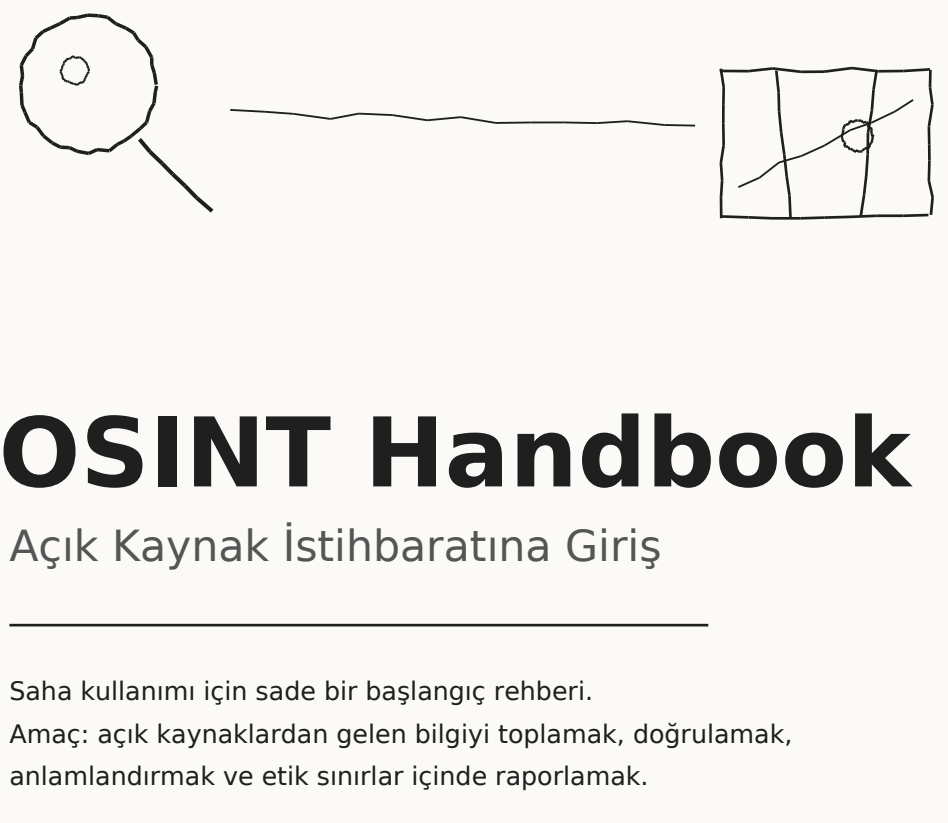

OSINT Handbook

Açık Kaynak İstihbaratına Giriş

Saha kullanımı için sade bir başlangıç rehberi.
Amaç: açık kaynaklardan gelen bilgiyi toplamak, doğrulamak, anlamlandırmak ve etik sınırlar içinde raporlamak.

Kısa ilke

OSINT; merakla değil, soruyla başlar. Her bulgu kaynak, tarih ve bağlamla birlikte tutulur. Doğrulanmamış veri sonuç gibi sunulmaz.

Hazırlayan: Ahmet için

Kısa tanım

OSINT, herkesin erişebildiği açık kaynaklardan bilgi toplama, doğrulama ve anlam çıkarma işidir. Buradaki 'açık' kelimesi, bilginin kamuya açık bir yerde bulunmasını anlatır; sınırsız kullanım hakkı verdiği anlamına gelmez.

İyi OSINT çalışması tek bir ekran görüntüsüne dayanmaz. Aynı bilgiyi farklı kaynaklarla karşılaştırır, zamanı kontrol eder, kaynağın güvenilirliğini tartar ve sonucu ihtiyatlı yazar.

OSINT ne değildir?

OSINT; hesap kırma, özel mesajlara girme, gizli veriyi sızdırma veya bir kişiyi hedef gösterme işi değildir. Açık kaynak araştırması yasal ve etik sınırlar içinde kalmalıdır.

Nerelerde kullanılır?

- Gazetecilik ve vaka doğrulama: görüntü, tarih, yer ve kaynak kontrolü.
- Siber güvenlik: kurumun internete açık varlıklarını ve sızıntı izlerini görmek.
- Dolandırıcılık önleme: sahte profil, sahte ilan veya taklit marka sinyallerini incelemek.
- Kurumsal araştırma: açık verilerden şirket, domain, haber ve bağlantı analizi yapmak.
- Akademik ve toplumsal araştırma: açık veri setlerini dikkatli biçimde yorumlamak.

2. OSINT Veri Kaynakları

Her kaynak aynı kalitede değildir. Sosyal medya hızlı sinyal verir ama kolay manipüle edilir. Resmi kayıtlar daha sağlamdır ama eksik veya eski olabilir. Bu yüzden kaynak türünü not etmek, bulgunun kendisi kadar önemlidir.

