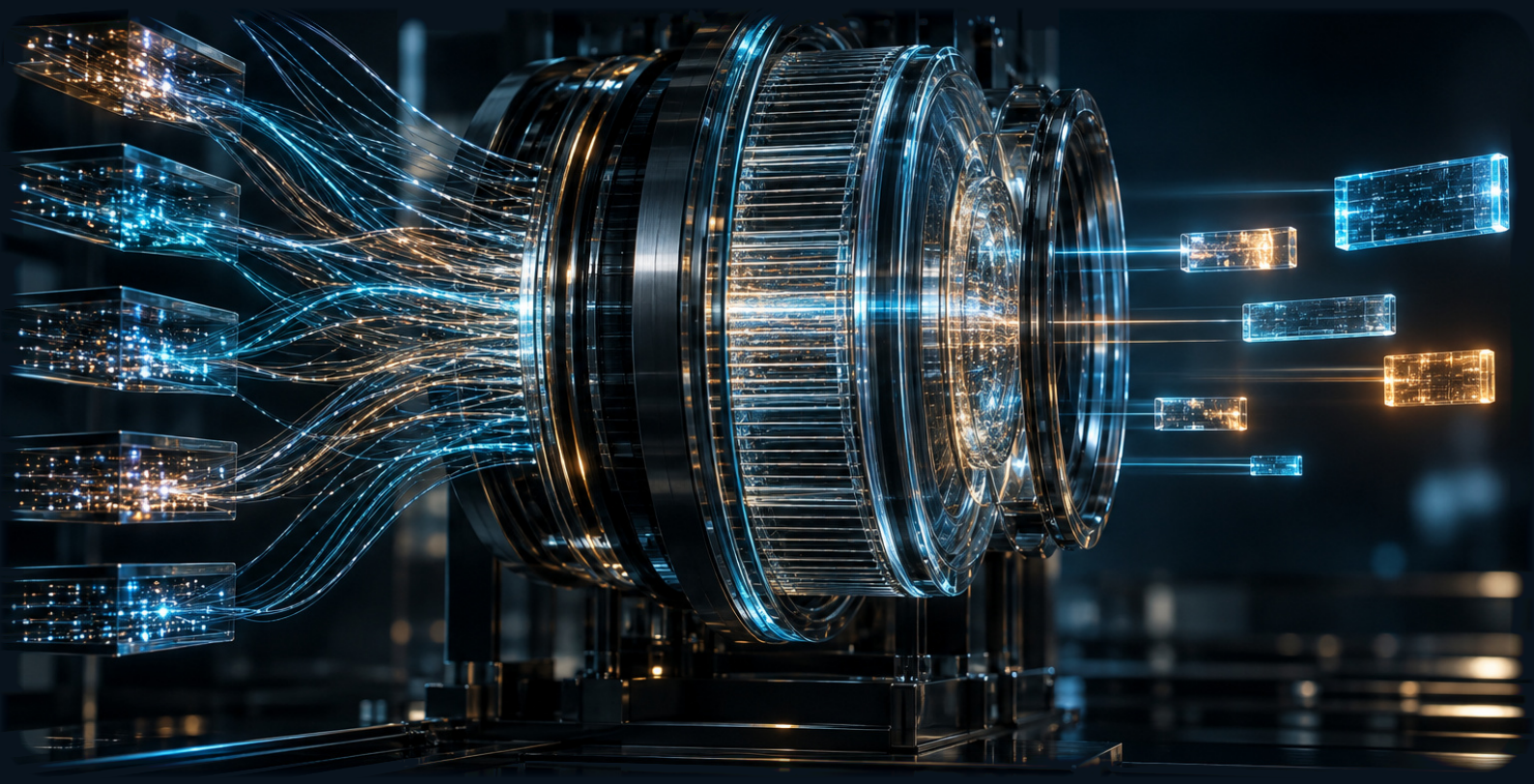
GNSAC

VIGIL

SİBER TEHDİT İSTİHBARATI / DİJİTAL RİSK İZLEME

Kurumunuzu hedef alan tehditleri görün.

Sızan hesaplardan marka taklidine; dış riskleri kaynağı, kanıtı ve müdahale adımlarıyla değerlendirin.



