CLUSIR
Nouvelle-Aquitaine

SOMMAIRE

ACTU CNA

AFTERWORK OSINT Vol 2

ACTU CNA

Agenda :

- Assemblée Générale, le ~~**mercredi 6 décembre**~~
- Pour 2024 : Sondage en préparation
  - ✓ Volonté d'avoir une visibilité des évènements sur l'année
  - ✓ Planifier les afters sur des jours fixes [6-8 afterworks/an]
  - ✓ Duplex avec le Clusif pour suivre ensemble le Panocrim
  - ✓ Réflexion en cours sur des évènements complémentaires, Webinaires, Podcats, soirées, ...

ACTU CNA

Sujet des Afterworks à venir :

- **Janvier :** Intégration de la sécurité dans le cycle de développement [Cloud, CI/CD, sécurité des données de développement]
- **Mars :** Retex ANSSI sur l'appel à commentaires des documents relatifs à la remédiation
- **Autres sujets en cours d'étude :** Sécurité physique et pentests / ANSSI référentiel PACS / Cryptographie appliquée / Invisibilité sur Internet / … et autres contributions des adhérents…

ACTU CNA

Le CLUSIR NA c'est aussi votre implication :

- **Faites-nous part de vos idées**, vos envies, nous nous chargeons de trouver les intervenants;
- **Vos Retex** (techniques, organisationnels, incidents, …) sont aussi très enrichissants pour le Club n'hésitez pas à contribuer !

AFTERWORK

L’OSINT au service de la cybersécurité

L’OSINT au service de la Cyber Sécurité

Serge RICHARD

Architecte & Consultant Sécurité – CISSP®

srichard@gameon-security.fr

Agenda

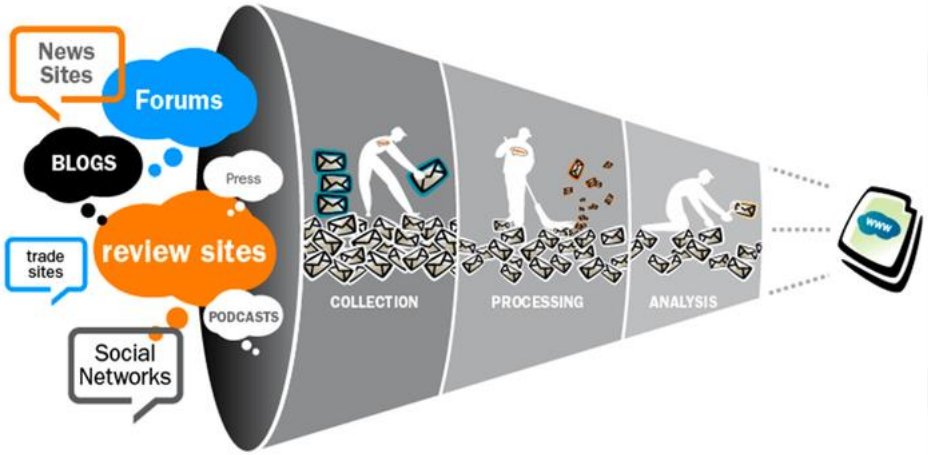
Agenda

A propos de l’OSINT…

- Le **renseignement de sources ouvertes** ou **renseignement d'origine sources ouvertes** (acronyme ROSO), (***open source intelligence***, *OSINT*) est un renseignement obtenu par une source d’information publique.
- L'expression OSINT désigne un **ensemble hétéroclite de pratiques d’investigation et d’analyse** visant à dévoiler une information préalablement dissimulée en récoltant, croisant ou analysant des données numériques disponibles en source ouverte.
- Les **données ouvertes** (*open data*) sont des données numériques dont l'accès et l'usage sont laissés libres aux usagers.
- L'**investigateur** qui recueille ce type de sources est appelé « osinteur ».
- Le développement de cette pratique permet d'observer l'existence d'une **communauté** OSINT.

En fait tout le monde à une part d’osinteur en lui…

En effet, le simple fait d’effectuer une recherche sur le web, d’avoir une interaction avec un contenu, etc.. sont des actions considérées comme de l’OSINT.



Tout le monde fait de l’OSINT… mais pas de la même façon ! (Guardia School)

Source : Wikipédia

Il faut des sources pour faire de l'OSINT…

Les sources de l'*OSINT* peuvent être divisées en six catégories différentes de flux d'informations :

- Les **médias**, journaux imprimés, magazines, radios, chaines de télévision dans les différents pays.
- L'**Internet**, les publications en ligne, les blogs, les groupes de discussion, les médias citoyens, YouTube et autres réseaux sociaux.
- Les **données gouvernementales**, rapports, budgets, auditions, annuaires, conférences de presse, sites web officiels et discours. Ces informations proviennent de sources officielles, mais sont bien publiquement accessibles et peuvent être utilisées librement et gratuitement.
- Les **publications professionnelles** et académiques, provenant de revues académiques, conférences, publications et thèses.
- Les **données commerciales**, imagerie satellite, évaluations financières et industrielles et bases de données.
- La **littérature grise** (qui n'entrent pas dans les circuits habituels d'édition et de distribution, rapports techniques, prépublications, brevets, documents de travail, documents commerciaux, travaux non publiés et lettres d'information.

Source : Wikipédia

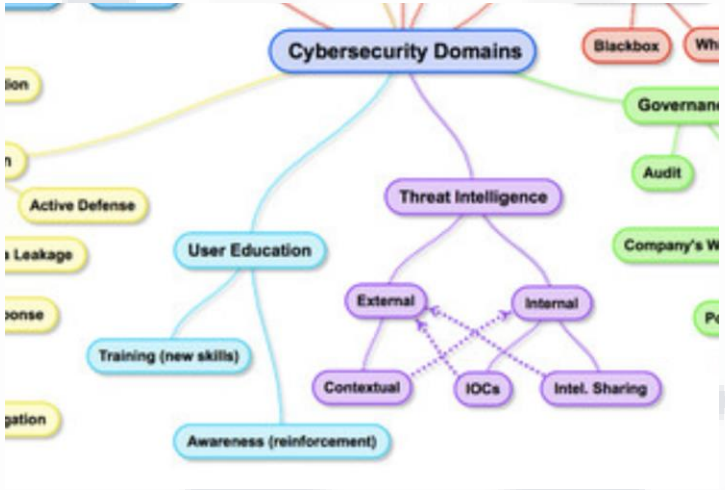
Il faut de la méthode pour faire de l'OSINT…

Postulats :

- Appréhender la quantité astronomique de données publique face à nous.
- Savoir effectuer une recherche.
- Savoir ce que nous cherchons pour savoir comment le chercher (pivot).
- Estimer les ressources techniques nécessaires.
- Gérer ses enquêtes, ses investigations.

Utilisation d'un outil pour nous permettre d'organiser nos investigations :

- cartographie.
- carte mentale.
- prise de note.
- rédaction de rapport.



Source : Diverses

Il faut respecter la loi pour faire de l'OSINT…

Des recherches en OSINT, OK... mais pour quoi faire ?

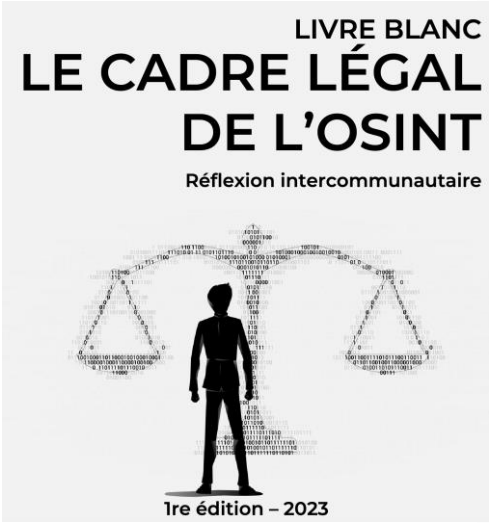
Je vous invite à consulter l'excellent blog sur site Ledieu Avocats concernant ce sujet :

→ https://technique-et-droit-du-numerique.fr

- épisode 1 (27 février 2023) : information ? donnée ? OSINT ? de quoi parle-on ?
- épisode 2 (2 mars 2023) : le droit d'accès légitime (à des données OSINT)
- épisode 3 (9 mars 2023) : le droit de copier des data accessible en OSINT ?
- épisode 4 (16 mars 2023) : le droit de ré-utiliser des data d'origine OSINT
- épisode 5 (23 mars 2023) : quelle preuve légale en droit pénal et en droit civil avec des data d'origine OSINT ?
- épisode 6 (30 mars 2023) : une conclusion ? un rappel du droit de la responsabilité entre employeur et salarié(e) ?