Sosyal medya

Profil, kullanıcı adı, etkileşim, takip ağı ve zaman çizelgesi incelenir. Tek başına kimlik kanıtı sayılmaz.

Domain kayıtları

WHOIS, DNS, sertifika ve subdomain kayıtları kurumun dijital ayak izini gösterir. Gizlilik servisleri yüzünden eksik olabilir.

Arama motorları

Site içi arama, önbellek, dosya türü ve tarih filtreleriyle dağınık bilgi bulunabilir. Sonuçlar sıralama algoritmasına bağlıdır.

Uydu ve harita verisi

Konum, yapı, yol, arazi ve zaman karşılaştırması için kullanılır. Görüntünün tarihi mutlaka kontrol edilir.

Forumlar ve topluluklar

Erken sinyal, kullanıcı dili ve teknik izler bulunabilir. Takma adlar yanıltıcı olabilir.

Haber siteleri

Olay kronolojisi için faydalıdır. Birincil kaynakla karşılaştırılmadan kesin kabul edilmemelidir.

Metadata

Dosya adı, tarih, cihaz, koordinat veya üretim izi verebilir. Platformlar çoğu zaman metadata'yı siler.

Açık veritabanları

Şirket kayıtları, ihale, siber tehdit, CVE, sertifika ve arşiv verileri analiz için omurga sağlar.

Kayıt disiplini

Toplanan her veri için kaynak linki, erişim tarihi, kısa açıklama ve doğrulama durumu tutulur. Bu basit alışkanlık raporu güvenilir yapar.

3. Temel OSINT Süreci

OSINT süreci düz bir çizgi gibi görünür ama pratikte sık sık geri dönülür. Yeni bir bulgu gelir, soru daraltılır, kaynak yeniden kontrol edilir. Ama omurga değişmez: amaç, kaynak, doğrulama, analiz, rapor.

1

Hedef belirleme

Ne öğrenmek istiyorsun? Kişi, kurum, domain, olay veya teknik gösterge net yazılır. Kapsam dışı alanlar da baştan belirtilir.

Veri toplama

Sadece açık kaynaklardan veri alınır. Link, tarih, ekran görüntüsü ve kısa not birlikte saklanır.

Doğrulama

Aynı bilgi bağımsız kaynaklarla karşılaştırılır. Zaman, konum, hesap geçmişi ve kaynak itibarı kontrol edilir.

Analiz

Dağınık bulgular anlamlı yapıya çevrilir. Kesin bilgi, güçlü ihtimal ve zayıf sinyal ayrı yazılır.

Raporlama

Sonuç kısa, izlenebilir ve kanıta bağlı olmalıdır. Okuyan kişi bulgunun nereden geldiğini görebilmelidir.

Pratik kural

Bir bulgu karar değiştiriyorsa, en az iki bağımsız kaynakla doğrulanmadan raporda kesin ifade kullanma.

4. Kullanılan Araçlar

Araçlar araştırmayı hızlandırır ama analistin yerine geçmez. Aynı araç farklı hedeflerde farklı sonuç verebilir. Bu yüzden araç çıktısı 'kanıt' değil, kontrol edilmesi gereken işaret olarak görülmelidir.

Shodan

İnternete açık cihaz ve servisleri aramak için kullanılır. Sahip olmadığın sisteme erişmeye çalışma; sadece görünür bilgiyi değerlendir.

Maltego

Kişi, domain, şirket ve teknik varlıklar arasındaki ilişkileri grafik üzerinde görmek için faydalıdır.

theHarvester

Domain etrafındaki e-posta, subdomain ve isim izlerini açık kaynaklardan toplamak için kullanılır.

SpiderFoot

Farklı kaynaklardan otomatik OSINT toplar. Hızlı envanter çıkarır ama sonuçları tek tek doğrulamak gerekir.

Google Dorking

Arama operatörleriyle açık web içindeki dosya, sayfa ve indeksleri bulmayı sağlar. Örnek: site:, filetype:, intitle:.

Wayback Machine

Bir web sayfasının eski hallerini görmek ve silinen/değişen içeriklerin zaman çizgisini kurmak için kullanılır.

crt.sh

Sertifika şeffaflığı kayıtlarından domain ve subdomain izlerini görmek için pratik bir kaynaktır.

VirusTotal

Dosya, URL, domain ve IP itibarını incelemeye yarar. Sonuçlar bağlamla birlikte okunmalıdır.

Araç notu

Otomasyon hatayı da hızlandırır. Büyük taramalar yerine önce dar kapsam, sonra kontrollü genişletme daha sağlıklıdır.

