CS-092 · Threat Intelligence

OSINT (Open Source Intelligence)

Gathering and analyzing publicly available information to support defensive security research.

Executive Summary

Open source intelligence, or OSINT, is the practice of collecting and analyzing information that is publicly and lawfully available to answer a security question. Sources include public websites, domain and certificate records, public code repositories, news, and social media. For defenders, OSINT reveals what an organization exposes to the outside world, supports threat research, and enriches investigations, all using only information anyone could legally access.

What It Is

OSINT is intelligence produced from publicly available information rather than from private or classified sources. In cybersecurity it is used to understand an organization's external attack surface, to research threat actors and campaigns, and to add context during incident investigations. Typical sources include public DNS and WHOIS records, TLS certificate transparency logs, search engines, public code and configuration repositories, job postings, corporate filings, and social media. The core of OSINT is not just collection but analysis: raw public data becomes intelligence only after it is verified, connected, and interpreted to answer a specific question. Done professionally, OSINT relies entirely on lawful access to information that is already public, and it is guided by a clear, authorized objective.

Why It Matters

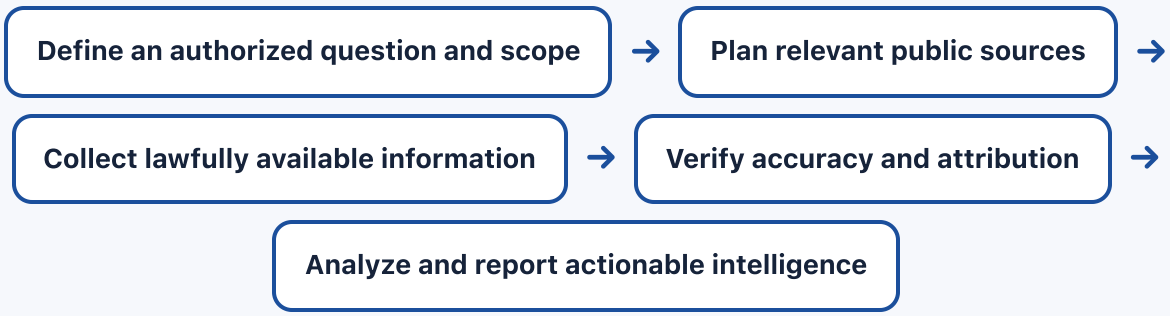
Attackers perform reconnaissance using the same public sources before they strike, so a defender who runs OSINT on their own organization sees themselves the way an adversary would. That surfaces exposed services, leaked credentials in public repositories, forgotten subdomains, and information that could fuel a convincing phishing message, all of which can be

fixed before they are exploited. OSINT also enriches threat intelligence by helping analysts research infrastructure and campaigns using open records. For professionals, OSINT skill is valuable across threat intelligence, security operations, penetration testing, and investigations, but it carries a responsibility: the same techniques must be applied ethically, within authorization and the law, and never to harass, stalk, or intrude on individuals.

How It Works

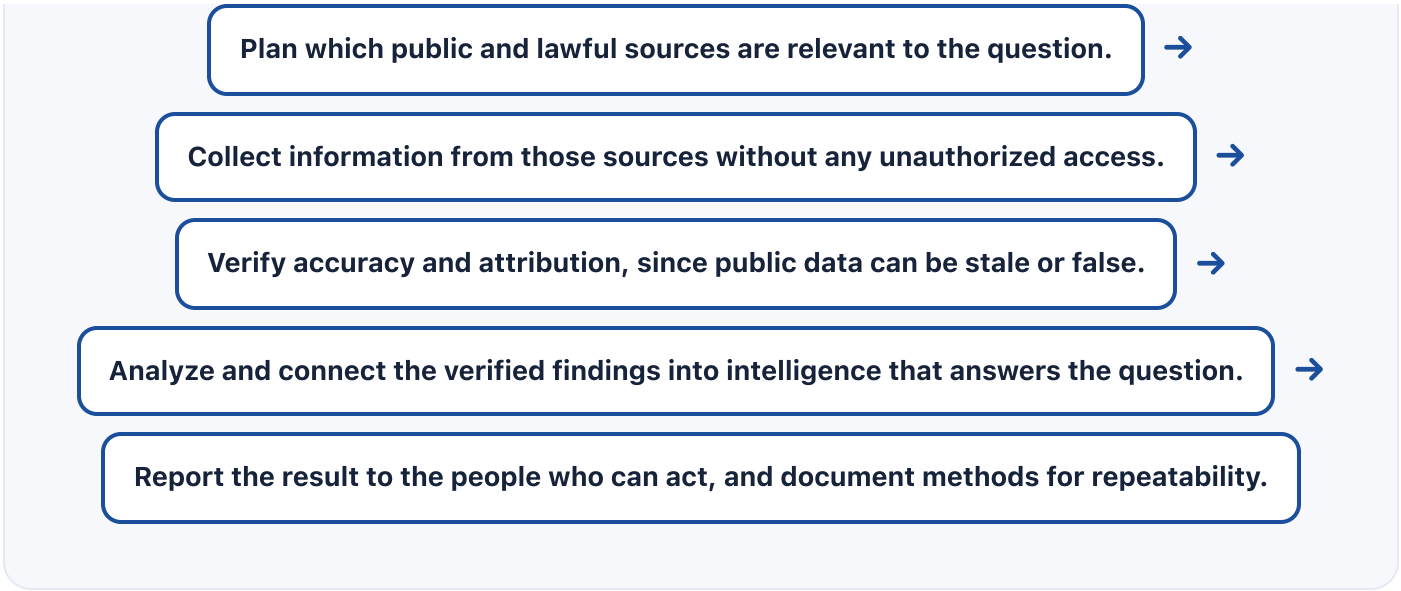
A sound OSINT process starts with a clear, authorized question, such as what does our organization expose externally. The analyst then plans which public sources are relevant, collects information from them, and, crucially, verifies it, since public data can be outdated, misattributed, or deliberately false. Verified findings are connected and analyzed to produce intelligence that answers the original question, and the result is reported to the people who can act on it. Automation and specialized tools help gather and organize large volumes of public data, but human judgment drives the analysis. Throughout, professional OSINT stays within scope and the law: it uses only publicly and lawfully available information, respects privacy, avoids any unauthorized access, and documents its methods so conclusions can be trusted and repeated.