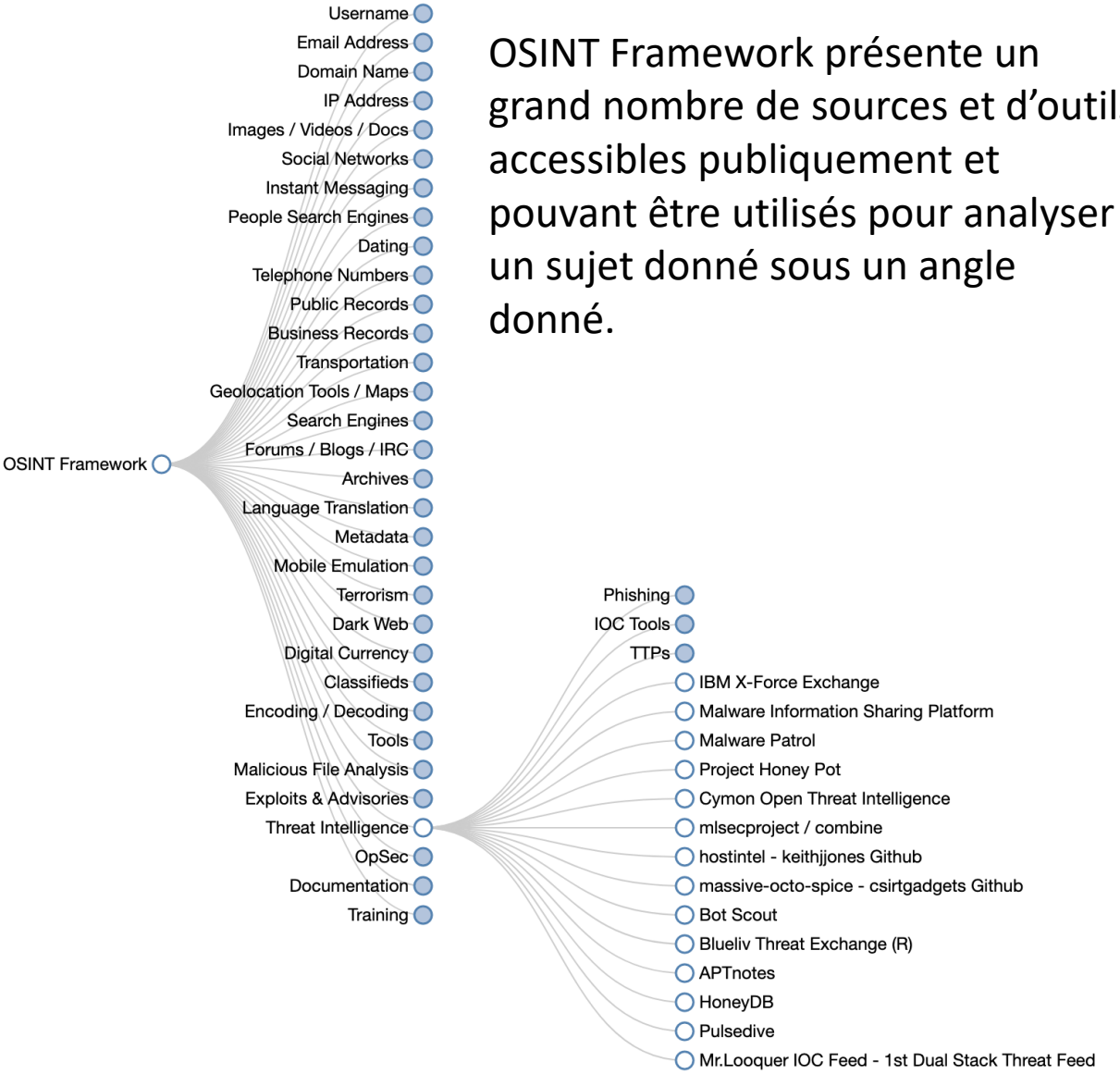
Ainsi que la lecture du livre blanc « le cadre légal de l'OSINT » :

→ https://ozint.eu/livre-blanc-cadre-legal-2023/



Source : technique-et-droit-du-numerique.fr / ozint.eu

Il faut de l'outillage pour faire de l'OSINT…



OSINT Framework présente un grand nombre de sources et d'outils accessibles publiquement et pouvant être utilisés pour analyser un sujet donné sous un angle donné.

Sur la communauté OSINT-FR , vous trouverez une sélection d'outils incontournables pour la pratique de l'OSINT.

Source : OsintFramework / OSINT-FR

Agenda

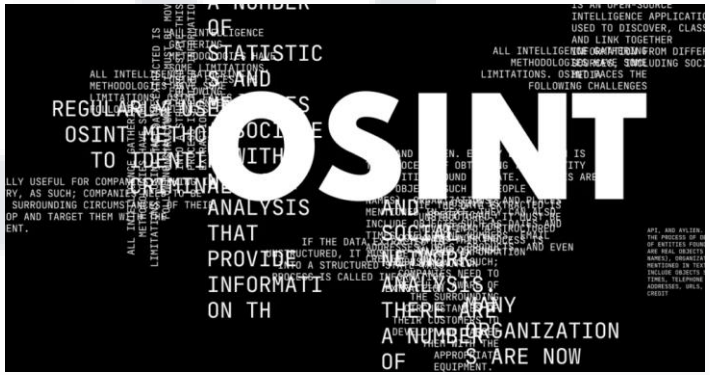
Utilité de l’OSINT pour la cybersécurité

Dans le domaine de la cybersécurité, nous utilisons les données open source pour mieux comprendre le paysage des menaces et aider les entreprises et les particuliers à se protéger des risques connus présents au sein de leur environnement informatique.

Les apports de l’investigation en sources ouvertes à la cybersécurité sont vastes.

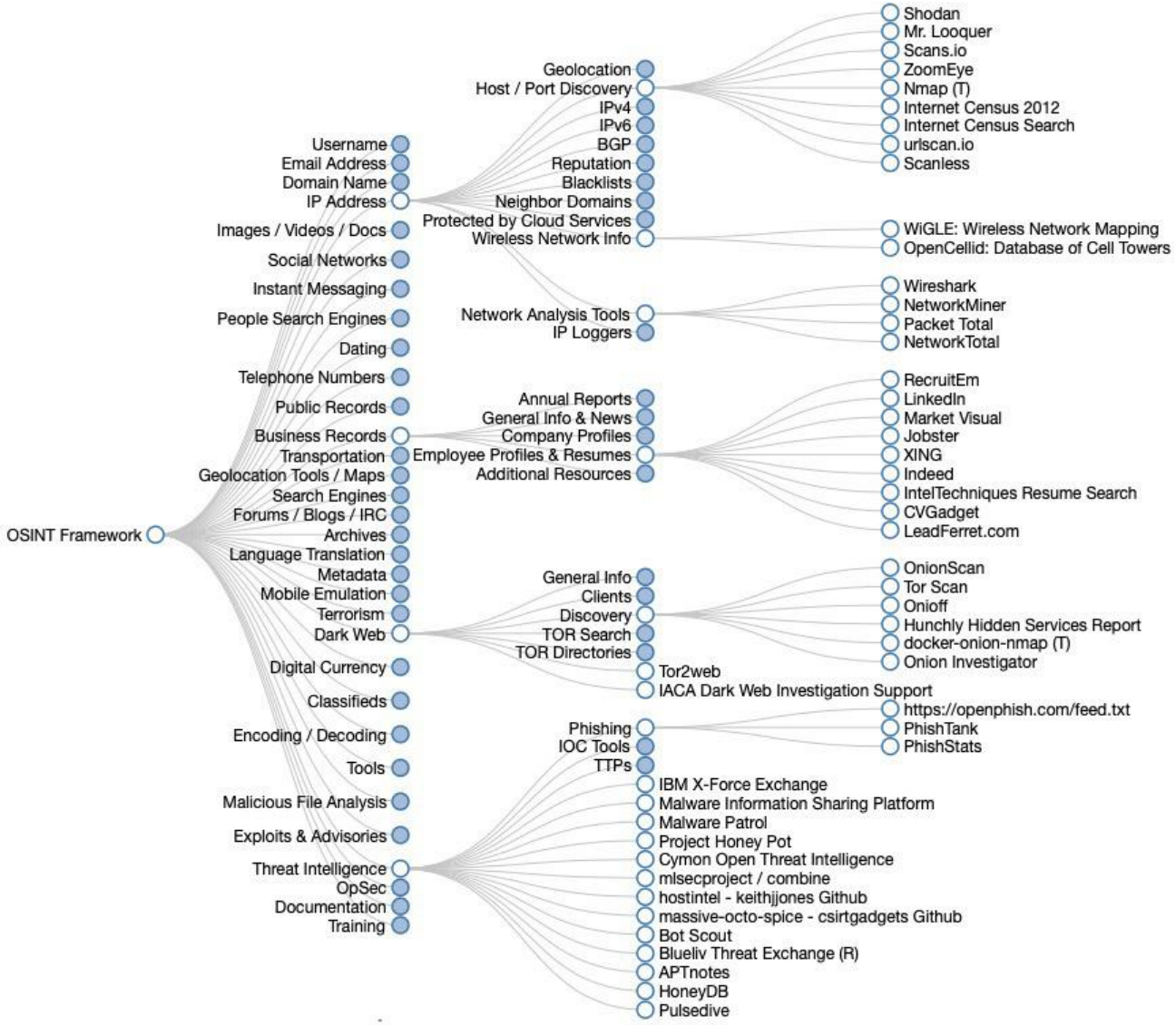
L'OSINT aide les entreprises à :
- Surveiller leur présence et leur réputation en ligne, en identifiant les menaces et vulnérabilités potentielles.
- Comprendre les tactiques, techniques et procédures (TTP) des acteurs menaçants et des cybercriminels.
- Rester informé des dernières vulnérabilités, menaces et tendances du paysage de la cybersécurité.
- Améliorer la connaissance de la situation en identifiant les cibles potentielles, les vecteurs d'attaque et les menaces émergentes.

Il est d’ailleurs très souvent associé les notions d’OSINT et de Cyber Threat Intelligence (CTI).



Source : Diverses

Des outils dédiés à la cybersécurité… ou pas



De nombreux outils sont disponibles pour permettre de découvrir des informations sur les entreprises, sur l'architecture de leur système d'information et sur les employés.

Si ces outils permettent aux entreprises d'analyser leur surface d'attaque et d'essayer d'atténuer les risques, ils permettent aussi aux attaquants de trouver des pivots d'attaques sur les entreprises.

Source : OSINT Framework

OSINT pour l'attaque (cyber offense)

La collecte de reconnaissance ou OSINT est une première étape importante dans une attaque.
Un « attaquant » s'efforce de recueillir autant d'informations sur votre organisation et les cibles potentielles à exploiter.

Un « attaquant » utilise une liste de contrôle exhaustive pour trouver les points d'entrée ouverts et les vulnérabilités au sein de l'organisation.
Le framework OSINT fournit une multitude de détails sur les sources d'informations ouvertes.

Les domaines les plus courants qu'un « attaquant » cartographiera et identifiera incluent :
- Actifs commerciaux : identifier et catégoriser les actifs de grande valeur
  - > Données des employés
  - > Données client
- Données techniques : identifier et catégoriser les menaces internes et externes
  - > Menaces internes : Direction, employés, fournisseurs, etc.
  - > Menaces externes : Ports, protocoles réseau, applications Web, trafic réseau, etc.

