



# Lutte Informatique Défensive

## SOC, CERT et CTI

Georges Bossert - SEKOIA  
Frédéric Guihéry - AMOSSYS

*6 novembre 2018 - Université Rennes 1*



---

# Cyber Threat Intelligence

**Abréviation :** CTI

**Domaine :** INFORMATIQUE - DÉFENSE


**Définition :** Un processus visant à fournir du renseignement actionnable et contextualisé sur les cybermenaces et les groupes d'attaquants informatiques ciblant une organisation.

*Interne Sekoia*

# Définition

**Gartner.**  
WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING

## Definition: Threat Intelligence

 **ARCHIVED** Published: 16 May 2013 ID: G002492

**Analyst(s):** [Rob McMillan](#)

### Summary

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

### Different Definitions

In the world of information and cyber security, threat intelligence is a young field and there are large numbers of threat intelligence vendors and advisory papers that describe very different products and activities under the banner of 'threat intelligence'. As with traditional intelligence, a core definition is that threat intelligence is information that can aid decisions, with the aim of preventing an attack or decreasing the time taken to discover an attack. Intelligence can also be information that, instead of aiding specific decisions, helps to illuminate the risk landscape.



# Définition

« Connais ton ennemi et connais-toi toi-même » (Sun Tzu - Art de la guerre)

- Moyens pour modéliser et suivre les menaces
- Connaissances pour décrire les menaces



# Historique

- La théorie provient du renseignement militaire
- Le terme de CTI apparaît en 2011
- Rapport APT1 en 2013 puis « buzzword » pendant 5 ans
- Maintenant ça a tendance à être réellement exploité



# Qui utilise la CTI

- SOC
  - Mise en oeuvre de mécanismes de détection adaptés
  - Suivi des menaces et adaptation des protections
- CERT
  - Accélération de la résolution des incidents
- Management
  - Outil de prise de décision (tactique et stratégie)



# Renseignement

- **Unknown unknown**
  - une menace ou un risque non identifié
    - « un inconnu attend à l'extérieur du bureau pour attaquer le directeur »
- **Known unknown**
  - une menace ou un risque identifié comme étant inconnu · non maîtrisé
    - « un inconnu veut attaquer le directeur à l'extérieur du bureau »
- **Known known**
  - une menace ou un risque identifié et maîtrisé
    - « M. Dupont va attaquer le directeur avec un couteau à sa sortie de bureau à 17h »

# Renseignement

- **Unknown unknown**
  - une menace ou un risque non identifié
    - « un inconnu attend à l'extérieur du bureau pour l'attaquer le directeur »
- **Known unknown**
  - une menace ou un risque identifié comme étant inconnu · non maîtrisé
    - « un inconnu veut attaquer le directeur à l'extérieur du bureau »
- **Known known**
  - une menace ou un risque identifié et maîtrisé
    - « M. Dupont va attaquer le directeur avec un couteau à sa sortie de bureau à 17h »

Le terme de renseignement regroupe l'ensemble des processus visant à déplacer un risque de la catégorie “unknown unknown” à “known known”

Renseignement





# Threat Intelligence

- **Objectifs**

- une majorité de menaces dans la catégorie “known known”
- traiter les menaces de la catégorie “known unknown”
- permettre un minimum de menaces en catégorie “unknown unknown”

- **Méthodes**

- collecter des informations qui peuvent
  - aider à la décision pour
    - empêcher une attaque
    - réduire le temps nécessaire à la détection d’une attaque
  - aider à l’identification des risques



# Threat Intelligence

- **Inconvénients**
  - les renseignements obtenus sont souvent incomplets
  - objectifs d'obscurcir le renseignement adverse
  - les mesures de protection autour des méthodes de renseignement produisent un effet mystique d'omniscience.



# Cyber Threat Intelligence (CTI)

- Renseignement sur des menaces informatiques
- Nombreux types de renseignements
  - N'importe quelle information peut être considérée comme un renseignement si elle informe d'une menace
    - *un article de journal sur la menace grandissante de la mafia Chinoise*
    - *une discussion avec un concurrent sur des tentatives de phishing avec un PDF en pièce jointe qu'il a subit récemment*
  - Besoin d'organiser ces informations
    - *un rapport stratégique ne sera pas exploitable avec les mêmes outils ni peut-être par les mêmes personnes qu'une adresse IP*



# Les catégories de CTI

- **Renseignement Stratégique**
  - Information de haut-niveau sur les évolutions de risques et de menaces
  - public adapté : équipe dirigeante en charge de la stratégie
- **Renseignement Tactique**
  - Outils, tactiques et procédures (TTPs) utilisées par les attaquants
  - public adapté : les architectes et adminsys
- **Renseignement Opérationnel**
  - Détails des groupes et des attaques attendues
  - public adapté : responsable sécurité, responsable de l'équipe réponse à incident
- **Renseignement Technique**
  - Données techniques consommables de manière automatisés
  - **public adapté:** équipe SOC / CERT

# Les catégories de CTI

- **Renseignement Stratégique**

- Information de haut-niveau sur les évolutions de risques et de menaces
- public adapté : équipe dirigeante en charge de la stratégie

- **Renseignement Tactique**

- Outils, tactiques et procédures (TTPs) utilisées par les attaquants
- public adapté : les architectes et admins

- **Renseignement Opérationnel**

- Détails des groupes et des attaques attendues
- public adapté : responsable sécurité, responsable de l'équipe réponse à incident

- **Renseignement Technique**

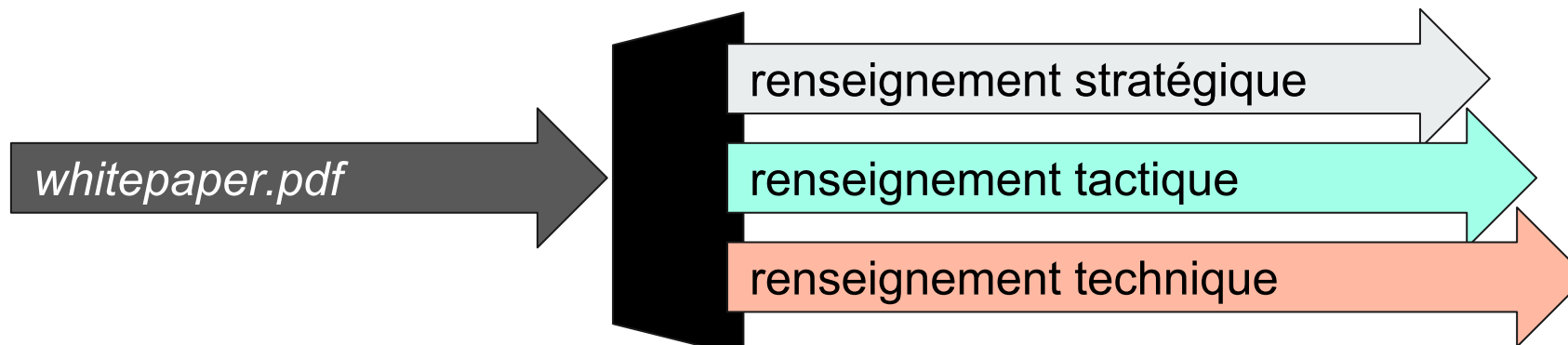
- Données techniques consommables de manière automatisés
- **public adapté:** équipe SOC / CERT

Long terme

Court terme

# Les catégories de CTI

- Une source peut produire des renseignements d'une même catégorie
  - exemple : un feed comprenant les adresses IP des machines infectées par le botnet ZeroAccess
- Une source peut produire des renseignements de catégories différentes
  - exemple : un *whitepaper* publié par un antivirus
    - identification des secteurs d'activités des cibles
    - description de la méthode utilisée pour s'infiltrer sur le réseau
    - adresses IPs des serveur de CnC



# Les règles

---



**KEEP  
CALM  
AND  
FOLLOW  
THE RULES**



# Traffic Light Protocol

- Spécification des règles de diffusion d'une information
- Plusieurs niveaux de diffusion
  - **WHITE** - *unlimited*: information sans risque, diffusable librement en respectant le copyright
  - **GREEN** - *community wide*: peut être partagée à toute une communauté identifiée
  - **AMBER** - *limited distribution*: peut-être partagée à un ensemble précis de destinataire
  - **RED** - *personal for named recipients only*: risque important, ne doit pas être diffusé



**ONE DOES NOT SIMPLY**

**BREAK TLP RULES**



# Chatham House

- Règle supplémentaire pour définir le partage d'informations au sein d'un cercle de confiance

## Chatham House Rule

The Chatham House Rule originated at Chatham House with the aim of providing anonymity to speakers and to encourage openness and the sharing of information. It is now used throughout the world as an aid to free discussion.

