CS401 - FİNAL PROJESİ

KÜRESEL SİBER GÜVENLİK ETKİNLİKLERİ İÇİN BÜTÜNLEŞİK TAKİP PLATFORMU

Kapsamlı Teknik Mimari, Veri Normalizasyonu ve Güvenlik Araştırması

MEVCUT DURUM: VERİ ENTROPİSİ

DAĞINIK EKOSİSTEM

Siber güvenlikte bilgi üretimi merkeziyetsizdir. Bir araştırmacının takip etmesi gereken kaynaklar:

> **CTFtime:** Yarışmalar için standart ama yetersiz API.

> **Konferanslar (BlackHat/DEFCON):** Kapalı devre mobil uygulamalar.

> **Topluluk (Discord/Twitter):** Standart dışı, kaybolan veriler.

Sonuç: "Information Noise" (Bilgi Gürültüsü) ve kaçırılan fırsatlar.

ÇÖZÜM: EVENT INTELLİGENCE

MERKEZİ VE AKILLI YÖNETİM

Siber güvenlik etkinlik verilerini bir "Tehdit İstihbaratı" verisi gibi işleyen mimari.

- **Çok Modlu Toplama:** REST API, GraphQL, XML Feed ve Web Scraping.
- **Semantik Analiz:** NLP ile otomatik içerik etiketleme (Örn: "Heap Spraying" -> "Exploit Dev").
- **Güvenli Entegrasyon:** "Security by Design" prensibiyle veri işleme.

VERİ KAYNAKLARI MİMARİSİ

1. CTFTİME (API)

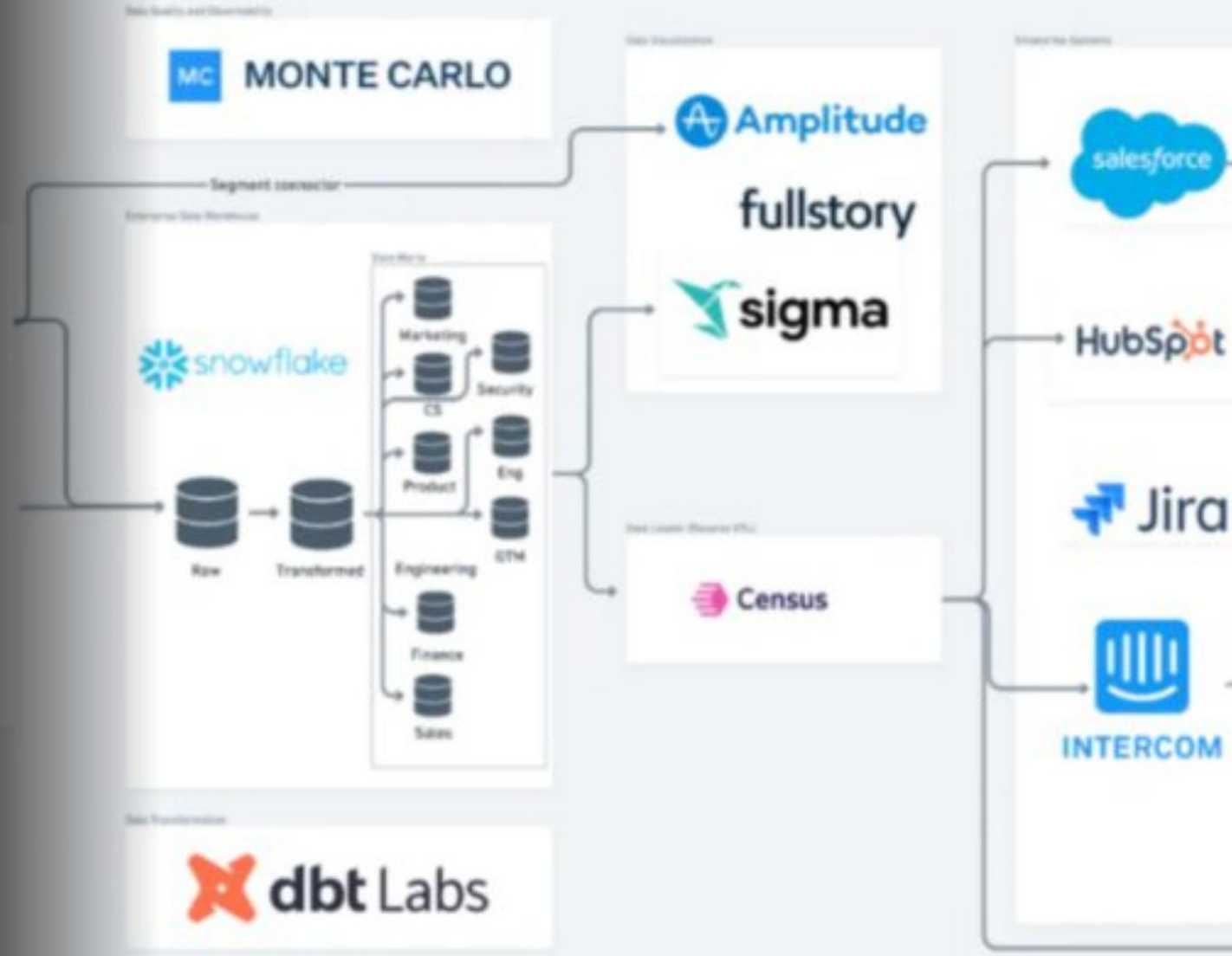
Artımlı çekme (Incremental Fetching) ve Redis önbellekleme ile API limitlerine uyum.