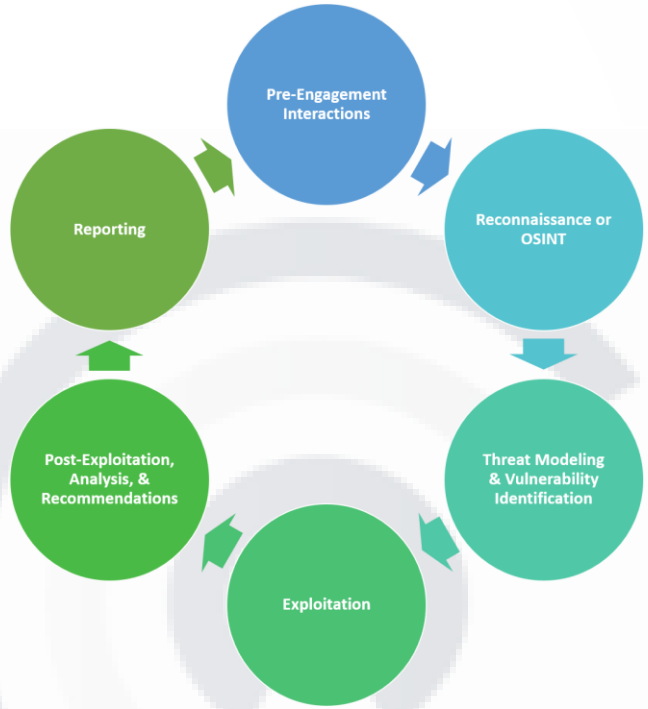
Les tactiques d'exploitation incluent aussi une approche OSINT, avec en autre :
- Attaques d'applications Web
- Attaques réseau
- Attaques Wi-Fi
- Attaque Zéro Day
- Ingénierie sociale
- …

```
msf6 > search type:post platform:android

Matching Modules
================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   post/android/gather/hashdump                                   normal  No     Android Gather Dump Password Hashes for Android S
ystems
   1   post/android/manage/remove_lock_root                           normal  No     Android Root Remove Device Locks (root)
   2   post/android/capture/screen                                    normal  No     Android Screen Capture
   3   post/android/manage/remove_lock               2013-10-11       normal  No     Android Settings Remove Device Locks (4.0-4.3)
   4   post/android/gather/wireless_ap                                normal  No     Displays wireless SSIDs and PSKs
   5   post/android/local/koffee                     2020-12-02       normal  No     KOFFEE - Kia OFFensivE Exploit
   6   post/multi/manage/set_wallpaper                                normal  No     Multi Manage Set Wallpaper
   7   post/multi/manage/play_youtube                                 normal  No     Multi Manage YouTube Broadcast
   8   post/multi/recon/local_exploit_suggester                       normal  No     Multi Recon Local Exploit Suggester
   9   post/multi/gather/enum_software_versions                       normal  No     Multiplatform Installed Software Version Enumerat
or
   10  post/multi/gather/wlan_geolocate                               normal  No     Multiplatform WLAN Enumeration and Geolocation
   11  post/android/gather/sub_info                                   normal  No     extracts subscriber info from target device

Interact with a module by name or index. For example info 11, use 11 or use post/android/gather/sub_info
```



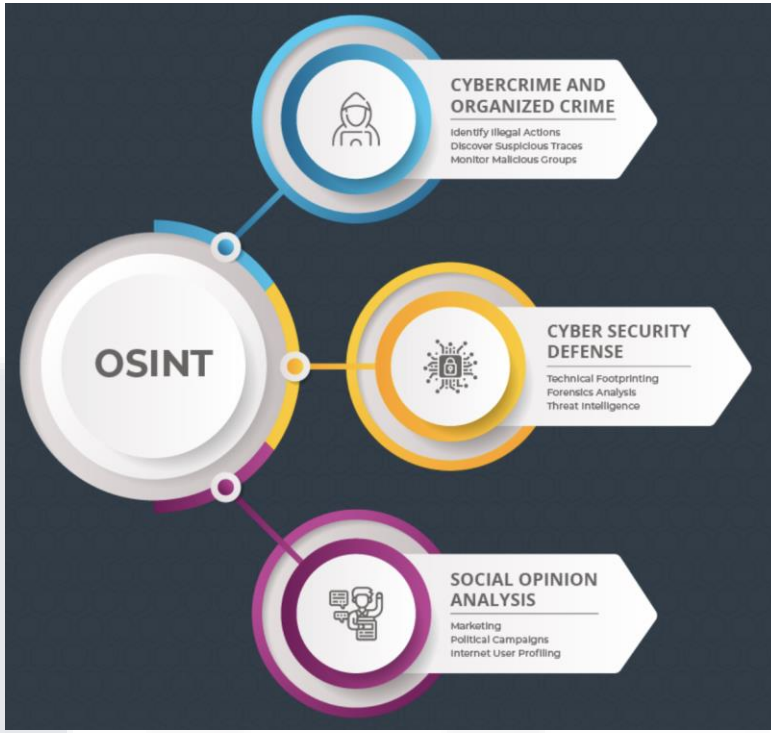
Source : Cypher

OSINT pour la défense (cyber defense)

Tests d'intrusion

Les professionnels de la sécurité utilisent les renseignements open source (OSINT)
pour découvrir les faiblesses potentielles des réseaux de l'organisation,
afin qu'elles puissent être corrigées avant qu'elles ne soient exploitées par des acteurs malveillants.
Les vulnérabilités fréquemment trouvées incluent :

- Ports ouverts ou appareils connectés à Internet non sécurisé.
- logiciels non corrigés.
- Habilitation des comptes utilisateurs.
- Fuite accidentelle d'informations sensibles.
- …



Source : DTS Solution

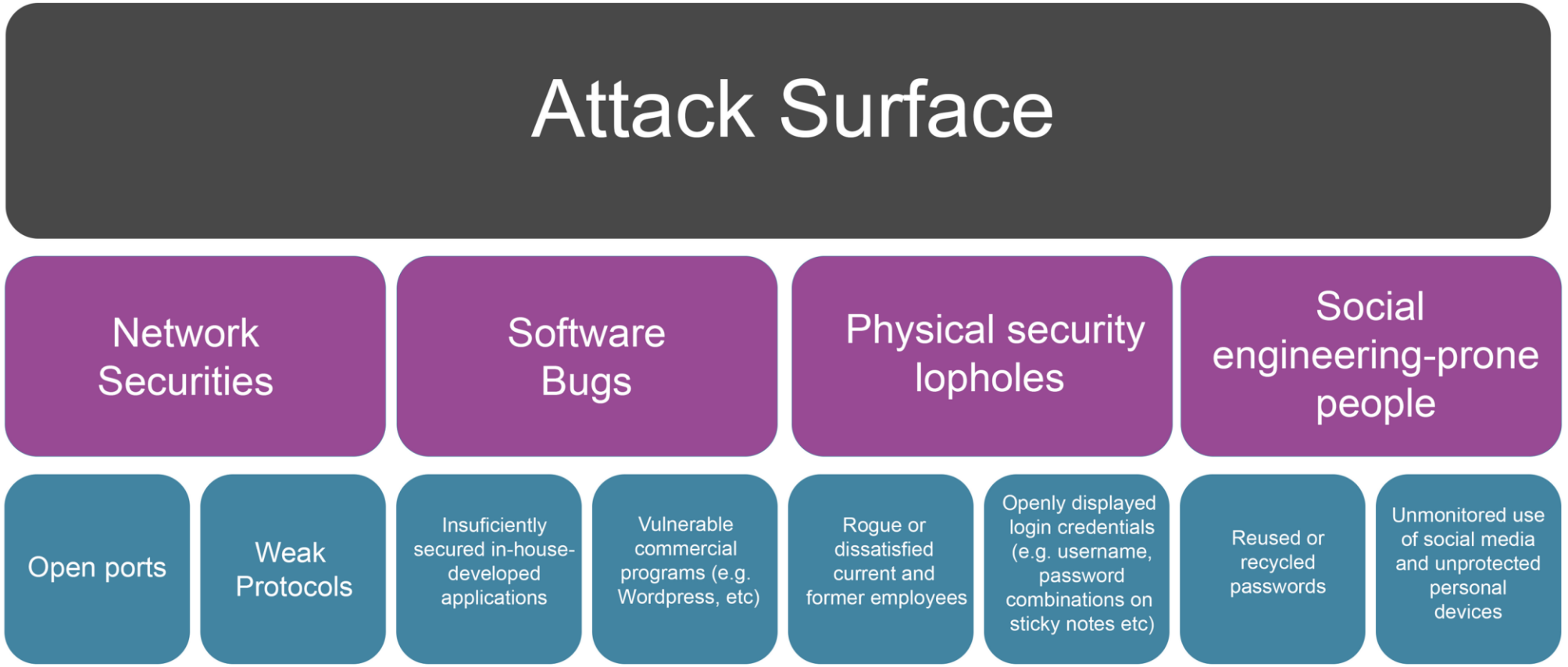
Identifier les menaces

L'OSINT permet aux professionnels de la sécurité informatique de prioriser leur temps
et leurs ressources pour faire face aux menaces les plus importantes afin de prévenir
et d'atténuer les violations de données, de contrecarrer les cyberattaques et également d'identifier
les nouvelles vulnérabilités activement exploitées.

Agenda

La surface d’attaque…

La surface d’attaque, qui fait référence aux points d’entrée que les attaquants peuvent utiliser pour accéder à un système d’information.
Une évaluation de la surface d'attaque identifie et analyse ces points d'entrée pour identifier les vulnérabilités que les attaquants pourraient exploiter pour accéder à votre système d’information.
Rappel : Un **vecteur d'attaque** est la façon dont un attaquant tente d'accéder, tandis que la **surface d'attaque** est ce qui est attaqué.

