

# Capitalisation des campagnes et incidents de manipulation de l'information dans OpenCTI

Doctrines d'utilisation de VIGINUM  
Version 1.0 | janvier 2024

Secrétariat général de la défense et de la sécurité nationale

--

VIGINUM

--

Crédits photos : photo de Henry Han sur Unsplash

--

Conception :

VIGINUM

Janvier 2024

# Table des matières

Décrire les campagnes .....	4
Une nécessaire interopérabilité .....	4
Pourquoi une doctrine .....	4
Intérêts de STIX 2.1 et d'OpenCTI .....	5
STIX 2.1 .....	5
OpenCTI .....	5
Fonctionnement .....	6
Prérequis .....	6
Grands principes .....	6
Langue de travail .....	6
Principe d'unicité .....	6
Principe d'exhaustivité .....	7
Principe de qualité .....	7
Choix des sections .....	7
Analyses .....	7
Cases .....	7
Règles d'usage .....	8
Description des éléments utilisés dans la plateforme .....	8
Entités ( <i>STIX Domain object</i> ) .....	8
Observables .....	11
<i>Relationships</i> .....	11
Gestion des labels, Markings et des statuts .....	12
Labels .....	12
<i>Markings</i> .....	12
Statuts .....	12
Niveau de confiance .....	12
Présenter l'information dans OpenCTI .....	13
Modèle pour une campagne .....	13
Modèle pour un incident .....	13
Modèle pour un intrusion set .....	14
Modèle pour une infrastructure .....	14
Annexe A .....	15
Exemples de nommages de <i>Channel</i> .....	15
Exemples de nommages de <i>Media content</i> .....	15

# DU BESOIN DE DECRIRE LES CAMPAGNES NUMERIQUES DE MANIPULATION DE L'INFORMATION

## UNE NECESSAIRE INTEROPERABILITE

Renforcer la coopération, les compétences et la connaissance dans le domaine de la lutte contre les manipulations de l'information (LMI) implique une démarche de partage d'éléments de compréhension et d'appréciation sur les campagnes d'influence numérique analysées en garantissant notamment la fiabilité des données, leur caractère partageable sur le plan juridique et leur interopérabilité entre partenaires.

Sur le plan de l'analyse, les ingérences numériques étrangères et autres campagnes numériques de manipulation de l'information correspondent à des manœuvres plus ou moins complexes, dont l'étude s'appuie sur cinq domaines fondamentaux : l'adversaire, ses capacités d'action, les moyens techniques dont il dispose, la victime qu'il cible et enfin les narratifs sur lesquels il s'appuie.

Cette structure d'analyse a été modélisée par Charity WRIGHT dans son *Diamond Model for Influence Operations Analysis*<sup>1</sup>.

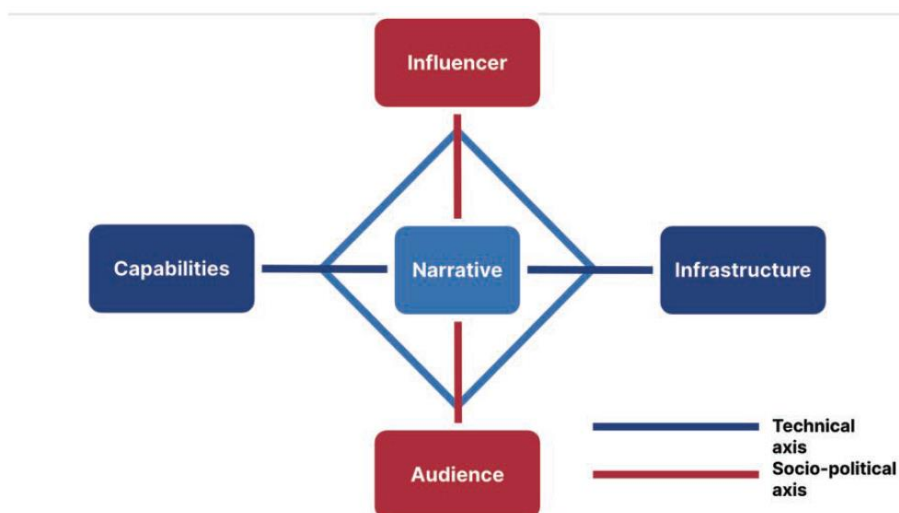


Figure 1. Modèle diamant pour les opérations d'influence, Charity WRIGHT

Afin de faciliter l'analyse partagée des éléments de connaissance sur la menace informationnelle, la réflexion des experts s'est donc portée sur la définition et l'utilisation d'un langage commun, permettant une description standardisée et qualitative. L'expérience de la *Cyber Threat Intelligence* (CTI) a mis en lumière des outils disponibles et efficaces avec un minimum de transformation (notamment en termes d'adaptation des normes et standards préexistants) pour répondre aux spécificités de la LMI, à savoir la matrice DISARM pour décrire le comportement de l'acteur malveillant (*Capabilities*) et le langage STIX 2.1 qui permet de décrire l'acteur malveillant (*Influencer*) et l'infrastructure qu'il exploite.