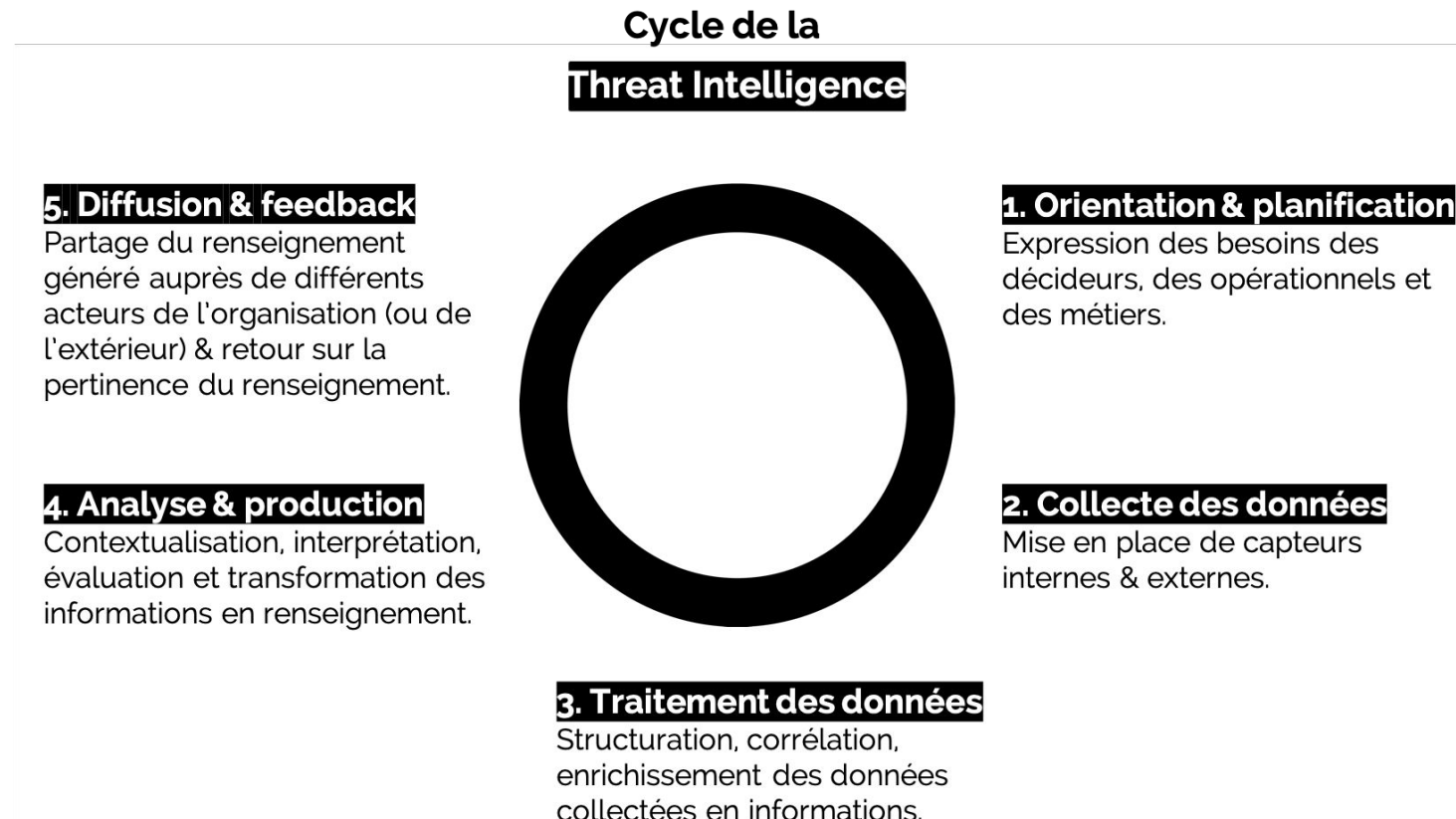
Share



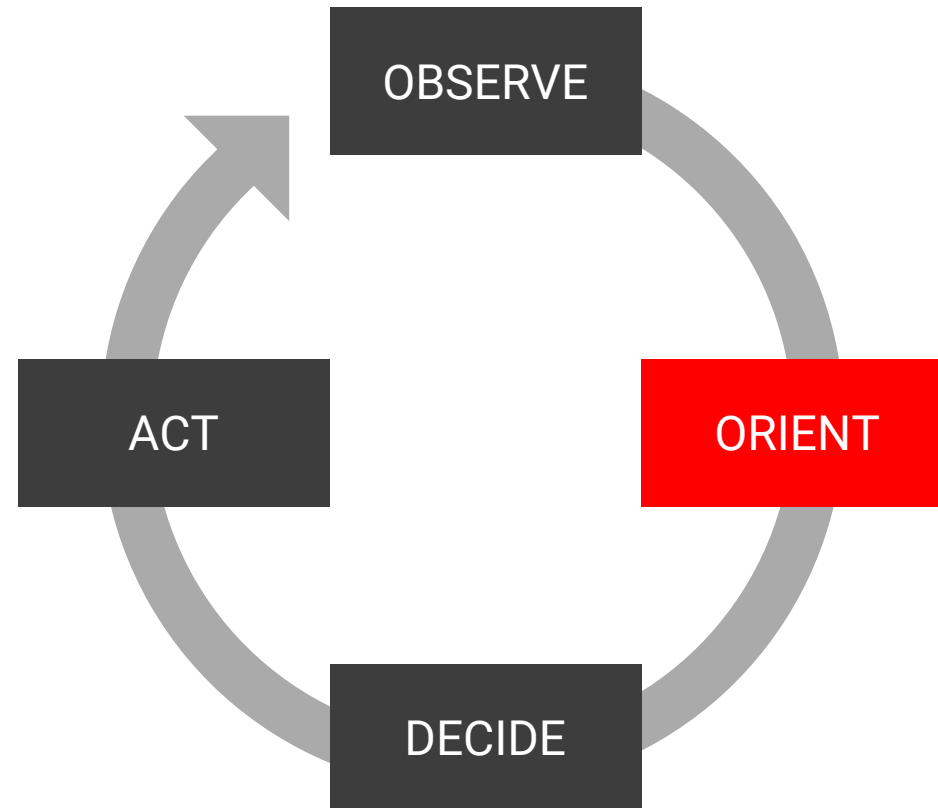
The Chatham House Rule reads as follows:

“ When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed. ”

# Le cycle du renseignement appliqué en CTI



# La boucle OODA



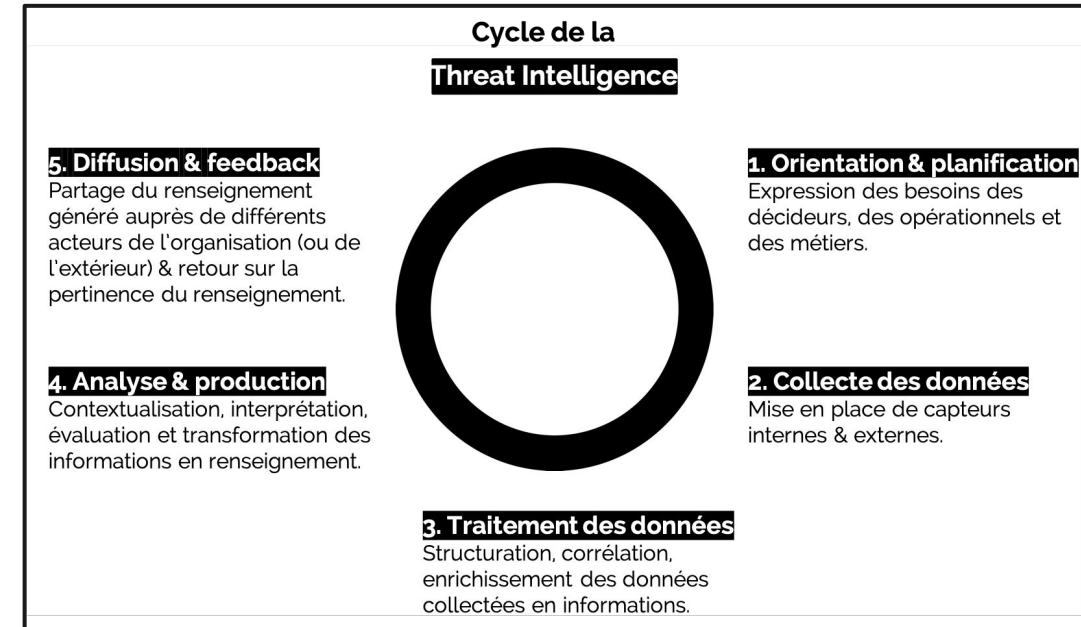
# Le cycle du renseignement

## Orientation et planification

### Plusieurs sources d'orientations

- Une analyse de risques
- Des questions des décideurs
- Un incident majeur
- L'ANSSI nous a communiqué des marqueurs de compromission classifiés concernant une campagne de cyber reconnaissance visant notre secteur d'activité.

Mise en place d'un plan de veille, de surveillance et d'investigation pour traquer les menaces, les adversaires potentiels.