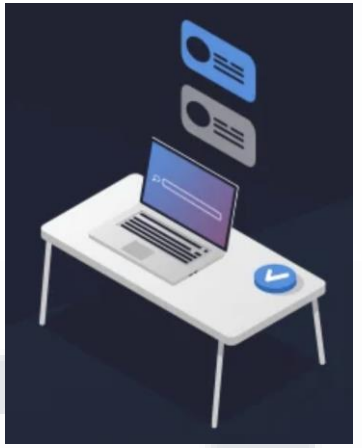


Source : AppCheck

Collecte Passive vs Collecte Active

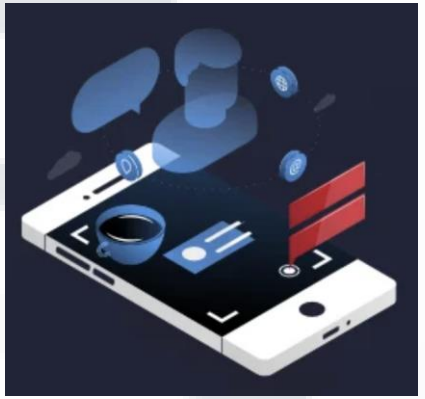
Collecte passive :

- Il s’agit de la forme de collecte de renseignements la plus utilisée.
- La collecte passive de données consiste à collecter des données librement disponibles à partir d'une source de données tierce telle qu'un moteur de recherche ou un site Web de renseignements sur les menaces.
- Les méthodes de collecte OSINT utilisent la collecte passive, car l'objectif principal de la collecte OSINT est de collecter des informations sur la cible via des sources de données accessibles au public sans avoir à interagir directement avec une cible.
- La reconnaissance passive permet à tout enquêteur de recueillir des informations en toute sécurité sans avoir besoin de converser directement avec une cible de manière à avertir la cible qu'elle fait l'objet d'une attaque ou à exposer l'attaquant à une détection.



Collecte active :

- l'OSINT actif nécessite un niveau d'interaction avec la cible afin de collecter des données.
- Contrairement à la collecte d’informations passive qui repose sur des informations accessibles au public, la collecte active d’OSINT implique une enquête ou une communication directe (par exemple avec les employés via l’ingénierie sociale, ou avec l’infrastructure d’une cible via une enquête réseau active).
- La collecte de données via ces mesures actives présente un risque plus élevé pour l'attaquant/enquêteur d'être détecté par la cible.
- Cela peut cependant donner lieu à des données plus ciblées, à jour et plus pertinentes que celles disponibles via des techniques purement passives.



Source : AppCheck

OSINT Cyber : Moteurs de recherche

Les moteurs de recherche sont un élément fondamental des opérations Open Source Intelligence (OSINT). Ils fournissent un moyen puissant de découvrir et d'accéder à des informations accessibles au public.

Techniques de recherche avancées : Les techniques de recherche avancées vous permettent d'affiner vos requêtes de recherche et d'obtenir des résultats plus précis. Ces techniques impliquent l'utilisation d'opérateurs de recherche et de modificateurs de requête pour cibler des informations spécifiques.

Utiliser les moteurs de recherche spécialisés : Les moteurs de recherche spécialisés sont conçus pour indexer et rechercher des types spécifiques.

Base de données de piratage Google (GHDB) : GHDB est une compilation de requêtes de recherche, également connue sous le nom de Google Dorks, qui exploitent des techniques de recherche avancées pour trouver des informations sensibles, des erreurs de configuration ou des vulnérabilités exposées sur Internet.

Plateformes de médias : SOCMINT fait référence à la collecte, à l'analyse et à l'interprétation d'informations provenant des plateformes de médias sociaux (profilage personnel et organisationnel, l'analyse des sentiments et la surveillance des tendances.

Analyser les sentiments et les tendances : L'analyse des sentiments est le processus consistant à déterminer le sentiment ou l'émotion derrière un morceau de texte, tandis que l'analyse des tendances implique l'identification de modèles ou de tendances dans de grands ensembles de données.

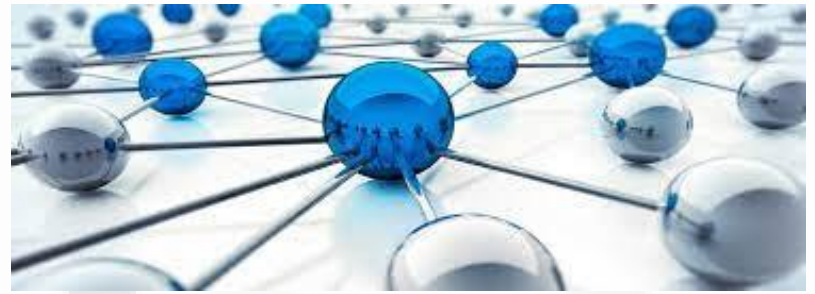
Source : hacksheets

OSINT Cyber : Domaine & IP

Énumération DNS et informations WHOIS : L'énumération du système de noms de domaine (DNS) implique la collecte d'informations sur un domaine et ses adresses IP, sous-domaines et enregistrements DNS associés. Les informations WHOIS fournissent des détails sur la propriété du domaine, l'enregistrement et les informations de contact. Ces deux sources de données peuvent être précieuses.

Analyse IP et ASN : Les adresses IP et les numéros de système autonome (ASN) peuvent fournir des informations essentielles sur l'infrastructure réseau d'une organisation et ses connexions à Internet.
L'analyse des adresses IP et des ASN peut aider à identifier :

- Localisation géographique des serveurs.
- Plages de réseau et espaces d'adressage.
- Fournisseurs d'accès Internet (FAI) et hébergeurs.
- Relations entre les différents réseaux.



Reconnaissance passive et active : La reconnaissance est le processus de collecte d'informations sur l'infrastructure réseau, les systèmes et les vulnérabilités d'une cible.

- La reconnaissance passive implique la collecte d'informations sans interagir directement avec la cible, comme l'observation des enregistrements DNS, l'analyse des informations WHOIS et la surveillance de l'activité des réseaux sociaux.
- La reconnaissance active, quant à elle, implique une interaction directe avec les systèmes de la cible, comme la recherche de ports ouverts, la réalisation d'évaluations de vulnérabilité ou la tentative d'accès aux pages de connexion. Même si la reconnaissance active peut fournir des informations plus détaillées, elle comporte également un risque de détection plus élevé et peut avoir des implications pénales.

Source hacksheets

OSINT Cyber : Applications WEB

Appréhender l'architecture des applications Web est essentiel pour identifier les vulnérabilités et les vecteurs d'attaque potentiels.
L'architecture des applications Web se compose généralement de trois composants principaux :
- le côté client (front-end).
- le côté serveur (back-end).
- la base de données.

Identifier et exploiter les erreurs de configuration : Des configurations incorrectes dans les applications Web peuvent conduire à des failles de sécurité qui peuvent être exploitées par les acteurs malveillants.
Les erreurs de configuration courantes incluent :
- Paramètres ou autorisations par défaut non sécurisés
- Contrôles d'accès et mécanismes d'authentification inappropriés
- Logiciels non corrigés ou bibliothèques obsolètes Pour identifier et exploiter les erreurs de configuration

Les professionnels de la cybersécurité utilisent divers outils et techniques, tels que des scanners de vulnérabilité, une révision manuelle du code et des tests d'intrusion.

Technologies Web de prise d'empreintes (fingerprint) : Ces technologies impliquent l'identification des logiciels, des bibliothèques et des frameworks utilisés par une application Web.
Ces informations peuvent être précieuses pour OSINT et les tests d'intrusion, car elles peuvent révéler des vulnérabilités potentielles ou des composants obsolètes pouvant être exploités.

Source : hacksheets

OSINT Cyber : Géospatial (GEOINT)

Outils de cartographie et de géolocalisation : Les outils de cartographie et de géolocalisation permettent la visualisation et l'analyse des données spatiales, fournissant ainsi un contexte et des informations précieuses pour les activités OSINT.

Analyse d'images satellite : L'analyse d'images satellitaires consiste à examiner des images prises par des satellites pour recueillir des informations sur un emplacement ou une zone spécifique.
Cette analyse peut révéler :
- Détails de l'infrastructure, tels que les bâtiments, les routes et les ponts.
- Modèles de végétation et d'utilisation des terres.
- Changements environnementaux, tels que la déforestation ou l'étalement urbain.

Données de géolocalisation et risques liés à la confidentialité : Ces données font références aux informations associées à un emplacement géographique spécifique, telles que les coordonnées GPS ou les adresses physiques. Ces données peuvent être trouvées dans diverses sources, notamment les publications sur les réseaux sociaux, les photographies numériques et les appareils IoT.
Si les données de géolocalisation peuvent fournir des informations précieuses sur les activités OSINT, elles présentent également des risques en matière de confidentialité, car elles peuvent révéler des informations sensibles sur des individus ou des organisations.
Lorsque vous travaillez avec des données de géolocalisation, il est essentiel de prendre en compte les implications éthiques et juridiques, en veillant à ce que les informations collectées soient utilisées de manière responsable et ne portent pas atteinte à la vie privée des individus ou des organisations.

Source : hacksheets

OSINT Cyber : Dark Web et CTI

Naviguer sur le dark web en toute sécurité : Le dark web est une partie d'Internet qui n'est pas indexée par les moteurs de recherche traditionnels et qui nécessite des outils spécifiques, tels que le navigateur Tor, pour y accéder.
Il est essentiel de naviguer sur le dark web en toute sécurité, car il peut s'agir d'un environnement dangereux et imprévisible.

Identifier et surveiller les cybermenaces : Le renseignement sur les cybermenaces implique la collecte, l'analyse et le partage d'informations sur les menaces et vulnérabilités potentielles.
Le dark web peut être une source d'informations précieuse pour identifier et surveiller les cybermenaces, telles que :

- Exploits et vulnérabilités du jour zéro.
- Distribution de logiciels malveillants et de rançongiciels.
- Forums et marchés cybercriminels.
- Campagnes de phishing et techniques d'ingénierie sociale.

Analyser le comportement cybercriminel : Comprendre le comportement des cybercriminels peut fournir des informations sur leurs tactiques, techniques et procédures (TTP), ce qui peut contribuer à améliorer la sécurité de votre organisation.
L'analyse du comportement des cybercriminels implique la surveillance des forums, des salons de discussion et des marchés sur le dark web, ainsi que l'étude des attaques, campagnes et tendances passées.