## POURQUOI UNE DOCTRINE

L'exploitation de l'outil OpenCTI dans le cadre de la capitalisation et du partage de l'information nécessite d'encadrer les pratiques. En effet, la subsidiarité offerte par le langage STIX 2.1 permet à l'analyste une certaine souplesse dans l'usage des objets permettant de décrire une campagne ou un

<sup>1</sup> <https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf>

« incident » de désinformation. C'est pourquoi il est nécessaire de coordonner les usages de la norme STIX 2.1 en lien avec les pratiques des acteurs de la LMI afin d'assurer une même compréhension (lisibilité et interopérabilité) des éléments capitalisés.

En l'état, cette doctrine se fonde sur la doctrine d'usage de l'ANSSI dans le cadre de leur besoin de capitalisation et d'exploitation de données en *Cyber Threat Intelligence*, du retour d'expérience des partenaires de VIGINUM et des enseignements opérationnels tirés par ce dernier.

Evolutive par nature, cette doctrine d'utilisation a pour objet de proposer un usage coordonné de la plateforme OpenCTI afin d'améliorer le partage de l'information.

## INTERETS REPRESENTES PAR LES OUTILS STIX 2.1 ET OPENCTI

---

### STIX 2.1

Le langage STIX (pour *Structured Threat Information Expression*) facilite le partage automatisé et la connaissance sur la menace d'origine cyber.

L'intérêt d'adopter ce langage réside dans sa structure :

- ▶ sa forme lui permet d'être lu aussi bien par une machine que par un humain ;
- ▶ il peut être interprété par différents langages de programmation ;
- ▶ son langage est très souple car la majorité des éléments de description sont optionnels.

Par ailleurs, en lien avec le consortium OASIS qui a créé STIX, la société française *Filigran* (qui développe l'outil OpenCTI) a proposé des adaptations de ce dernier aux besoins spécifiques de la LMI.

### OPENCTI

À ce jour, OpenCTI est la seule plateforme permettant d'exploiter le langage STIX 2.1 adapté à la LMI. Après exploitation, VIGINUM préconise l'utilisation du langage STIX 2.1 et l'usage de la plateforme OpenCTI pour les raisons suivantes :

- ▶ adaptation par la plateforme du langage STIX 2.1 à l'usage de la LMI *via* la création d'objets spécifiques<sup>2</sup> ;
- ▶ intégration et capitalisation d'informations de manière structurée sur les campagnes : acteurs malveillants, comportements, infrastructures, victimologies, etc. ;
- ▶ enrichissement et visualisation des données ;
- ▶ partage d'informations structuré.

En facilitant la capitalisation des rapports disponibles en sources ouvertes et/ou des données issues d'enquêtes, la plateforme OpenCTI offre une véritable démarche de partage de la connaissance (*knowledge management*). Par ailleurs, en tant que référentiel standardisé, il permet de construire la résilience d'un service autour d'une capitalisation commune.

---

<sup>2</sup> Les entités *Channel*, *Event*, *Narrative*, et l'observable *Media content*.



