🛡️ TACTICAL SENTRY C2 – PROJE TEKNİK RAPORU

Proje Adı: Tactical Sentry Command & Control (C2) System

Sürüm: v4.1 (Local Secure Edition)

Mimari: Clean Architecture (Onion) + MVVM

Platform: Windows Desktop (WPF / .NET)

---

1. YÖNETİCİ ÖZETİ

Tactical Sentry C2; askeri tesisler, sınır karakolları ve yüksek güvenlikli bölgeler için geliştirilmiş, **Yapay Zeka (AI) destekli bir otonom gözetleme ve karar destek sistemidir.**

Sistem, IP kameralardan veya webcams'den gelen canlı görüntüleri gerçek zamanlı olarak işler. Görüntü üzerindeki nesneleri (tabanca, tüfek, bıçak vb.) milisaniyeler içinde tespit eder, tehdit seviyesini analiz eder ve operatör müdahalesine gerek kalmadan sesli alarm, görsel kayıt ve veritabanı loglama işlemlerini otomatik gerçekleştirir. Ayrıca geçmiş verileri analizerek bölgenin güvenlik risk haritasını çıkarır.

---

2. TEKNİK ALTYAPI VE MİMARİ

Proje, yazılım dünyasında kabul görmüş en sürdürülebilir mimari olan **Clean Architecture (Temiz Mimari)** prensiplerine göre 4 ana katmana ayrılmıştır. Bu yapı, kodun modüler olmasını ve bir parçanın bozulmadan değiştirilebilmesini sağlar.

A. Katmanlar (Layers)

1. **Core (Çekirdek):** Projenin anayasasıdır. Hiçbir dış kütüphaneye bağımlı değildir. Veritabanı modelleri (`SecurityLog`, `OperatorUser`) ve soyut arayüzler (`ITargetDetector`, `IVideoSource`) burada tanımlıdır.
2. **Domain (İş Mantığı):** Sistemin beynidir. Karar mekanizmaları burada çalışır.
    - `ThreatClassifier`: Görülen nesnenin (Örn: "Pistol") bir tehdit olup olmadığına karar verir.
    - `EngagementRuleEngine`: Tehdidin güven skoruna (Confidence) bakarak alarma geçilip geçilmeyeceğine karar verir.
3. **Infrastructure (Altyapı):** Sistemin kaslarıdır. Ağır işleri yapan teknolojiler buradadır.
    - `YoloDetectorService`: ONNX Runtime kullanarak AI modelini çalıştırır.
    - `IpCameraService`: OpenCV ile görüntü akışını sağlar.
    - `TacticalDbContext`: SQLite veritabanı işlemlerini yönetir.
4. **Presentation (Sunum):** Kullanıcının gördüğü kısımdır (WPF). MVVM (Model-View-ViewModel) deseni ile arayüz ve kod birbirinden ayrılmıştır.

3. TEMEL FONKSİYONLAR VE YETENEKLER

1. Yapay Zeka Destekli Tehdit Tespiti

- **Teknoloji:** YOLOv8 (You Only Look Once) mimarisi kullanılarak eğitilmiş özel bir `.onnx` modeli kullanılır.
- **Hedef Sınıflar:** Sistem şu nesneleri ayırt edebilir: `Pistol` (Tabanca), `Rifle` (Tüfek), `Knife` (Bıçak), `Grenade` (El Bombası).
- **Performans:** Ortalama bir bilgisayarda 30 FPS hızında çalışarak gecikmesiz tespit yapar.

2. Otonom Karar ve Alarm Sistemi

Sadece tespit etmekle kalmaz, tepki verir:

- **Görsel Kanıt:** Tehdit tespit edildiği anda o karenin fotoğrafını çeker ve şifreli bir klasöre (`Evidence/`) tarih-saat damgasıyla kaydeder.
- **Sesli Uyarı:** Operatörü uyarmak için sistem hoparlörlerinden taktiksel siren/alarm sesi verir.
- **Loglama:** Olayı milisaniyesi milisaniyesine yerel veritabanına (`SQLite`) işler.

3. Kullanıcı ve Yetki Yönetimi (RBAC)

Sistemde askeri hiyerarşiye uygun bir yetkilendirme mekanizması vardır:

- **Giriş Güvenliği:** Kullanıcı adı ve şifre veritabanından doğrulanmadan sistem açılmaz.
- **Standart Operatör (Seviye 1):** Sadece izleme yapabilir.
- **Komutan / Admin (Seviye 5):** Geçmiş kayıtları silebilir, yeni personel ekleyebilir/silebilir ve sistem ayarlarını değiştirebilir.

4. Saha ve İstihbarat Analizi (YENİ)

Sistemin en stratejik özelliğidir. İnternet bağlantısına ihtiyaç duymadan, **yerel veritabanındaki geçmiş verileri** analiz eder.

- **Risk Analizi:** Toplam olay sayısı ile silahlı (kritik) olay sayısını oranlar.
- **Yapay Zeka Tavsiyesi:** Örneğin; "Son 1 haftada tespit edilen olayların %60'ı silahlı saldırı girişimidir. Bölge 'Kırmızı Alarm' seviyesine çekilmelidir" şeklinde operatöre yazılı rapor sunar.
- **Güvenilirlik:** Rastgele veri üretmez, %100 sahada yaşanan gerçek olaylara dayanır.

---

4. VERİ AKIŞ SENARYOSU (WORKFLOW)

Sistem çalıştığında arka planda şu döngü saniyede defalarca tekrarlanır:

1. **Görüntü Alma:** `IpCameraService`, kameradan 1 kare fotoğraf (Frame) alır.
2. **AI Analizi:** `YoloDetectorService`, bu kareyi analiz eder ve koordinatları/isimleri çıkarır (Örn: "Pistol, %88 Güven").

3. **Sınıflandırma:** `ThreatClassifier`, "Pistol" isminin `HostileInput` (Düşman) olduğunu belirler.
4. **Kural Motoru:** `EngagementRuleEngine`, eğer güven skoru kullanıcının belirlediği eşik değerin (Örn: %50) üzerindeyse "MÜDAHALE ET" emri verir.
5. **Aksiyon:**
    - `SoundAlerter` -> Ses çalar.
    - `EvidenceLocker` -> Fotoğrafı diske yazar.
    - `MissionLogger` -> Veritabanına kayıt atar.
6. **Raporlama:** Komutan istediği zaman "Ayarlar" menüsünden bu olayların istatistiksel dökümünü görür.

---

5. KULLANILAN TEKNOLOJİLER

- **Dil:** C# (.NET 6/7/8)
- **Arayüz:** WPF (Windows Presentation Foundation) & XAML
- **Veritabanı:** SQLite (Yerel, dosya tabanlı, sunucu gerektirmez)
- **AI Motoru:** Microsoft ONNX Runtime
- **Görüntü İşleme:** OpenCvSharp4
- **Veri Görselleştirme:** WPF Standart Kontrolleri (DataGrid, ProgressBar)

---

6. SONUÇ

Tactical Sentry C2; dış dünyaya veri sızdırmayan (Offline çalışabilen), askeri standartlarda güvenliğe sahip, modüler ve geliştirilebilir bir yazılımdır. Geleneksel güvenlik kameralarının "sadece kayıt etme" pasifliğinin aksine, bu sistem olay anında "tespit etme ve uyarma" proaktifliğine sahiptir.

---

7. GITHUB LİNKİ

https://github.com/Naxyay/22040101051_gorsel