Source : hacksheets

OSINT Cyber : Vols et Fuites d’information

Identifier les vols de données : Les vols de données se produisent lorsque des personnes non autorisées accèdent à des données sensibles (en autre), ce qui peut entraîner d'importants dommages financiers et de réputation. L'identification des vols de données implique de surveiller diverses sources, telles que :
- Forums et marchés du Dark Web, où les données volées sont souvent vendues ou partagées.
- Blogs de sécurité et sites d'actualités, qui rendent compte des failles et vulnérabilités majeures.

Analyser les données divulguées : L'analyse des données divulguées peut aider à identifier les risques et les vulnérabilités potentiels au sein d'une organisation ou d'un système.
Cette analyse peut impliquer :
- Vérifier l'authenticité des données divulguées.
- Identifier les types de données compromises, telles que les informations personnelles, les informations financières, etc.
- Évaluer l'impact potentiel sur l'organisation et ses parties prenantes.

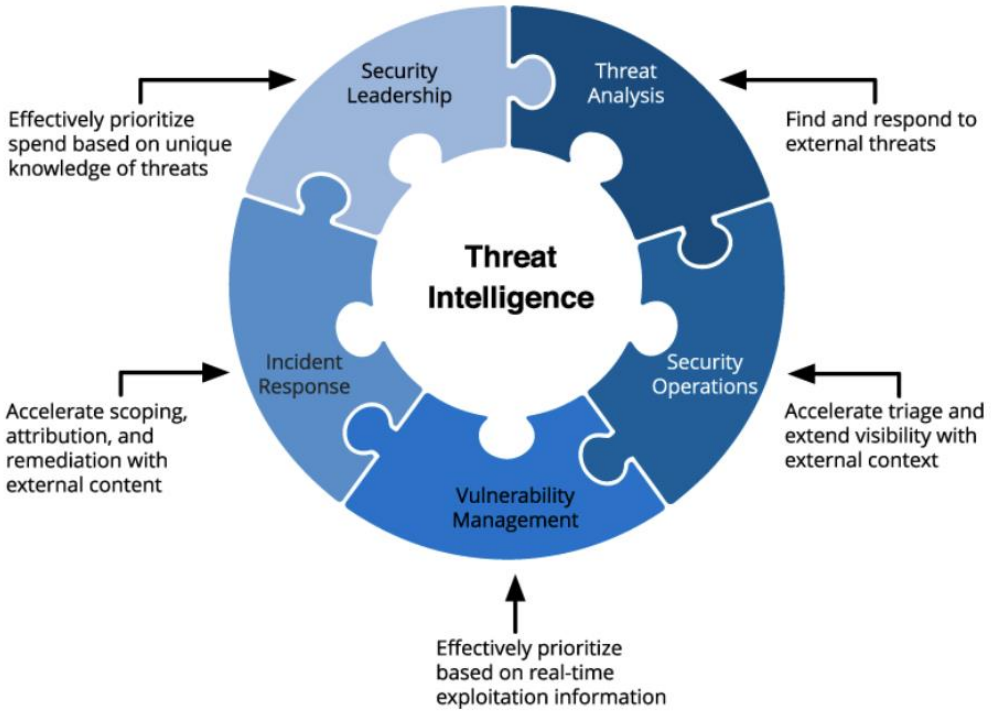
Atténuer les risques associés aux fuites de données : Pour atténuer les risques associés aux fuites de données, les organisations doivent prendre plusieurs mesures préventives et réactives, notamment :
- Mise en œuvre de mesures de sécurité robustes, telles que le chiffrement, les contrôles d'accès et les mises à jour logicielles régulières.
- Réalisation régulière d'audits de sécurité et d'évaluations des vulnérabilités.
- Établir un plan de réponse aux incidents pour gérer et contenir efficacement les vols de données.
- Proposer des programmes de formation et de sensibilisation aux employés pour améliorer leurs pratiques en ce qui concerne la sécurité de l’information.

Source : hacksheets

Agenda

OSINT CTI : Définition

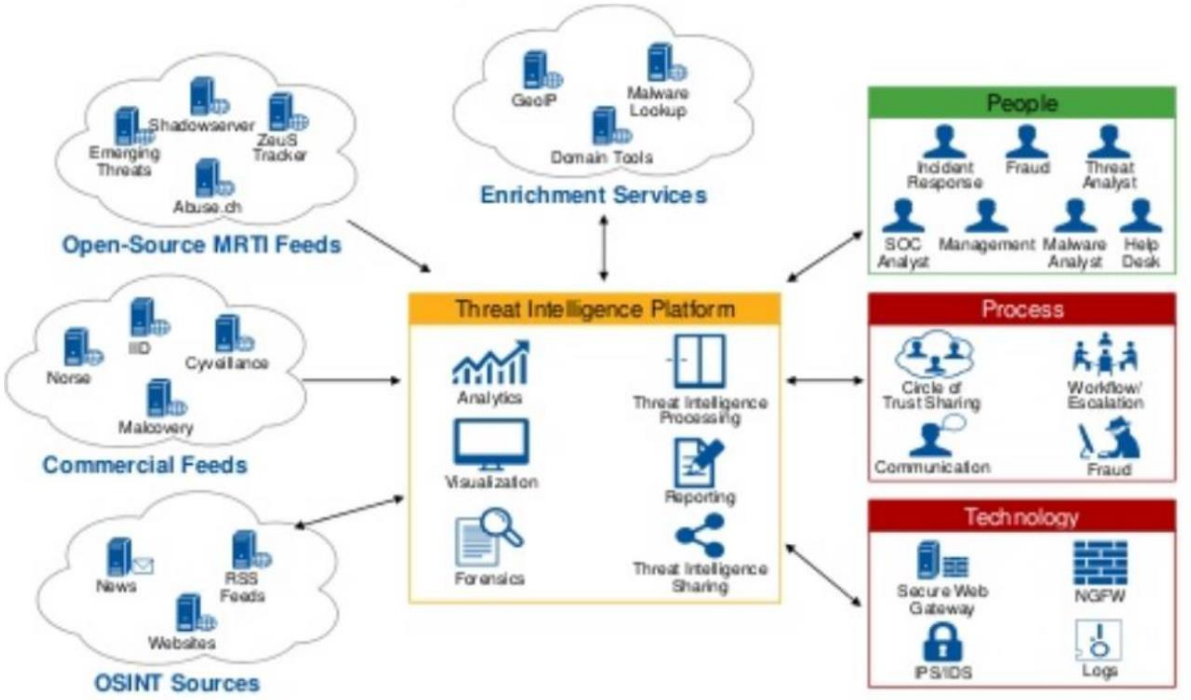
La **Threat Intelligence**, ou **Cyber Threat Intelligence** (**CTI**) est une discipline basée sur des techniques du renseignement, qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyberespace (cyber-attaques), afin de dresser un portrait des attaquants ou de mettre en exergue des tendances (secteurs d'activités touchés, méthode utilisée, etc.).
Ce profiling permet de mieux se défendre et d'anticiper au mieux les différents incidents en permettant une détection aux prémices d'une attaque d'envergure.



Source : Wikipedia / Enisa

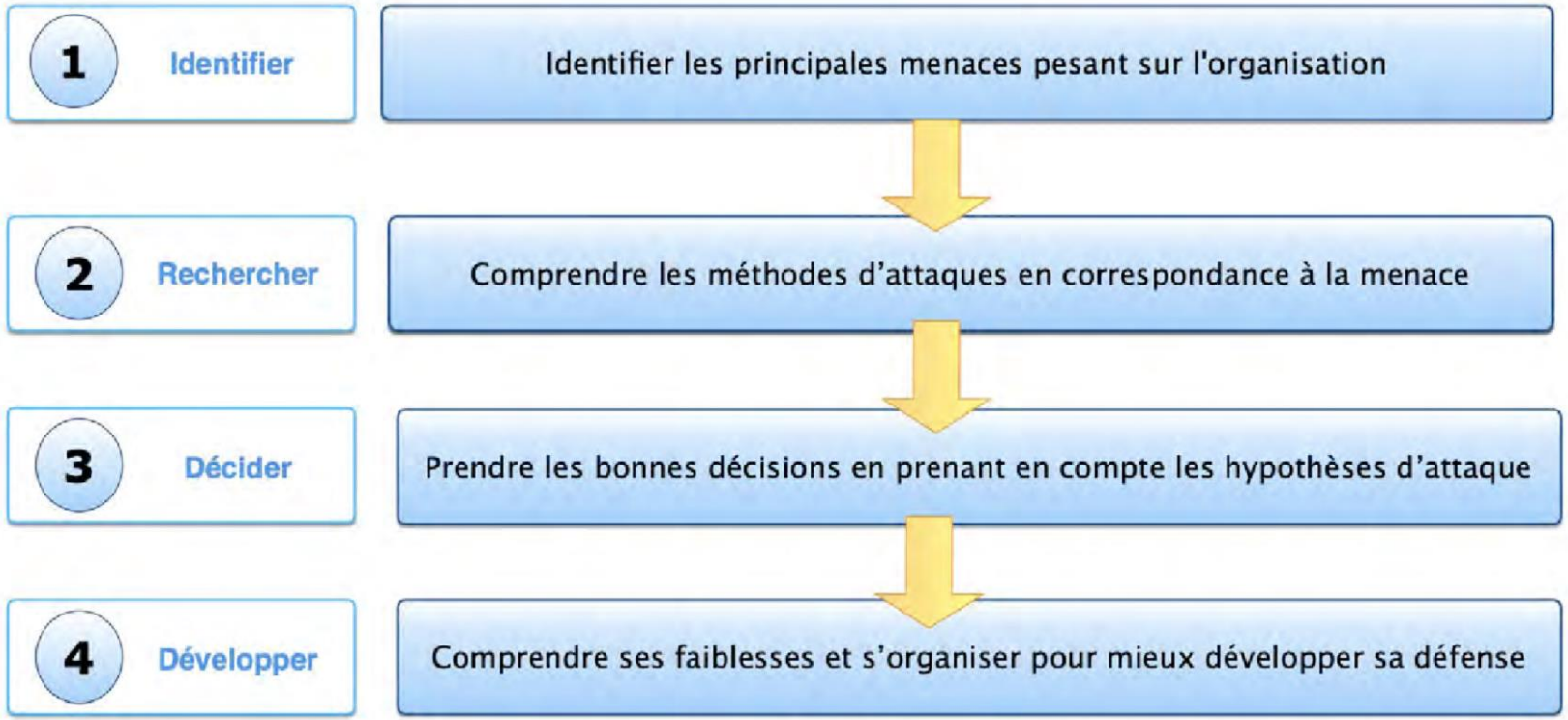
OSINT CTI : Définition TIP

Une **Threat Intelligente Platform** est une approche technologique qui participe aux programmes de renseignement sur les menaces des entreprises et des organisations et les aide à améliorer leurs capacités de renseignement sur les cybermenaces.
Les **TIP** permettent aux entreprises et aux organisations d'amorcer facilement les processus de base de collecte, de normalisation, d'enrichissement, de corrélation, d'analyse, de diffusion et de partage des informations relatives aux menaces.