2. AÇIK KAYNAK (XML)

Frab ve Pentabarf kullanan topluluk etkinlikleri için özel XML ayrıştırıcılar.

3. KAPALI DEVRE (MOBİLE)

BlackHat/DEFCON için mobil uygulama trafiği analizi (Traffic Interception) ve tersine mühendislik.



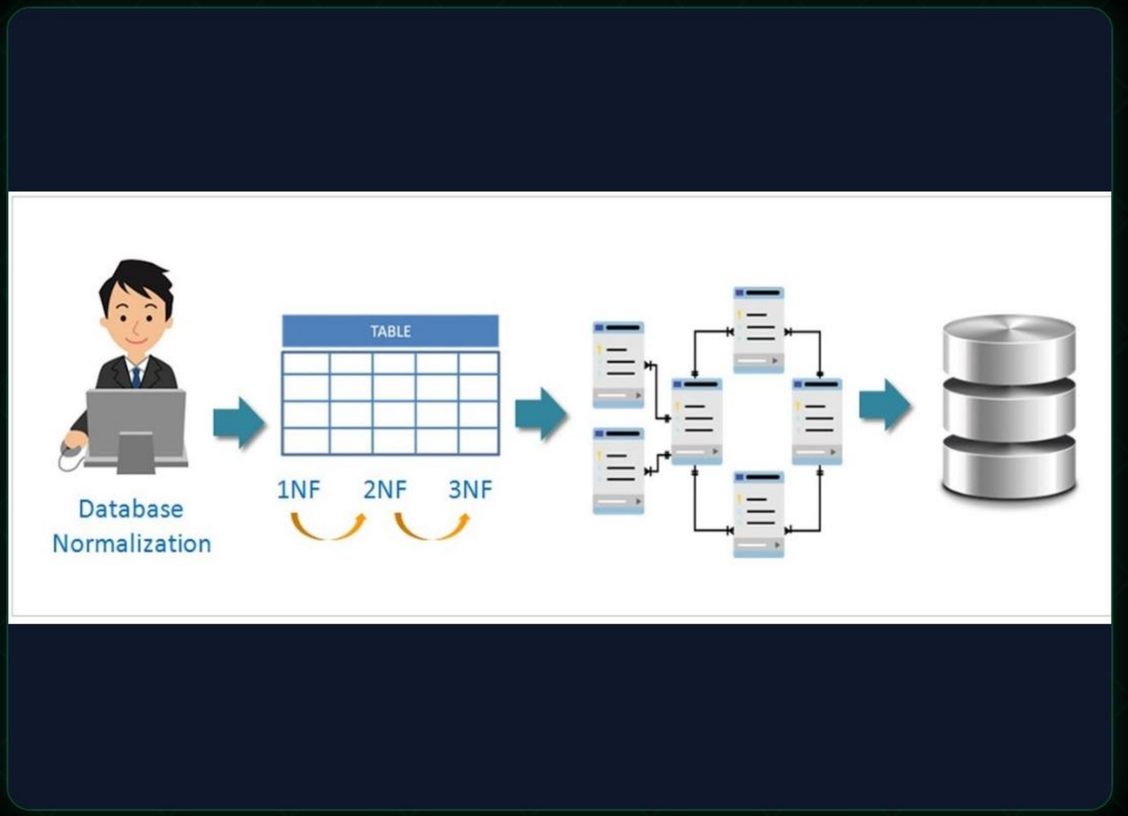
BİRLEŞİK ETKİNLİK MODELİ (UNİFİED SCHEMA)

HETEROJEN VERİDEN STANDARTA

Tüm kaynaklar ortak bir veritabanı şemasına dönüştürülür.