# FONCTIONNEMENT

---

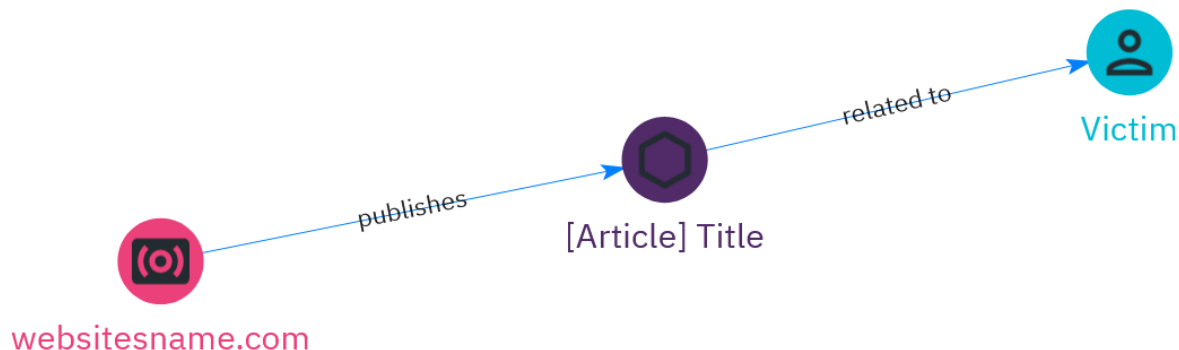
## PREREQUIS

À l'instar de la « philosophie » portée par le langage STIX 2.1 et la plateforme OpenCTI, peu d'obligations existent sur la manière d'intégrer les éléments dans la plateforme. Toutefois, certains préalables demeurent nécessaires. En effet, la capitalisation des informations doit avant tout servir à la construction d'une base de connaissance de campagnes et d'incidents de manipulation de l'information. Pour que cette base soit utile pour la connaissance et serve l'investigation, la qualité des informations capitalisées dans l'outil est essentielle. Celle-ci passe par les pratiques énumérées ci-après.

## GRANDS PRINCIPES

L'outil se fonde sur la capitalisation des trois éléments structurants : entités (*STIX Domain Objects*), observables (*STIX Cyber-observable Objects*) et relations (*STIX Relationship Objects*). Les entités représentent les éléments macro d'un rapport : *Campaign*, *Threat Actor*, *Individual*, etc. Ils publient, génèrent des données observables (*Media Content*, *IP Address*, etc.). Mais ils peuvent également représenter des victimes, qu'il s'agisse d'une institution (*Organisation*) ou d'un événement (*Event*). Les observables sont les données d'observation remontées par l'analyste (URL, nom de domaine, adresse IP, etc.). Enfin, les relations créent les liens entre ces différents éléments en explicitant la nature des liens.

ex. : l'entité **Channel** de type site internet publie un observable **Media Content** sous la forme d'un article de presse visant une entité de type **Individual** représentant le président du pays visé.



## Langue de travail

Suivant les usages de la CTI et en lien avec les besoins de partage de l'information, la capitalisation des données se fait en anglais.

## Principe d'unicité

Les campagnes ou incidents sont intégrés de manière unique. Autrement dit, lorsqu'une campagne a été capitalisée dans OpenCTI, toute nouvelle publication sur le même sujet peut aider à l'enrichissement de la donnée mais ne doit pas donner lieu à une nouvelle entrée dans l'instance.

Si une entité n'est pas présente dans la base (pays, organisation, acteur malveillant, etc.), l'analyste peut la créer. Pour ce faire, il doit vérifier d'abord que celle-ci n'existe pas déjà.

Ce principe d'unicité implique également de rentrer les *alias* dans la description des différents objets (ainsi, la campagne RRN doit être enrichie de son alias *Doppelgänger*, par exemple). En effet, l'outil n'accepte pas le doublonnage des entités ni des observables<sup>3</sup>.

## Principe d'exhaustivité

Les rapports intégrés dans OpenCTI doivent être analytiques et non synthétiques, basés sur des « incidents » ou des campagnes circonscrites dans le temps. Les états de la menace ou les études sur le comportement d'un acteur malveillant sur de longues périodes de temps ne sont pas des éléments capitalisables dans la plateforme. Ils peuvent, par contre, être ajoutés sous forme de lien ou de pièce jointe pour confirmer ou étayer des informations intégrées dans l'instance.

Par ailleurs, il est fortement conseillé d'utiliser les champs de description de l'information pour rentrer le maximum de données non structurées en complément des champs disponibles.

## Principe de qualité

Les données doivent être intégrées de manière claire (chaines de caractères exactes), avec le niveau d'information maximal disponible. Cela implique, notamment, de vérifier l'orthographe des termes utilisés, leur présence dans la plateforme, et leurs différentes acceptions.

Il est également nécessaire de vérifier les informations et les données techniques (refaire les pivots par exemple). L'information rentrée doit être juste, vérifiée et vérifiable.

Enfin, il est nécessaire, pour l'analyste, de prendre le temps de réfléchir, avant l'intégration de données dans la plateforme, à ce qu'il souhaite présenter, aux données qu'il veut archiver et à ce qu'il souhaite pouvoir requêter par la suite. Sachant que, s'il n'est pas toujours possible de rentrer l'information avec le niveau de détail maximal, il est en revanche nécessaire de rentrer les éléments clés d'une campagne ou d'un incident pour mettre en évidence la mécanique de celle-ci ou de celui-ci.

## CHOIX DES SECTIONS

La plateforme OpenCTI offre un large choix d'entrées et d'enrichissements possibles. Ces choix sont liés, entre autres, à la matière que l'on souhaite capitaliser (LMI, Cyber) et à sa forme (rapport d'analyse, bulletin de recherche, note, réponse à incident, etc.).