4,17 milyar
istihbarat kaydı

190+
alan adı kontrolü

24
alarm kategorisi

İstihbarat hacmi: 20.09.2026

DIŞ RİSKLERİ AYNI İNCELEMEDE BİRLEŞTİRİN

Kurumunuzun dijital izi. Tek bir çalışma alanı.

Vigil; hesap, marka, varlık ve tedarikçi risklerini ortak bir bulgu akışında toplar. Ekibiniz, hangi kaydın kurumu ilgilendirdiğini ve sonraki adımı aynı platformda değerlendirir.

01 Hesaplar
Sızmış kimlik bilgileri ve infostealer kayıtları.

02 Marka
Taklit adresler, sahte profiller ve görsel eşleşmeler.

03 Dijital varlıklar
Açık servisler, yapılandırmalar ve zafiyetler.

04 Tedarikçiler
İhlal, altyapı değişimi ve taklit riski.

05 Kritik kişiler
VIP kişilere özel maruziyet ve raporlama.

06 Ödeme kimlikleri
MID, TID, BIN ve ödeme paneli sızıntıları.

BİR BULGUYLA BAŞLAYAN İŞ AKIŞI

01 Eşleştir
Kuruma ait sinyali ayır.

02 İncele
Kaynağı ve kanıtı aç.

03 Önceliklendir
Önem ve bağlamı gör.

04 Takip et
Vakayı ve raporu yönet.

Dashboard, Findings ve Alarms ekranları; kaynak, önem, durum ve zaman bilgilerini aynı çalışma akışında sunar.

20 EYLÜL 2026 TARİHLİ ÜRÜN VERİLERİ

Büyük arşiv. Kuruma odaklı istihbarat.

Kayıtlar GNSAC'ın merkezî altyapısında toplanır. Müşteri kurulumu, kurumuyla ilgili istihbaratı senkronla alır; inceleme ve müdahale kendi çalışma alanında yürür.

93 milyon+

son 7 günde işlenen kayıt

- **3,49 milyar kimlik bilgisi kaydı**
- Diğer istihbarat kayıtları

1.754

kayıtlı istihbarat kaynağı

≈8.500

günlük yeni IOC kaydı

125.775

Tor üzerinden arşivlenmiş kanıt sayfası

61.587

zafiyet (CVE) kaydı

1,2 milyon+

phishing URL kaydı

3,49 milyar kimlik bilgisi kaydı, 4,17 milyarlık toplamın içindedir. Hacimler ürün dokümanındaki tarihli arşiv sayımlarıdır.

KAYNAKTAN KURUMA AİT KANITA

Sızan hesabın izini sürün.

Bir alan adı veya e-postayla sızıntı arşivini sorgulayın. Kimlik bilgilerini, infostealer kayıtlarını ve kurumunuzun geçtiği paylaşımları kaynağıyla inceleyin.

PASTE	TELEGRAM	RANSOMWARE	FORUM / GITHUB
5 dk	10 dk	15 dk	30 dk

Kaynağı görün

Alan adı ve e-posta indeksleriyle ilgili kayıtlara erişin.

Kanıtı inceleyin

Arşivlenmiş sızıntı sayfasını panel içinde izole açın.

Takibi sürdürün

Yeni bulguları, önem seviyesini ve alarm durumunu takip edin.

Üstteki süreler varsayılan kaynak tarama aralıklarıdır; uçtan uca bildirim süresi değildir. Görsel, eşleştirme akışını temsil eder.

DOĞRULANMIŞ ALAN ADINDAN AYRINTILI RAPORA

190’dan fazla kontrol. 12 fazda inceleme.

Alan adınızı DNS TXT kaydıyla doğrulayın. Keşif, maruziyet, ilişki ve risk analizlerini bir tarama hattında birleştirin; sonraki taramalarla karşılaştırılacak başlangıç kaydını oluşturun.

01 - 04

Keşif ve maruziyet

Kurum profili, varlık keşfi, yapılandırma, e-posta ve marka.

05 - 08

Tehdit ve bağımlılıklar

Sızıntı, zafiyet, aktör / MITRE ve üçüncü taraf ilişkileri.

09 - 12

Bağlantı ve öncelik

IOC / itibar, saldırı yolu, risk / iyileştirme ve rapor.

13 dakika

29 ölçülmüş taramada ortanca süre.
27 tarama yarım saatin altında tamamlandı.

