SOC AI

YAPAY ZEKA DESTEKLİ HİBRİT SALDIRI TESPİT SİSTEMİ

Gerçek zamanlı ağ izleme, hibrit tespit ve AI destekli SOC analizi.

Zeek tabanlı ağ görünürlüğü, XGBoost davranış modeli, Suricata imza motoru, davranışsal aggregator ve tehdit istihbaratı entegrasyonları tek bir profesyonel IDS platformunda birleştirilmiştir.

98.94%
Model Accuracy

96.72%
Macro F1 Score

31
Özel Suricata Kuralı

3
Threat Intel Entegrasyonu

01 / KONUMLANDIRMA

Akademik Modelden Operasyonel IDS Platformuna

Bu proje yalnızca bir sınıflandırma modeli değildir. Ağdan veri toplayan, modeli canlı sistemde çalıştıran, imza tabanlı tespitle modelin sınırlarını tamamlayan, tekrar eden davranışları korele eden ve SOC analistine karar desteği sunan bütünleşik bir hibrit IDS prototipidir.

> **Flow tabanlı ML davranışı öğrenir; Suricata içerik ve imza seviyesini tamamlar; aggregator tekrarlı bağlantıları anlamlı saldırı olayına dönüştürür.**

Gerçek zamanlı görünürlük

Zeek sensörü bağlantı, DNS, HTTP, SSL ve anomali loglarını izleyerek canlı IDS motoruna ağ davranışı sağlar.

Çok katmanlı tespit

XGBoost modeli, Suricata imzaları, risk skoru, sanity filter, deduplication ve aggregator birlikte çalışır.

SOC odaklı çıktı

Alarm yönetimi, IP istihbaratı, AI analiz, Raw/Packet View, Zeek flow eşleşmesi ve PDF raporlama sunulur.

Neden hibrit mimari?

Flow tabanlı ML bağlantı süresi, paket sayısı, bayt oranı, servis, bağlantı durumu ve yanıt varlığı gibi davranışsal sinyalleri güçlü biçimde kullanır. Ancak HTTP payload içeriği, exploit imzası, SQLi/XSS kalıbı veya saldırı aracına ait özel izler gibi içerik seviyesindeki kanıtları doğrudan göremez. Suricata bu sınırı tamamlayan imza ve payload katmanı olarak mimariye eklenmiştir.

Model rolü
Akış davranışından olasılıksal sınıflandırma.

Suricata rolü
Payload ve bilinen saldırı imzalarını yakalama.

Aggregator rolü
Tekrarlı denemeleri saldırı olayına dönüştürme.

Dashboard rolü
Kanıtı analiste anlaşılır ve raporlanabilir sunma.

02 / SİSTEM MİMARİSİ

Uçtan Uca Çalışan Hibrit IDS Akışı

Sistem, sensör katmanından dashboard katmanına kadar modüler tasarlanmıştır. Her katman tek başına değil, birbirinin eksiklerini tamamlayacak şekilde konumlandırılmıştır.

1. Sensör Katmanı

Zeek conn/dns/http/ssl/weird logları
Suricata eve.json
Canlı trafik gözlemi

→

2. Tespit Katmanı

XGBoost davranış modeli
Suricata kural korelasyonu
Brute-force aggregator
Risk skorlama

→

3. SOC Katmanı

Alarm ekranı
Threat intelligence
AI analiz
Raw Packet View
PDF raporlama

01 Veri toplama

Zeek ve Suricata canlı trafik kanıtlarını üretir.

02 Feature çıkarımı

Akışlar eğitimdeki feature yapısıyla uyumlu vektöre dönüşür.

03 ML tahmini

XGBoost model sınıf olasılıkları üretir.

04 Korelasyon

Suricata, aggregator ve sanity filter alarmı zenginleştirir.

05 Analist çıktısı

Dashboard alarmı, risk ve AI yorumu ile sunar.

Alarm zenginleştirme

MITRE eşleştirme

Alarm tipi ATT&CK teknikleriyle ilişkilendirilir ve analistin olay dilini standartlaştırır.

Risk skoru

ML confidence, Suricata eşleşmesi ve kaynak bilgisi birlikte değerlendirilir.

Kanıt bağlamı

Zeek flow, matched rule, detection source ve raw JSON birlikte saklanır.

03 / MAKİNE ÖĞRENMESİ MODELİ

XGBoost Tabanlı Davranış Analizi Motoru

Model, ağ akışlarının davranışsal özelliklerini kullanarak normal trafik ve saldırı davranışlarını olasılıksal olarak ayırt eder. Modelin amacı payload okumak değil, akış seviyesindeki örüntüleri öğrenmektir.

98.94%	96.72%	98.96%	434
Accuracy	**Macro F1**	**Weighted F1**	**Best Iteration**
Test seti	Sınıf dengesi	Genel performans	Early stopping

Eğitim stratejisi

- Model: XGBoost Classifier, multi:softprob objective.
- Veri ayrımı: 147,724 train, 31,662 validation, 31,657 test.
- IP, timestamp, src_port ve label gibi ezberletici alanlar çıkarılarak data leakage riski azaltıldı.
- MITM, scanning, XSS ve injection için öncelik ağırlıkları tanımlandı.