5. Sosyal Medya Analizi

Sosyal medya OSINT çalışmasında hızlı sinyal verir: kullanıcı adı, profil dili, paylaşım saati, etkileşim ağı, görsel izleri ve tekrar eden davranışlar. Fakat burada hata payı yüksektir. Taklit hesap, eski içerik, şaka, ironi veya bağlam kopması raporu bozabilir.

Bakılacak alanlar

- Kullanıcı adı: Aynı rumuz farklı platformlarda tekrar ediyor mu? Yazım tarzı ve tarih uyuyor mu?
- Profil ilişkileri: Kimlerle sık etkileşim var? Bu ilişki gerçekten bağlantı mı, yoksa sadece tek taraflı takip mi?
- Zaman analizi: Paylaşım saatleri, olay günü aktivitesi ve hesap açılış tarihi tutarlı mı?
- Paylaşım davranışı: Dil, konu, görsel tarzı ve tekrar eden alışkanlıklar profili destekliyor mu?
- Görsel kontrol: Fotoğraf eski mi, başka yerden mi alınmış, kırpılmış veya yapay üretilmiş olabilir mi?
- Arşiv kontrolü: Silinmiş veya değiştirilmiş içerik varsa Wayback, ekran görüntüsü ve üçüncü kaynaklarla kontrol edilir.

Dikkat

Bir sosyal medya hesabı ile gerçek kişi arasında bağ kurarken çok ihtiyatlı olun. Aynı ad, aynı fotoğraf veya benzer kullanıcı adı tek başına kimlik kanıtı değildir. Rapor dili buna göre yumuşak yazılmalıdır.

Mini kontrol cümlesi

'Bu hesap, X kişiyle kesin olarak aynıdır' demek yerine; 'Kullanıcı adı, profil tarihi ve tekrar eden bağlantılar X kişiyle ilişkili olabileceğini gösteriyor; ancak bağımsız doğrulama gerekir' demek daha güvenlidir.

6. Domain ve Altyapı Analizi

Domain ve altyapı analizi, bir kurumun internette görünen teknik izlerini anlamaya çalışır. Bu çalışma mümkün olduğunca pasif yürütülmelidir: açık kayıtları okumak, sertifika geçmişine bakmak, DNS kayıtlarını incelemek ve arşivleri karşılaştırmak.

Temel bakış sırası

WHOIS	Domain sahibi, kayıt tarihi, registrar ve güncelleme bilgisi görülebilir. Birçok kayıtta gizlilik servisi bulunur.
DNS kayıtları	A, AAAA, MX, NS, TXT gibi kayıtlar altyapının yönünü gösterir. SPF/DMARC gibi e-posta güvenliği izleri de incelenir.
Subdomain keşfi	Alt alan adları test, panel, staging veya eski sistem izleri verebilir. Sertifika kayıtları burada çok işe yarar.
Sertifika kayıtları	Certificate Transparency kayıtları yeni veya eski subdomainleri yakalamaya yardım eder. crt.sh pratik bir başlangıçtır.
IP ve servis görünürlüğü	Shodan gibi araçlar açık servisler, portlar ve banner bilgisi gösterebilir. Bu bilgi erişim denemesi için kullanılmamalıdır.
Arşiv karşılaştırması	Wayback Machine ile eski sayfa yapısı, kaldırılan endpointler ve marka değişimleri takip edilebilir.

Sınır

OSINT raporunda 'şu sistem açık görünüyor' demek başka, yetkisiz erişim denemek başkadır. İzin yoksa aktif tarama, parola denemesi veya zafiyet sömürüsü yapılmaz.

7. Riskler ve Manipülasyon

OSINT'in en büyük riski veri eksikliği değil, veriye fazla güvenmektir. Açık kaynaklarda yanlış bilgi, kasıtlı manipülasyon, eski içerik, sahte hesap ve yapay üretim çok sık görülür. Bu yüzden raporun kalitesi toplama hızından değil, doğrulama disiplininden gelir.

Yanlış bilgi

Hata sonucu yayılmış olabilir. Niyet kötü olmayabilir ama sonuç yine yanıltıcıdır.

Dezenformasyon

Kasıtlı olarak yanıltmak, algı kurmak veya zarar vermek için hazırlanmış içeriktir.

Sahte hesaplar

Yeni açılmış, yapay etkileşimli veya çalıntı fotoğraflı hesaplar yanlış bağlantı kurdurabilir.

Deepfake / yapay içerik

Ses, yüz, fotoğraf veya video gerçek gibi görünebilir. Teknik ve bağlamsal kontrol gerekir.

Eski görüntü

Başka ülkedeki veya başka tarihteki görüntü yeni olay gibi paylaşılabilir.

Manipüle ekran görüntüsü

Kırpılmış, düzenlenmiş veya bağlamı silinmiş ekran görüntüsü tek başına kanıt değildir.