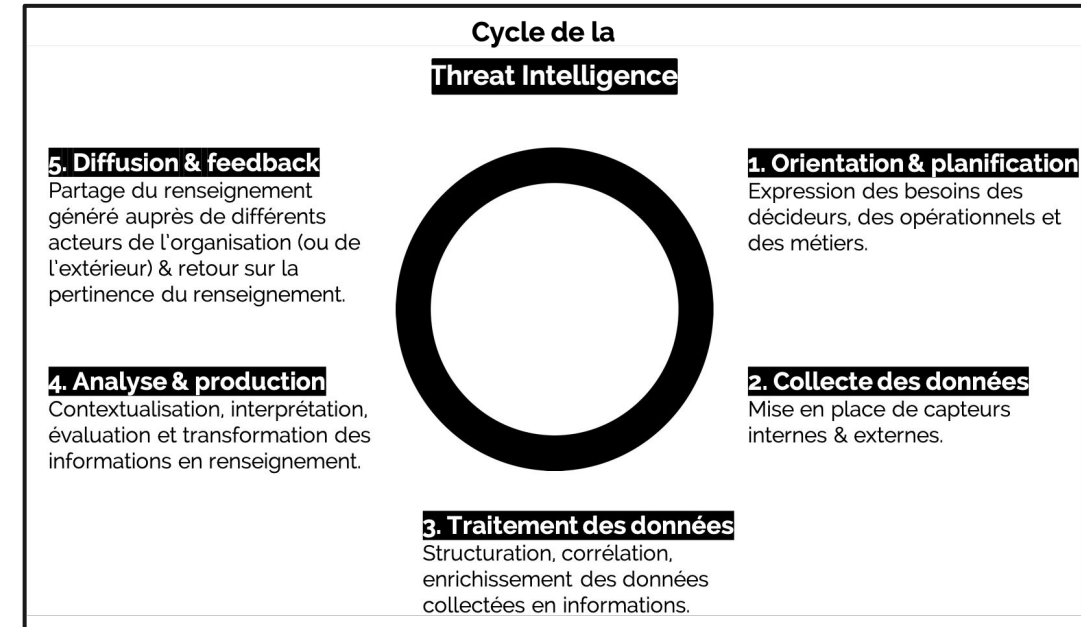
# Le cycle du renseignement

## Collecte des données

## Mise en place de capteurs adaptés aux besoins

- OSINT

- collectes d'informations analysées (blogs, articles, rapports...)
- informations techniques bruts (IPs et URLs malveillantes, hash de malware, empreinte certificats...)
- suivi des infrastructures et des activités des groupes d'attaquants
  - Alertes Virus Total, Domain tool ...
- réseau de honeypots
- télémétrie des éditeurs de solutions de cybersécurité (antivirus, sandbox, firewall NG, ...)
- plateformes d'analyses en lignes de fichiers malveillants
- outils spécifiques, ...



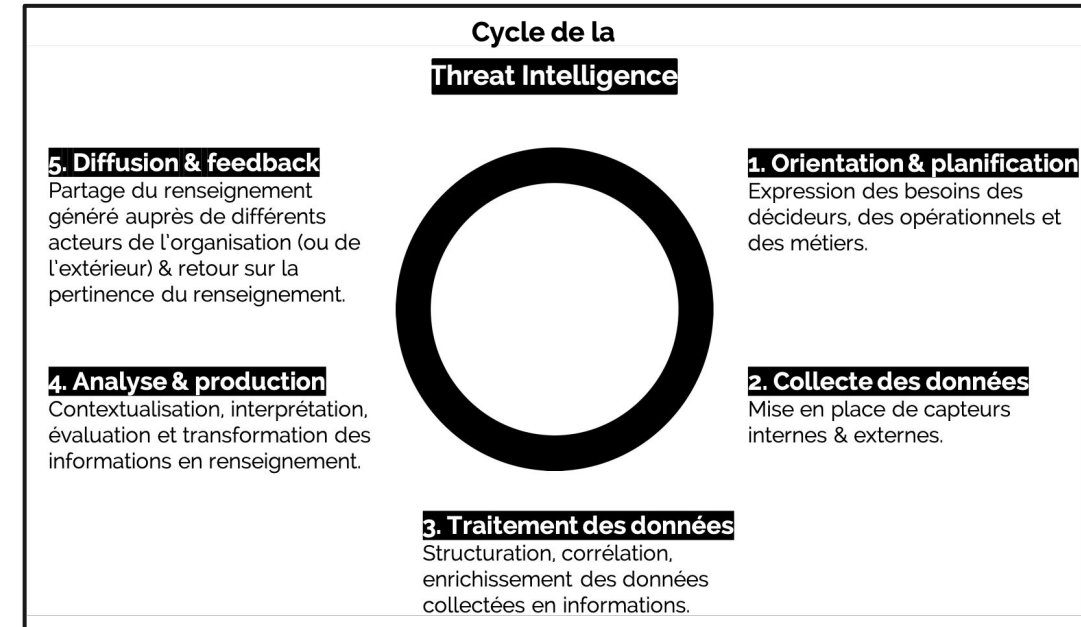


# Le cycle du renseignement

Collecte des données

Mise en place de capteurs adaptés aux besoins

- Humain
  - participation à des événements dédiés à la cybersécurité (conférence, workshop, ...)
  - créer des liens humains
    - rencontrer ses pairs
    - partager des méthodologies, des analyses, des IOCs