Feature engineering

- **is_empty_flow:** boş/cevapsız akış ayrımı.
- **has_response:** hedef yanıt davranışı.
- **bytes_per_pkt:** veri yoğunluğu.
- **byte_ratio / pkt_ratio:** kaynak-hedef asimetrisi.
- **proto / service / conn_state:** protokol ve bağlantı bağlamı.

Mevcut operasyonel odak: Canlı demo aşamasında özellikle port scanning, brute-force, DoS ve SQLi/XSS gibi web saldırıları öne çıkarılmıştır. MITM, DDoS, backdoor ve ransomware sınıfları araştırma/geliştirme alanı olarak tutulmuş; daha geniş gerçek trafikle gelecekte iyileştirilmesi planlanmıştır.

Eğitimden canlı sisteme aktarım

01 Temizleme
Leakage riski taşıyan alanlar çıkarıldı.

02 Feature
Akış davranışını temsil eden yeni özellikler üretildi.

03 Eğitim
XGBoost model validation set ile erken durduruldu.

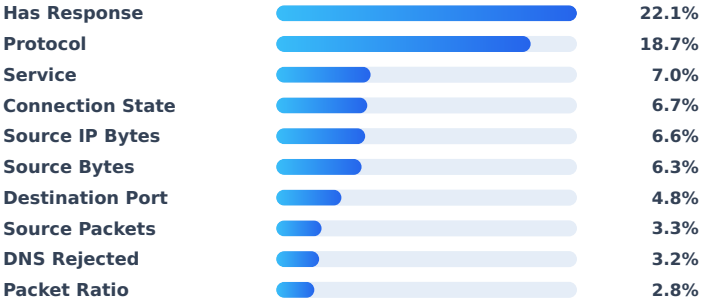
04 Artefakt
Model, encoder ve feature listesi kaydedildi.

05 Canlı IDS
Aynı feature şemasıyla gerçek trafik işlendi.

Performans ve Açıklanabilirlik

Model değerlendirmesinde yalnızca toplam doğruluk değil, sınıf bazlı precision/recall, confusion matrix ve feature importance analizleri de üretilmiştir. Bu yaklaşım modelin hangi sinyallere dayandığını ve hangi sınıflarda sınırları olduğunu göstermeye yardımcı olur.

En etkili özellikler



Sınıf bazlı precision / recall

Sınıf	Precision	Recall
Normal	99.7%	99.7%
Port Scanning	98.3%	99.5%
Brute Force	99.5%	99.1%
DoS	99.6%	98.0%
Injection	98.5%	96.7%
XSS	97.1%	98.9%
MITM	68.2%	87.3%
DDoS	98.8%	98.1%
Backdoor	100.0%	99.9%
Ransomware	100.0%	99.9%

Açıklanabilirlik yorumu: Feature importance sonuçları modelin bağlantı yanıtı, protokol, servis, bağlantı durumu, paket/bayt yoğunluğu gibi flow seviyesindeki sinyallerden beslendiğini göstermektedir. Bu nedenle model davranışsal tespitlerde güçlüdür; içerik/payload bağımlı web saldırılarında ise Suricata katmanı bilinçli olarak tamamlayıcı biçimde kullanılmıştır.

Model sınırı

Payload içeriği doğrudan görülmediği için SQLi/XSS gibi saldırılar imza katmanıyla desteklenir.

Canlı uyumluluk

Eğitimde üretilen model, encoder ve feature listesi canlı IDS motoruna aktarılmıştır.

Analiz çıktıları

Feature importance, confusion matrix, probability analysis ve örnek top-3 tahminler üretilmiştir.

Bu analiz neden önemli?

Güven
Yüksek metrikler karar desteği sağlar.

Sınır
Düşük/karışan sınıflar mimariyle desteklenir.

Açıklama
Feature importance model davranışını görünür kılar.

İyileştirme
Confusion çıktıları yol haritasını belirler.

ML, Suricata ve Aggregator Neyi Neden Yapar?

Sistemin profesyonel tarafı, her saldırıyı tek yöntemle yakalamaya çalışmamasıdır. Her katman kendi güçlü olduğu veri seviyesinde çalışır ve sonuçlar tek alarm modelinde birleştirilir.

Flow tabanlı ML	Port tarama, brute-force eğilimi, DoS davranışı ve genel ağ anomalilerinde bağlantı davranışını yorumlar. Payload okumadan akış örüntülerinden karar verir.
Suricata	SQL injection, XSS, command injection, LFI/RFI, web fuzzing ve bilinen exploit kalıpları gibi içerik/payload seviyesinde görülen tehditleri yakalar. Bu katman flow tabanlı modelin doğal sınırlarını kapatır.
Aggregator	Tekil akışta zayıf olan fakat kısa sürede tekrarlandığında saldırı davranışı oluşturan olayları korele eder. Brute-force için hızlı ve tekrarlı kimlik doğrulama denemelerini anlamlı bir güvenlik olayına dönüştürür.
Risk skoru	ML ve Suricata aynı olayı desteklediğinde risk yükselir. Böylece analist çok kaynaklı kanıta sahip olayları öncelikli inceler.