- **EventSeries:** Etkinliğin üst kimliği (Örn: DEFCON).
- **EventInstance:** Belirli bir yılın etkinliği (Örn: DEFCON 33).
- **Session:** En küçük yapı taşı (Konuşma, Challenge).

Timezone Engineering: Tüm veriler veritabanında UTC saklanır, kullanıcı arayüzünde yerel saate dinamik çevrilir.



TEKNİK ALTYAPI

PYTHON & GO

Veri işleme ve parsing için zengin kütüphaneleriyle Python; yüksek eşzamanlılık (concurrency) gerektiren crawler servisleri için Go.

POSTGRESQL

İlişkisel veriler için sağlam yapı. JSONB desteği sayesinde şemasız (schema-less) CTF skor verilerini esnek tutabilme yeteneği.

REDİS

API yanıtlarını önbellekleme (Caching) ve Celery iş kuyrukları (Task Queues) için yüksek performanslı broker.

GÜVENLİK MİMARİSİ: XXE KORUMASI

XML EXTERNAL ENTİTY (XXE) RİSKİ

Konferans verileri (Frab/Pentabarf) XML formatındadır. Saldırganlar zararlı XML ile sunucu dosyalarını okuyabilir (/etc/passwd).

SAVUNMA STRATEJİSİ

- **Kütüphane:** Standart parserlar yerine `defusedxml` kullanımı.
- **Konfigürasyon:** Entity expansion ve DTD (Document Type Definition) erişiminin çekirdek seviyesinde bloklanması.
- **Limitler:** "Billion Laughs" (XML Bomb) saldırılarına karşı derinlik limitleri.

AĞ VE İÇERİK GÜVENLİĞİ

SSRF (SERVER-SİDE REQUEST FORGERY)

Kullanıcı tanımlı URL'lerden veri çekerken sunucuyu koruma.

- **DNS Rebinding:** İstek atılmadan önce IP kontrolü.
- **Blacklist:** Localhost (127.0.0.1) ve Cloud Metadata (169.254.169.254) bloklaması.
- **İzolasyon:** Fetcher servislerinin izole VLAN/Container içinde çalışması.

İCALENDAR INJECTİON

Takvim dosyaları üzerinden yapılabilecek saldırılar.

- **Sanitasyon:** DESCRIPTION alanlarındaki HTML/Link temizliği (Bleach kütüphanesi).
- **Kısıtlama:** VALARM (Alarm) ve ATTACH özelliklerinin tamamen devre dışı bırakılması.
- **Prompt Injection:** AI modellerine giden verinin izole edilmesi.