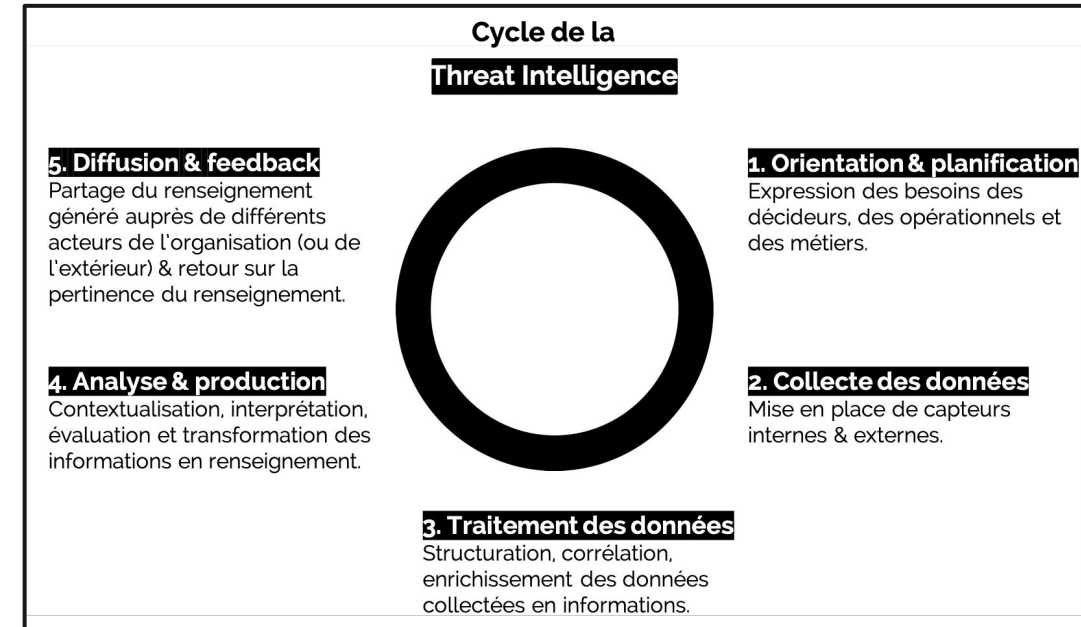


# Le cycle du renseignement

## Traitement des données

## Organisation des données collectées avant l'analyse humaine

- Normalisation
- Qualification
- Enrichissement



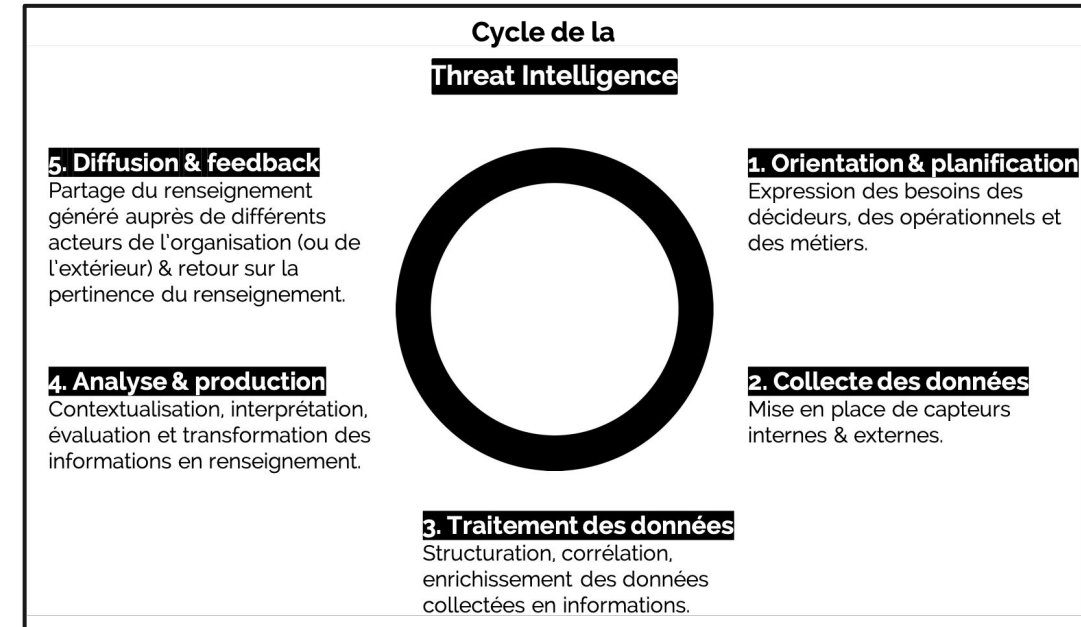


# Le cycle du renseignement

## Analyse et production

Transformation des informations en renseignements contextualisés et actionnables

- Peu de méthodes structurées d'analyses
  - Intuition et expérience de l'analyste
  - ACH : Analyse des hypothèses concurrentes
- Production
  - rapport synthétique
  - ensemble d'indicateurs pour la construction d'un tableau de bord (exposition au risque)
  - rapport sur un groupe d'attaquant, un outil, une infrastructure
  - des IOCs contextualisées avec CoAs...

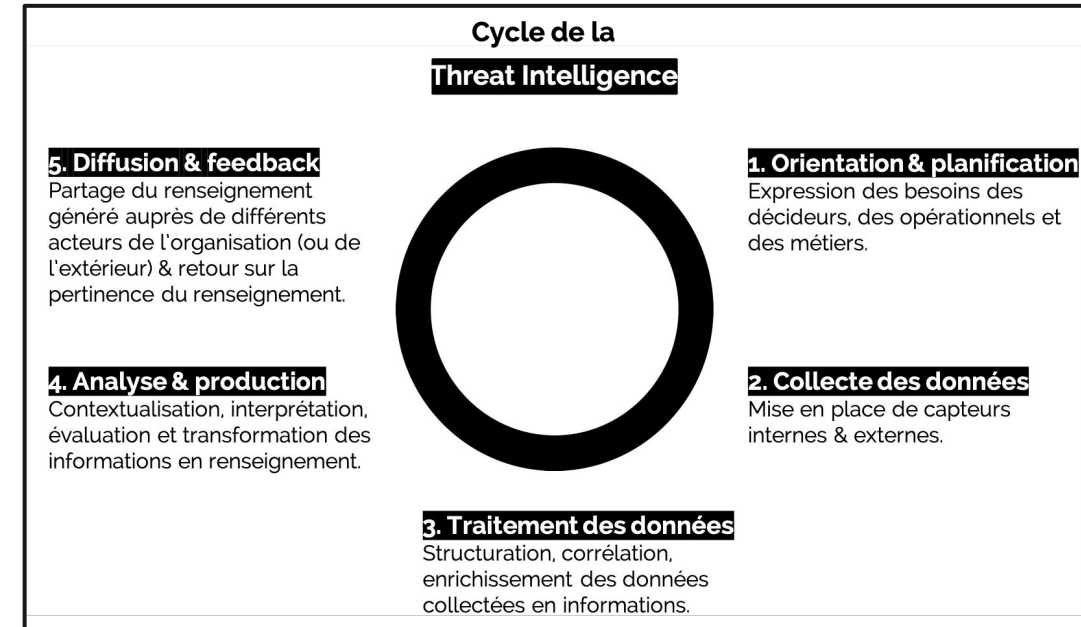


# Le cycle du renseignement

## Diffusion et feedback

Diffusion aux bonnes personnes, dans le bon timing et dans un format adapté des renseignements

- Les clients potentiels d'une équipe CTI
  - les décideurs de la cybersécurité
  - le risk manager
  - le Security Operation Center
  - le CERT/CSIRT
  - la red team
- Le feedback est nécessaire à l'amélioration continue
  - quels IOCs ont levé des alertes, le RSSI a-t-il bien compris la menace ?



# Analyser une intrusion

—



# Comment analyser une intrusion ?

Pour son travail, un analyste doit analyser et comprendre une intrusion.

Il utilise une méthodologie pour

- caractériser les menaces
- assurer le suivi de l'évolution des menaces
- trier les menaces

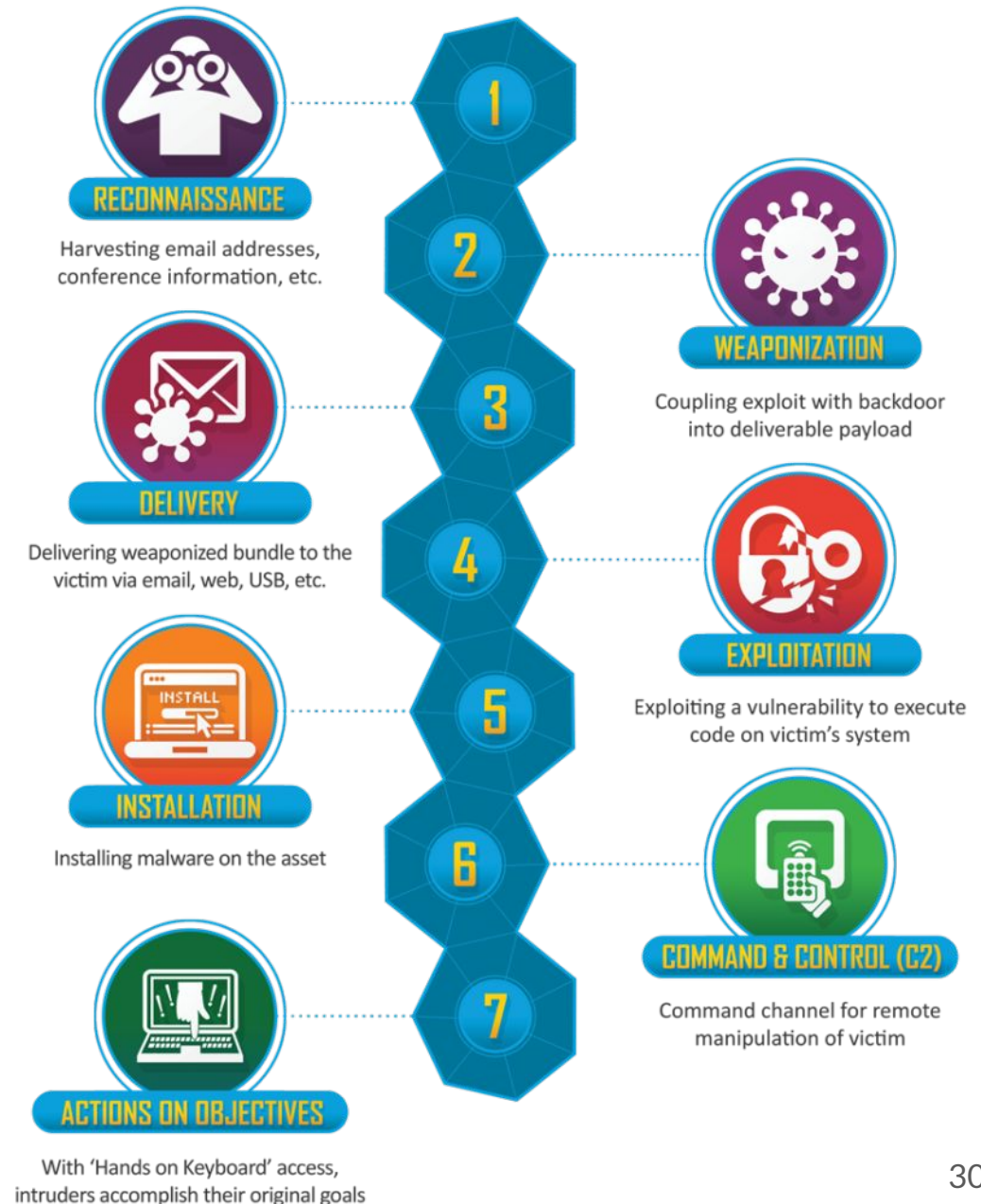


# Kill chain

- Référence : domaine militaire
- Modèle F2T2EA : Identifier les étapes d'une attaque
  - **Find:** rechercher des cibles adverses à engager
  - **Fix:** établir la localisation des cibles
  - **Track:** observer le comportement des cibles
  - **Target:** cibler avec des armes (ressources) adaptées aux effets souhaités
  - **Engage:** engager l'adversaire
  - **Assess:** évaluer les effets de l'attaque
- Aucune étape n'est obligatoire