Suricata özel kural kapsamı

Sql Injection · Xss · Web Fuzzing · Command Injection & Lfi · Brute Force

SQLi
UNION, boolean, time-based ve schema enumeration kalıpları.

XSS
script tag, javascript URI ve event handler sinyalleri.

Brute-force
Kısa sürede tekrar eden auth denemeleri.

Web fuzzing
Tarama ve keşif amaçlı yoğun HTTP denemeleri.

Hibrit karar mantığı

ML sinyali
Akışın davranışsal sınıf olasılığı alınır.

İmza sinyali
Suricata eşleşmesi varsa kanıt güçlenir.

Tekrar sinyali
Aggregator kısa zaman penceresindeki denemeleri toplar.

Risk
Çok kaynaklı kanıt daha yüksek öncelik alır.

Analist
Dashboard olayı açıklama ve ham kanıtla sunar.

06 / ANALİST DENEYİMİ

SOC Dashboard ve Olay İnceleme Ekranı

Dashboard, canlı IDS çıktısını yalnızca listelemek yerine; alarm önceliklendirme, ilişkili olayları görme, IP istihbaratı, AI yorumlama, ham kanıt inceleme ve raporlama işlevleriyle analistin iş akışını hızlandırır.

Alarm Yönetimi

Severity, saldırı türü, kaynak/hedef IP, risk skoru ve zaman çizelgesiyle önceliklendirme.

Threat Intel

VirusTotal, AbuseIPDB ve Shodan ile şüpheli IP'nin dış kaynaklardan zenginleştirilmesi.

AI Analiz

Alarm geçmişi ve IP istihbaratıyla açıklama, risk, öneri ve MITRE ATT&CK eşleştirmesi.

Raporlama

Otomatik PDF rapor, metrikler, saldırı grafikleri ve olay özetleri.

Raw / Packet View

Alarm objesi, Zeek flow eşleşmesi, ilişkili alarmlar ve meta bilgiler yapılandırılmış JSON görünümüyle incelenebilir. Bu özellik analistin kanıt seviyesine inmesini sağlar.

Zeek flow eşleşmesi

Alarm zamanı, kaynak/hedef IP ve hedef port üzerinden conn.log satırı aranır. Eşleşen akış, alarm detay ekranında doğrudan gösterilir.

VirusTotal

Malicious/suspicious istatistikleri, reputation, ülke ve ASN bilgisi.

AbuseIPDB

Abuse confidence score, rapor sayısı, kullanım tipi ve ISP bağlamı.

Shodan

Açık portlar, host bilgisi, organizasyon, OS ve varsa CVE bilgileri.

Desteklenen Senaryolar, Katman Rolleri ve Gelişim Planı

Saldırı türleri farklı veri seviyelerinde görünür. SOC AI davranışsal, imza tabanlı ve korelasyon tabanlı tespiti birlikte kullanır; geliştirme planı ise şu an zayıf olan sınıfları daha fazla gerçek trafikle güçlendirmeye odaklanır.

Senaryo	Birincil Katman	Tamamlayıcı Katman	Neden Bu Yaklaşım?
Port Tarama	ML davranış modeli	Dashboard gruplama	Boş/cevapsız akışlar, servis ve port davranışı flow seviyesinde güçlü sinyal üretir.
Brute Force	Aggregator	ML + Suricata auth kuralları	Tekil deneme normal görünebilir; kısa sürede tekrarlandığında saldırı davranışına dönüşür.
DoS	ML davranış modeli	Risk skoru / stacking	Paket/bayt yoğunluğu ve trafik asimetrisi davranışsal olarak analiz edilir.
SQL Injection	Suricata	AI analiz + risk skoru	UNION SELECT, boolean tautology ve time-based payload gibi içerik kalıpları imzayla yakalanır.
XSS	Suricata	AI analiz + dashboard	script tag, javascript URI ve event handler gibi payload göstergeleri içerik seviyesinde tespit edilir.

Yol haritası: MITM, DDoS, backdoor ve ransomware sınıfları için daha geniş gerçek trafik verisi, gelişmiş korelasyon, payload analizinin genişletilmesi ve analist geri bildirimlerine dayalı aktif öğrenme planlanmaktadır.

Güçlü yön

Yüksek model metrikleri, imza motoru, aggregator ve dashboard ile operasyonel sisteme dönüştürülmüştür.

Operasyonel değer

Threat intel, AI analiz, otomatik rapor ve raw inceleme analistin karar sürecini hızlandırır.

Sonuç

Flow tabanlı ML'in sınırlarını bilen ve bu sınırları Suricata ile tamamlayan profesyonel IDS prototipi elde edilmiştir.