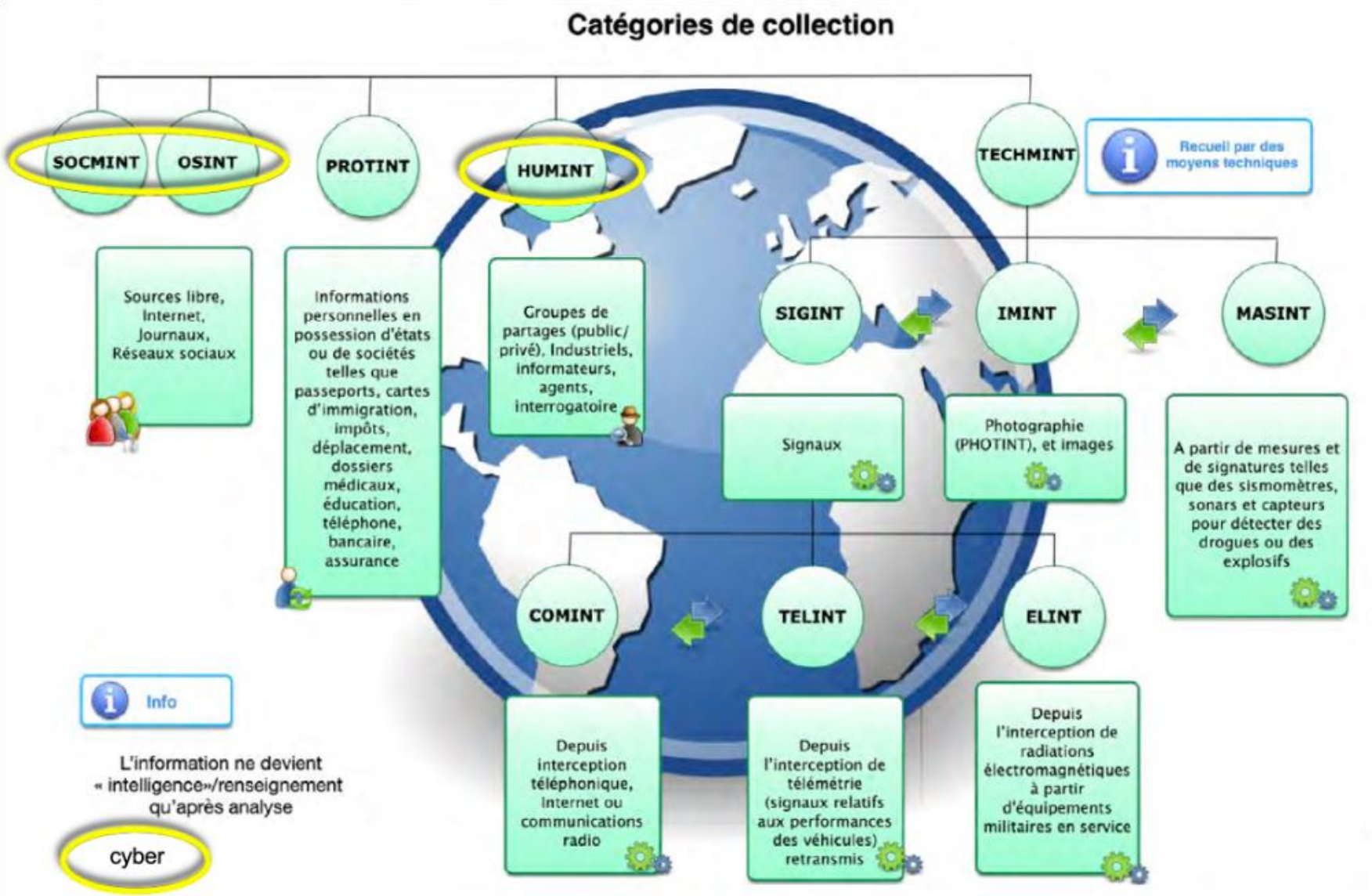
Source : Enisa

OSINT CTI : Les apports



Source : Abakus

OSINT CTI : Domaines de collection



Source : Abakus

OSINT CTI : Domaines de collection (suite)

Sources libre, Internet, Journaux, Réseaux sociaux

OSINT

- Plate-forme de Threat Intelligence
- « bac à sable » de malware
- Services de réputations
- Rapports de menace
- Sources (feeds)
- Solutions et produits

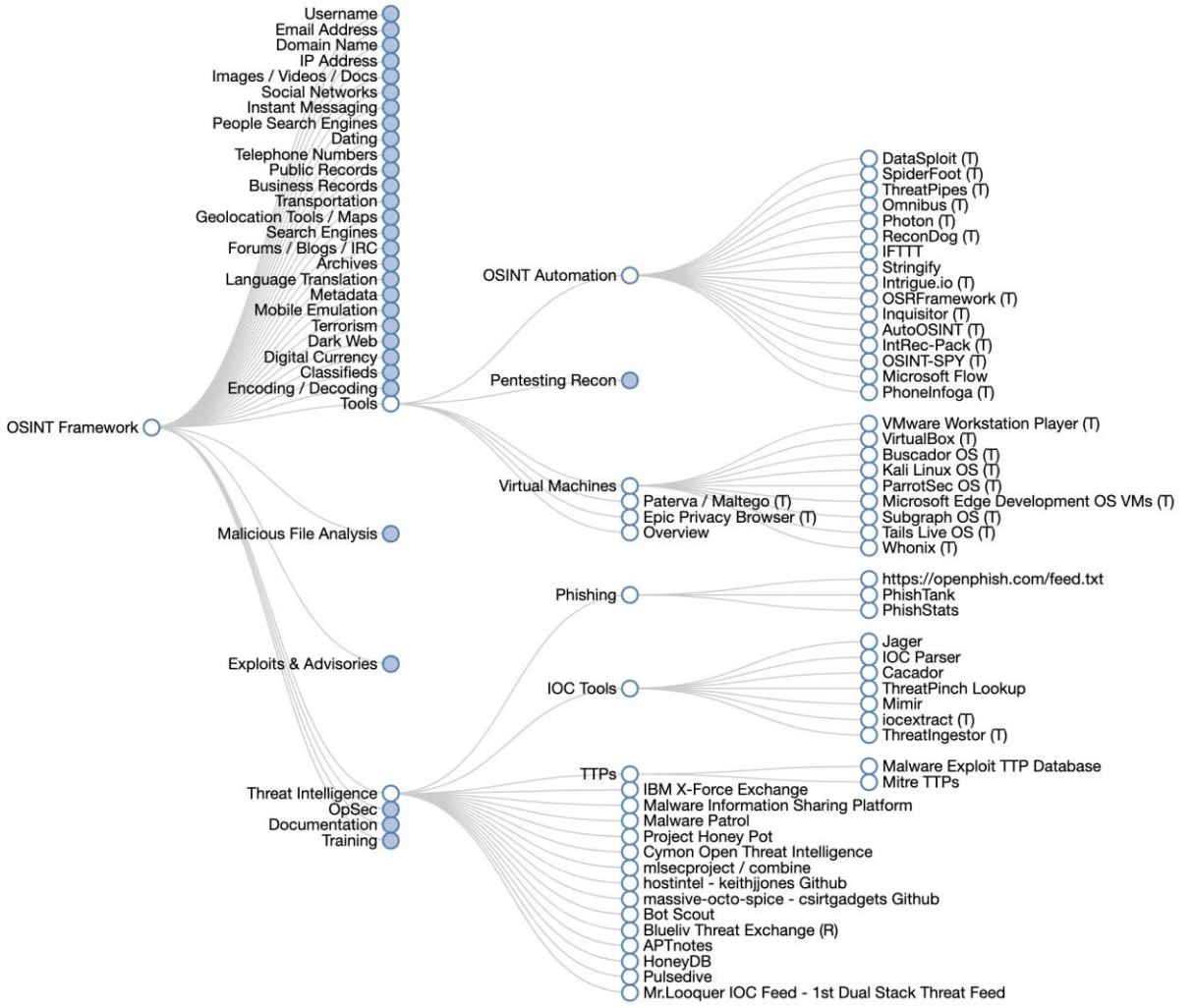
SOCMINT

- Réseaux sociaux
- Médias
- Fake news

Groupes de partages (public/ privé), Industriels, informateurs, agents, interrogatoire