Düzenli takip

Günlük, haftalık veya aylık tarama; alan adı bitişi ve TLS sertifikası için süre takibi.

Tarama süresi kapsam ve alan adına göre değişir. 13 dakika, 29 taramanın ortancasıdır; tamamlanma süresi garantisi değildir.

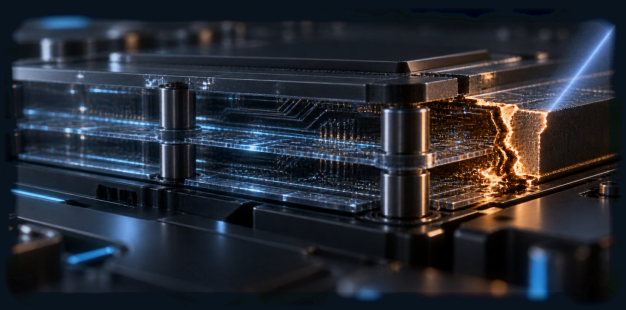
CİDDİYETİN YANINA SÖMÜRÜ BAĞLAMINI KOYUN

Hangi açığı önce ele almalısınız?

Zafiyeti teknik puanının yanında aktif sömürü, olasılık ve yayımlanmış exploit bilgisiyle değerlendirin. İlgili üretici ve ürün kaydını aynı incelemede görün.

61.587
CVE kaydı

149
KEV işaretli kayıt



CVSS

Teknik ciddiyet

Açığın teorik etkisini ve ciddiyetini değerlendirin.

EPSS

Sömürülme olasılığı

Önümüzdeki 30 güne ilişkin olasılık bilgisini inceleyin.

KEV

Aktif sömürü

CISA kataloğunda aktif sömürü bilgisi bulunan kayıtları ayırın.

EXPLOIT

Yayımlanmış yöntem

Kamuya açık exploit bulunup bulunmadığını görün.

TEDARİKÇİYLE EŞLEŞEN ZAFİYETLER İÇİN ALARM

Kritik, yüksek, KEV işaretli veya exploit'i yayımlanmış bir kayıt izlenen tedarikçiyi adlandırdığında ilgili alarm akışına girer.

CVE ve KEV adetleri: 20 Eylül 2026 tarihli ürün dokümanı. CVSS, EPSS ve KEV farklı değerlendirme boyutlarıdır.

MARKANIZIN KOPYALANAN İZLERİNİ İNCELEYİN

Benzer adresi bulun. Görsel taklidi yakalayın.

Vigil, marka taklidini alan adı, phishing, sosyal profil ve uygulama bulgularıyla birlikte değerlendirmenizi sağlar. Logo ve favicon karşılaştırmaları incelemeye somut dayanak ekler.

1,2 milyon+

phishing URL kaydı
20 Eylül 2026

Birebir dosya eşitliği ve algısal özet karşılaştırması; kopyalanmış veya yeniden boyutlandırılmış logo ve favicon dosyalarını ayırt etmeye yardımcı olur.

Benzer alan adı | Sahte sosyal profil | Mağaza uygulaması | Takedown vakası

Görsel, taklit karşılaştırmasını temsil eder. Sosyal platformların erişim kısıtları sonuç kapsamını etkileyebilir.

OLAYIN DURUMUNU VE ATILAN ADIMI KAYDEDİN

Tespiti, takip edilebilir müdahaleye dönüştürün.

Takedown Center; vakayı, ihbarı, yanıtı ve kanıtı tek süreçte tutar. İhbarın gönderilmiş sayılması, e-posta sunucusunun mesajı kabul etmesine bağlıdır.

01

Vaka ve iletişim

Hedefi kaydedin; registrar iletişim bilgisini ve kanıtı toplayın.

02

Onaylı ihbar

Kurumunuzun SMTP sunucusundan gönderin; gönderim durumunu izleyin.