Dans le cadre du travail de VIGINUM, l'accent a été mis sur l'exploitation de la section *Report* et *Analyses* afin de rentrer les différentes campagnes et « incidents ». Cependant, selon les besoins des analystes et la mission de leur organisation, les champs *Incident responses* ou bien encore *Request for information* de la section *Cases*, peuvent être utilisés.

### Analyses

Les *Analyses* permettent d'accéder à la section *Reports* qui sera privilégiée par l'analyste pour capitaliser un rapport interne ou externe décrivant un « incident » ou une campagne de manipulation de l'information. Cette section permet de capitaliser la donnée sous forme de graphe relationnel.

### Cases

Cette section permet de rentrer de l'information nécessitant une action du service ou de la communauté sous la forme d'une réponse à incident, demande d'information etc.

---

<sup>3</sup> Une information entrée en doublon engendre un message d'erreur et peut rendre l'export du fichier STIX impossible.

# RÈGLES D'USAGE

---

## DESCRIPTION DES ELEMENTS UTILISES DANS LA PLATEFORME

Tout *STIX Domain Object* (SDO), *relationship* ou *observable* présent et décrit dans le référentiel STIX 2.1 d'OASIS peut être utilisé à partir du moment où il décrit pertinemment les données que l'on souhaite capitaliser.

Cependant, à la suite de l'adaptation des éléments exploités dans la CTI au domaine de la LMI, il est nécessaire de définir les éléments les plus couramment employés dans la plateforme OpenCTI, ainsi que les entités (SDO) et observables proposés par Filigran<sup>4</sup> afin de décrire l'intégralité des campagnes de manipulation de l'information.

### Entités (STIX Domain object)

#### ATTACK PATTERN

(Objet STIX natif)

Ce *STIX Domain Object* (SDO) permet de décrire le comportement de l'adversaire. Les campagnes et incidents hybrides, combinant attaques cyber et manipulation de l'information, peuvent être représentées, dans la même modélisation, par des *attack pattern* issus des matrices DISARM et ATT&CK.

#### CAMPAIGN

(Objet STIX natif)

Une campagne est définie comme une attaque planifiée sur la durée, généralement mise en place par un acteur malveillant persistant. Dans OpenCTI, elle peut être reliée à un acteur malveillant (*Threat actor*), exploiter des outils, des infrastructures ou des tactiques, techniques et procédures (TTPs), cibler des individus, etc.

Quand la campagne possède déjà un nom public, il est recommandé de capitaliser celui-ci et de rentrer en alias les possibles différentes acceptions de celle-ci. Ensuite, l'analyste doit rentrer la campagne sous des termes précis.

#### CHANNEL

(Ajout Filigran)

Un *channel* (canal) publie des observables (sous la forme de *media content* en général).

Le nom du *channel* doit faire apparaître son origine (compte de réseau social, site web ou blog) et être unique. Le nommage doit, autant que faire se peut, rendre visible, sur le graphe de la section *Knowledge*, les éléments permettant d'identifier simplement le *channel* (*pseudo*, ou *nom de domaine par exemple*). L'exploitation de l'alias et des champs de description du *channel* permettront d'intégrer les différents éléments d'information liés, entre autres, aux comptes de réseaux sociaux (*handle*, ID, URL, etc.).

---

<sup>4</sup> Ces entités et observables sont, à ce jour (20/11/2023), en cours d'étude par le consortium OASIS afin de les faire entrer dans le standard STIX.



## Create an entity

Channel

Name

twitter.com/nomducompte

No potential duplicate entities has been found.








Channel type

Twitter

Description

Write

Preview

**H** **B** **I**       

All available information

Confidence level

75

2 - Probably True

twitter.com/nomducompte

⋮

@handleducompte

✕

DETAILS

Description

Channel types

All available information

TWITTER

Le *channel* doit représenter un vecteur de diffusion unique et non un ensemble. Autrement dit, il représente un compte, un site, mais pas un groupe de comptes ou une infrastructure de sites.

Autant que possible, l'URL du canal doit être indiquée (dans sa version originale et non par un lien d'archivage). Le *channel* peut **cibler** (*targets*) un individu, une organisation, une ville ou bien encore un pays ; **appartenir à** (*belongs-to*) un individu, une organisation, un compte utilisateur, etc. ; **utiliser** (*uses*) un compte utilisateur, un narratif, un mode opératoire et **publier** (*publishes*) un contenu média, un courriel, etc.

La convention de nommage exploitée est détaillée en annexe A.