# Cyber Kill Chain

- Concept créé par Lockheed Martin
- Définition · des étapes · d'une attaque informatique
- 7 étapes
  - *Reconnaissance*
  - *Weaponization*
  - *Delivery*
  - *Exploitation*
  - *Installation*
  - *Command and Control*
  - *Actions on Objective*



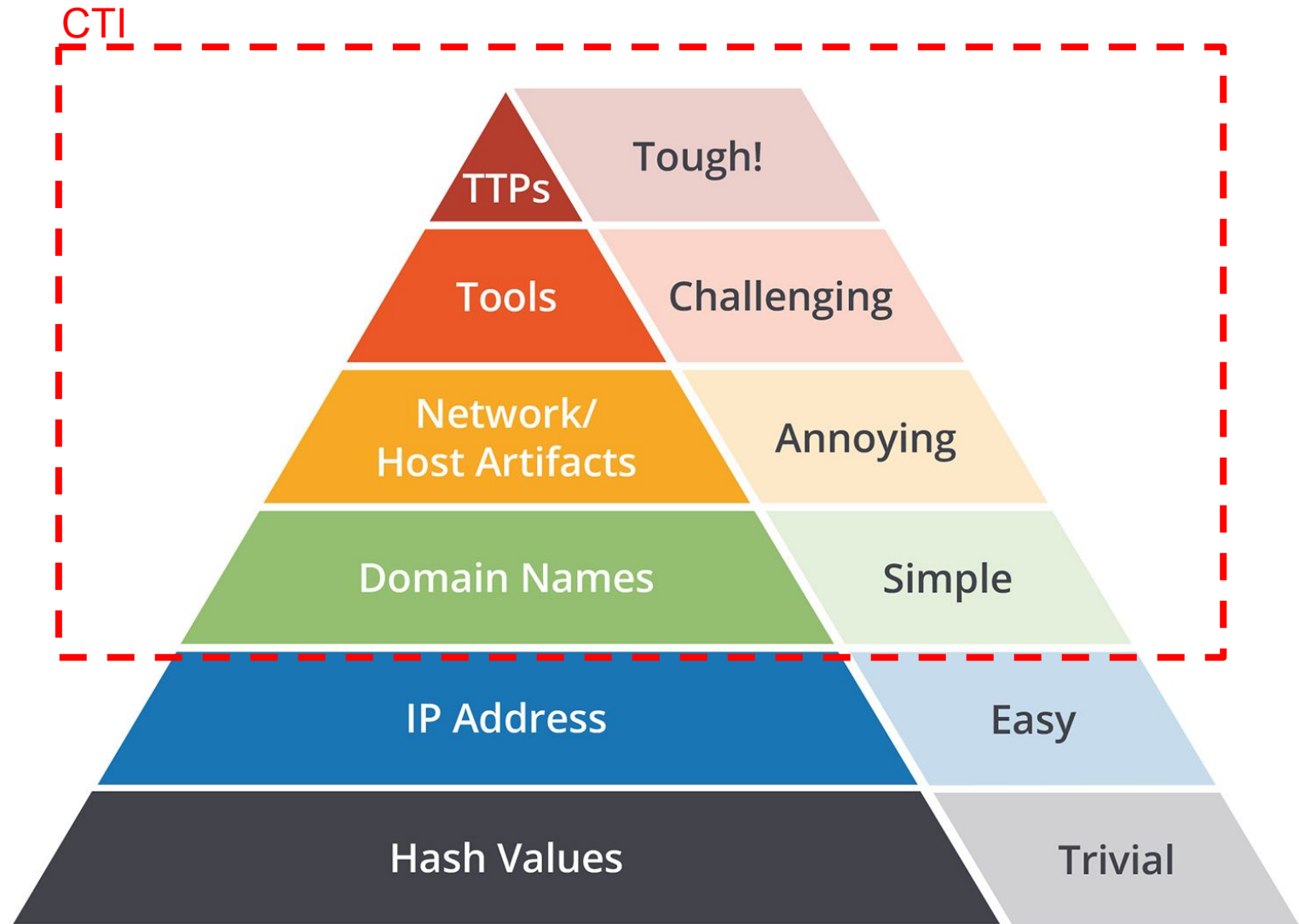
# TTPs

- TTP
  - Tactics
  - Techniques
  - Procedures
- Modélisation de la stratégie de l'attaquant



# Pyramid of Pain

Évolution de la complexité du  
changement du point de  
vue de l'attaquant



Source: David J. Bianco, personal blog





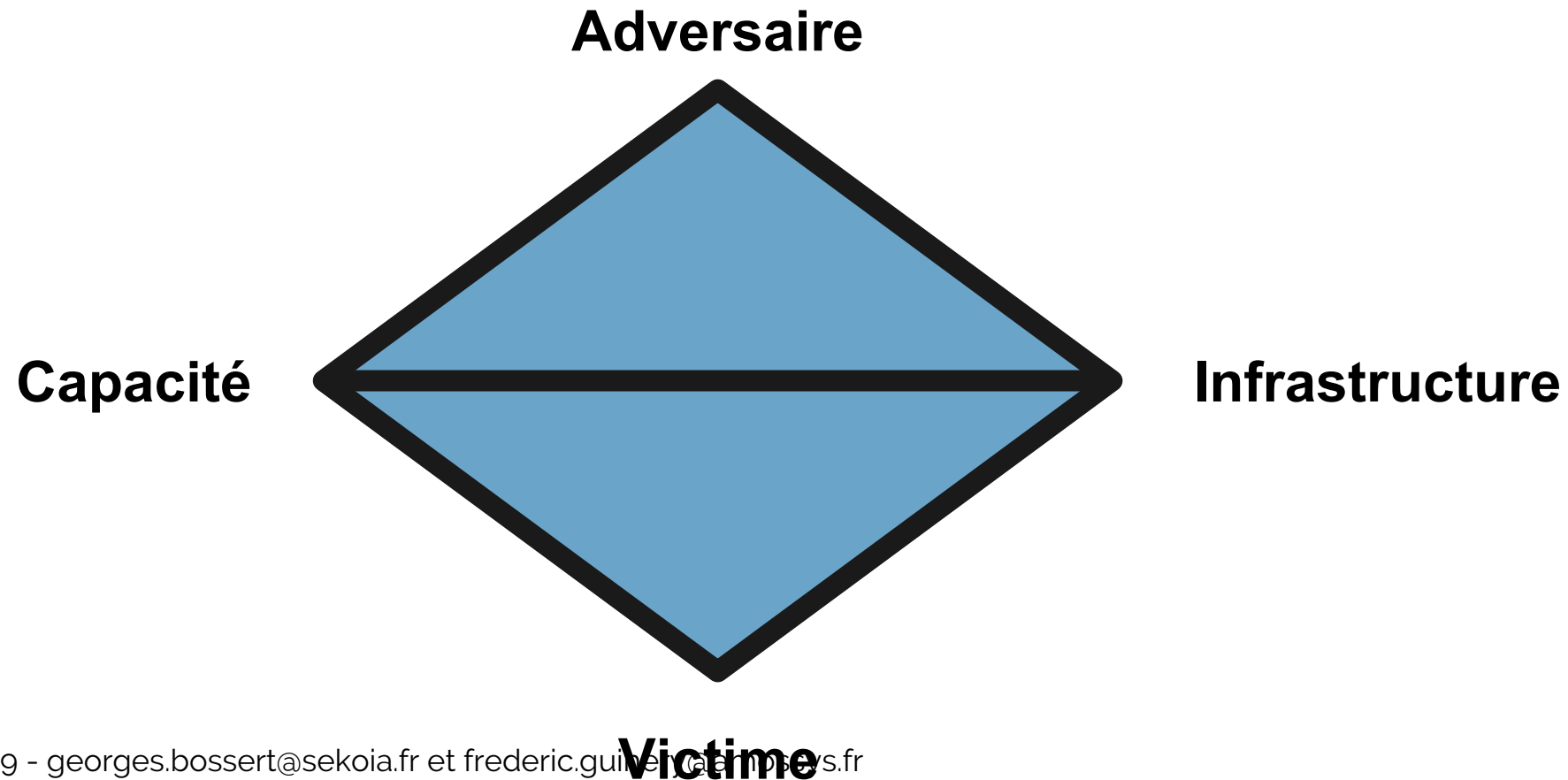
# Modèle en diamant

- Modèle pour l'analyse et la remédiation de menaces d'intrusions
- Établit les éléments de base d'une intrusion:
  - l'adversaire
  - l'infrastructure
  - la capacité, les outils
  - la victime

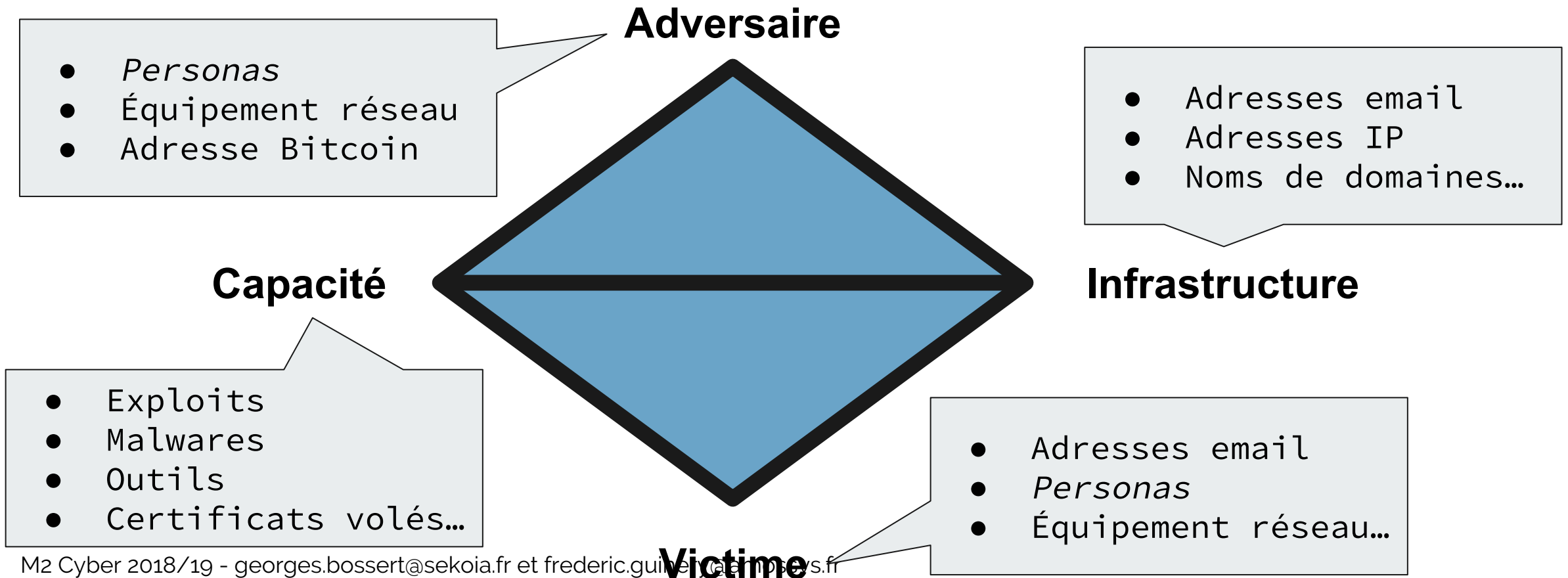
Un adversaire exploite un outil sur une infrastructure contre une victime

- Permet de documenter, synthétiser et corrélérer une intrusion
  - i.e. comment mesurer, tester et reproduire une intrusion ?

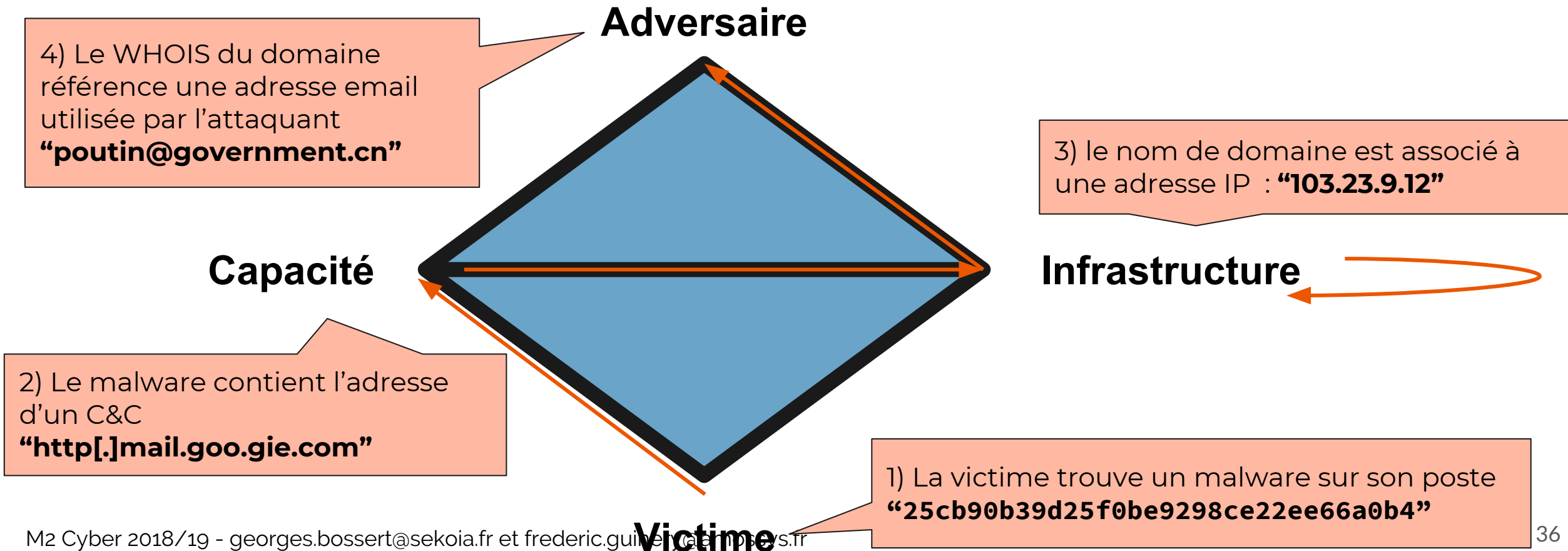
# Modèle en diamant



# Modèle en diamant

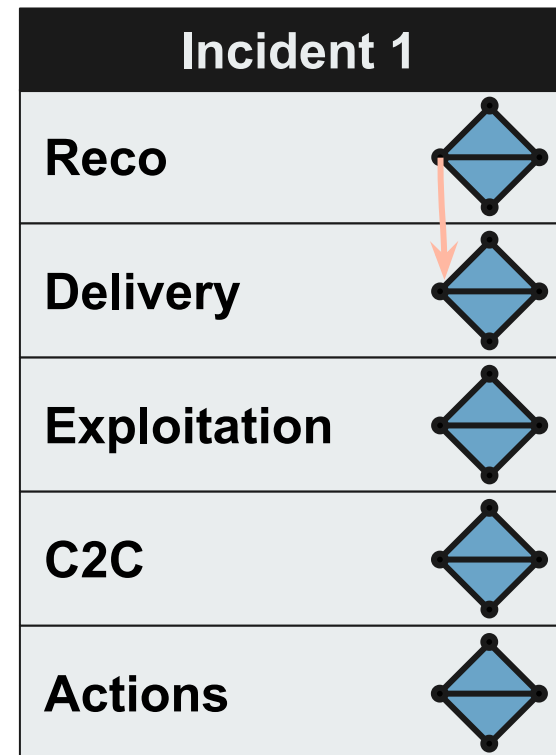


# Modèle en diamant



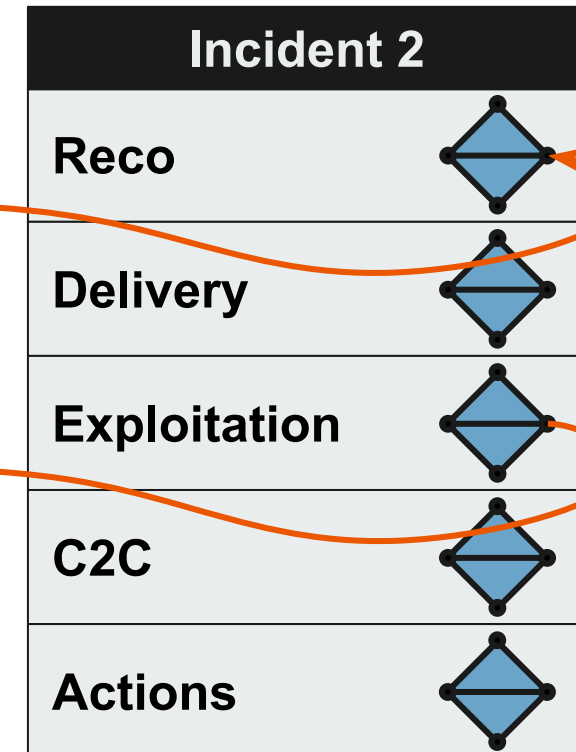
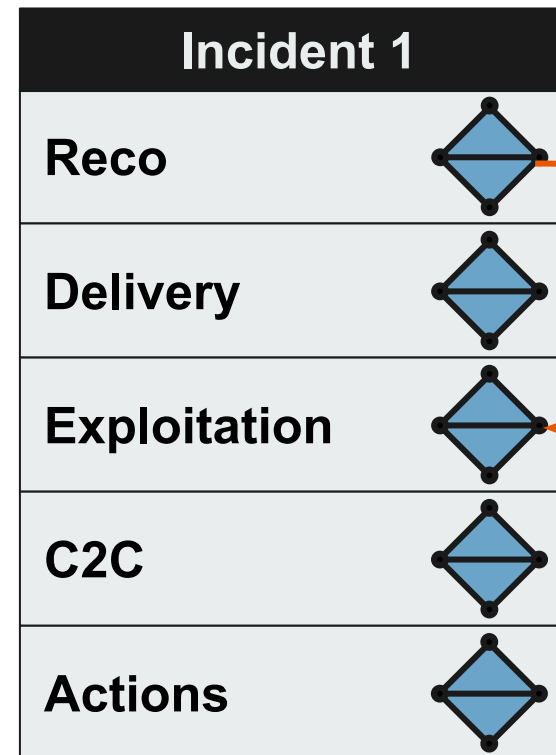
# Modèle en diamant + Cyber Kill Chain

- Chaque phase est représentée par un diamant
- Possibilité d'utiliser des "meta-features"
  - le timestamp de l'évènement
  - l'état de l'évènement (success, failure, ...)
  - la direction de l'évènement (i2v, v2i)
  - la classe de l'évènement...
- Corrélation verticale
  - Identifier un lien de causalité entre des plusieurs activités malveillantes



# Modèle en diamant + Cyber Kill Chain

- Chaque phase est représentée par un diamant
- Possibilité d'utiliser des "meta-features"
  - le timestamp de l'évènement
  - l'état de l'évènement (success, failure, ...)
  - la direction de l'évènement (i2v, v2i)
  - la classe de l'évènement...
- Corrélation verticale
  - Identifier un lien de causalité entre des plusieurs activités malveillantes
- Corrélation horizontale
  - Regrouper des incidents grâce à l'identification de TTPs



# Threat Actors

APT Groups and Operations													
README	China	Russia	North Korea	Iran	Israel	NATO	Middle East	Others	Unknown	_Download	_Schemes	_Malware	_Sources
China													
Common Name	CrowdStrike	IRL	Kaspersky	Secureworks	Mandiant	FireEye	Symantec	iSight	Cisco (Sourcefire/ Palo Alto Unit 42	Other Names	Operation 1	Operation 2	
Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT 1			BrownFox	Group 3	GIF89a, ShadyRAT, Shanghai Group, Byzantine C	Shady RAT		
APT 2	Putter Panda	PLA Unit 61486		TG-6952	APT 2				Group 36	SearchFire			
UPS	Gothic Panda			TG-0110	APT 3		Buckeye	UPS Team	Group 6	Boyusec - the Guangzhou Boyu Information Tech	Clandestine Fox	Double	
IXESHE	Numbered Panda			TG-2754 (tentative	APT 12	BeeBus		Calc Team	Group 22	DynCalc, Crimson Iron, DNSCalc	NYT Oct 2012		
APT 16					APT 16								
Hidden Lynx	Aurora Panda				APT 17	Deputy Dog	Hidden Lynx	Tailgater Team	Group 8	Axiom, SportsFans, Winnti Umbrella	Ephemeral Hydra		
Wekby	Dynamite Panda	PLA Navy		TG-0416	APT 18								
Axiom					APT 17			Tailgater Team	Group 72	Dogfish (iDefense), Deputy Dog (iDefense), Winn	SMN		
Winnti Group	Wicked Panda									Winnti Umbrella			
Shell Crew	Deep Panda		WebMasters		APT 19	KungFu Kittens			Group 13	Sh3llCr3w, PinkPanther	Anthem	OPM	
Naikon	Lotus Panda	PLA Unit 78020	Naikon		APT 30		Firefly				MsnMM	Naikon	
PLATINUM													
Lotus Blossom			Spring Dragon							TwoForOne	Hellsing		
										ST Group, Esile	Operation Lotus Blossom		

https://docs.google.com/spreadsheets/u/2/d/1H9\_xaxQHpWaa4O\_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml#

[https://docs.google.com/spreadsheets/u/2/d/1H9\\_xaxQHpwaa4O\\_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml#](https://docs.google.com/spreadsheets/u/2/d/1H9_xaxQHpwaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml#)

Les groupes d'attaquants organisés sont nommés

- classification souvent réalisée par pays
- métaphore animale utilisée par CrowdStrike



Jackal  
(Afghanistan)



Tiger  
(India)



Bear  
(Russia)



Kitten  
(Iran)



Panda  
(China)

# Partager

---



# MISP - OpenSource CTI Platform

The screenshot displays the MISP OpenSource CTI Platform interface. The top navigation bar includes tabs for Scope, Reference, Physics, Display, Filters, Export, and History. A search bar is located on the right. The main area shows a network graph with nodes representing various objects and their relationships. An 'Export' dropdown menu is open, showing options like png, json, png, jpeg, and DOT Language. The graph includes nodes for 'file: dc40f11eb6815ca9adea0a3b8c[...]', 'file: edc83f5b08d3d009e60f3700d6[...]', 'file: 374896a75493a406eb427f35ee[...]', 'file: 687464d6c668b59f85b0e02012[...]', 'file: 75fa78e2cc42ad885c722a7[...]', 'file: 44d5d647016b04a095f3658260[...]', 'text: C2 Server', 'whois: C2 Server', 'registrant-phone: +3800564040808', and 'domain: marina-info.net'. The bottom section features a table of events with columns for Date, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, Distribution, Sightings, Activity, and Actions. The table lists two events: one from 2018-07-17 with category 'External analysis' and type 'attachment', and another from 2018-07-17 with category 'External analysis' and type 'attachment'.

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2018-07-17		External analysis	attachment					<input checked="" type="checkbox"/>			No	Inherit			
2018-07-17		External analysis	attachment	20180713_CSE_APT28_X-Agent_Op-Roman Holiday-Report_v6_1.pdf			http://csecybsec.com/download/20180713_CSE_APT28_X-Agent_Op-Roman Holiday-Report_v6_1.pdf	<input checked="" type="checkbox"/>			No	Inherit			





# YARA

## **{ }** YARA in a nutshell

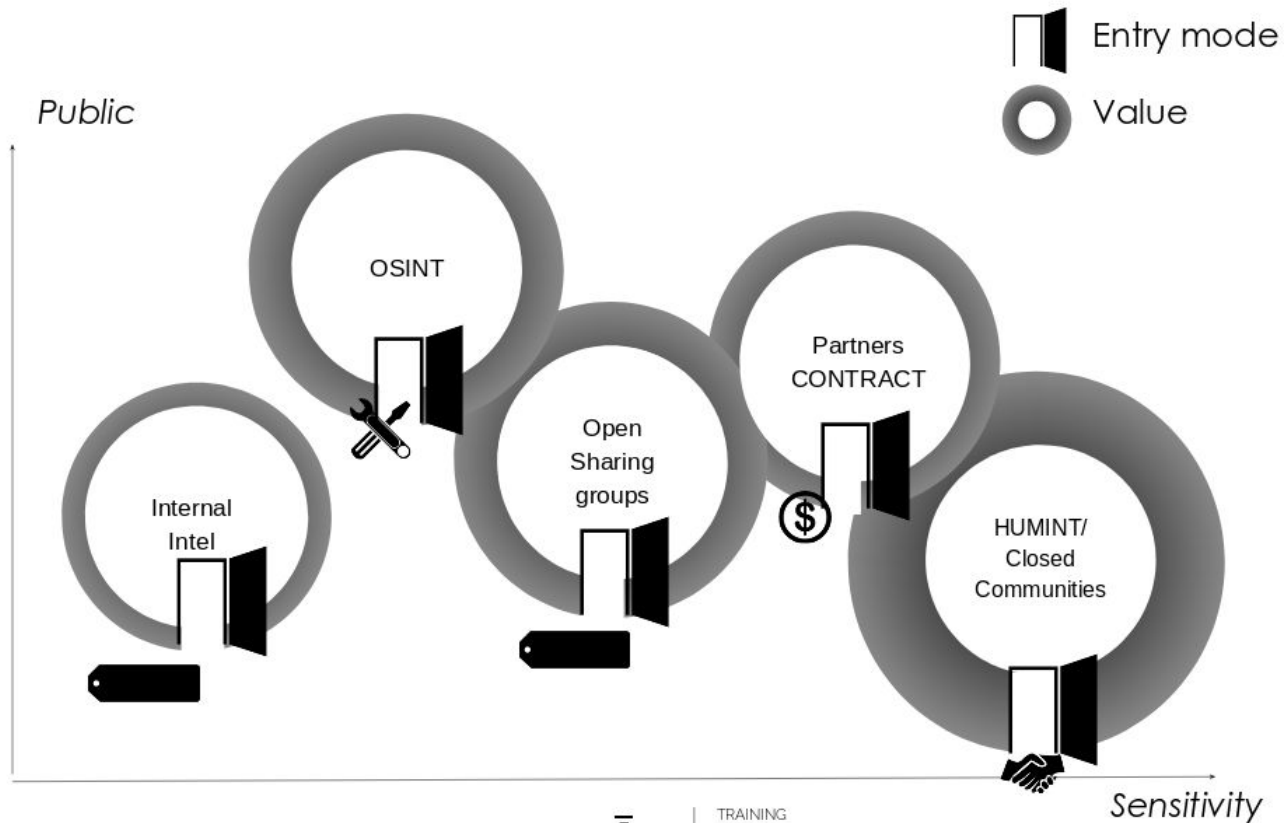
YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