03

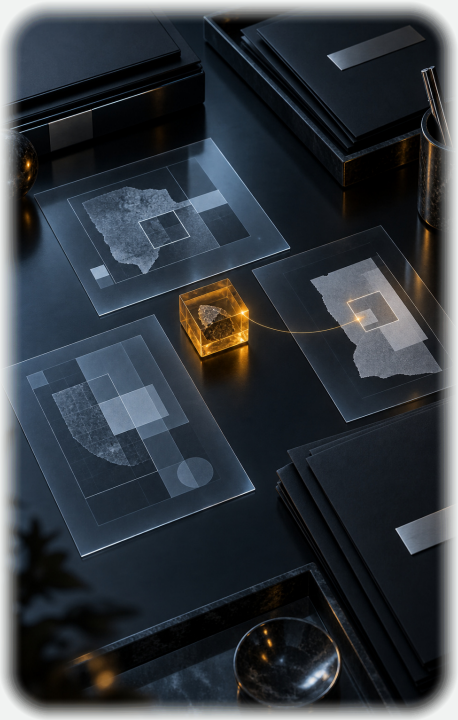
Yanıt ve eskalasyon

Karşı tarafın yanıtını kaydedin; gerekirse sonraki sağlayıcıya ilerleyin.

04

Kanıtlı kapanış

Kaldırma veya ret sonucunu notları ve kanıtlarıyla kapatın.



12 saat

sayfa kanıtını yeniden yakalama

7 gün

yanıtsız ihbar için takip

14 gün

eskalasyonda gecikme takibi

6 hazır playbook: hesap sızıntısı, phishing, VIP, marka, tedarikçi ihlali ve manuel inceleme. Ekibiniz kendi playbook'larını da oluşturabilir.

Süreler varsayılan takip ayarlarıdır. İhbar ve eskalasyon kullanıcı kararıdır; kaldırma kararı ilgili sağlayıcı veya platforma aittir.

İHLAL SİNYALLERİNDEN ALTYAPI DEĞİŞİMLERİNE

Tedarikçi riskini sekiz sinyalle izleyin.

Tedarikçiyi adı ve alan adıyla ekleyin. İzleyici önceki durumla karşılaştırma yapar; yeni olan değişimleri ve yeni maruziyetleri ilgili alarm kategorisine taşır.

01 **Ransomware kaydı**

02 **İhlal kaydı**

03 **İnfostealer bulgusu**

04 **Benzer alan adı**

05 **DNS değişikliği**

06 **Sertifika değişikliği**

07 **E-posta taklit riski**

08 **Tedarikçi zafiyeti**

30 dakika

Varsayılan izleme turu. Benzer alan adı ve sertifika şeffaflığı kontrolleri günlük çalışır.

Tedarikçi listesi müşteri kurulumunda tutulur. Günde bir kaydedilen durum kopyaları eğilim takibine temel olur.

KİŞİ VE ÖDEME KİMLİĞİNE ÖZEL İZLEME

Kritik kişileri ve ödeme kimliklerini izleyin.

Yönetici maruziyeti ve ödeme kimliği sızıntıları ayrı kapsamlarla izlenir. İlgili bulgular, kaynaklar ve bildirimler ekibinizin ortak çalışma alanına gelir.

VIP Protection

Yöneticiler ve kritik kişiler için e-posta temelli maruziyet taraması.

- Sızmış hesap ve infostealer kayıtları.
- Dark web izleri ve kamuya açık maruziyet bilgileri.
- Kişiye özel TR / EN PDF raporu.

POS & Payment

MID, TID, BIN ve ödeme paneli girişleri için sızıntı izlemesi.

- Ticari unvan ve anahtar kelime eşleşmeleri.
- Ödeme paneli girişleri ve geçmiş kayıt sorguları.
- Ödeme temalı taklit alan adları.

Varsayılan izleme: 30 dakika

VIP ve ödeme izleyicileri düzenli çalışır; manuel sorgu ve tarama seçenekleri ilgili incelemeyi destekler.

Ödeme modülü kart işlemlerini görmez veya durdurmaz; ödeme kimliklerinin ve girişlerinin sızıntısını izler.

KAYITLARIN ARASINDAKİ İLİŞKİYİ AÇIĞA ÇIKARIN

Bir bulgudan ilişkiler ağına.

Hangi hesabın hangi sızıntıda yer aldığını, alan adının hangi altyapıyla ilişkili olduğunu ve IOC'lerin kampanyalara nasıl bağlandığını görsel olarak inceleyin.

Kimlik bilgileri **Sızıntılar** **Tehdit aktörleri** **Alan adları** **IP / IOC** **Kampanyalar**

Kaydı açın

İlgili düğümden aktör veya olay ayrıntısına geçin; kaynağın bağlamını inceleyin.

