

<https://www.dane.ac-versailles.fr/spip.php?article615>



**ACADÉMIE  
DE VERSAILLES**

*Liberté  
Égalité  
Fraternité*

**Sécurité numérique : l'affaire de tous !**

# L'OSINT, l'art de l'investigation numérique

- Mes enjeux - Sécurité numérique -



Date de mise en ligne : mardi 29 août 2023

---

**Copyright © Délégation Académique au Numérique Éducatif - Tous droits**

**réservés**

---

Dans le monde numérique d'aujourd'hui, les informations personnelles et professionnelles sont souvent publiées en ligne, et il est important de **comprendre comment ces données sont utilisées** à diverses fins.

L'OSINT [1] est une branche de la cybersécurité axée sur la collecte et l'analyse d'informations publiques.

Cet article couvre les bases d'OSINT et son importance croissante dans le domaine de la sécurité informatique.

## Qu'est-ce que l'OSINT ?

L'OSINT est le **domaine de la collecte, de l'analyse et de l'utilisation des informations publiques disponibles en ligne pour obtenir des informations précieuses sur les individus, les entreprises et les organisations**. Ces informations peuvent provenir de sources telles que les médias sociaux, les bases de données publiques, les sites Web, les forums de discussion, les blogs et les reportages.

Contrairement aux techniques de piratage et d'intrusion, l'OSINT **ne nécessite pas de compromettre un système informatique ou d'enfreindre la loi pour obtenir des informations**.

## Pourquoi l'OSINT est désormais incontournable en cybersécurité ?

L'OSINT est devenu un **outil précieux** pour les professionnels de la cybersécurité. Cela fournit des **informations importantes pour évaluer les vulnérabilités potentielles des systèmes, des individus ou des organisations**. La technologie OSINT permet aux professionnels de la cybersécurité d'**identifier les modèles de comportement, les menaces émergentes, les vulnérabilités et les acteurs malveillants**.

## Quel est le champ d'application de l'OSINT ?

L'OSINT peut être mobilisé dans divers scénarios de cybersécurité :

- **Profilage des menaces** : il permet aux analystes de profiler les attaquants potentiels en recueillant des informations sur leurs activités passées, leurs compétences techniques et leurs motivations.
- **Enquête d'incident** : en cas d'incident de sécurité, il aide à reconstituer l'événement en rassemblant des preuves numériques et en suivant les empreintes laissées par les attaquants.
- **Audit** : avant de conclure un accord commercial ou un partenariat, OSINT peut être utilisé pour filtrer les antécédents d'une entreprise, y compris le conseil d'administration, la situation financière et la réputation en ligne.
- **Veille concurrentielle** : les entreprises peuvent l'utiliser pour surveiller les concurrents, suivre les tendances du marché, recueillir des informations sur les nouveaux produits ou services et mesurer la perception publique de ces produits ou services.

# Quelles sont les principales techniques utilisées par l'OSINT ?

L'OSINT utilise un large éventail de techniques et d'outils pour collecter et analyser des informations.

## La recherche sur les moteurs de recherche

C'est l'une des techniques les plus couramment utilisées dans OSINT. Cependant, pour maximiser l'efficacité de la recherche, il faut souvent tirer parti des fonctionnalités avancées d'un moteur de recherche ou d'un opérateur de recherche particulier.

## La surveillance des médias sociaux

Suivre les activités, les publications et les interactions sur les plateformes de médias sociaux pour obtenir des renseignements sur des individus, des groupes ou des événements.

## L'analyse de sites Web

Permet d'examiner attentivement les sites Web, les blogs et les forums pour extraire des informations telles que les contacts, les affiliations, les adresses IP et les vulnérabilités potentielles.

## L'analyse d'images et de vidéos

Des outils spécialisés permettent d'extraire des métadonnées, des informations de localisation ou d'autres détails cachés dans les images et les vidéos.

## La recherche de domaines et d'infrastructures

Identifier les noms de domaine, les adresses IP et les enregistrements WHOIS [\[2\]](#) pour comprendre la structure et les propriétaires d'une infrastructure en ligne.

## L'analyse de données publiques

Explorer les bases de données publiques, les registres gouvernementaux, les archives en ligne et d'autres sources d'informations accessibles au public.

# Quelles sont les implications éthiques et juridiques de l'OSINT ?

Bien que l'OSINT soit une puissante méthode de recherche d'informations, **il est important de souligner l'importance des considérations éthiques et juridiques**. Lors de la collecte d'informations publiques, il est important de se conformer aux lois applicables en matière de confidentialité, aux lois sur le droit d'auteur et à

d'autres réglementations.

## Respect de la vie privée

Lors de la collecte d'informations publiques, il est important de ne pas violer la vie privée d'un individu. Cela signifie que la collecte de données sensibles ou personnelles peut être contournée sans consentement approprié.

## Utilisation légale des informations

Il est important que la collecte et l'utilisation des informations ne violent pas les droits de propriété intellectuelle, les droits d'auteur, les secrets commerciaux ou d'autres lois applicables. Les informations collectées sur OSINT ne peuvent pas être utilisées à des fins illégales, diffamatoires ou malveillantes.

## Éthique de la collecte d'informations

Aucune méthode illégale ou invasive n'est utilisée pour obtenir des informations. Il est important de respecter les conditions d'utilisation des sites Web et des plateformes en ligne et toute restriction imposée par les propriétaires des informations publiques. L'OSINT doit être utilisé dans des contextes juridiques et éthiques qui exigent des informations ouvertes.

## Protection des données personnelles

Cela signifie qu'il faut éviter la divulgation de données personnelles sensibles qui pourraient affecter la vie privée ou la sécurité de la personne concernée. Les professionnels de l'OSINT doivent prendre les mesures appropriées pour protéger les données collectées et empêcher qu'elles ne soient utilisées à mauvais escient ou utilisées sans autorisation.

## Transparence et responsabilité

La mise en œuvre de l'OSINT comprend la notification aux personnes concernées de la collecte et de l'utilisation de leurs informations dans la mesure du possible, et le respect des principes de transparence et de responsabilité dans le processus d'investigation numérique. Les professionnels de l'OSINT doivent être tenus responsables de leurs actes et des conséquences de l'utilisation des informations collectées.

---

[1] Open Source Intelligence : Le renseignement de sources ouvertes ou renseignement d'origine sources ouvertes, est un renseignement obtenu par une source d'information publique

[2] Whois est un service de recherche fourni par les registres Internet, par exemple les Registres Internet régionaux ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine.