

COURS OSINT

23.01.2023



PROGRAMME

Description du Cours

Ce cours d'Open Source Intelligence (OSINT) fournira aux étudiants la capacité à rassembler des informations sur des personnes, des groupes ou des entreprises à partir de sources diverses. Il fournira une série de compétences allant de la préservation de l'anonymat à la création de fausses identités en ligne, en passant par la compréhension du besoin, la collecte, le traitement, la diffusion et la capitalisation de l'information. Les étudiants se verront présenter les méthodologies et les outils les plus utilisés en renseignement cyber de sources ouvertes, au travers de modules théoriques, techniques et d'ateliers pratiques.

OBJECTIFS DES ATELIERS

- Donner à l'étudiant les compétences nécessaires pour réaliser des techniques d'investigation tout en restant anonyme ;
- Permettre à l'étudiant de se familiariser avec des outils spécialisés et d'en comprendre les résultats ;
- Présenter des ressources en ligne peu connues ;
- Formaliser les résultats d'une investigation.

Admission

Semestre A2S1, A2S2

Pré-requis : Aucun

Règles de savoir vivre





















L'assiduité au cours est la base d'un apprentissage réussi.

Si vous ne pouvez pas assister au cours pour des raisons personnelles ou liées à votre alternance, il est de bon ton de prévenir à l'avance l'enseignant.

Un registre des présents sera tenu sur toute la durée du cours.

Compétences à acquérir en 2ème Année

 Table

Aa Code_compétence...	Description	Ref_RNCP_Competence	Ref_RNCP_Activite	Ref_RNCP_Block	Année	Syllabus
SEC-OSI_2_01	Employer des opérateurs de recherche avancés	 RNCP_CO13	 RNCP_AC04	 RNCP_BLK03	2	 OSINT
SEC-OSI_2_02	Concevoir une investigation numérique à base de source ouverte ciblant un acteur ou une organisation.	 RNCP_CO04	 RNCP_AC02	 RNCP_BLK01	2	 OSINT
SEC-OSI_2_03	Évaluer les différents outils en source ouverte à des fins d'investigations numériques.	 RNCP_CO07	 RNCP_AC03	 RNCP_BLK02	2	 OSINT
SEC-OSI_2_04	Formaliser les résultats d'une investigation	 RNCP_CO03	 RNCP_AC01	 RNCP_BLK01	2	 OSINT
SEC-OSI_2_05	Restituer oralement les résultats d'une investigation	 RNCP_CO03	 RNCP_AC01	 RNCP_BLK01	2	 OSINT

Agenda du cours

Table

Aa Intitulé	Type	Semestre	Promo	Date	Matière
OSINT n°1	Cours Magistral	A2S1	2024	23 janvier 2023 9:30-11:30	! OSINT
Exercices d'OSINT n°1	TP	A2S1	2024	23 janvier 2023 12:30-17:30	! OSINT
OSINT n°2	Cours Magistral	A2S1	2024	24 janvier 2023 9:30-11:30	! OSINT
Exercices d'OSINT n°2	TP	A2S1	2024	24 janvier 2023 12:30-17:30	! OSINT
OSINT n°3	Cours Magistral	A2S1	2024	25 janvier 2023 10:30-11:30	! OSINT
Exercices d'OSINT n°3	TP	A2S1	2024	25 janvier 2023 12:30-17:30	! OSINT
OSINT n 4	Cours Magistral	A2S1	2024	26 janvier 2023 9:30-11:30	! OSINT
Exercices d'OSINT n 4	TP	A2S1	2024	26 janvier 2023 12:30-17:30	! OSINT
OSINT Projet	Suivi	A2S2	2024	6 mars 2023 17:00-17:30	! OSINT
OSINT Devoir	Devoir	A2S2	2024	16 avril 2023 23:59	! OSINT
OSINT Soutenance 1	Soutenance	A2S2	2024	17 avril 2023 9:30-11:30	! OSINT
OSINT Soutenance 2	Soutenance	A2S2	2024	17 avril 2023 12:30-15:30	! OSINT



Évaluation

La session de cours de A2S1 sera évaluée par la réalisation de mini défis individuels. Les réponses seront transmises via un questionnaire interactif en ligne. Un temps imparti sera défini au début de chaque défi.

La session de cours de A2S2 sera évaluée par la réalisation d'un projet en groupe de 6-7 étudiants (même groupe que Forensic) donnant lieu au rendu d'un rapport et à une soutenance de projet 20 minutes (15 minutes de présentation, 5 minutes de questions).



Notation

Pondération

Mini défis (30%)

Rapport (40%)

Soutenance (30%)

Échelle de notation

0 Compétence non constatée

1 Compétence non acquise

2 Compétence en cours
d'acquisition

3 Compétence acquise

4 Maîtrise

5 Expertise

Correspondance sur 20

0 devoir non rendu

1 $1 \leq \text{note} < 7.5$

2 $7.5 \leq \text{note} < 11.5$

3 $11.5 \leq \text{note} < 13.5$

4 $13.5 \leq \text{note} < 20$

5 $\text{note} \geq 20$

Rendu des devoirs

Les mini défis de A2S1 seront à rendre sous la forme d'un questionnaire interactif en ligne.

Les rapports de A2S2 seront envoyés à l'adresse pierre.blondel.ext@ecole2600.com par le chef de projet de chaque groupe au plus tard le 16 avril 2022 à 23h59.

La soutenance se déroulera le 17 avril 2022 et fera l'objet d'une présentation.

Devoirs non rendus ou rendus en retard

Tout devoir non rendu se verra attribuer la note minimale (zéro).

Tout devoir rendu au-delà des délais impartis se verra sanctionné par une pénalité d'1 niveau dans l'échelle de notation avec pour minimal le niveau 1.

DEFI 0

(OSINT OFF)

Monter une tour en spaghetti

Matériel :



26 spaghettis



1 paire de ciseaux



26 cm de ficelle



1 chamallow



26 cm de scotch

Règles :

- Désigner dans chaque groupe un observateur, qui va prendre des notes pour capitaliser la manière dont le groupe s'est organisé;
- L'observateur restituera sa prise de note à l'oral à la fin des 20 minutes;
- Réaliser en équipe de 5 à 7 membres, la tour la plus haute possible en spaghetti en moins de 20 minutes;
- L'équipe gagnante est celle qui positionnera le chamallow, sur la tour la plus haute !

DISCLAIMER

OSINT

Loi Godfrain

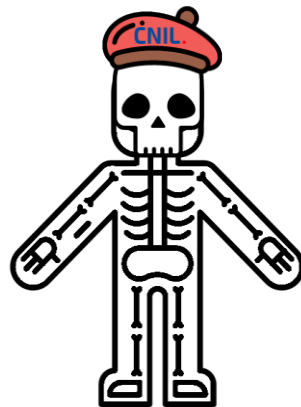
Première loi française punissant les actes de cybercriminalité et de piratage.

Les atteintes aux traitements et systèmes automatisés de données (STAD) prennent leur fondement dans **la loi Godfrain** du 5 janvier 1988, ou Loi n° 88-19 du 5 janvier 1988 (actualisée depuis).

L'article 323-3 du Code pénal prévoit :

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de **cinq ans d'emprisonnement** et de **150 000 € d'amende**. »

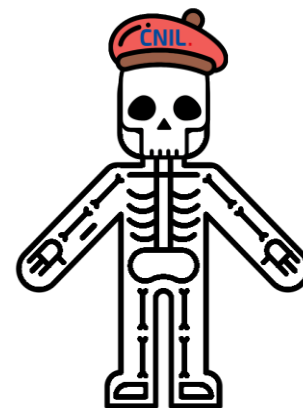
« Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'**Etat**, la peine est portée à **sept ans d'emprisonnement** et à **300 000 € d'amende**. »



Le cas « Bluetouff » (2005-2015)

En **2005**, **Bluetouff** avait récupéré et publié près de 8 Go de données de l'Agence Nationale Sécurité Sanitaire Alimentaire Nationale (**ANSES**) qui lui étaient librement accessibles en naviguant dans l'arborescence des fichiers du **site web depuis son navigateur**. Bluetouff a été accusé d'accès et de **maintien frauduleux** dans un STAD et de soustraction frauduleuse de données.

Il a été condamné en 2015 en appel à **3.000 € d'amende**, pour « maintien frauduleux dans un système de traitement automatisé de données et pour vol de données par la Cour d'Appel de Paris ».

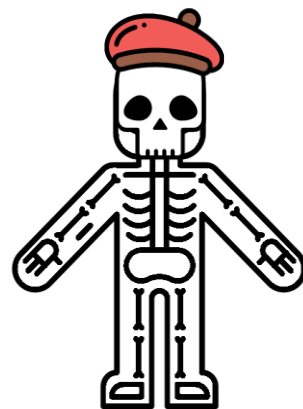


Règlement Général sur la Protection des Données (RGPD)

Le **règlement UE 2016/679** du Parlement européen et du Conseil du **27 avril 2016** s'applique depuis le **25 mai 2018** à toute **donnée identifiant une personne physique directement ou indirectement**. Et ce quel que soit le traitement effectué (stockage, transfert, transit, exploitation)

- Lorsque que le responsable du traitement est établi en **Union Européenne** ou lorsque le responsable de donnée traite des données personnelles d'une personne établie chez un membre de l'UE
- Le responsable de traitement doit être en **capacité de démontrer sa conformité** à la réglementation
- Lister et **décrire** les **finalités des traitements**
- Le responsable de traitement **limite la durée de conservation** de ses données de **manière proportionnée** aux finalités
- **pseudonymisation/anonymisation**

Ce n'est pas parce qu'une information, notamment une donnée personnelle, est librement accessible que son traitement ne viole pas les droits individuels.



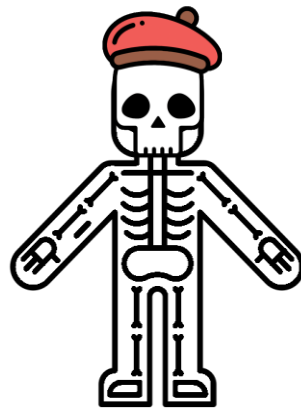
La recherche sur Internet de fuites d'informations (RIFI)

La **recherche sur Internet de fuites d'informations (RIFI)** a pour objectif de **détecter**, au plus tôt, une **fuite de données**. Les organismes qui souhaitent y recourir, ainsi que les prestataires de RIFI eux-mêmes, doivent respecter certaines **règles**, notamment le **RGPD** et le **code pénal**.

La RIFI consiste à **analyser le web de manière automatisée**, afin de vérifier si des **informations**, ont été **rendues publiques**. Cela implique d'analyser un important volume de données, y compris, des **données personnelles**.

La **CNIL** décompose une opération de RIFI en **4 étapes** :

- Le **choix des mots-clés** permet d'affiner la recherche et de se limiter aux données qui sont le plus susceptibles d'être pertinentes ;
- la **recherche effective de données** correspondant aux mots-clés préalablement déterminés, y compris des zones spécifiques (forums spécialisés dans la revente de données par exemple) ;
- la **remontée** et le **traitement** des alertes par le prestataire ;
- la communication d'**alertes qualifiées** au client concerné.



Statut d'Agence de Recherche Privée

- La loi précise dans son article L621-1 du livre VI du Code de la sécurité intérieure, que le statut d'agent de recherche privée est reconnu comme une « profession libérale qui consiste, pour une personne, à recueillir, même sans faire état de sa qualité ni révéler l'objet de sa mission, des informations ou renseignements destinés à des tiers, en vue de la défense de leurs intérêts. »

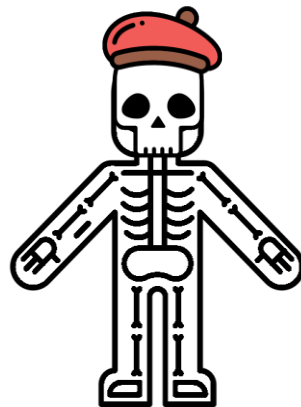
Loi informatique et libertés

- l'article 34 de loi informatique & Libertés qui indique que « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès».

Secret des correspondances

Propriété intellectuelle

L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous



Creative Commons & Licences

Exemples de licences de logiciel libre compatibles avec la GNU General Public License (GPL) :

- **GNU General Public License (GPL)**, version 3 : licence de logiciel libre et d'un copyleft
- **GNU Lesser General Public License (LGPL)**, version 3 : licence de logiciel libre, mais qui n'est pas un copyleft fort,
- **Licence Apache, version 2.0** : licence de logiciel libre, compatible avec la version 3 de la GNU GPL
- **Licence BSD modifiée** : licence BSD d'origine, mais privée de sa clause publicitaire
- **MIT License** : La licence donne à toute personne recevant le logiciel (et ses fichiers) le droit illimité de l'utiliser, le copier, le modifier, le fusionner, le publier, le distribuer, le vendre et le « sous-licencier » (l'incorporer dans une autre licence). La seule obligation est d'incorporer la notice de licence et de copyright dans toutes les copies.
- ...

Source : creativecommons.org



Traffic Light Protocol 2.0 (TLP)

Le **Traffic Light Protocol (TLP)** est un système de marquage qui indique dans quelle mesure les destinataires peuvent **partager** des **informations potentiellement sensibles**.

Bien que le protocole soit utilisé depuis presque 20 ans par la communauté de coordination et de réponse aux incidents, le **Forum of Incident Response and Security Teams (FIRST)** a officiellement publié le TLP **1.0** en août 2016 et la version **2.0** en août 2022.

Le TLP n'est pas juridiquement contraignant et **ne remplace pas les restrictions ou obligations légales**. Le TLP **n'est pas un système de classification** et n'a pas été conçu pour gérer les termes de licence, ni les règles de traitement de l'information ou de chiffrement.

Source : cisa.gov/sites/default/files/publications/tlp-2-0-user-guide_508c.pdf

Traffic Light Protocol 2.0 (TLP)

Comment utiliser le TLP dans les documents

TLP:RED = Pour les yeux et les oreilles des destinataires individuels uniquement, aucune autre divulgation. Les sources peuvent utiliser le TLP:RED lorsque les informations ne peuvent pas être traitées efficacement sans risque significatif pour la vie privée, la réputation ou les opérations des organisations concernées. Les destinataires ne peuvent donc pas partager les informations TLP:RED avec qui que ce soit. Dans le contexte d'une réunion, par exemple, les informations TLP:RED sont limitées aux personnes présentes à la réunion.

TLP:AMBER = Diffusion limitée, les destinataires ne peuvent diffuser ces informations qu'en fonction du besoin d'en connaître au sein de leur organisation et de ses clients. Notez que TLP:AMBER+STRICT restreint le partage à l'organisation uniquement. Les sources peuvent utiliser TLP:AMBER lorsque l'information nécessite un soutien pour être traitée efficacement, mais présente un risque pour la vie privée, la réputation ou les opérations si elle est partagée en dehors des organisations concernées. Les destinataires peuvent partager les informations TLP:AMBER avec les membres de leur propre organisation et ses clients, mais uniquement sur la base du besoin d'en connaître afin de protéger leur organisation et ses clients et d'éviter tout préjudice supplémentaire.

Note : Si la source veut restreindre le partage à l'organisation uniquement, elle doit spécifier TLP:AMBER+STRICT.

TLP:GREEN = En cas de diffusion limitée, les destinataires peuvent diffuser l'information au sein de leur communauté. Les destinataires peuvent utiliser TLP:GREEN lorsque l'information est utile pour accroître la sensibilisation au sein de leur communauté. Les destinataires peuvent partager les informations TLP:GREEN avec leurs pairs et les organisations partenaires au sein de leur communauté, mais pas via des canaux accessibles au public. Les informations TLP:GREEN ne peuvent pas être partagées en dehors de la communauté. Note : Lorsque le terme "communauté" n'est pas défini, il s'agit de la communauté de la cybersécurité/cyberdéfense.

TLP:CLEAR = Les destinataires peuvent diffuser cette information au monde entier, il n'y a pas de limite à la divulgation. Les sources peuvent utiliser TLP:CLEAR lorsque l'information présente un risque minimal ou non prévisible d'utilisation abusive, conformément aux règles et procédures applicables à la diffusion publique. Sous réserve des règles standard de copyright, les informations TLP:CLEAR peuvent être partagées sans restriction.

Permissible Actions Protocol (PAP)

Le protocole d'actions permises (PAP) est un protocole qui décrit dans quelle mesure il est acceptable qu'un attaquant puisse détecter l'état actuel de l'analyse ou les actions défensives. Il est conçu pour indiquer ce que le destinataire peut faire avec l'information et utilise pour cela un schéma de couleurs. Le PAP utilise le même schéma de couleurs que le TLP. Notez que contrairement au TLP, où les sources peuvent spécifier des limites de partage supplémentaires pour le TLP:AMBER, aucune exception de ce type n'existe pour le PAP:AMBER. Le PAP est inclus dans la taxonomie Malware Information Sharing Platform (MISP) et est pris en charge par TheHive.

PAP:RED : Actions non détectables uniquement. Les destinataires ne peuvent pas utiliser les informations PAP:RED sur le réseau. Uniquement des actions passives sur les logs, qui ne sont pas détectables de l'extérieur.

PAP:AMBER : Les destinataires peuvent utiliser les informations PAP:AMBER pour effectuer des vérifications en ligne, comme l'utilisation de services fournis par des tiers (par exemple VirusTotal), ou mettre en place un pot de miel de surveillance.

PAP:GREEN : Les destinataires peuvent utiliser les informations de PAP:GREEN pour envoyer un ping à la cible, bloquer le trafic entrant/sortant de/vers la cible ou configurer spécifiquement les pots de miel pour interagir avec la cible.

PAP:WHITE : Ouvert, sans restrictions

Source : github.com/MISP/misp-taxonomies/blob/main/PAP/machinetag.json

EXAMPLE

OWN
OWN-SECURITY

XXX
XXX

Type de rapport	XXX
Source	CERT-OWN
Date de création	XX/XX/20XX
Date de mise à jour	N/A
Référence	XXX

OWN CERT TEAM
OWN-SECURITY
(BRIDA Service)

Sources may use TLP/WHITE when information carries minimal or no foreseeable risk of release, in accordance with applicable rules and procedures for public release.
PAP/WHITE: Open, no restrictions

TLP/WHITE PAP/WHITE OWN-SECURITY

Description TLP

Description PAP

TLP Box

PAP Box

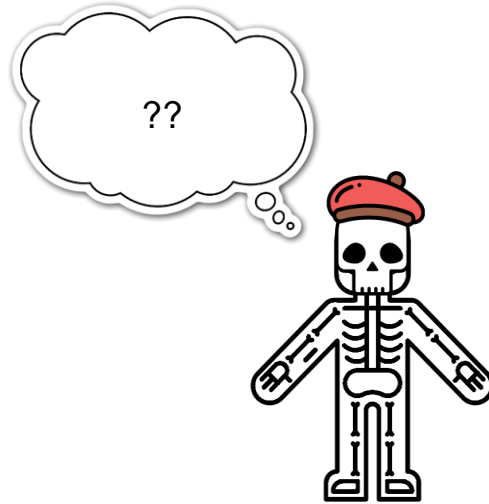
Une donnée à caractère personnel, c'est quoi ?



« C'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement . »

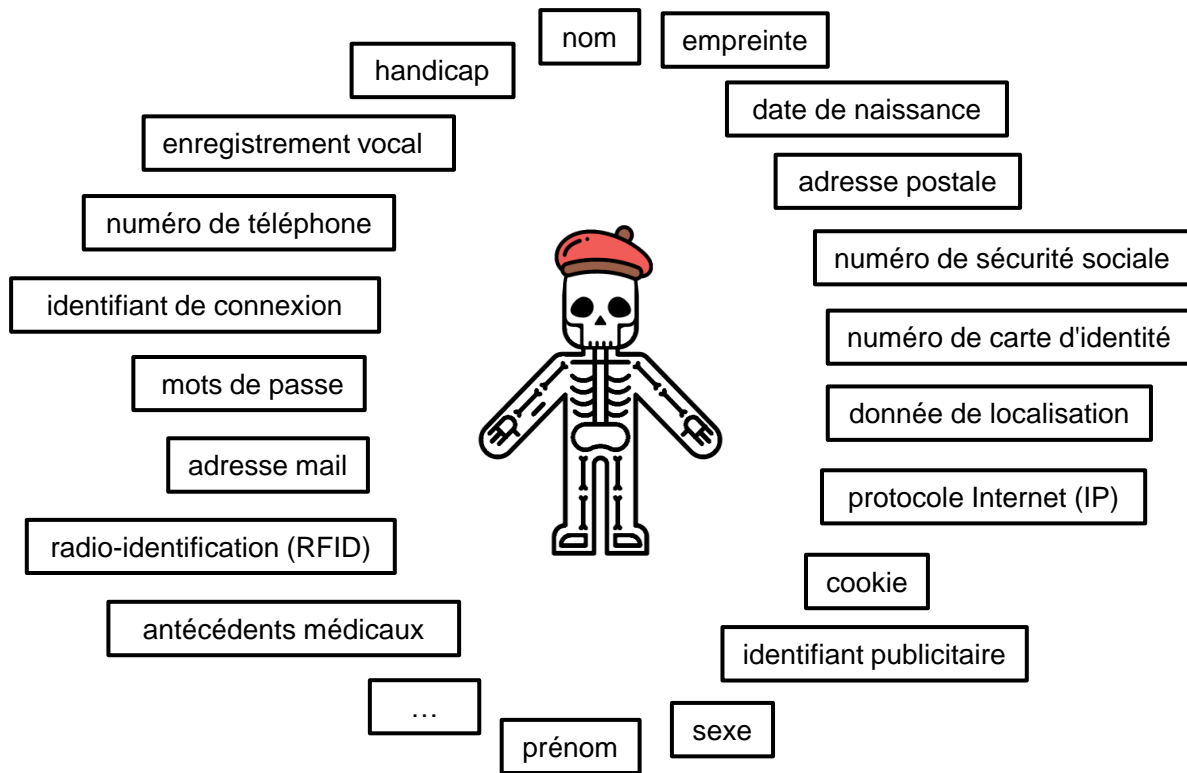
Pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.

Une donnée à caractère personnel, c'est quoi ?



Listez les types de données à caractère personnel

Une donnée à caractère personnel, c'est quoi ?



ce n'est pas parce qu'une information, notamment une donnée personnelle, est librement accessible que son traitement ne viole pas les droits individuels.

Divulgation de données personnelles (DOXING)

La divulgation de données personnelles, appelée doxing ou doxxing est une pratique consistant à rechercher et à divulguer sur l'internet des informations sur l'identité et la vie privée d'un individu dans le but de lui nuire. Les informations révélées peuvent être l'identité, l'adresse, le numéro de sécurité sociale, le numéro de compte bancaire, etc.



```
=====
[                               0x1 Basic Information                               ]
=====
Alias: [REDACTED]
Full Name: [REDACTED]
Phone Number : [REDACTED]
Country : USA
State(s) : [REDACTED]

=====
[                               0x2 Social Information                               ]
=====
Tiktok : [REDACTED]
Instagram : [REDACTED]
Discord : [REDACTED]
Telegram (Status Unknown) : [REDACTED]
Website (Larped): [REDACTED]

=====
[                               0x3 Home Information                               ]
=====
Address (1) : [REDACTED]
Information : [REDACTED]
Rent : [REDACTED]
Status : [REDACTED]
Built : [REDACTED]

=====
Address (2) : [REDACTED]
Information : [REDACTED]
Rent : [REDACTED]
Status : [REDACTED]
Built : [REDACTED]
Last 30-day Change : [REDACTED]
Estimate per sqft : [REDACTED]

=====
[                               0x4 Additional Information                               ]
=====
Race : [REDACTED]
Gender: [REDACTED]
Height : [REDACTED]
Eye Color : [REDACTED]
Blood Type : [REDACTED]
```

OBJECTIFS

Principaux cas d'usage

Il est important de garder à l'esprit que les types de mission varient et qu'il n'y a pas une seule et unique liste de choses à faire ou ne pas faire. Les types de mission OSINT les plus courants sont les suivantes :

- **Évaluation de la menace** : Il peut s'agir d'événements spécifiques à court terme ou d'un suivi à plus long terme des acteurs de la menace et/ou des victimes potentielles.
- **Évaluation des vulnérabilités** : Recherche et cartographie des données personnelles ou professionnelles exposées qui pourraient constituer une menace si elles tombaient entre de mauvaises mains.
- **Préservation des preuves** : Localiser et préserver le contenu en ligne en tant que preuve ou pour étayer un ensemble de conclusions.
- **Recherche générale** : Cela peut aller du journalisme à la collecte plus occasionnelle d'informations dans n'importe quel domaine d'intérêt.
- **Enseignement** : Parfois, l'OSINT est mené pour le plaisir ou simplement pour s'entraîner. Exemple :compétitions CTF
- **Attribution** : C'est l'objectif de la plupart des forces de l'ordre.
- **Veille concurrentielle**
- **Protection de la marque**
- **Détection des fuites de données**
- **Surveillance des *darkwebs***
- **Vérification des antécédents**
- **Image / Video / Text / Audio/IoT/DNS**
- ...

DEFI 1

(OSINT ON)

The T-REX hunt

Matériel :



>> anonfiles.com/k1V7vaT7ya <<

Règles :

- Retrouver la photo d'origine issu
- Retrouver l'adresse où a été prise cette photo
- Retrouver la date exacte de prise de cette photo
- Retrouver la géolocalisation (latitude /Longitude) en Degrés, minutes et secondes (DMS)
- Retrouver le pseudo, le nom et le prénom du photographe

Durée :

30 min

DEFINITIONS

DEFI 2

(OSINT ON)

Liste des « Int »

- **HUMINT** : Human **Int**elligence
- **OSINT** : Open-source **Int**elligence
- ...

- **Règle :**

Trouvez un maximum de disciplines de recueil de renseignements.

- **Durée :**

20 minutes

Liste des disciplines de recueil de renseignements

- **HUMINT** : Human **Intelligence**
- **GEOINT** : Geospatial **Intelligence**
- **MASINT** : Measurement and signature **Intelligence**
- **IMINT** : Imagery **Intelligence**
- **OSINT** : Open-source **Intelligence**
- **SIGINT** : Signals **Intelligence**
- **COMINT** : Communications **Intelligence**
- **TECHINT** : Technical **Intelligence**
- **SOCMINT** : Social media **Intelligence**
- **CYBINT/CYBERINT/DNINT** : Cyber **Intelligence** / digital network **Intelligence**
- **DNINT** : digital network **Intelligence**
- **VISINT** : Visual **Intelligence**
- **FININT** : Financial **Intelligence**
- **MEDINT** : Medical **Intelligence**
- **PHOTOINT** : Photographic **Intelligence**
- **TELINT** : Telemetry **Intelligence**
- **FISINT** : Foreign Instrumentation Signals **Intelligence**
- **DARKINT** : Darknet **Intelligence**
- **BLOCKINT** : Blockchain **Intelligence**
- **ACOUSTINT** : Acoustic **Intelligence**
- **NUCINT** : Nuclear **Intelligence**
- **LASINT** : Laser **Intelligence**
- **CBINT** : Chemical and Biological **Intelligence**
- **COMINT** : communications **Intelligence**
- **ELINT** : electronic **Intelligence**

OSINT

Open-Source Intelligence (OSINT)

- **Open-source intelligence (OSINT)** est un **renseignement** produit à **partir d'informations accessibles publiquement** et qui est **collecté, exploité et diffusé** en temps utile à **un public approprié** dans le but de **répondre à un besoin** spécifique en matière de renseignement. La diffusion et l'utilisation de renseignements validés de source ouverte permettent intrinsèquement le partage de l'information, puisque les renseignements de source ouverte sont produits **sans l'utilisation de sources et de méthodes sensibles**. Les produits de renseignement de source ouverte peuvent être partagés avec le public américain et les alliés étrangers en raison de la nature non classifiée du renseignement de source ouverte. . (SEC. 931 NOTE: 50 USC 403-5 note. DEPARTMENT OF DEFENSE STRATEGY)
- La Commission nationale sur les attaques terroristes contre les États-Unis (communément appelée "Commission 9/11"), dans son rapport final publié le 22 juillet 2004, a identifié des lacunes dans la capacité des États-Unis à utiliser les renseignements de toutes sources, dont une grande partie est constituée de renseignements de sources ouvertes.



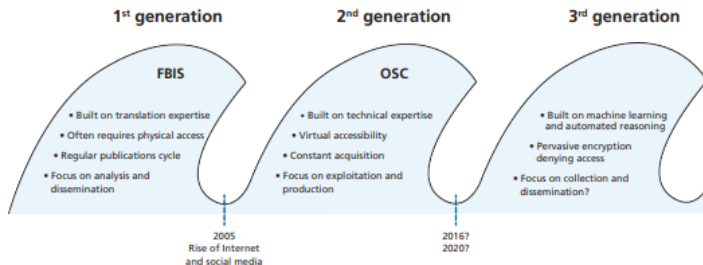
Open-Source Intelligence (OSINT)

- Research AND Development (**RAND**) Corporation est une company de conseil de l'armée américaine. Elle a sorti son rapport « Defining Second Génération Open-Source Intelligence (OSINT) for the Defense Enterprise » en **2018** ce rapport synthétise des documents déclassifiés de la CIA.
- **Web 1.0** OSINT
- **Web 2.0** Web participatif/social **OSINT 2.0**
- **Web 3.0** Web sémantique/décentralisé **OSINT 3.0**



Defining Second
Generation Open
Source Intelligence
(OSINT) for the
Defense Enterprise

Figure 4.1
Characteristics of OSINT Generations

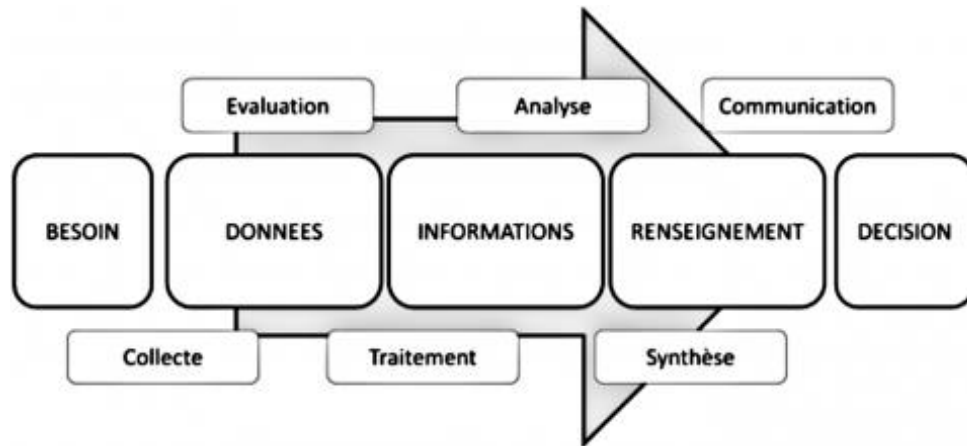


SOURCE: RAND analysis.
RAND RR1964-4.1

Heather J. Williams, Sara Blum

Open-Source Intelligence (OSINT)

- La communauté du renseignement français traduit OSINT par Renseignement d'Origine Source Ouverte (ROSO)
- Processus de renseignement :



Une donnée

Une donnée, par définition, est une **information brute, sans contexte**, un fait sans aucun arrière-plan. Elle ne peut pas être exploitée telle qu'elle. Une donnée brute **peut prendre différents aspects**. Cela peut être des données **numériques, textuelles**, ou un **mélange de texte et de chiffres**, mais aussi un **tableau, un graphique...**

Le PIA 02-200 introduit par ailleurs la notion de donnée, définie comme un « **élément de connaissance élémentaire (heure, lieu, événement, acteur, moyen, etc.)** »

Les **données** permettent de **produire des informations**, lesquelles permettent de **produire le renseignement**. Il s'ensuit une notion de processus qui vise la transformation des données en informations et des informations en renseignement.

L'Open Source Data (OSD)

L'OSD correspond aux données de première impression : la diffusion et le compte rendu oral d'informations à partir d'une source primaire. Il peut s'agir d'une photographie, d'un enregistrement ou encore d'une lettre personnelle d'un individu.

Une information

Le **PIA 02-200** définit l'information comme un « **renseignement brut** », alors que le renseignement serait un produit finalisé, c'est-à-dire une connaissance utile au décideur.

Selon **Lacoste** (2002) : « une information élaborée, pertinente et utile, correspondant aux besoins de celui qui la reçoit, qui doit donc lui parvenir à bon escient et en temps utile pour qu'il puisse en tirer profit ».

L'Open Source Information (OSIF)

L'OSIF se compose de données pouvant être assemblées, généralement par un processus éditorial qui assure le filtrage, la validation et la gestion de la présentation. Cette information générique est souvent largement diffusée dans les journaux, les livres ou rapports quotidiens.

Un renseignement

Chopin (2011) souligne l'absence de définition théorique précise dans la littérature consacrée au renseignement. Il précise que les définitions existantes renvoient généralement à des concepts techniques.

Pour Baud (1998), « un renseignement est une **information évaluée** et **exploitée** ayant passé le **cycle du renseignement** et prête à être diffusée à un client ». (distinction entre le renseignement et l'informatin

Opposition

Pour Silberzahn (1995) et **Chouet** (1997), « le renseignement a trait à la recherche d'informations secrètes ». Réduisant le renseignement à une information secrète et l'activité de renseignement à l'espionnage, ils soutiennent que le renseignement relèverait exclusivement des services spéciaux dont l'objectif est de « connaître ce qu'on veut leur cacher ». Ainsi le terme « renseignement ouvert » serait un oxymore, car ce qu'on appelle abusivement « renseignement ouvert » serait tout simplement de l'information.

L'Open Source Intelligence (OSINT)

L'OSINT est une information qui a été délibérément ouverte, diffusée à un public choisi pour répondre à une question spécifique. Finalement, l'Open Source Intelligence applique le processus éprouvé du renseignement aux multiples sources d'informations ouvertes.

Validated OSINT (OSINT-V)

L'OSINT-V correspond à une information à laquelle à un haut degré de sécurité peut être attribué. Celui-ci peut être produit par un professionnel du renseignement ou une source ouverte.

Le cycle du renseignement

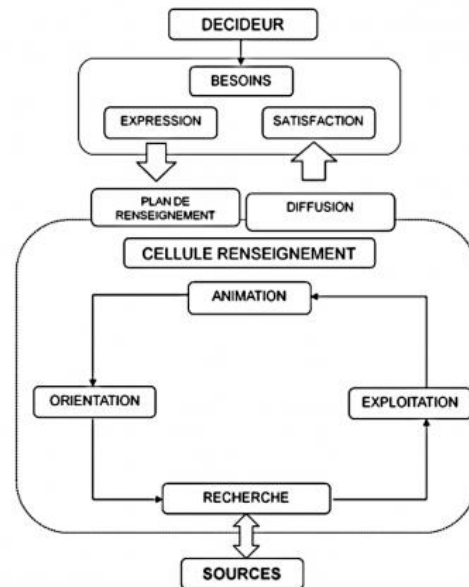
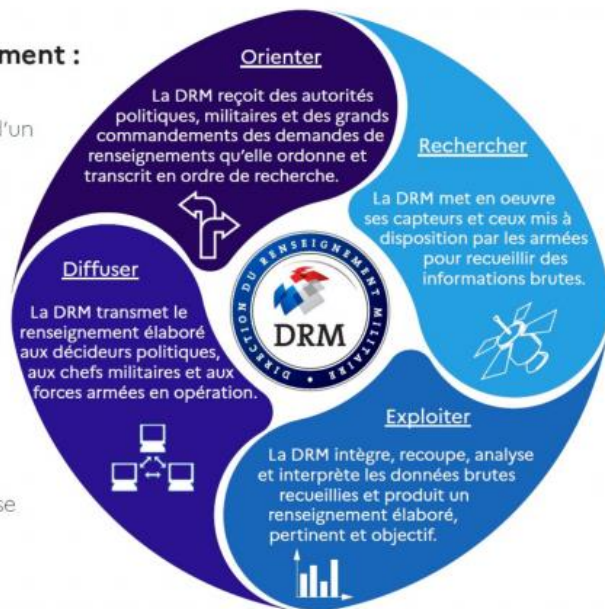
Le cycle du renseignement :

Déclenché par l'expression d'un besoin en renseignement ;

Continu car il organise de manière cohérente et progressive la réalisation des besoins ;

Réactif car il s'achève par la confrontation entre les besoins exprimés et ceux satisfaits, générant ainsi des besoins nouveaux ou une relance de la recherche ;

Dynamique car chaque phase du cycle est activée en permanence.



Le renseignement d'origine cyber et le renseignement d'intérêt cyber

Le renseignement d'origine cyber (ROC)

- exploiter les données en sources ouvertes
- peut être issu de due diligences
- analyse de l'empreinte numérique d'une entité
- analyse des réseaux sociaux (SOCMINT, pour Social Media Intelligence).

Le renseignement d'intérêt cyber (RIC)

- analyse des systèmes d'information
- connaissance des matériels numériques,
- étude des malwares et la rétro-ingénierie pour identifier les auteurs malveillants.

Ces pratiques sont régulées par un cadre légal, notamment en termes de protection des données personnelles dans le cadre du Règlement général sur la Protection des Données (RGPD).

COMMUNAUTÉ



OZINT OpenFacto^o



OSINTOSPHERE



bellÿngcat



SANS
INSTITUTE



xmco

We deliver cybersecurity expertise

OWN-SECURITY

INTRINSEC
Innovative by design

Orange
Cyberdefense

alternativ

THALES

avisa partners

RISK&CO

ANTICIP GROUP

AIRBUS

Owlint
Smart data

PREDICTA
LAB

BAE SYSTEMS

COBWEBS
TECHNOLOGIES

DARKYOWL

Recorded
Future®

SOCIAL LINKS

Cellebrite
OSINT
ANALYZE

FLASHPOINT

GROUP-IB

INTEL471

SHADOWDRAGON

NISOS

MÉTHODOLOGIE

Conseils et astuces

- Une des **erreurs** les plus courantes est de **se lancer** dans la recherche **sans prendre le temps** de clarifier vos pistes connues et les objectifs de votre mission.
- Prendre **quelques minutes** au début d'une nouvelle mission pour **clarifier** les attentes.
- Vous devez **comprendre la technologie** avec laquelle vous travaillez et comment elle peut affecter positivement ou négativement vos résultats. Exemple : l'utilisation d'un VPN/VPS/proxy peut présenter l'avantage de masquer votre adresse IP, mais elle peut aussi vous empêcher de vous connecter à certains sites et services.
- Vous devez être capables d'établir un **processus** d'investigation **structuré** et **reproductible**. Un bon processus peut également améliorer votre efficacité
- L'**organisation du processus d'investigation** réduit également les risques de se perdre au cours de vos recherches.
- **Gestion du temps**: Il est essentiel d'adapter votre approche de l'enquête aux objectifs de la mission et aux contraintes de temps.
- **Erreurs de copier/coller** : l'un des cas les plus courants d'erreur est le résultat de fautes de frappe ou de copier/coller incomplets. Exemple : l'ajout d'un espace au début ou à la fin d'un terme de recherche lorsque nous utilisons nos outils OSINT personnalisés
- **Défaut de conservation** - Il n'y a rien de pire que de trouver un message important pour votre enquête et de découvrir qu'il a été supprimé ou privatisé peu de temps après.
- **Traduire sans attendre**

Conseils et astuces

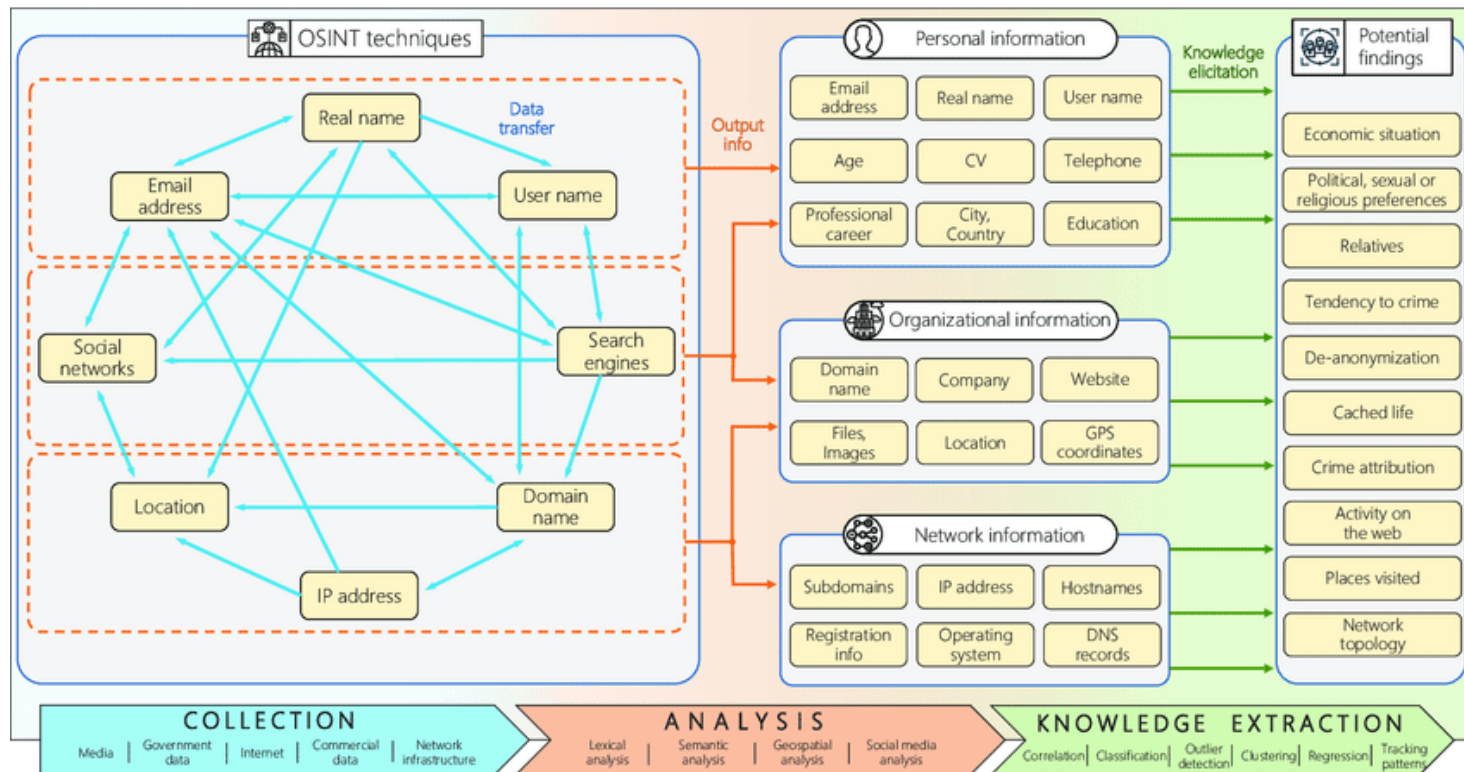
- Une **information** n'est pas utile au processus de **renseignement** tant qu'elle n'est pas de **contextualisé**.
- Une bonne recherche de **sources** permet de rendre les **renseignements exploitables**.
- Un rapport sur les vulnérabilités n'est utile que si le client peut voir exactement où sont exposées ses données personnelles et privées.
- Dans la mesure du possible, vous devez **croiser plusieurs sources**, pour étayer vos conclusions et **éviter les faux positifs**.
- Il est fortement recommandé de **faire relire** votre travail
- **L'OSINT évolue constamment**. Vous ne saurez jamais tout
- Plus vous la **pratiquez**, plus vos **tactiques** seront **efficaces** et **efficaces**.
- Il n'existe **pas de méthode unique** pour mener à bien un travail de renseignement en ligne
- **Esprit critique** : assimilé à la **démarche scientifique**, ou limité à la capacité à faire preuve d'un **doute rationnel**, et souvent cantonné à la correction des **fausses informations**. Il s'agit généralement de discerner le **vrai** du **faux**, mais aussi de la désinformation.

L'art du pivot



One Pivot to rule them all, One Pivot to find them, One Pivot to bring them all, and in the darkness bind them, In the Land of OSINT where the Shadows lie.

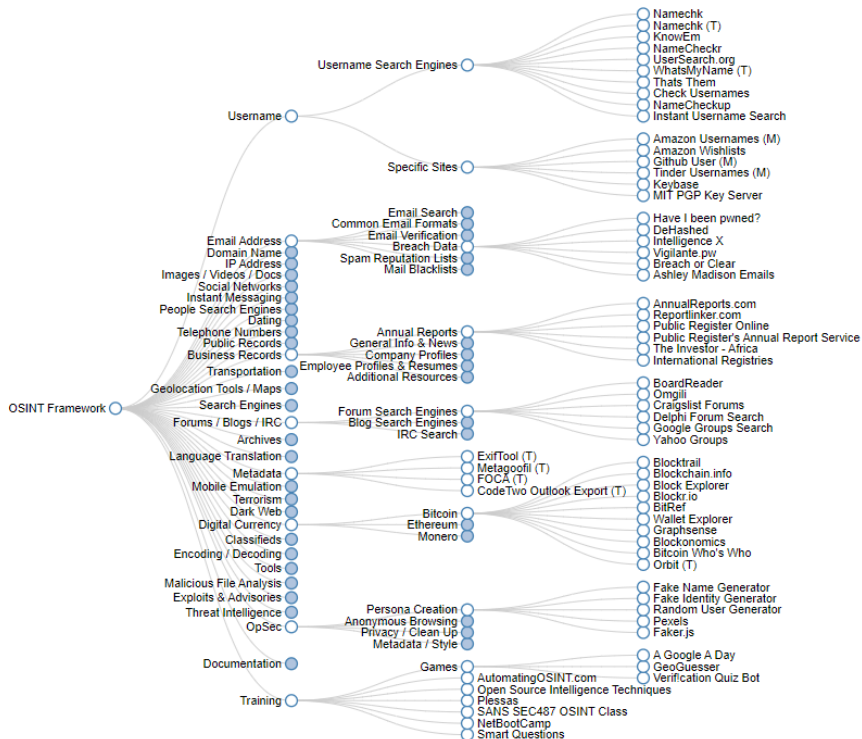
Workflow



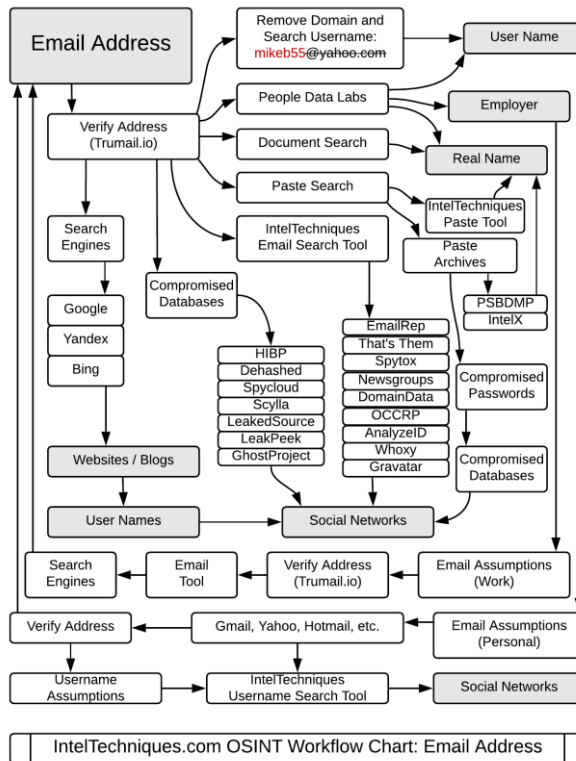
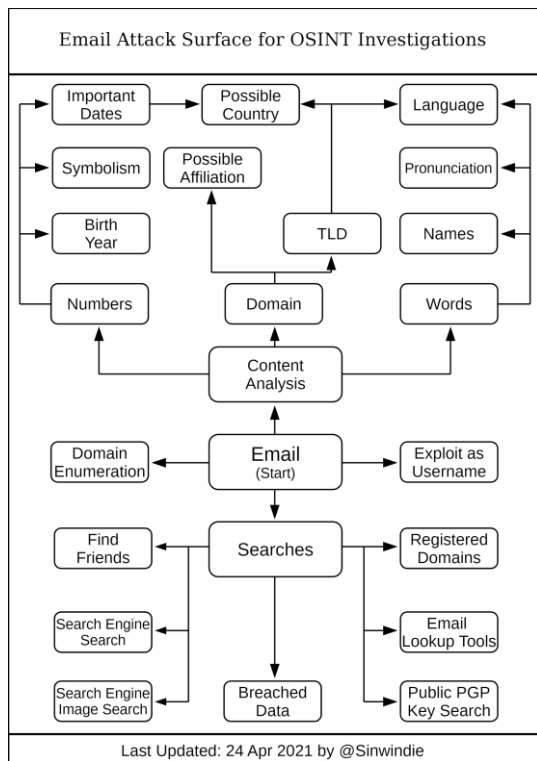
Workflow

OSINT Framework

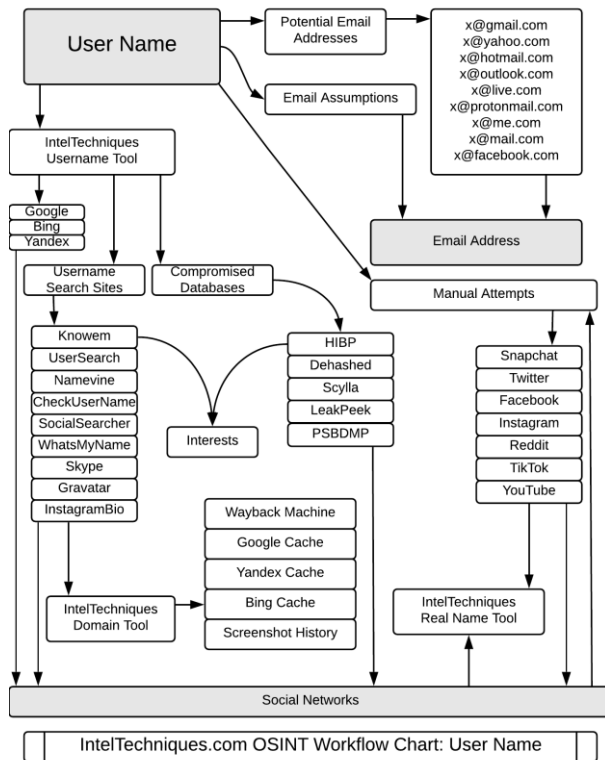
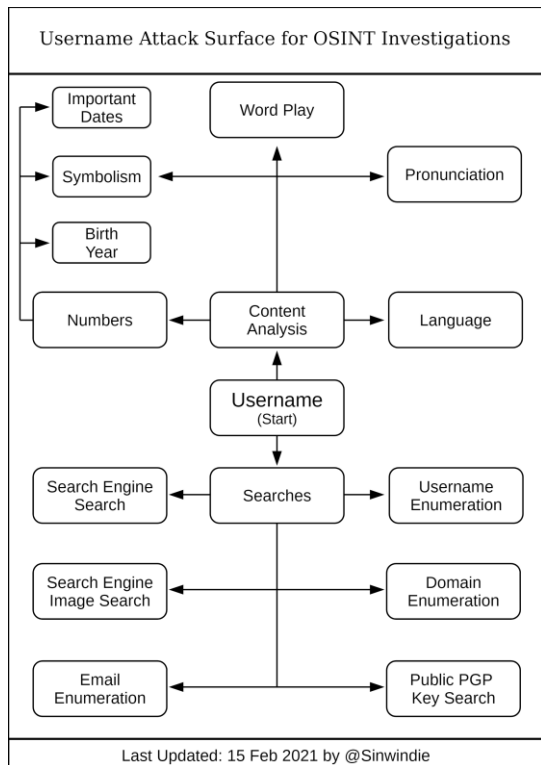
(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: [Google Hacking](#)
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually



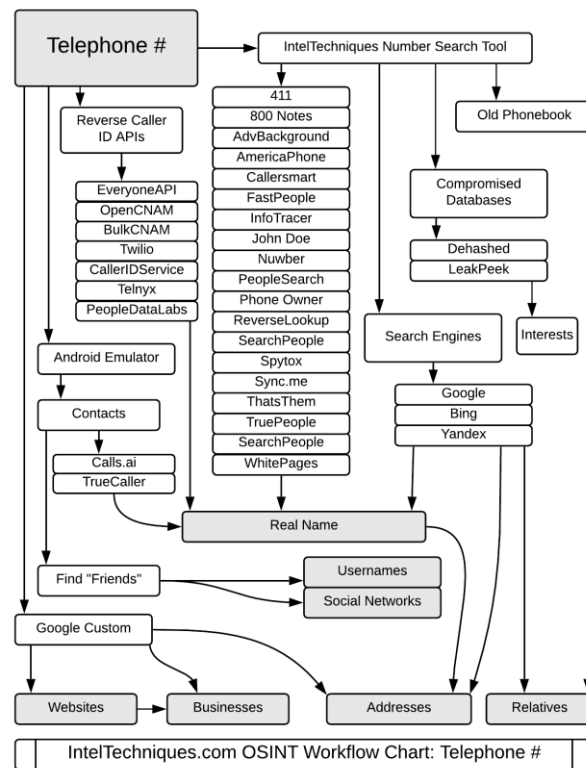
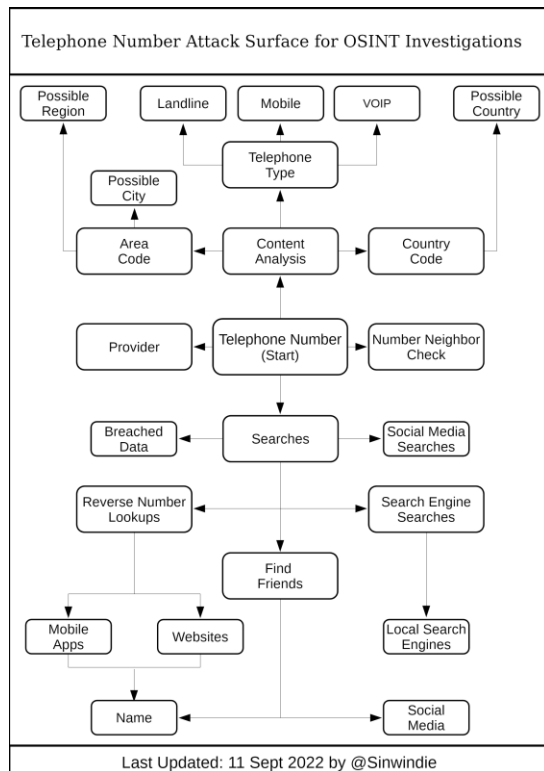
Workflow (email)



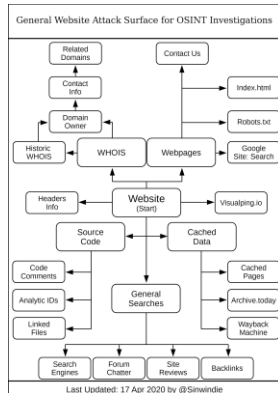
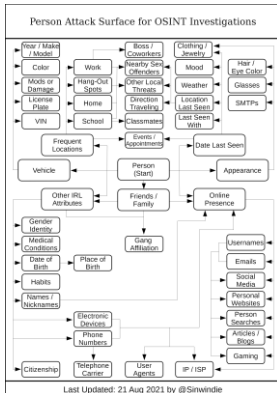
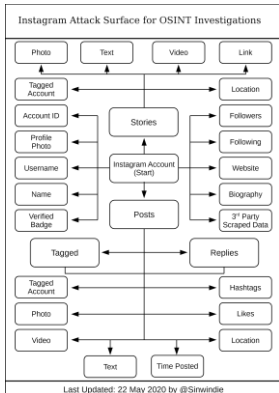
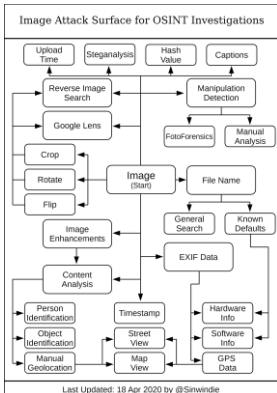
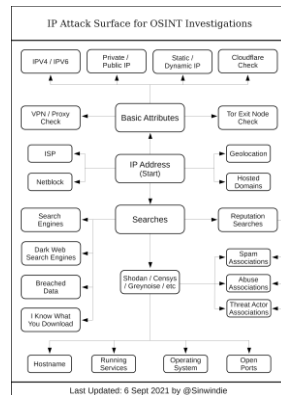
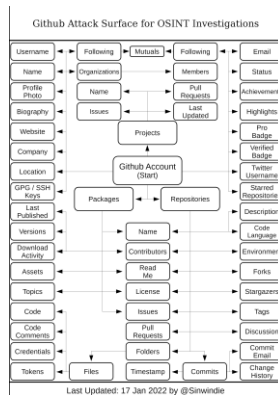
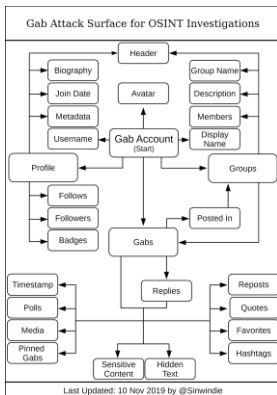
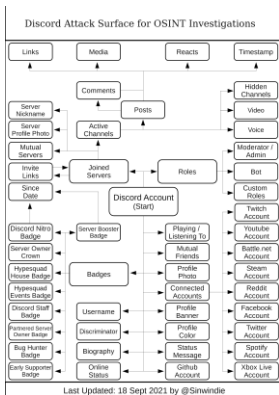
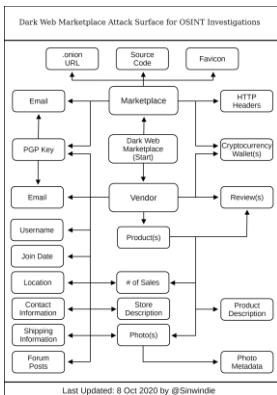
Workflow (username)



Workflow (numéro de téléphone)



Workflow (...)



SECOPS

Cloisonnement

Il est préférable de viser un cloisonnement maximal de ses comptes, outils et infrastructures numériques. L'objectif est de réduire les risques de contamination croisée entre votre travail OSINT et tout actif personnel ou professionnel.

- **La couche interactive** : habitudes sociales, comportementales, communication, etc.
- **Comptes** : Courriel, messagerie, mobile, bureau, médias sociaux, etc.
- **Navigateurs** : cookies, sessions/comptes du navigateur, empreinte numérique du navigateur
- **Poste de travail** : environnement de bureau, compartimentage de votre système d'exploitation et de vos systèmes de fichiers.
- **Connexion** : trafic et association d'IP

Types de cloisonnements :

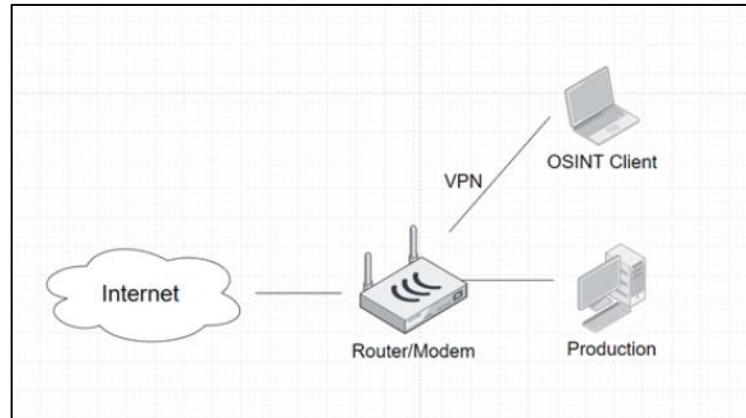
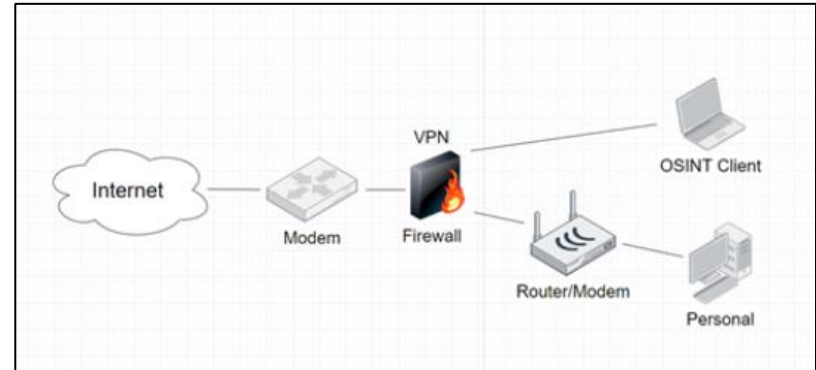
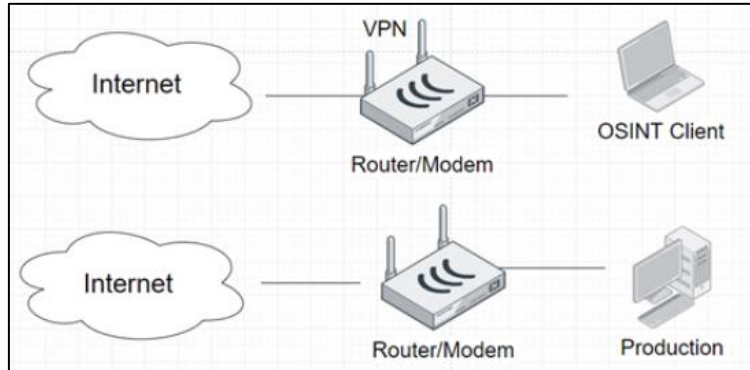
- **Isolation matérielle** : Le scénario idéal est de disposer d'un ordinateur pour les enquêtes, un ordinateur qui n'est utilisé que pour l'OSINT.
- **Dual Boot** : Pas très populaire et moins bénéfique que la véritable isolation matérielle.
- **Isolation virtuelle** : L'approche la plus courante est d'utiliser des machines virtuelles (hyperviseurs) pour compartimenter et surtout isoler plusieurs systèmes d'exploitation
- **Navigateurs sandboxés** - Si vous ne pouvez pas créer une VM complète (authentic8)

Virtualisation



MACHINE VIRTUELLE

Cloisonnement (réseaux)



Distribution/OS



Virtual Private Network (VPN)



Virtual Private Server (VPS)



Emulateur Android

Genymotion



developers 

Navigateur

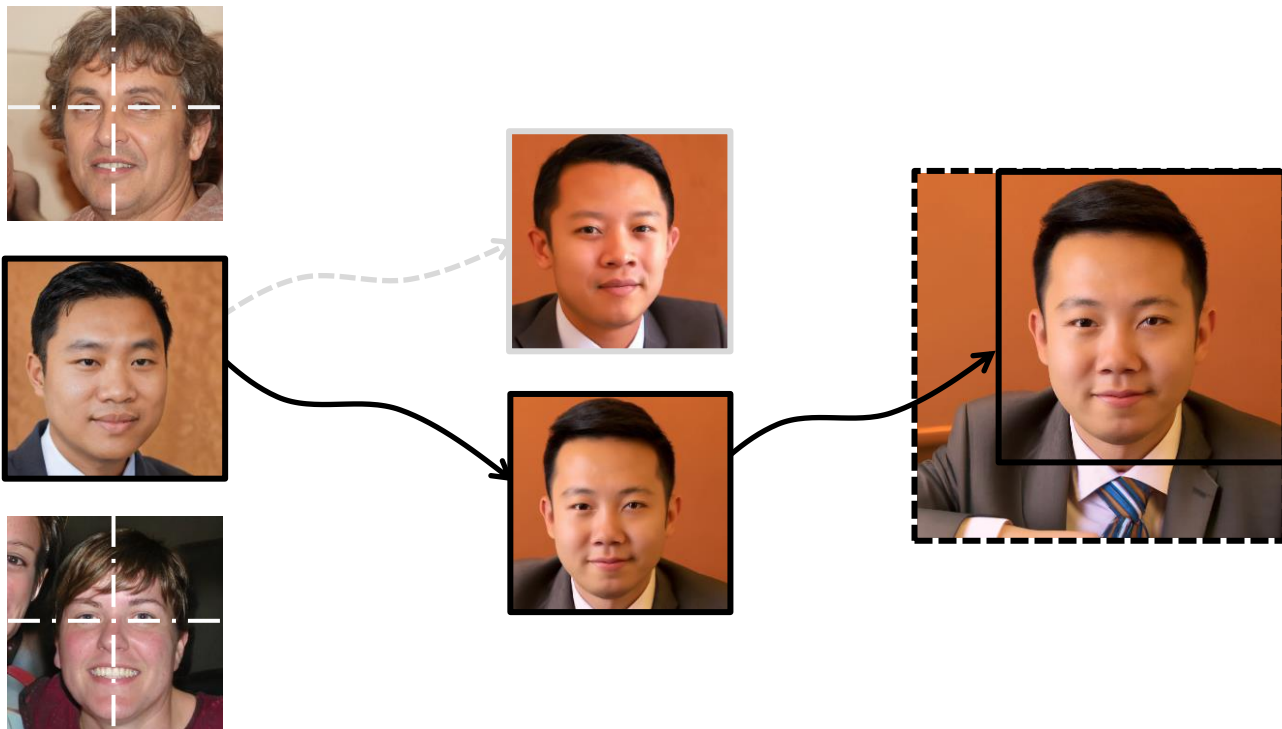


SOCKPUPPET

AVATAR



AVATAR



MERCI POUR VOTRE ATTENTION