À savoir qu'il est possible de compléter les types de *Channel* disponibles dans la plateforme en intégrant le nom de ceux-ci dans les paramètres d'OpenCTI (section *Vocabularies* du menu *Taxonomies*).

## EVENT

(Ajout Filigran)

L'Event décrit un événement de la vie réelle exploité par un « incident » ou une campagne de manipulation de l'information. Il peut tout aussi bien s'agir d'élections, d'un événement sportif que d'un événement d'actualité exploité de manière opportuniste par les *Threat actors*.

## GROUPING

(Objet STIX natif)

Cet objet natif n'a pas encore été exploité. Il devrait cependant pouvoir être utilisé pour représenter des investigations en cours sur lesquelles les informations sont encore lacunaires.

## IDENTITY

(Objet STIX natif)

Ce SDO regroupe tous les éléments d'identification exploitables dans la plateforme : individus, organisations, ou localisations. Ils sont entrés en anglais et leur orthographe doit être consciencieusement respectée. Ainsi, les graphies ou alias en langues cyrilliques (par exemple) sont à ajouter dans la description de celui-ci.

## INCIDENT

(Objet STIX natif)

Un incident est une activité de manipulation de l'information circonscrite autour d'un sujet spécifique ou d'un événement particulier. Les campagnes sont, en général, constituées de multiples incidents liés au même acteur.

Cet objet permet de décrire les informations basiques liées à un incident (nom, description, dates de début et de fin, objectifs, etc.).

## INFRASTRUCTURE

(Objet STIX natif)

Cet objet STIX modélise tout type de système, de logiciel et toute ressource physique ou virtuelle associée qui supporte la cause de la campagne, de l'acteur ou de l'incident. Il décrit notamment les réseaux de bots sur les réseaux sociaux qui poussent les narratifs de la campagne. Il peut aussi décrire un réseau de sites internet ou un système de collaboration permettant de construire les supports nécessaires à la campagne (narratifs, visuels, etc.). À cet égard, une infrastructure peut publier des observables, même si cette nature du lien n'existe pas encore. Elle peut être considérée comme une somme de *channels* dans le cas où la donnée sur les *channels* n'est pas disponible.

## INTRUSION SET

(Objet STIX natif)

Cet objet décrit une compilation de comportements adverses et de ressources aux propriétés communes pouvant être orchestrées par une même organisation. Les attributs communs peuvent indiquer un *Threat actor* connu ou inconnu, être utilisés dans différentes campagnes et persister dans le temps. Cet objet doit être exploité dès que l'analyste pense pouvoir lui imputer une campagne ou un incident. En effet, cet élément de capitalisation est aussi structurant en CTI qu'en LMI et permet de suivre la conjonction de modes opératoires et d'infrastructure dans le temps et de les mettre en valeur.

## NARRATIVE

(Ajout Filigran)

Ce SDO décrit les narratifs exploités par un *Threat actor* lors d'une campagne ou d'un incident.

## THREAT ACTOR

(Objet STIX natif)

Individus, groupes ou organisations opérant pour des motifs malveillants et responsables de la campagne ou de l'incident. Le *Threat actor* peut être lié à différents *Intrusion sets*, groupes ou organisations à travers le temps. Il peut développer des ressources qui lui sont propres ou faire appel à un *Intrusion set* connu pour conduire des attaques ou des campagnes. Le *Threat actor* peut être caractérisé par ses capacités, ses buts, son niveau de sophistication, ses activités passées et son rôle dans une organisation.

## TTPS

(Objet STIX natif)

Les matrices MITRE ATT&CK et DISARM doivent être implémentées dans OpenCTI, notamment dans l'optique de décrire à terme des campagnes hybrides (cyber et manipulation de l'information). Les connecteurs et leur mode d'emploi sont disponibles sur le site de *Filigran*<sup>5</sup>.

Ces matrices sont nécessaires pour décrire les modes opératoires cyber et LMI utilisés pour décrire le comportement des acteurs de la menace.

ex. : une activité de *spear phishing* pour diffuser un narratif par e-mail via un article visant une organisation spécifique fera appel à la TTP MITRE ATT&CK **Spear Phishing** et la TTP DISARM **T0089.002 Create Inauthentic Document** et **T0082 Develop New Narratives**.

## TOOL

(Objet STIX natif)

Le SDO *Tool* décrit des logiciels légitimes exploités par un *Threat actor* dans le cadre de ses campagnes. S'agissant de la LMI, il peut décrire un outil non légitime, à l'instar de AIMS, utilisé par l'acteur *Team Jorge* pour créer et gérer des avatars « profonds » sur les réseaux sociaux.

