan koordinasyonu üzerine çalıştım.
- Ürün gereksinimlerinin analizi, uygun AI çözümlerinin belirlenmesi, prototipleme ve geliştirilen özelliklerin mevcut sistemlere entegrasyonu süreçlerinde görev aldım.

Microsoft | Yapay Zeka Yaz Stajı Programı | İstanbul, Türkiye (Remote) | Stajyer | Haziran 2026 – Eylül 2026

- Azure AI Foundry ve Azure Machine Learning üzerinde yapay zekâ modellerinin geliştirilmesi, eğitilmesi, değerlendirilmesi ve deployment süreçlerinde çalıştım.
- Büyük Dil Modelleri (LLM), RAG, Prompt Engineering ve Fine-Tuning teknikleriyle AI tabanlı uygulamalar geliştirdim.
- Azure OpenAI Service ve Azure AI Services kullanarak model entegrasyonu, performans analizi ve optimizasyon çalışmaları gerçekleştirdim.
- Microsoft Entra ID (Azure AD), RBAC ve Managed Identities kapsamında kimlik ve erişim yönetimi ile bulut güvenliği mekanizmalarını inceledim.
- Azure Key Vault, Azure Monitor ve Responsible AI yaklaşımlarıyla güvenli, ölçeklenebilir ve izlenebilir AI uygulama mimarileri üzerine çalışmalar yürüttüm.

T.C. Cumhurbaşkanlığı Genel Sekreterliği | Sistem, Ağ Yönetimi ve Bilgi Güvenliği Daire Başkanlığı Stajyeri | Kasım 2025 – Şubat 2026

- Sistem, Ağ Yönetimi ve Bilgi Güvenliği Daire Başkanlığına bağlı olarak çalıştım.

Peakeye Group | Uygulama Güvenliği Mühendisi | İstanbul, Türkiye (Remote) | Stajyer | Temmuz 2025 – Kasım 2025

- Kurumsal ölçekte SAST, DAST ve SCA taramaları gerçekleştirdim; bulguları triage ederek geliştirme ekipleriyle remediation SLA süreçlerini yönettim.
- OWASP ASVS kontrollerini SDLC ve Pull Request süreçlerine entegre ettim.
- GitHub Actions ve GitLab CI kullanarak DevSecOps kontrollerini CI/CD pipeline'larına entegre ettim.
- SAST, SCA, container ve IaC taramalarını pipeline güvenlik kapısı olarak konumlandırımdım.
- CVSS v3.1 ve EPSS ile risk önceliklendirmesi yaparak zafiyet yaşam döngüsünü yönettim.
- Manuel güvenli kod incelemesi ve tehdit modelleme çalışmaları yürüttüm.

Tech Pioneers | Siber Güvenlik/AI Mühendisi & Eğitmen | Mart 2023 – Eylül 2025

- Uygulama Güvenliği, Kubernetes Güvenliği, SIEM Tespit Mühendisliği ve Olay Müdahale konularında 5'ten fazla uygulamalı workshop ve bootcamp düzenledim.
- LoRA/QLoRA fine-tuning, Retrieval-Augmented Generation (RAG) ve optimize model sunumu (vLLM, Triton, ONNX) alanlarında yapay zekâ sistemleri geliştirdim.
- Bulut tabanlı siber güvenlik laboratuvarları ve CTF ortamları kurdum.
- ISO 27001 ve NIST CSF ile uyumlu güvenli SDLC çerçevelerini standardize ettim.

SkyArt Teknoloji | Developer | Remote | Haziran 2023 – Haziran 2025

- Sigma ve KQL ile detection-as-code yaklaşımını CI/CD entegrasyonu ile uygulayarak yanlış pozitifleri %25 düşürdüm.
- FastAPI ve Kafka tabanlı event-driven mimari ile SAST/DAST/SCA bulgularını konsolide eden sistem geliştirdim.
- Jira ve GitHub issue'larını SLA takibi ile otomatik oluşturan entegrasyonlar geliştirdim.
- GCP, AWS ve Azure ortamlarında Terraform ve OPA/Conftest ile policy-as-code guardrail'ler uyguladım.

