OSINT 2026: The Practitioner's Map

Open-Source Intelligence — what attackers see about you, what defenders see about themselves.

15+	6	3	Legal
ESSENTIAL TOOLS	SOURCE CATEGORIES	ADVERSARY TIERS	WHERE IT COUNTS

The 6 source categories

HIGHEST YIELD

Public records + people-search

Property records, voter rolls, court records. Spokeo, BeenVerified, Whitepages. Data brokers aggregate it all.

DNS / WHOIS / Certs

crt.sh for cert transparency. Reveals every subdomain a target has ever published.

Mass scanners

Shodan, Censys, FOFA, ZoomEye. Index every public IP — devices, services, banners.

Social media

Username + email pivots across platforms. Photos with EXIF or backgrounds.

Search operators

Google Dorks: site: filetype: intitle: inurl: — surgical query power.

Breach data + dark forums

HIBP, DeHashed, IntelX. Cyber-side OSINT for stealer logs, credential reuse.

DEFENDER'S FIRST MOVE

Self-audit. Search your name + email + phone in Google. Run HIBP. Check Spokeo. What you find is what an attacker finds in 5 minutes.

LEGAL FLOOR (US, BROAD)

Public data: generally fine. Defeating access controls: CFAA. Aggregation harm: civil/ethical, even when each piece is "public." For org work — written authorization.

ADVERSARY TIERS

1. **Tier 1 — opportunistic**
   Hours. Most defenses target them.
2. **Tier 2 — motivated**
   Time, specific target. Persistence.
3. **Tier 3 — resourced**
   Org crime, intel agencies. Hire help.

DEFENDER PLAYBOOK

1. **CT log monitor (weekly)**
   Find your shadow subdomains
2. **Breach feed for your domain**
   HIBP Enterprise, SpyCloud
3. **Continuous port/service scan**
   Shodan ID your asset, monthly
4. **Brand-impersonation watch**
   PhishStats, URLscan

Cornerstone: **djenterprises.ai/blog/osint-introduction** → 10-post OSINT series indexed there.