

Siber-Fiziksel Güvenlik Yakınsaması

SOC Ekipleri İçin Vultureye Çözümü

SIEM Dijital Dünyayı Biliyor. Peki Fiziksel Dünyada Neler Oluyor?

SIEM dijital dünyada ne olduğunu bilir. Vultureye fiziksel dünyada ne olduğunu söyler. Birlikte SOC olayın tamamını görür.

DIJİTAL TELEMETRİ



DATA FLOW ACTIVE
VULNERABILITY 1.5 TERA
STATUS NORMAL



DATA FLOW ACTIVE
VULNERABILITY 1.5 TERA
STATUS NORMAL



DATA FLOW ACTIVE
VULNERABILITY 1.5 TERA
STATUS NORMAL



DATA FLOW ACTIVE
VULNERABILITY 1.5 TERA
STATUS NORMAL

SIEM

FİZİKSEL GERÇEKLİK



SIEM dijital dünyada ne olduğunu bilir.
Vultureye fiziksel dünyada ne olduğunu söyler.
Birlikte SOC olayın tamamını görür.

COMPLETE VISIBILITY ACHIEVED
UNIFIED SOC VIEW: 100%

Güvenlik Üçgenini Birleştiriyoruz: IT, OT ve Fiziksel Telemetri

Vultureye, SIEM'in yerine geçmez; ona fiziksel dünya ve OT bağlamı sağlayan bir telemetri katmanı olarak konumlanır.