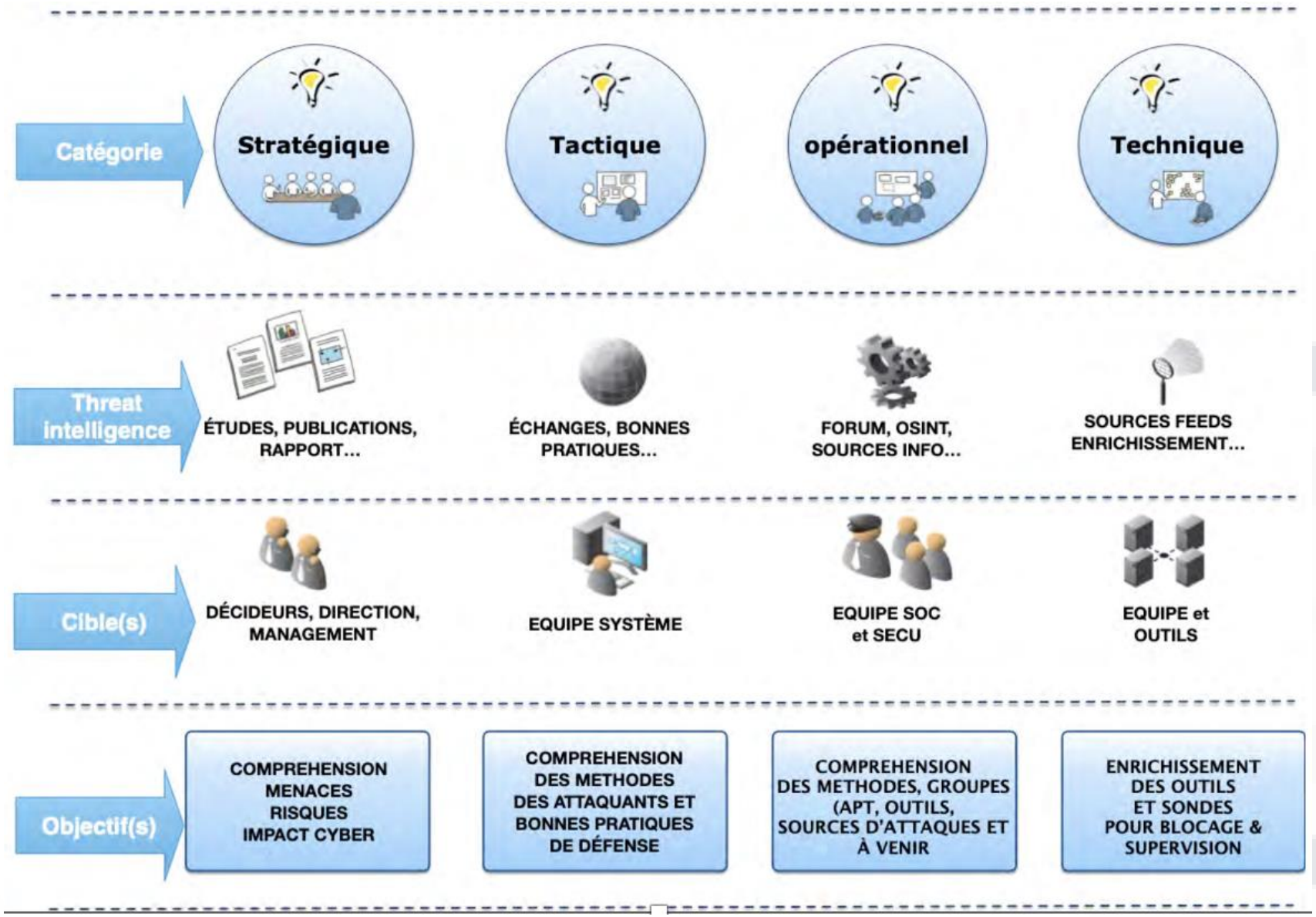
HUMINT

- Groupes de partage de menace
  - Public
  - Privé
- Spécifique métier ou industrie
- Solutions et produits



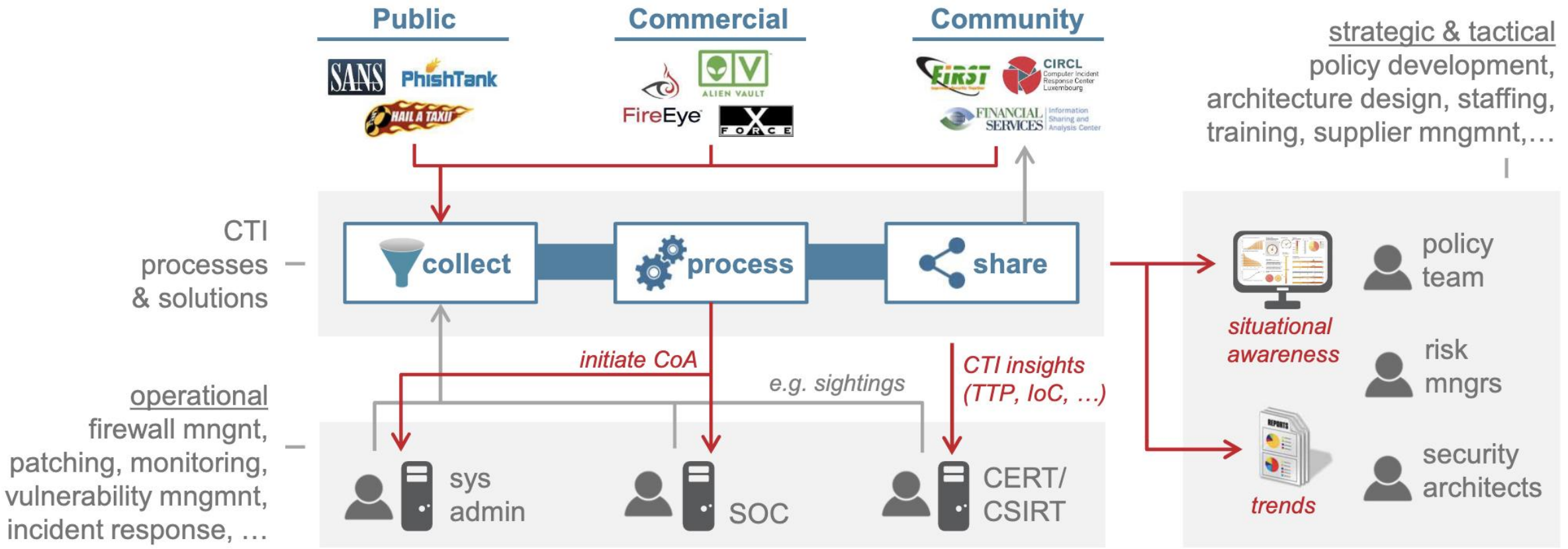
Source : Enisa

OSINT CTI : Les usages dans l'entreprise



Source : Abakus

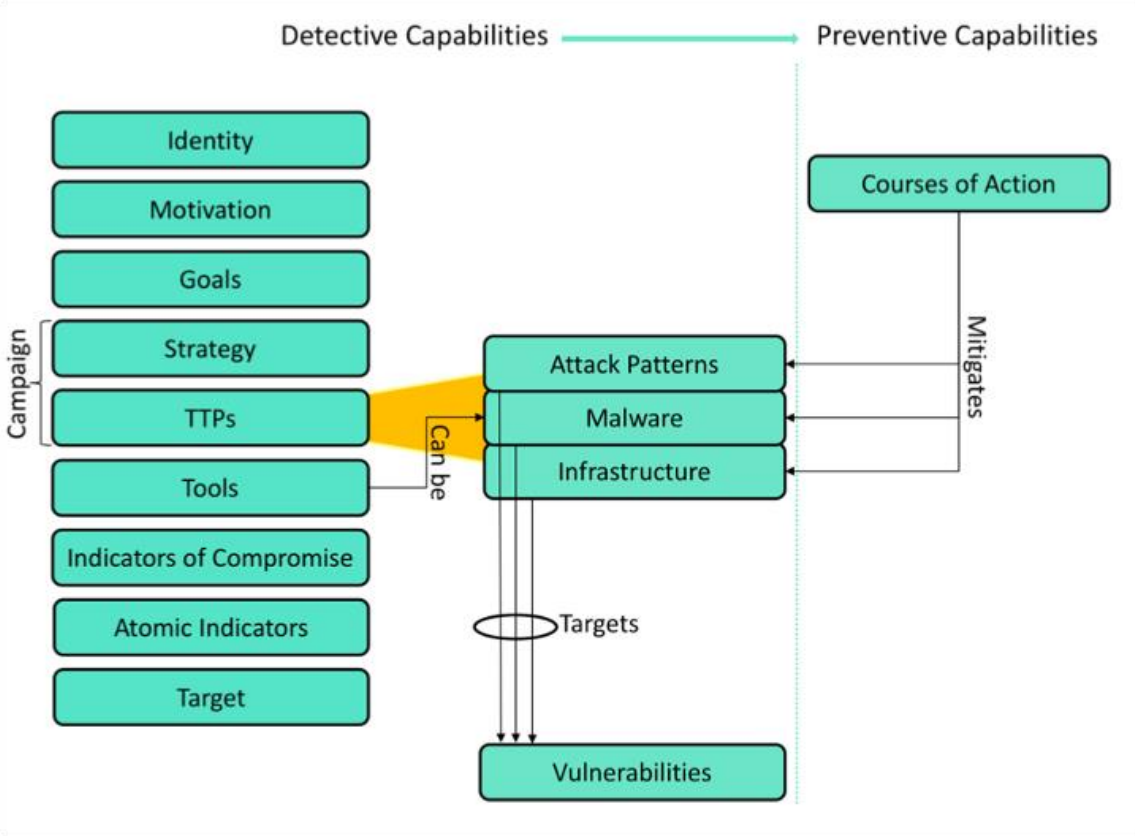
OSINT CTI : Architecture fonctionnelle



Source : Enisa

OSINT CTI : Modèle

Sans une connaissance de l'écosystème, il est difficile de comprendre l'apport d'une CTI pour l'entreprise



Identity: Threat actor can be the real name of a person, an organization, a group's affiliates, ...

Motivation: Described as the driving force that enables actions to pursue specific goals.

Goals: An overall end state and the behaviour objects and plans needed for attaining it.

Strategy: A non-technical high-level description of the planned attack.

TTPs: Tactics, Techniques, and Procedures characterize adversary behaviour in terms of what they want to achieve technically and how they are doing it.

Attack Pattern: Type of TTP that describes behaviour attackers use to carry out their attacks.

Malware: Type of TTP and refers to a software that is inserted into a system.

Infrastructure: Describes any systems, software services intended to support an adversarial operation, such as using purchased domains to support Command and Control,...

Tools: Dedicated software developed for malicious reasons and software intended for different use.

Indicators of Compromise: Are actionable technical elements and are directly consumable by cyber defence systems and components for detecting malicious or suspicious activity.