Architecture Diagram



OSINT moves from an authorized question through planned collection and verification into analysis and a reported result.

Visual Workflow



Common Attacks

- Adversary reconnaissance of an organization's public attack surface before an intrusion
- Harvesting exposed credentials or secrets from public code repositories
- Discovery of forgotten subdomains and services left publicly reachable
- Gathering employee details to craft convincing phishing and pretexting
- Mapping technology and vendors from public postings to plan an attack

Common Mistakes

- Collecting public data without verifying it, then acting on inaccurate information
- Straying beyond authorization into unauthorized access, which is no longer OSINT
- Ignoring privacy and ethics when the subject is an individual
- Confusing raw collection with intelligence and skipping analysis
- Failing to document sources and methods, so conclusions cannot be trusted or repeated

Best Practices

- Start every effort with a clear, authorized objective and defined scope
- Use only publicly and lawfully available information and never unauthorized access
- Verify findings and attribution before drawing conclusions
- Apply OSINT to your own attack surface regularly to fix exposures before attackers find them

- Respect privacy and act ethically, especially when a person is involved
- Document sources and methods so intelligence is trustworthy and repeatable

Quick Checklist

- [x] Each OSINT effort has a written, authorized objective and scope
- [x] Only public and lawful sources are used, with no unauthorized access
- [x] Findings are verified for accuracy and correct attribution
- [x] Your own external exposure is reviewed on a regular schedule
- [x] Privacy and ethical limits are respected and enforced
- [x] Sources and methods are documented for repeatability and review

Recommended Tools

Search engines and advanced search operators
Locate publicly indexed information efficiently

DNS, WHOIS, and certificate transparency lookups
Reveal domains, subdomains, and infrastructure from public records

Attack surface discovery tools
Map an organization's externally reachable assets from public data

OSINT collection and mapping frameworks
Organize and link findings from many public sources

Industry Standards

MITRE ATT&CK (Reconnaissance and Resource Development)
Describes how adversaries gather public information before an attack

NIST SP 800-115
Technical guide to security testing where information gathering is a phase

CISA guidance on reducing external exposure
Defensive context for acting on OSINT findings

Career Relevance

OSINT is used by threat intelligence analysts researching actors and infrastructure, SOC analysts enriching alerts, threat hunters chasing leads, and penetration testers performing authorized reconnaissance. The ability to gather and, more importantly, verify and analyze public information is a valued and portable skill across security, and it is directly relevant to GRC and AI governance professionals assessing an organization's external exposure and the ethical limits of intelligence gathering.

Interview Questions

- What is OSINT, and what separates raw public data from finished intelligence?
- How would you use OSINT to assess your own organization's external attack surface?
- Why is verification essential when working with publicly available information?
- Where is the ethical and legal line between OSINT and unauthorized access?
- How does OSINT support threat intelligence and incident investigations?

Related Certifications

GIAC Open Source Intelligence (GOSI) **GIAC Cyber Threat Intelligence (GCTI)** **CompTIA CySA+**

Further Reading

- MITRE ATT&CK: Reconnaissance
- NIST SP 800-115: Technical Guide to Information Security Testing
- CISA: Cybersecurity Best Practices

Key Takeaways

- OSINT is intelligence produced from publicly and lawfully available information.
- For defenders it reveals external exposure and enriches threat research and investigations.
- Collection is only the start; verification and analysis turn public data into intelligence.
- Professional OSINT stays within authorization and the law and respects privacy.
- OSINT skill is portable across threat intelligence, operations, hunting, and testing careers.

FAQ

▶ **Is OSINT legal?**

▶ **How is OSINT different from threat intelligence?**

▶ **Why should defenders run OSINT on their own organization?**

Related Careers

RELATED ROLES

Threat Intelligence Analyst

Soc Analyst

Threat Hunter

Security Engineer

RELATED CERTIFICATIONS

GIAC Open Source Intelligence (GOSI)

GIAC Cyber Threat Intelligence (GCTI)

CompTIA CySA+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides

Role roadmaps

Salary data

Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **OSINT (Open Source Intelligence)**
3. Go deeper: Indicators of Compromise (IOCs)
4. Go deeper: Indicators of Attack (IOAs)
5. Validate it: work toward **GIAC Open Source Intelligence (GOSI)**
6. Find the role: browse current openings

RELATED SHEETS

CS-089 Indicators of Compromise (IOCs) | CS-090 Indicators of Attack (IOAs) | CS-091 Threat Feeds | CS-088 Threat Hunting | CS-008 MITRE ATT&CK