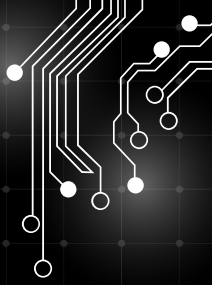


# OSINT 101

Açık Kaynak İstihbaratı





# OSINT 101

01

Nedir?

02

Kimler kullanır?

03

Araçlar

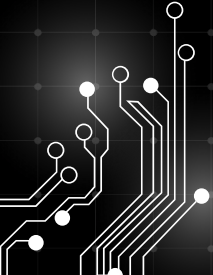


04

Kaynaklar

05

Yasal ve etik sınırlar

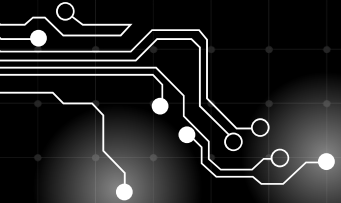




01

---

**OSINT NEDİR?**





# OSINT

(Open Source Intelligence)

**OSINT**, kamuya açık bilgi kaynaklarından elde edilen istihbarat verilerini ifade eder.

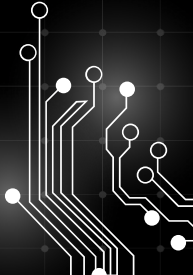
Bu tür veriler, genel kamuya açık olan kaynaklardan toplanan bilgilerdir ve genellikle internet, sosyal medya, haber siteleri, devlet raporları, akademik yayınlar ve diğer açık platformlar aracılığıyla elde edilir.



# OSINT'in Temel Özellikleri

- **Açık Kaynaklardan Elde Edilir:** Herkesin erişebileceği verilere dayanır.
- **Hızlı ve Etkin:** Geniş bir veri havuzundan hızla bilgi çekilebilir.
- **Yasal ve Etik:** Kamuya açık bilgilerin toplanması, yasal sınırlamalar içinde yapılır.
- **Veri Kaynakları:** Web siteleri, sosyal medya platformları, forumlar, bloglar, basın açıklamaları, haritalar ve coğrafi bilgi sistemleri gibi kaynaklar.

Özetle OSINT, internetteki halka açık bilgileri toplayıp analiz ederek anlamlı hale getirme sürecidir.

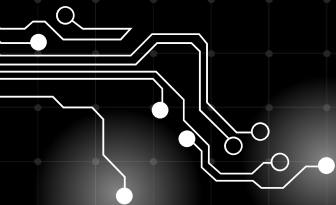




02

---

**KİM KULLANIR?**





OSINT, farklı disiplinlerden ve sektörlerden birçok profesyonel tarafından kullanılır:

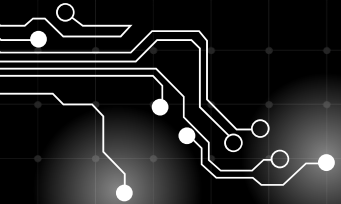
- **Siber Güvenlik Uzmanları:** Siber tehditleri tespit etmek, siber saldırıları önceden öngörmek ve güvenlik açıklarını kapatmak.
- **Ulusal Güvenlik Ajansları:** Terörizmi izlemek, devlet güvenliğini sağlamak, tehditleri analiz etmek.
- **Kolluk Kuvvetleri:** Dijital suçları araştırmak, kaybolan kişileri bulmak, suçluları izlemek.
- **Gazeteciler ve Araştırmacı Gazeteciler:** Kamuya açık verilerden haber doğrulamak, analiz yapmak, araştırma raporları hazırlamak.
- **Pazar Araştırmacıları:** Rakip analizleri yapmak, sektörel trendleri incelemek, iş dünyasında stratejik kararlar almak.
- **Bireysel Kullanıcılar:** Kişisel güvenliği artırmak, çevrimiçi tehditleri önceden tespit etmek, sosyal mühendislik saldırılarından korunmak.