Fırat Üniversitesi, Bilgi İşlem Daire Başkanlığı | Siber Güvenlik Mühendisliği Stajyeri | Elazığ, Türkiye | Haziran 2022 – Eylül 2022

- Kritik sistemler için zafiyet analizi gerçekleştirdim.
- ISO 27001 uyumlu tespit kuralları ve güvenlik dokümantasyonu geliştirdim.
- Kural optimizasyonu ile yanlış pozitif oranlarını düşürdüm.

PROJELER

iOS Süreç Yönetimi Kullanarak Makine Öğrenmesi ve Sinir Ağları ile Güvenlik Açığı Sınıflandırma

- Akademik Proje

Akıllı Taktik Sistemler için Yapay Zekâ Tabanlı Coğrafi Konumlama ve Stratejik Nokta Analizi (GAIT)

- TEKNOFEST 2025 Kibris

Çoktan Seçmeli Soru Üretimi için Yapay Zekâ Tabanlı Büyük Dil Modeli (SorAI)

- TEKNOFEST 2024 En İyi Sunum Ödülü
- TEKNOFEST 2024 Antalya Finalisti

IoT Cihazları ve Ağları için Yapay Zekâ Tabanlı Siber Saldırı Tespit Sistemi

- TEKNOFEST 2024 Antalya Finalisti

EĞİTİM

- Fırat Üniversitesi | Adli Bilişim Mühendisliği Lisans | 2022 - 2026 **GPA 3.30**

YETENEKLER

- Bulut Güvenliği ve Platformlar: GCP, AWS, Azure; IAM, İş Yüklü Güvenliği (Workload Security), Zafiyet Yönetimi, Uyumluluk Entegrasyonu
- Uygulama Güvenliği: SAST, DAST, Güvenli Kod İnceleme, Tehdit Modelleme, OWASP ASVS/Cheat Sheets.
- Tespit Mühendisliği ve Olay Müdahale: SIEM (Splunk, ELK/Elastic, QRadar), EDR, IDS/IPS; Alarm Ayarlama (Alert Tuning), Tehdit Avcılığı, Zararlı Yazılım Analizi,
- LLM, NLP ve Makine Öğrenmesi: PyTorch, HF Transformers; LoRA/QLoRA; RAG (FAISS/Milvus/pgvector); SentencePiece; Değerlendirme Metrikleri (MMLU, GLUE, ROUGE, BLEU); vLLM/Triton sunumu, 8/4-bit quantization; MLflow/W&B/DVC; güvenlik (DPO/RLHF, prompt-injection savunma, PII maskeleyme).
- Ağ ve Platformlar: TCP/IP, Güvenlik Duvarları, VPN; Linux, Windows, macOS.
- Güvenlik için ML/LLM: Zafiyet Sınıflandırma, Güvenli Kodlama Asistanları, Exploit Desen Analizi.

SERTİFİKASYONLAR

Harvard University - Computer Science (2024)
HackerRank - CyberSecurity Engineer (2024)
HackerRank - Software Engineer (2024)
Oracle - Certified Cloud Manager (2025)
Fortigate - Certified Fortigate Operator (2025)

YABANCI DİL

- Türkçe - Ana Dil
- İngilizce - B2

REFERANSLAR

Prof. Dr. Türker TUNCER
Fırat Üniversitesi / Adli Bilişim
Mühendisliği

turkertuncer@firat.edu.tr
+90 *** **

Prof. Dr. Mehmet YILMAZ
Fırat Üniversitesi / Rektör Yardımcısı

mehmetyilmaz@firat.edu.tr
0424 *** **

Yusuf DURUMLU
Cezeri Yapay Zeka
& Robotik Teknolojileri /
Kontrol ve Otomasyon Mühendisi

yusuf.durumlu@cezerirobot.com
+90 *** **

Prof. Dr. Nazif ÇALIŞ
İskenderun Teknik Üniversitesi / Rektör Yardımcısı

nazif.calis@iste.edu.tr
0326 *** **

Prof. Dr. Şengül DOĞAN
Fırat Üniversitesi / Adli Bilişim
Mühendisliği

sdogan@firat.edu.tr
+90 *** **