KULLANICI DENEYİMİ

AKILLI FİLTRELEME

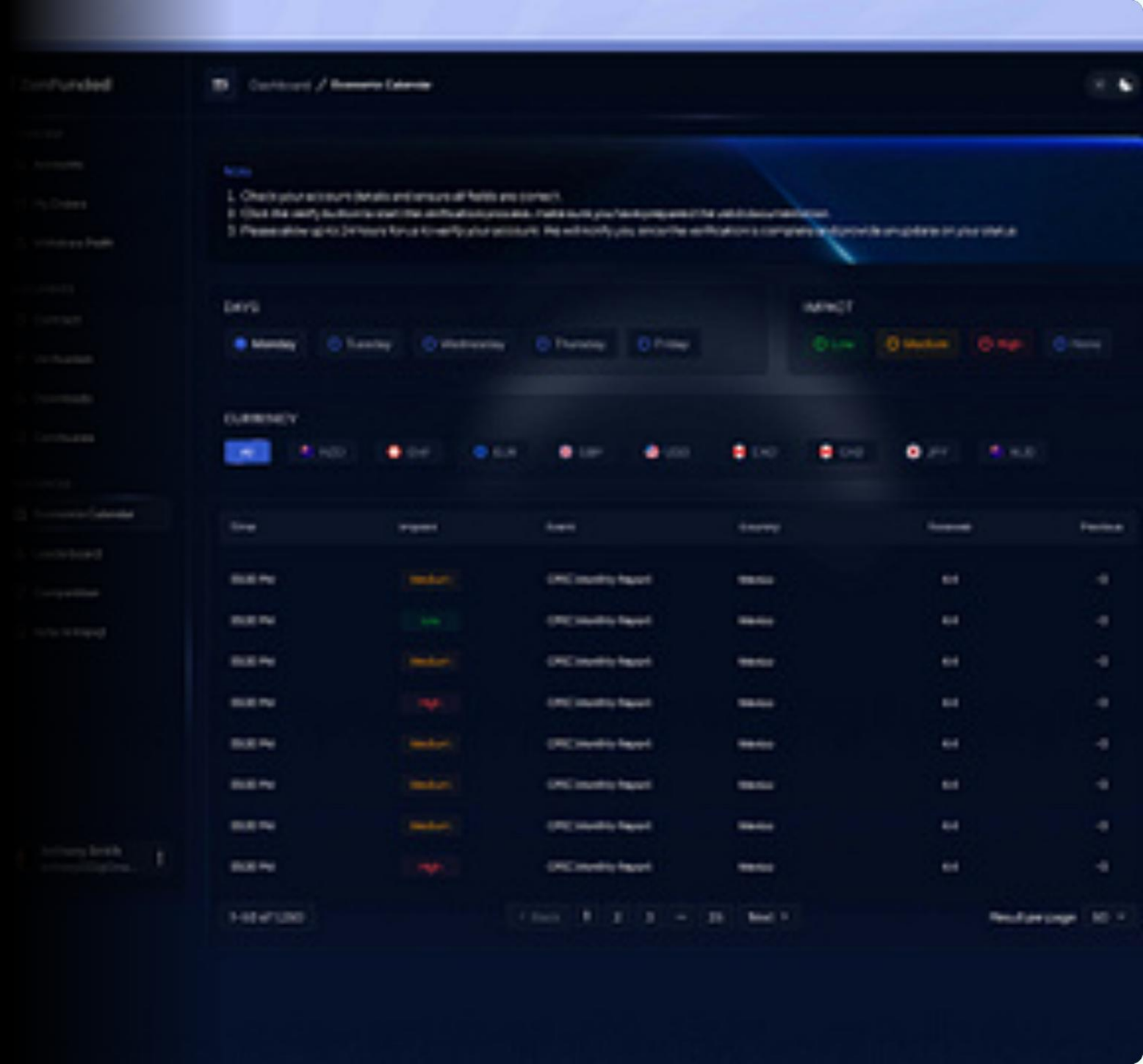
Boolean mantığıyla çalışan filtreler (Örn: `category:web AND difficulty:medium`).

DİNAMİK TAKVİM (SUBSCRİPTİON)

Kullanıcıların Google/Outlook takvimlerine entegre olabilen, arka planda güncellenen dinamik .ics beslemesi.

GAMİFİKASYON

Kişisel CTF skor tabloları ve otomatik Write-up arşivi oluşturma.



GELECEK VİZYONU

Bu platform, siber güvenlik profesyonellerinin "Information Noise" içinde kaybolmasını önleyen stratejik bir merkezdir. Gelecekte AI ajanlarının da veri tüketebileceği standartlara (JSON-LD) hazır, ölçeklenebilir bir istihbarat altyapısı sunar.

?

SORU & CEVAP

Dinlediğiniz için teşekkürler.

IMAGE SOURCES

https://plus.unsplash.com/premium_photo-1764691235091-ded85505e95b?fm=jpg&q=60&w=3000&ixlib=rb-4.1.0&ixid=M3wxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8fA%3D%3D

Source: unsplash.com

https://visiblenetworklabs.com/wp-content/uploads/2023/06/Hub-and-Spoke-Networks.png

Source: visiblenetworklabs.com

https://www.montecarlodata.com/wp-content/uploads/2023/07/Data-Pipeline-Architecture-Drata-1024x547.jpg

Source: www.montecarlodata.com

https://editor.analyticsvidhya.com/uploads/55956normalization.jpg

Source: www.analyticsvidhya.com

https://cdn.dribbble.com/userupload/45086102/file/838650b74c53ebb5eeed62269fa148e0.jpg?resize=400x0

Source: dribbble.com

https://png.pngtree.com/background/20250128/original/pngtree-abstract-blue-digital-network-connection-background-futuristic-technology-concept-picture-image_15972138.jpg

Source: pngtree.com