03

---

# OSINT ARAÇLARI







# OSINT Araçları ve En Yaygın Kullanılan Yöntemler

Araçlar	İşlevi
<u>Maltego</u>	Veri bağlantılarını görselleştiren güçlü bir araçtır. IP adresleri, alan adları, e-posta adresleri gibi birçok kaynaktan bilgi toplar.
<u>Shodan</u>	İnternete bağlı cihazları aramak için kullanılır. Özellikle IoT cihazları ve açık portlar üzerinde araştırma yapılabilir.
<u>TheHarvester</u>	E-posta adresleri, alt alan adları ve IP adresleri toplamak için kullanılan açık kaynak bir araçtır.
<u>Spiderfoot</u>	IP adresleri, domain isimleri ve diğer açık kaynaklardan otomatik veri toplayan bir araçtır.
<u>OSINT Framework</u>	OSINT araçlarının bir arada bulunduğu bir framework'tür, kullanıcılara birçok farklı kaynağa erişim sağlar.



# En Yaygın Kullanılan OSINT Yöntemleri:

Aşağıda, en yaygın kullanılan OSINT (Açık Kaynak İstihbarat) yöntemleri yer almaktadır.

## Sosyal Medya Araştırmaları

- Twitter, Facebook, LinkedIn gibi platformlardan kullanıcı bilgileri toplanabilir. Sosyal medya üzerindeki paylaşımlar, etkileşimler ve kullanıcı profilleri analiz edilebilir.

## Dijital Ayak İzlerinin Takibi

- IP adresi, DNS sorguları, e-posta izleri gibi dijital izlerin analiz edilmesi, bir kişinin çevrimiçi etkinliklerinin izlenmesini sağlar.

## Veritabanı Sorgulamaları

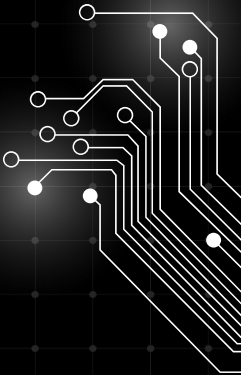
- Whois, DNS, IP ve URL veritabanları üzerinden aramalar yapılabilir. Bu, kişilerin veya organizasyonların dijital kimliklerini araştırmak için kullanılır.

## Geolokasyon Analizi

- Sosyal medya fotoğraflarından, GPS koordinatlarından ve harita verilerinden konum bilgisi elde edilebilir.

## Web Tarama ve Web Kazıma (Web Scraping)

- Farklı web sitelerinden otomatik olarak veri çekme yöntemidir. Bu yöntem, geniş veri setlerinden faydalı bilgilerin hızlıca toplanmasını sağlar.

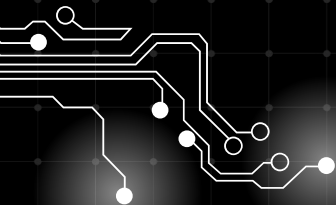




# 04

---

## OSINT KAYNAKLARI





# Kaynaklar

## Sosyal Medya Siteleri

Twitter, Facebook, Instagram, LinkedIn gibi sosyal medya platformlarından kullanıcı bilgileri, paylaşımlar, etkileşimler ve konum etiketleri toplanarak analiz edilebilir.

## Herkes Açık Veritabanları

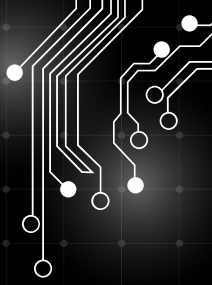
Whois, Shodan, Censys gibi araçlar, IP adresleri, domain bilgileri, bağlı cihazlar, açık portlar ve ağ yapılarına dair kapsamlı ve detaylı bilgi sağlayarak, siber güvenlik araştırmalarına önemli katkı sunar.

## Resmi ve Kamuya Açık Belgeler

Hükümet raporları, mahkeme belgeleri ve açık kaynak haber siteleri, kamuya açık bilgilere erişim sağlayarak, olayların daha derinlemesine analiz edilmesine olanak tanır.

## Hikayeler ve Bloglar

Reddit, Medium ve diğer forumlar gibi platformlardan, kullanıcılar, tartışmalar, yorumlar ve görüşler hakkında veri toplanarak, toplulukların eğilimleri ve düşünce kalıpları hakkında bilgi edinilebilir.



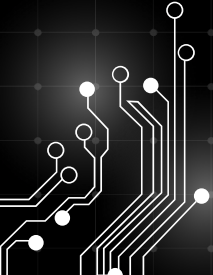
# Kaynaklar

## Harita ve Coğrafi Bilgi Sistemleri

Google Maps, OpenStreetMap gibi harita servisleri, konum bilgileri, yol tarifleri, coğrafi veriler ve mekansal analizler sağlayarak, yer belirleme, güzergah planlaması ve coğrafi bilgilerin elde edilmesinde önemli bir kaynak oluşturur.