Yerel olarak değerlendirin

Eğilim, anomali, risk ve güven değerlendirmelerini kurulum içindeki verilerle üretin.

Ağ kavramsal bir ilişki örneğidir; düğüm sayıları müşteri verisi değildir. Öngörüler mevcut bulgulardan türetilen değerlendirmelerdir.

BÖLGE BAĞLAMI VE DOSYA GÖSTERGELERİ

İncelemeyi ayrıntılandırın.

Bölgesel kaynakları, ilgili tehdit gruplarını ve sektörel dağılımı izleyin. Şüpheli dosyaları hash istihbaratı, YARA kuralları ve yerel statik analizle inceleyin.

TR **Türkiye**
USOM ve yerel kaynaklar

US **ABD**
CISA KEV, FBI / CISA duyuruları

UK **Birleşik Krallık**
NCSC kaynakları

CA **Kanada**
CCCS kaynakları

AU **Avustralya**
ACSC duyuruları

RU **Rusya**
Rusça forum ve kanal kaynakları

Hash sorgusu

VirusTotal ve MalwareBazaar kaynakları üzerinden motor kararları, dosya meta verisi, aile ve etiket bilgilerini inceleyin.

Yerel statik analiz ve YARA

Dosya türü, entropi, okunabilir metinler ve ağ göstergelerini değerlendirin; kurulu YARA kurallarıyla eşleştirin. Yüklenen dosya kurulum dışına çıkmaz ve saklanmaz.

6 ÜLKE İSTİHBARAT MODÜLÜ

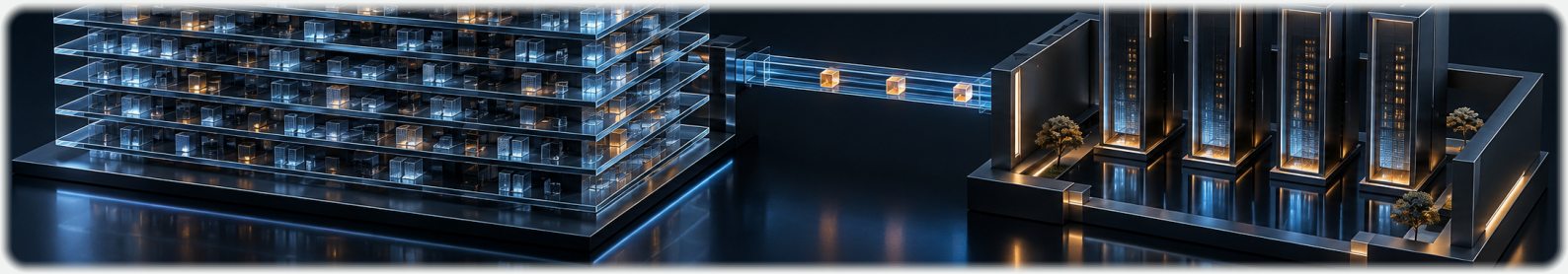
YARA EŞLEŞTİRME • ÇALIŞTIRMADAN İNCELEME

Statik inceleme dosyanın çalıştırıldığı bir sandbox hizmeti değildir. Bölgesel veri güncellemeleri ilgili kaynakların sıklığına bağlıdır.

MERKEZÎ TOPLAMA, MÜŞTERİYE AYRI KURULUM

İstihbarat merkezde. Analiz kurulumunuzda.

Kurumunuzla ilgili kayıtlar ayrı müşteri kurulumuna alınır. Yerel analiz motoru, veriyi dış yapay zekâ servislerine göndermeden eğilim ve korelasyon hesaplar.



GNSAC MERKEZİ

Toplama katmanı
Dark web, açık kaynaklar, forumlar

İstihbarat arşivi
Kimlik bilgisi, IOC, CVE, phishing

Kanıt arşivleme
Tor üzerinden sayfa kopyaları

MÜŞTERİ KURULUMU

Kuruma ait varlıklar
Alan adı, marka, VIP, tedarikçi

Bulgu ve alarm
Eşleştirme, önem, durum, kanıt

Analiz ve çıktı
Yerel analiz, playbook, rapor

Senkron ve sorgu

OLAYI EKİBİNİZİN KANALINA TAŞIYIN

Slack	Microsoft Teams	Jira	Webhook / SOAR	STIX / TAXII

Kurumsal SMTP ile e-posta; yönetici / görüntüleyici rol ayrımı; TOTP ile iki adımlı doğrulama. Ortak istihbarat, TAXII 2.1 üzerinden STIX 2.1 beslemesi olarak da sunulur.