IT Telemetrisi

Firewall, VPN,
Sunucu Logları, AD

OT / Altyapı

SNMP, UPS Alarmları, Redfish,
Çevresel Sensörler, Yangın

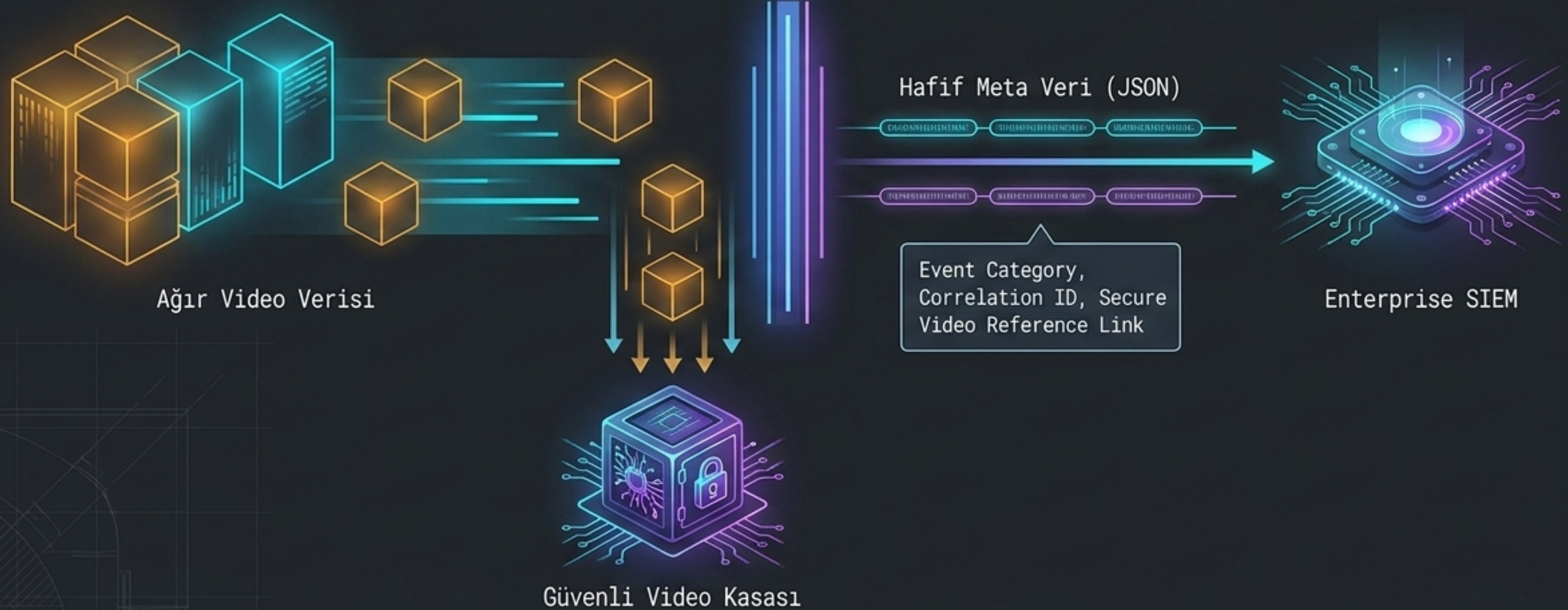
Fiziksel Telemetri

Erişim Kontrolü, Duress/Panic,
Tailgating, Yüz Analitiği, Tamper

Ağırlık Yapmayan Bağlam: Videodan Ziyade Meta Veri

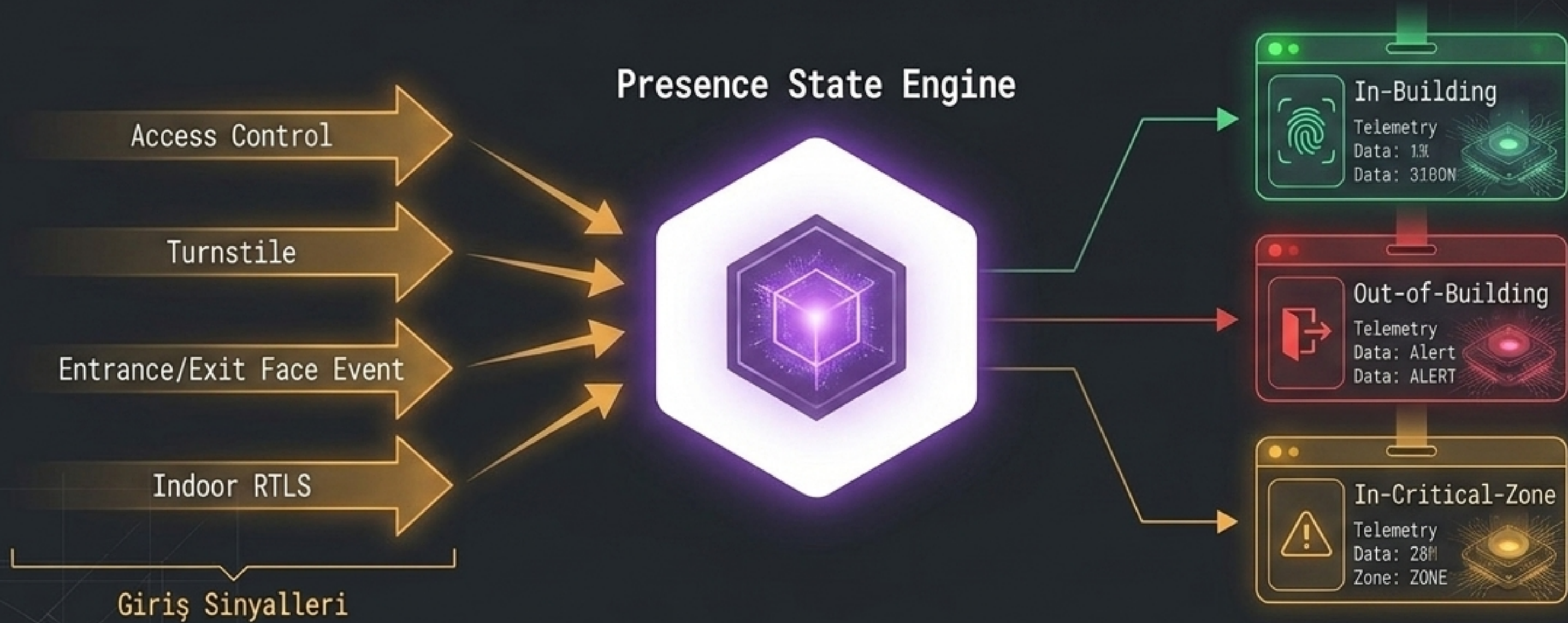
SIEM'e sürekli video stream göndermek doğru mimari değildir. Video OmniStor'da kalır. SIEM yalnızca güvenli referans (deep-link/API identifier) taşır.