## Observables

Comme leur nom l'indique, les observables permettent de modéliser les éléments techniques observés lors de la campagne ou de l'incident (adresse IP, nom de domaine, etc...).

Tous les observables nécessaires à la description d'une campagne ou d'un incident décrits dans le référentiel STIX 2.1 sont utilisables. OpenCTI offre également l'usage de l'observable *Media Content* décrit ci-dessous.

## MEDIA CONTENT

(Ajout Filigran)

Cet observable modélise un contenu média de type publication, post de blog, vidéo, audio, image, etc.

Sa présentation dans OpenCTI doit mettre en avant le type de média auquel il a affaire. Son nommage est déterminé selon une convention disponible en Annexe A.

Un *Media Content* peut être caractérisé par l'URL par le biais de laquelle l'analyste a observé ce média, ou bien encore par des fichiers. La convention de nommage de cet observable est disponible en Annexe A.

## Relationships

Les relations entre les différentes entités et les observables créent ou modélisent le renseignement disponible sur les éléments analysés. Les relations que l'on crée entre les différents nœuds de la visualisation graphique des campagnes ou incidents peuvent avoir des natures de lien différentes.

Il manque encore un certain nombre de *relationships* nécessaires pour décrire finement les liens entre les différents objets créés spécifiquement pour la LMI. Mais, par défaut, tout objet peut être relié par un autre avec une relation de base nommée « *related-to* ». Toutefois, l'analyste privilégiera toujours le lien disponible le plus précis possible : « *targets*, *uses*, *own*, *located-at*, etc. ».

---

<sup>5</sup> Plus d'information sur la matrice Disarm : <https://www.disarm.foundation/>

## GESTION DES LABELS, MARKINGS ET DES STATUTS

### Labels

Les labels doivent permettre à l'analyste de catégoriser l'information via une taxonomie propre à son service ou à ses pratiques d'archivage. La création de label est libre et s'effectue, entre autres, dans le menu « Paramètres/Taxonomie ». Le label est utilisé pour filtrer l'information sur des données non structurées. Il peut également être exploité pour identifier les informations à communiquer avec des acteurs spécifiques dans le cadre du partage d'information entre instances OpenCTI par exemple.

Les labels peuvent également être utilisés pour catégoriser les objets créés pour la LMI mais ne représentant pas un élément précis. Ils permettent ainsi de labéliser les *Media Content* en leur adjoignant une étiquette décrivant le type de *Media Content* décrit : article, podcast, image, vidéo, hashtag, etc. Il appartient alors à l'entité qui utilise OpenCTI de gérer ces labels en cohérence, entre autres, avec le nommage des *Media Content* décrits en annexe de ce document.

Enfin, les rapports décrivant de multiples campagnes, à l'instar de *Story Killers (Forbidden stories)*, ou bien encore de *Ghostwriter* (université de Cardiff), peuvent être labélisées par le nom du rapport lors de la description des différentes campagnes.

### Markings

L'outil labellise la sensibilité de l'information intégrée dans la plateforme en se fondant sur la norme CISA. Par défaut, le marqueur de sensibilité Traffic Light Protocol (TLP) sera toujours **CLEAR**, c'est-à-dire partageable sans restriction.

**TLP:GREEN** : l'information est partageable au sein d'une communauté prédéfinie.

**TLP:AMBER** : l'information peut être partagée au sein de l'organisation et auprès de partenaires proches.

**TLP:AMBER+STRICT** : l'information est réservée à l'organisation.

**TLP:RED** : l'information est réservée aux participants.

### Statuts

OpenCTI offre la possibilité de mettre en avant le statut des analyses capitalisées dans la plateforme : *New, In\_Progress, Analysed, Closed*.

#### New

Ce statut indique qu'une nouvelle campagne a été entrée et va être analysée. Cela permet de faire savoir que le sujet est vu même s'il n'a pas encore été travaillé.

#### In\_Progress

Indique que l'analyse est débutée et peut être soit en cours d'enrichissement, soit ouverte à d'autres investigations et enrichissements ultérieurs.

#### Analysed

Indique que l'analyse est close et qu'elle ne sera plus enrichie, soit parce que le rapport a été capitalisé dans son intégralité, soit parce que la campagne ou l'incident sont considérés comme intégralement investigués.