Doğrulama alışkanlığı

Bir içerik önemliyse şu üç soruyu sor: Bunu ilk kim paylaştı? Aynı bilgi bağımsız kaynaklarda var mı? Zaman ve yer bilgisi gerçekten tutuyor mu? Bu üç soru çoğu hatayı erken yakalar.

OSINT çalışması bilgiye ulaşabildiğin için değil, o bilgiyi meşru ve ölçülü biçimde kullanabildiğin için değerlidir. Kamuya açık veri, kişiyi hedef göstermek veya özel hayatı ifşa etmek için bahane değildir.

Temel ilkeler

- Sadece açık kaynak veri kullan: giriş gerektirmeyen, yetki aşımı içermeyen ve meşru erişilebilen kaynaklarla çalış.
- Doxxing yapma: adres, telefon, aile bilgisi, özel hayat detayı gibi kişiyi riske atacak bilgileri yayınlama.
- Veri minimizasyonu uygula: rapor için gerekli olmayan kişisel veriyi toplama, saklama veya paylaşma.
- Bağlamı koru: bir paylaşımı kesip farklı anlam çıkarma. Tarih, kaynak ve olay bağlamını yaz.
- KVKK / GDPR mantığını unutma: kişisel veri işlenirken amaç, ölçülülük, güvenlik ve hukuki dayanak önemlidir.
- Yetkisiz erişim yok: parola denemesi, kapalı gruplara sızma, özel mesaj okuma veya güvenlik açığı sömürme OSINT değildir.

Kırmızı çizgi

Raporun amacı riski azaltmak olmalı; kişiyi küçük düşürmek, taciz ettirmek veya hedef yapmak olmamalıdır. Şüpheli sinyal varsa kesin hüküm verme. Gerekirse 'doğrulanamadı' yazmak en doğru cevaptır.

Saha notu

Profesyonel OSINT'te iyi araştırmacı, bulduğu her şeyi yazan kişi değildir. Gereksiz veriyi eleyen, kaynağı tartan ve zarar doğurabilecek ayrıntıyı kontrol eden kişidir.

İyi rapor kısa, izlenebilir ve sakin dille yazılır. Okuyan kişi hangi bilginin kesin, hangisinin sinyal olduğunu hemen anlamalıdır.

Kısa rapor şablonu

Hedef	Araştırılan kişi / kurum / domain / olay. Kapsam ve tarih aralığı yazılır.
Bulgular	Her bulgu kısa cümleyle verilir. Kaynak linki ve erişim tarihi eklenir.
Doğrulanan bilgiler	Bağımsız kaynaklarla desteklenen bilgiler [Fact] gibi işaretlenebilir.
Şüpheli sinyaller	Tek kaynağa dayanan, eksik veya erken işaretler [Unverified] olarak ayrılır.
Kaynaklar	Resmi sayfa, arşiv linki, ekran görüntüsü, veri tabanı ve araç çıktısı listelenir.
Genel değerlendirme	Ne anlama geldiği, belirsizlikler ve önerilen sonraki adım yazılır.

Örnek değerlendirme dili

'Bulgu X kaynağında görülüyor; Y ve Z kaynaklarıyla destekleniyor. Ancak kayıt tarihi eski olduğu için güncel durum ayrıca doğrulanmalıdır.'

Kaynakça ve başvuru noktaları

1. **Bellingcat Online Investigation Toolkit**
   https://bellingcat.gitbook.io/toolkit
2. **Bellingcat Guides & Handbooks**
   https://bellingcat.gitbook.io/toolkit/resources/guides-and-handbooks
3. **SANS - What is Open-Source Intelligence**
   https://www.sans.org/blog/what-is-open-source-intelligence
4. **OSINT Framework**
   https://osintframework.com/
5. **CISA - Tactics of Disinformation**
   https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
6. **NIST Privacy Framework**
   https://www.nist.gov/privacy-framework
7. **MITRE ATT&CK**
   https://attack.mitre.org/
8. **Europol - IOCTA Report**
   https://www.europol.europa.eu/publications-events/main-reports/iocta-report
9. **European Commission - Data Protection / GDPR**
   https://commission.europa.eu/law/law-topic/data-protection_en
10. **KVKK - Kişisel Verileri Koruma Kurumu**
    https://www.kvkk.gov.tr/
11. **Shodan Developer Docs**
    https://developer.shodan.io/
12. **VirusTotal Docs**
    https://docs.virustotal.com/docs/results-reports
13. **Internet Archive - Wayback Machine**
    https://wayback.archive.org/
14. **theHarvester Official Repository**
    https://github.com/laramies/theHarvester
15. **SpiderFoot Official Repository**
    https://github.com/smicallef/spiderfoot
16. **Maltego**
    https://www.maltego.com/
17. **crt.sh Certificate Search**
    https://crt.sh/