Vultureye / OmniStor Filtresi



Fiziksel Varlık ve Dijital Kimlik Motoru (Presence State Engine)

Dijital hesap etkinliklerinin fiziksel gerçeklikle sürekli doğrulanması.



[⚠️] Kritik korelasyonlarda tek başına yüz analitiği yerine, geçiş kontrolü ve diğer fiziksel sinyallerle çoklu doğrulama tercih edilir.

Korelasyon Kuralı 1: İmkansız Kimlik Uyuşmazlığı

The Ghost Login



Korelasyon Kuralı 2: Siber Olaylara Yol Açan Fiziksel İhlaller

Zaman Çizelgesi: Sunucu Odası İhlali

Olay 1: Tailgating Tespiti



OMNIA AI, sunucu odası kapısında yetkisiz giriş saptadı.

Olay 2: Fiziksel Hareket (Duress)



Vultureye bölge içinde şüpheli hareket ve ihlal kaydetti.

Olay 3: Ağ Kesintisi / Yetkili Giriş



SIEM, sunucu odasından fiziksel bir kablo çekildiğini veya lokal admin girişi yapıldığını tespit etti.

KRİTİK UYARI: Insider Threat / Fiziksel Sızma



Tekil alarmlar göz ardı edilebilir. Birleştirilmiş sinyaller anında SOC müdahalesi gerektirir.



Korelasyon Kuralı 3: Dijital Sızmaları Gizleyen Fiziksel Saldırılar

Fiziksel Panel (Vultureye) ve Siber Panel (SIEM) Entegrasyonu



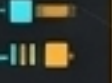
Edge Verilerini SOC Merkezine Taşıyoruz: OT ve Altyapı Telemetrisi