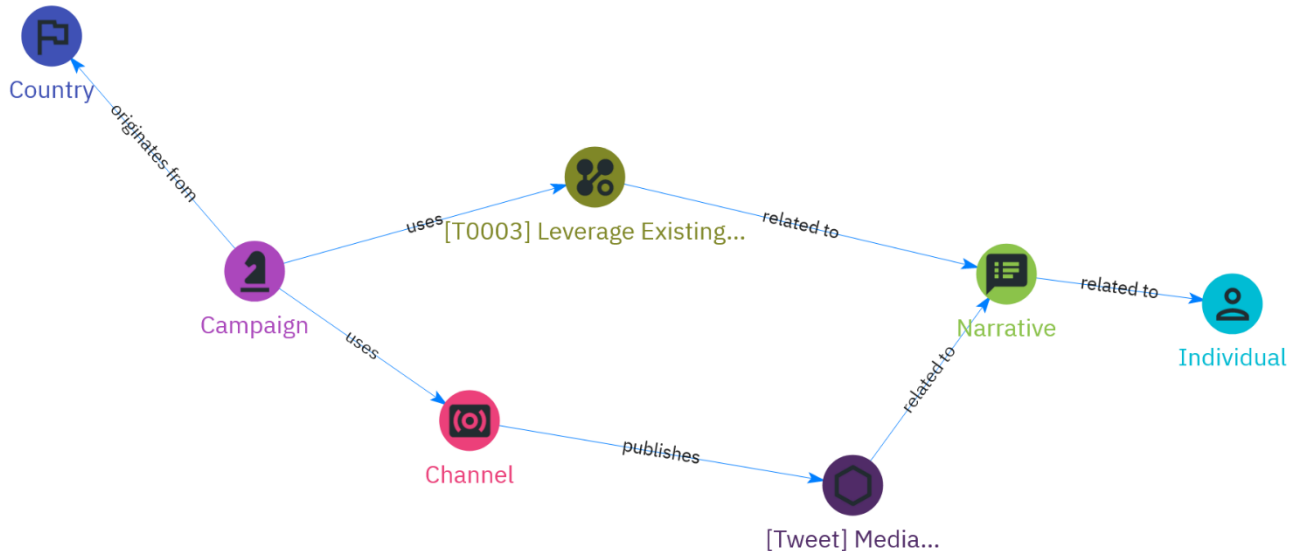
### Niveau de confiance

OpenCTI permet d'indiquer un niveau de confiance en lien avec les éléments décrits dans la plateforme. Il est recommandé à l'analyste de baisser celui-ci (qui par défaut est situé à 75 % - « *Probably true* ») à un niveau de 50 % - « *Possibly true* » lorsque l'analyste n'a pas investigué la campagne ou l'incident ou se réfère à une documentation externe à son organisme (*Threat report*)

## PRESENTER L'INFORMATION DANS OPENCTI

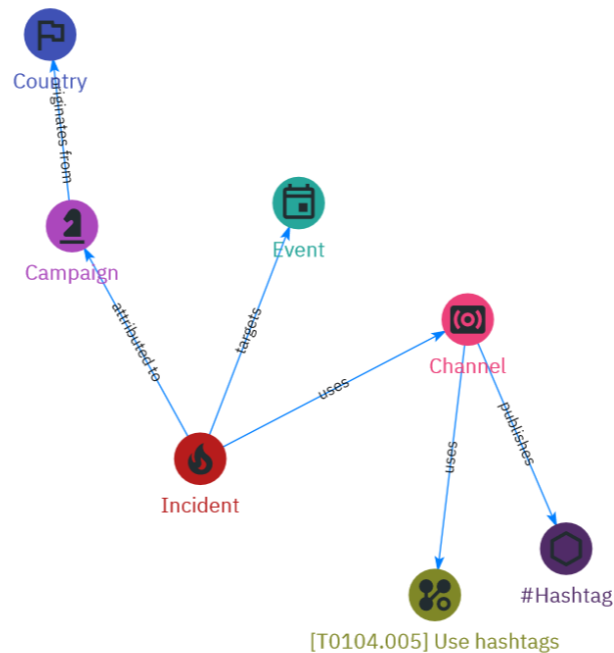
Par convention, les entités sont écrites en gras et les observables en *italiques*.