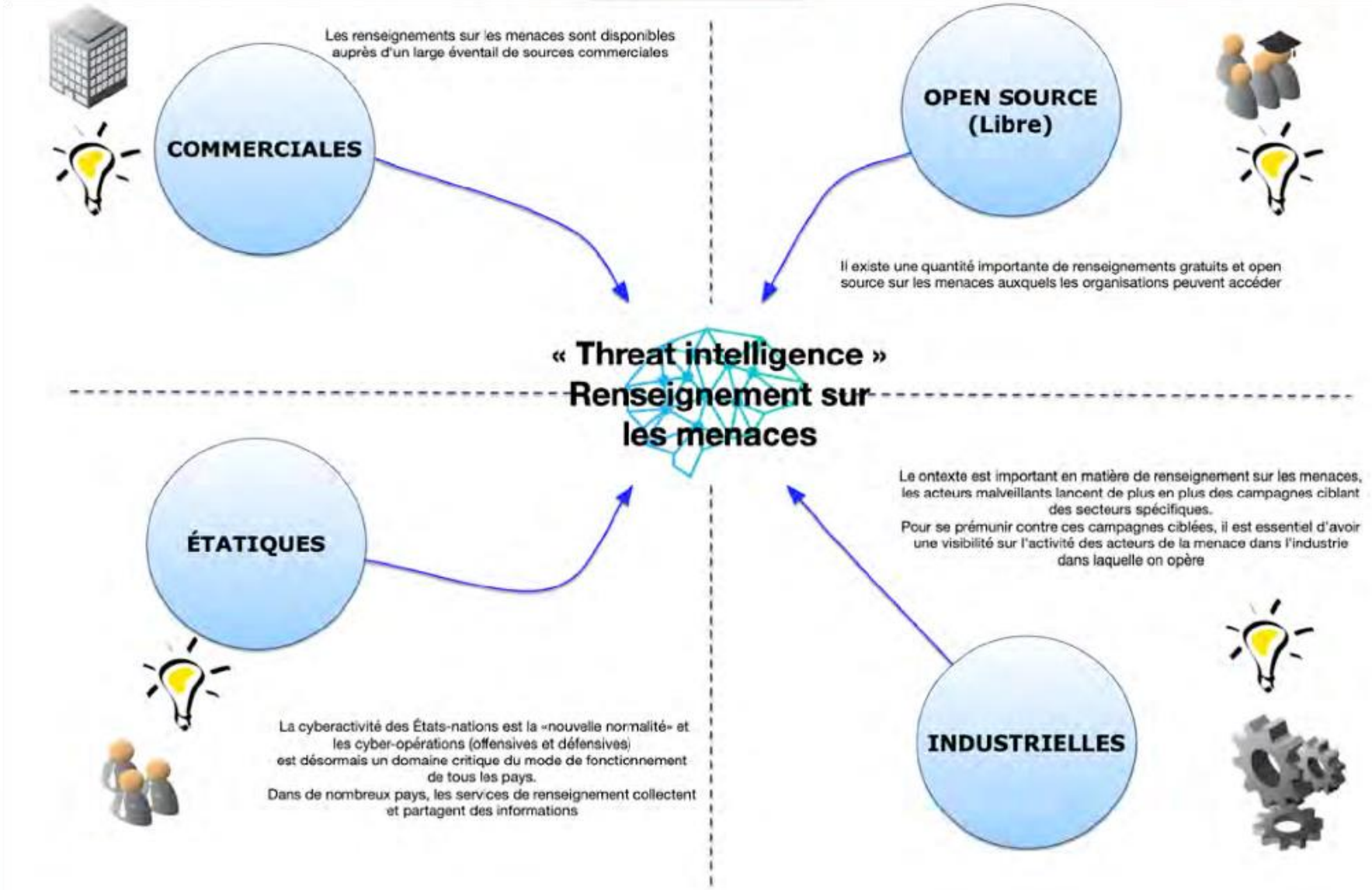
Atomic Indicators: The value of atomic indicators is limited due to their short shelf life. Atomic indicators include file hashes, domain names, and IPs.

Target: Entity an attack is directed to and can be an organization, a sector, a nation, or individuals.

Course of Action: Refers to measures that can be taken to prevent or respond to attacks.

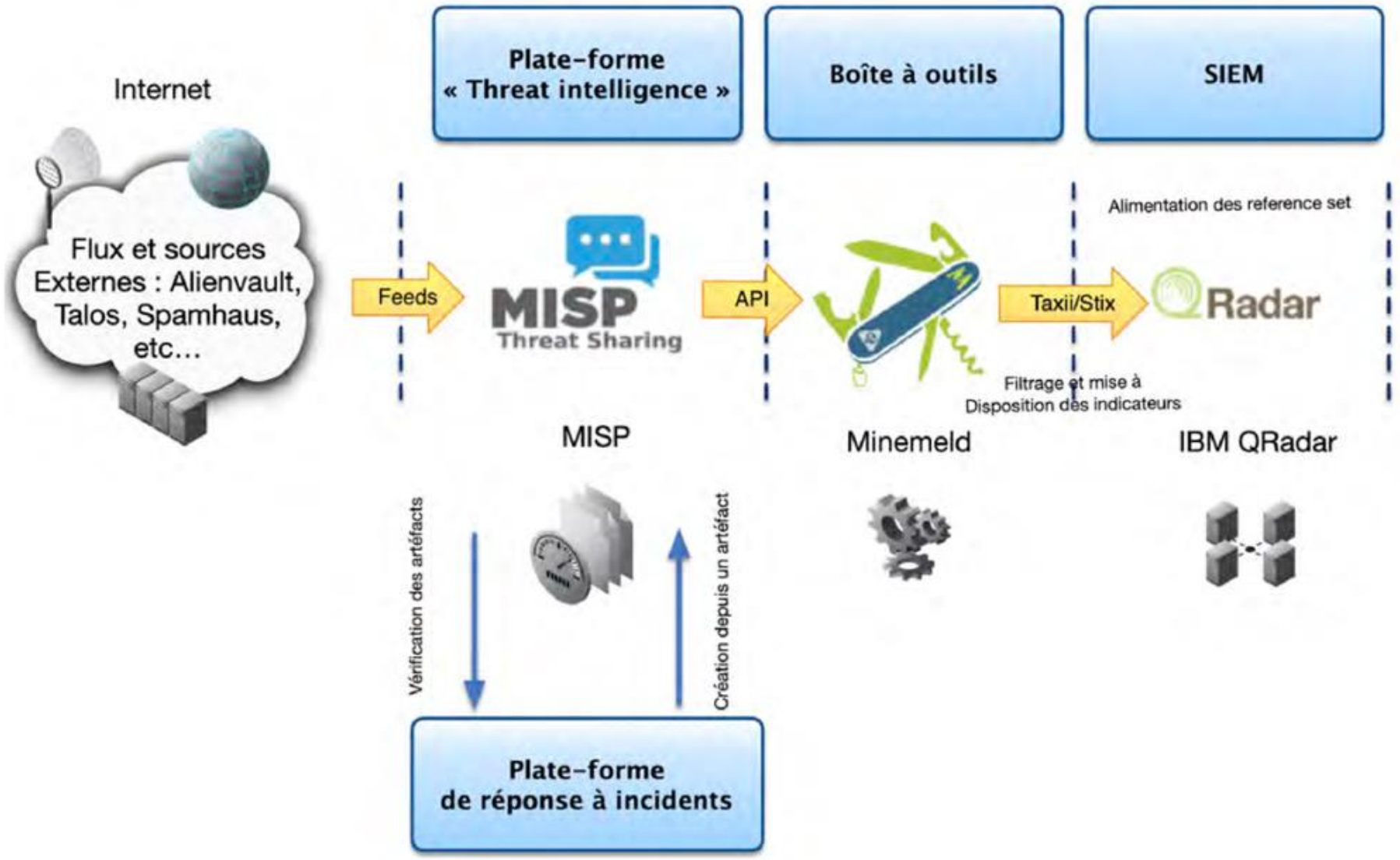
Source : Cyber Threat Intelligence Model

OSINT CTI : Choix des sources



Source : Abakus

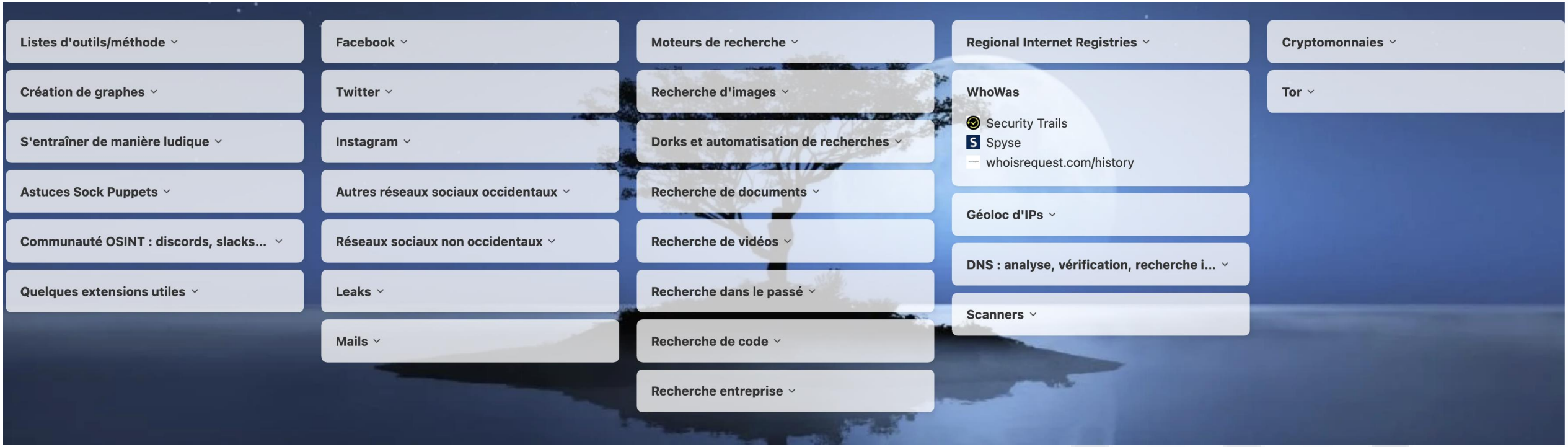
OSINT CTI : Exemple architecture technique



Agenda

OSINT on Stage

OSINT : Exemples Outils



Merci de votre attention