## Sızdırılmış Veriler (Gri Alan)

Sızdırılmış veriler, genellikle hukuki ve etik sorunlar yaratabilir. Bu veriler, yasal olarak korunmaya devam eder ve bu tür verilerin toplanması veya yayılması yasadışı olabilir. Sızdırılmış veriler, OSINT'in **gri alanı** olarak kabul edilir ve etik sorunlara yol açabilir.

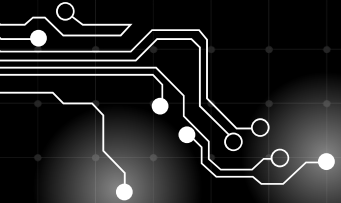




# 05

---

## YASAL VE ETİK SINIRLAR





# OSINT'in Yasal ve Etik Sınırları

OSINT'in etik ve yasal sınırları aşağıda belirtilen ilkelere dayanmaktadır:

## Yasal Durum:

- Sızdırılmış veriler, yasal olarak halka açık değildir ve bu tür veriler üzerinde işlem yapmak veya yaymak hukuki sorunlara yol açabilir. Sızdırılmış veriler, genellikle açık kaynak sayılmaz.

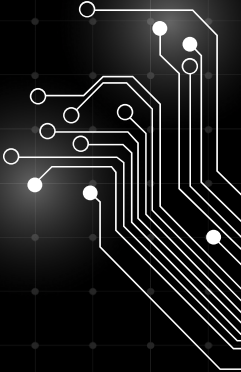
## Etik Yaklaşım:

- OSINT'in temel ilkelerinden biri, yalnızca **yasal ve halka açık** kaynaklardan bilgi toplamaktır. Etik olarak, yetkisiz yollarla elde edilen bilgiler kullanılmamalıdır.

## Pratikteki Yaklaşım ve Riskler:

- Sızdırılmış veriler kamuya açık hale gelse bile, bu verilerin OSINT kapsamında değerlendirilmesi, yasal ve etik açıdan sorunlu olabilir. Bu tür veriler, gri alan olarak kalır.

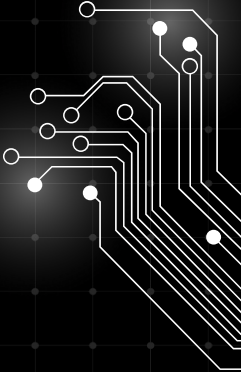
OSINT, yalnızca yasal ve halka açık kaynaklardan bilgi toplamayı amaçlar; sızdırılmış veriler, hem etik hem de yasal açıdan riskler taşıyabilir ve bu tür verilerin kullanımı dikkatle değerlendirilmelidir.






# SONUÇ

- **OSINT**, dijital dünyada önemli bir bilgi toplama aracıdır ve çeşitli profesyonel alanlarda kullanılabilir.
- **Yasal ve etik sorumluluklar** içinde kalınarak yapılmalıdır. Bu, güvenilirliğini ve meşruiyetini korur.
- **Araçlar ve yöntemler**, verilerin hızlı ve etkili bir şekilde toplanmasını sağlar. Ancak, doğru araç ve tekniklerin seçilmesi önemlidir.
- **Simülasyonlar**, katılımcılara pratik deneyim kazandırarak teorik bilgileri pekiştirmelerine yardımcı olur.





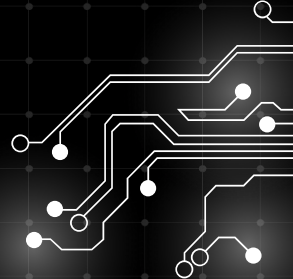
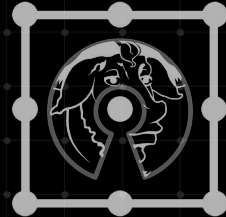


# Teşekkürler!

**OSINT 101**

**Ondokuz Mayıs Üniversitesi**

**Özgür Yazılım ve Açık Kaynak Topluluğu**





CREDITS: This presentation template was created, by [Slidesgo](#) and includes icons by [Flaticon](#) and infographics & images by [Freepik](#)