### MODELE POUR UNE CAMPAGNE



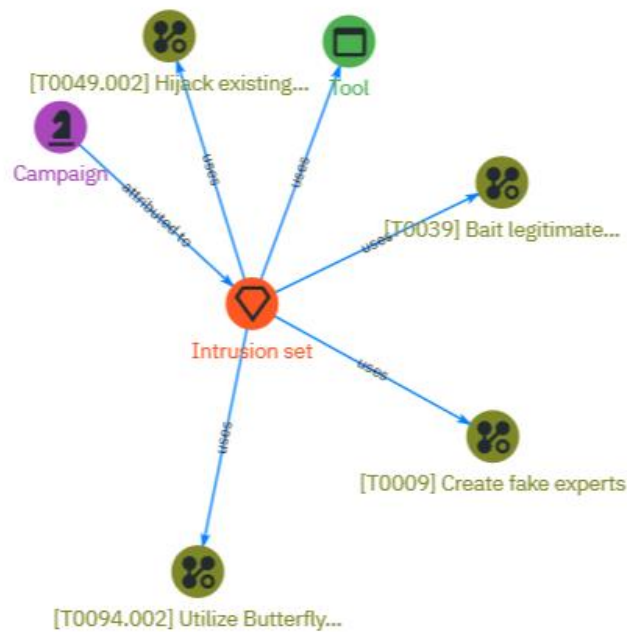
La **Campaign** est originaire d'un pays, elle utilise une **TTP** liée à la création d'un **Narrative** existant. Le dit **Narrative** cible un **Individual**. Il est publié sur un **Media content** produit par un **Channel** lié à la **Campaign**.

### MODELE POUR UN INCIDENT



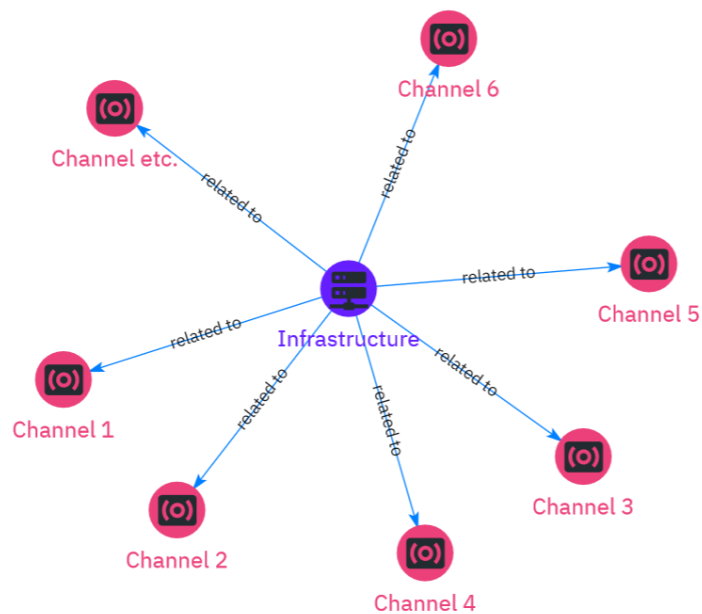
L'**Incident** ainsi décrit fait partie de la **Campaign** localisée dans le **Country**, il cible un **Event** par le biais d'un **Channel** qui publie des **Hashtags**.

## MODELE POUR UN INTRUSION SET



L'**Intrusion set** exploité par la **Campaign** est relié à un **acteur donné**, utilise des **TTPs** ainsi qu'un **Tool**.

## MODELE POUR UNE INFRASTRUCTURE



Une **Infrastructure** exploite des **Channels** pour publier de l'information dans le cadre d'une campagne ou d'un incident. Dans le cas où la donnée est manquante pour les *channels*, l'infrastructure peut à défaut publier des observables.



## ANNEXE A

---

### EXEMPLES DE NOMMAGES DE *CHANNEL*

1. Facebook (as a platform): facebook.com
2. Facebook Profile: facebook.com/username (UserID en alias)
3. Facebook Group: facebook.com/groups (groupid en alias)
4. Facebook Page: facebook.com/pagename (pageID en alias)
5. Twitter (as platform): twitter.com
6. Twitter profile: twitter.com/username (handle en alias)
7. Telegram (as platform): telegram.org
8. Telegram Channel: t.me/channelname
9. Telegram Group: t.me/groupname
10. A website: website.com

### EXEMPLES DE NOMMAGES DE *MEDIA CONTENT*

1. [Video] Titre de la vidéo en langue originale
2. [Article] Titre de l'article en langue originale
3. [Podcast] Titre du podcast en langue originale
4. [Tweet] Titre du tweet en langue originale
5. [Facebook] Titre du post en langue originale

## À PROPOS DE VIGINUM



Créé le 13 juillet 2021 et rattaché au SGDSN, le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) a pour raison d'être la protection du débat public numérique touchant aux intérêts fondamentaux de la Nation.

Ce service technique et opérationnel de l'État a pour mission de détecter et caractériser les campagnes de manipulation de l'information sur les plateformes numériques, impliquant des acteurs étrangers dans le but de nuire à la France et à ses intérêts.

[Décret n° 2021-922 du 13 juillet 2021]

[Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN](#)