Vultureye Node Entegrasyonu

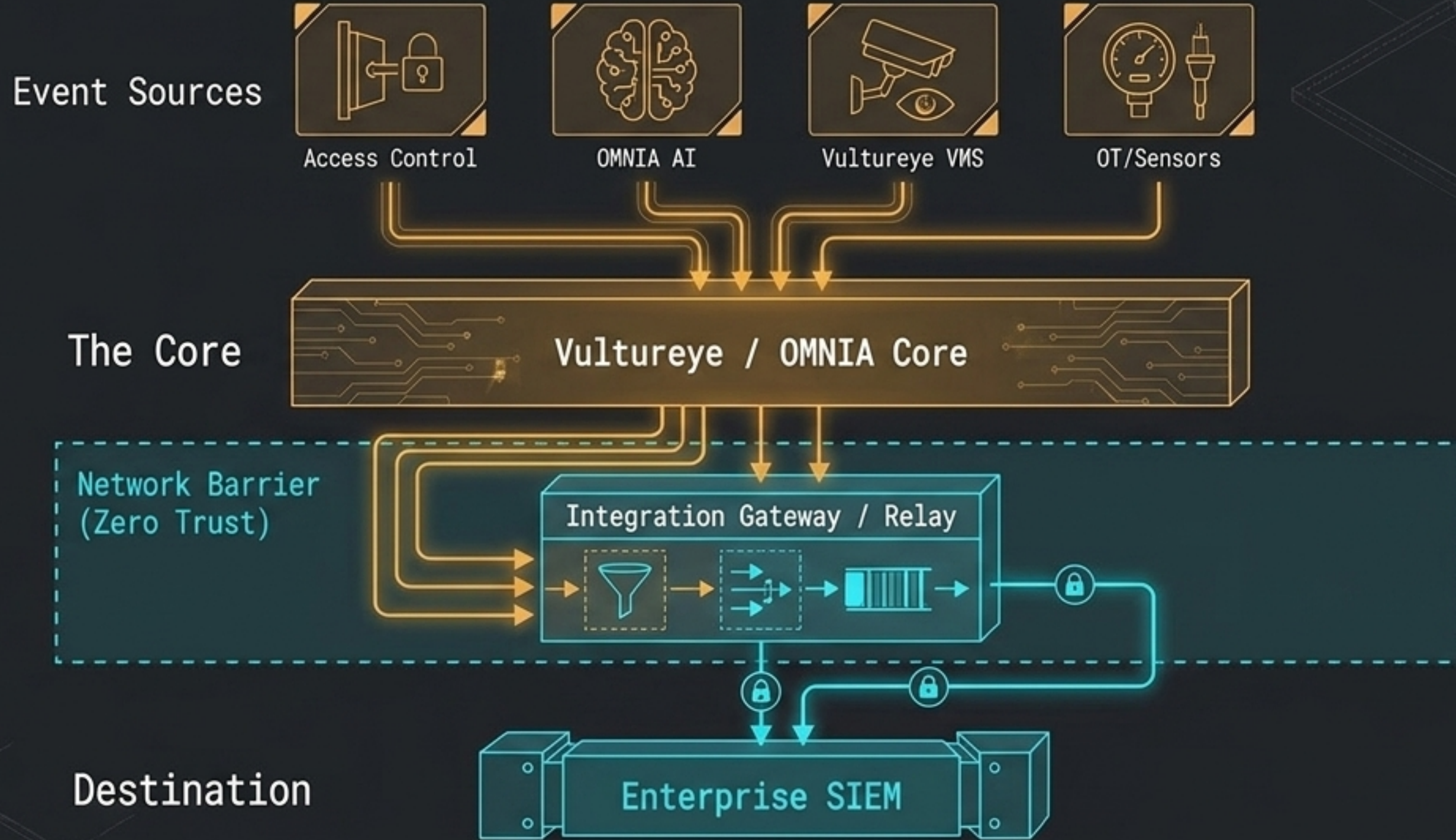


Yalıtılmış Gerçekliğe Karşı Birleşik Operasyon Merkezi

Fiziksel ve Dijital Dünyaların Birleşimi ile İleri Tehdit Tespiti

Boyut	Geleneksel SOC (Siloed)	Vultureye & OMNIA (Converged) 
Görünürlük	SIEM yalnızca IT olaylarını görür.	Access, Face ve RTLS ile fiziksel bağlam eklenir.
Kimlik Kontrolü	Kişi tesiste değilken hesabı kullanıldığında fark edilmez.	Fiziksel varlık ile dijital kimlik anında korele edilir.
Saldırı Tespiti	VMS brute-force ve kamera sabotajları SOC'ta görünmez.	Vultureye Auth olayları ve sabotaj alarmları doğrudan SIEM'e akar.
Kayıt Güvenliği	Hassas video export işlemleri audit edilemez.	Export ve konfigürasyon değişiklikleri SIEM'de denetlenir.

Güvenli ve Ölçeklenebilir Entegrasyon Mimarisi



Zero Trust prensipleri gereği network segmentasyonu sağlanır. Integration Gateway, sistemler arası güvenli ve kontrollü bir köprü görevi görür.

Modern SOC Platformlarının Ortak Dili

Desteklenen Protokoller

Syslog TLS (RFC 5425)

JSON

REST API (HTTPS)

Webhook

CEF

Normalized Event Schema Örneği

```
{  
  "timestamp": "2023-10-24T18:15:00Z",  
  "event_type": "tailgating",  
  "user_id": "usr_8921",  
  "source_ip": "192.168.10.55",  
  "confidence": 98,  
  "media_reference": "vlt://vault-id/882a"  
}
```

Farklı fiziksel ve OT kaynakları ortak bir şemaya (Normalized Event Schema) dönüştürülür.
Kritik üretim sistemlerinde güvenilir veri aktarımı için TCP/TLS tercih edilir.

Güvenilirlik ve Veri Bütünlüğü: NTP ve Store-and-Forward

1. NTP Senkronizasyonu



Siber-fiziksel korelasyonların doğruluğu için güvenilir ortak zaman kaynağı zorunludur.

2. Store-and-Forward Mekanizması



Geçici ağ veya SIEM kesintilerinde kritik fiziksel olay kayıplarını önler.

Birleşik SOC Panosu ve SOAR Otomasyonu



Siber-Fiziksel Tehdit Avcılığı Döngüsü