Varsayılan merkez senkronu 15 dakikadır. Tor bağlantısı merkezde yürür; müşteri kurulumu sızıntı sitelerine doğrudan bağlanmaz.

NEYE BAKILACAĞINI, NE ZAMAN HABER VERİLECEĞİNİ SEÇİN

24 alarm kategorisi. Kurumunuza göre bildirim.

Her kategori için bildirim durumunu, en düşük önem seviyesini ve e-posta tercihini belirleyin. Kritik ve yüksek bulgular ürün içindeki alarm akışına yansır.

- Kimlik bilgileri 3
- Marka 7
- Varlıklar 2
- VIP 1
- Ödemeler 1
- Dark web 1
- Platform 1
- Tedarik zinciri 8

30 sn

yeni kayıtlar için alarm kontrol turu

9 besleme

tazelik denetimi

Tekrar eden aynı olay için bildirim gürültüsünü azaltan kontroller ve durmuş beslemeler için ayrı bulgular; izleme zincirinin durumunu da görünür kılar.

30 saniye, alarm izleyicisinin varsayılan kontrol aralığıdır; olayın ortaya çıkışından bildirime kadar geçen toplam süre değildir.

AYNI BULGUYU FARKLI KARAR İHTİYAÇLARINA TAŞIYIN

Yönetime özet. Teknik ekibe ayrıntı.

Altı rapor türünü Türkçe ve İngilizce PDF olarak üretin. İndirme, e-posta ve zamanlanmış teslimat seçenekleriyle raporu ilgili ekibe ulaştırın.

GNSAC VIGIL
Yönetici
Risk görünümü ve öncelikler
TR / EN

GNSAC VIGIL
Teknik
Bulgu ve inceleme ayrıntıları
TR / EN

GNSAC VIGIL
Uyum
Uyum / denetim incelemesi
TR / EN

GNSAC VIGIL
VIP
Kişiye özel maruziyet
TR / EN

GNSAC VIGIL
Tedarikçi
Tedarikçi istihbaratı
TR / EN

GNSAC VIGIL
Marka
Marka tehditleri ve bulgular
TR / EN

RAPOR TÜRLERİNİN ŞEMATİK GÖSTERİMİ

Dönemi sabitleyin

Rapor anındaki kimlik bilgisi, sızıntı, IOC, zafiyet ve marka tehdidi sayıları saklanır.

Değişimi karşılaştırın

Sonraki rapor önceki kaydedilmiş dönemle karşılaştırılır; ilk raporda başlangıç kapsamı belirtilir.

Executive, Technical, Compliance, VIP, Vendor ve Brand raporları; tek platform içinde farklı inceleme ihtiyaçlarını karşılar.

GNSAC

VIGIL

Kendi kurumunuzun riskleriyle değerlendirin.

Alan adınızdan başlayın. Sızıntıyı, marka tehdidini veya tedarikçi bulgusunu kaynağı ve kanıtıyla inceleyin.

01 Alan adını ekleyin ve doğrulayın.

02 Tarama ve izleme kapsamını tanımlayın.

03 Bulguyu inceleyip müdahale akışına taşıyın.

04 Sonucu raporlayın; sonraki dönemle karşılaştırın.

DEMO VE İLETİŞİM

GNSAC Bilişim Teknolojileri Ltd. Şti.

gnsac.com.tr

info@gnsac.com.tr

+90 216 706 40 65

support@gnsac.com.tr

WhatsApp +90 532 203 32 89

İSTANBUL OFİSİ

Şefikbey Sokak, Archerson Köşkü No:3
Oda No:301, Zühtüpaşa, Kadıköy
34724 İstanbul, Türkiye

DUBAİ OFİSİ

Levels 41 & 42, Emirates Towers
Sheikh Zayed Road, Dubai, BAE

Ürün kapsamı: 2026.08.24.279 / İstihbarat hacimleri: 20 Eylül 2026 tarihli GNSAC Vigil ürün dokümanı.