# Les groupes de partage





# Les groupes de partage

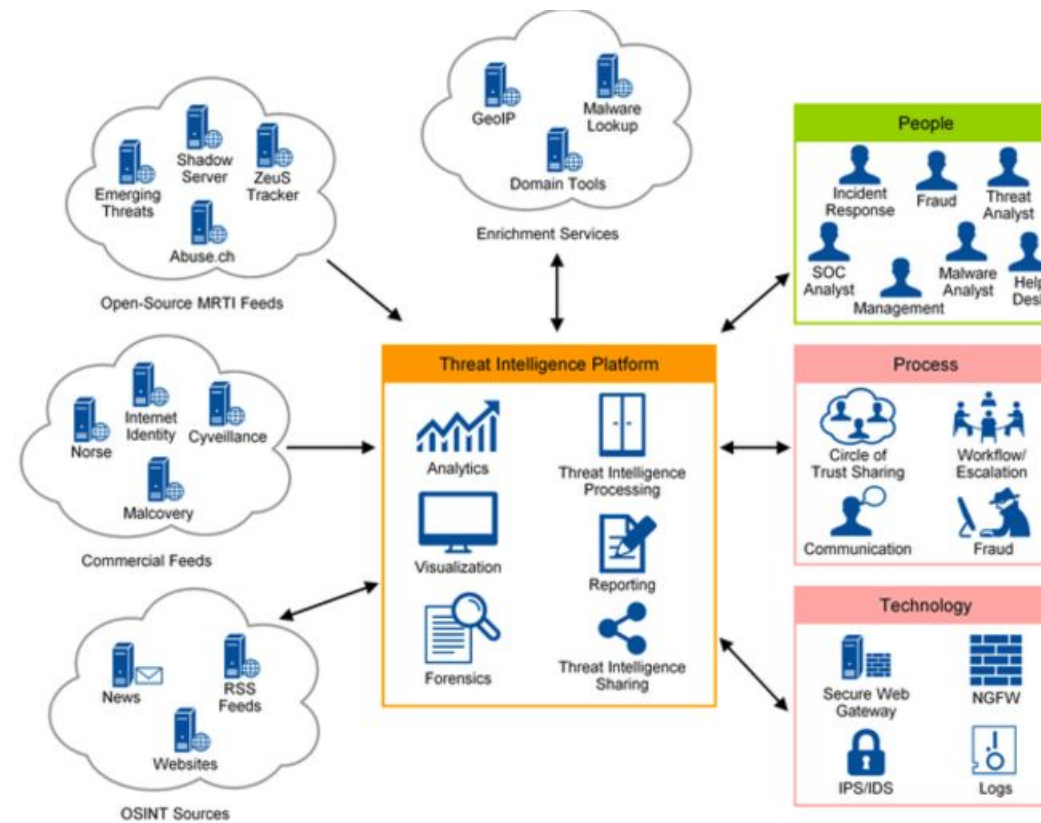
« Sharing is carying »

- Dans une communauté, quand quelqu'un partage, cela profite à tous
- Tout le monde doit partager autant que possible avec la communauté
- Plus vous partagez, plus votre réputation sera forte dans la communauté

« Sharing is scaring »

- Lorsque vous dites quelque chose de mal, vous pouvez être blâmé
- En cas d'erreur, des informations sensibles peuvent fuir

# Threat Intelligence Platform



Source: Gartner (December 2014)



# OASIS

Consortium mondial pour la standardisation de formats de fichiers

Créé en 1993.

+/- 3500 membres, 600 organisation, 100 pays

Adhésion payante, surtout de grosses entreprises mais quelques exceptions (Debian)

Fonctionnement en Groupes de Travail : ***Technical Committees***



# OASIS

143 standards approuvés

- Advanced Message Queuing Protocol - AMQP
- Common Alerting Protocol - CAP
- DocBook
- SAML
- Stack *Ws-Security*...



# OASIS

138 spécifications en phases finales (« fully implementable »)

- AMQP WebSocket Binding (WSB)
- OpenDocument Format for Accessibility
- Election Markup Language (EML)
- SAML v2
- TAXII™ 1.1.1
- TAXI™ 2.0
- STIX™ 1.2.1
- STIX™ 2.0





# STIX

Structured Ihreat Information eXpression

- Language + format de sérialisation de données CTI
- Initié par le DHS → MITRE → OASIS
- Spécifications de la version 1.2.1 votée en mai 2016
- Spécifications de la version 2.0 votée en juillet 2017

# STIX v2

Le langage s'articule autour:

- d'objets (SDO - STIX Domain Objects)
- de relations entre les objets (SRO - Stix Relationship Objects)

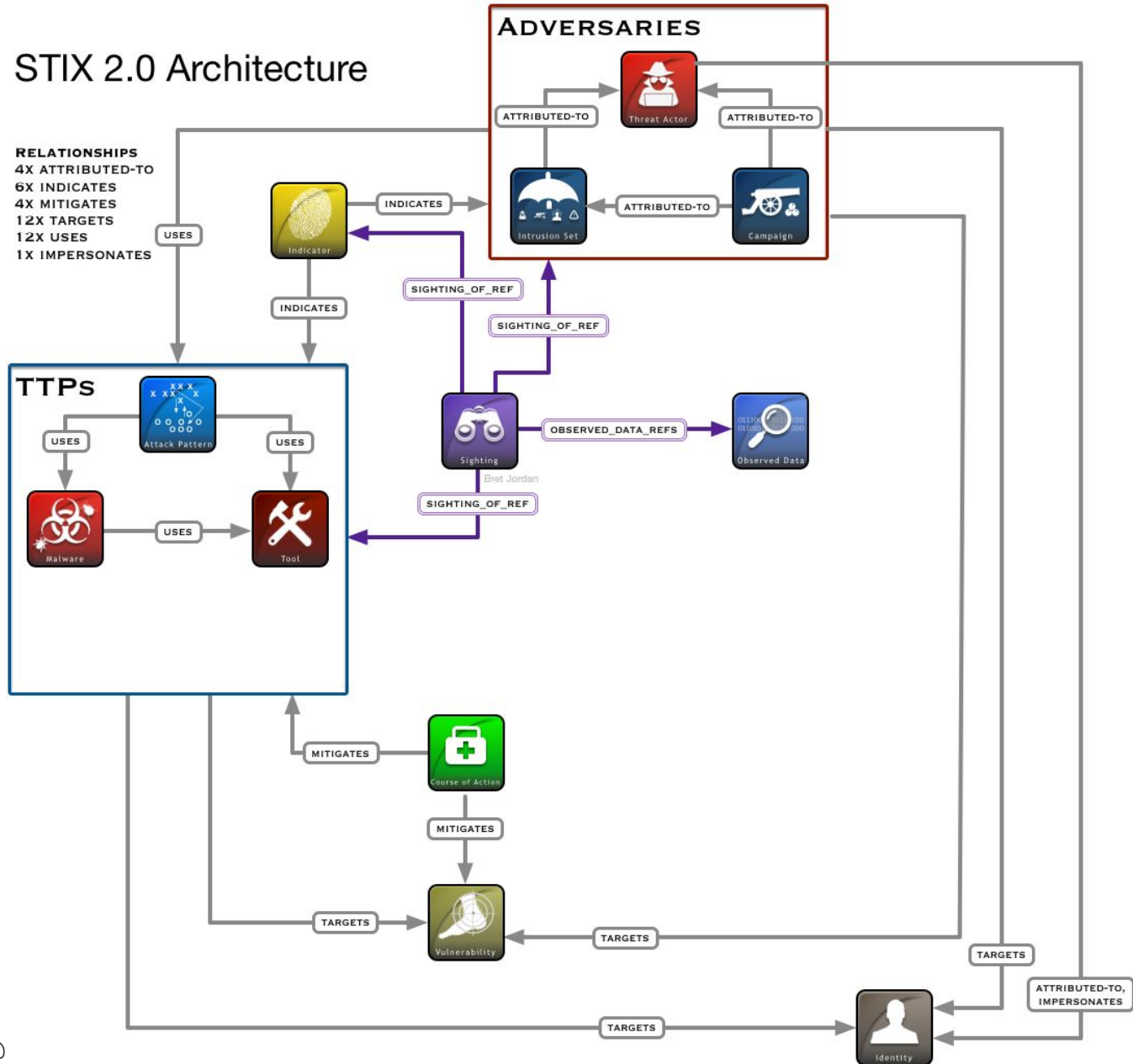
Permet également de spécifier

- les restrictions, permissions et autres contraintes sur les droits d'accès (Data Markings)
  - notion de granular marking



# STIX v2

## STIX 2.0 Architecture





# STIX v2

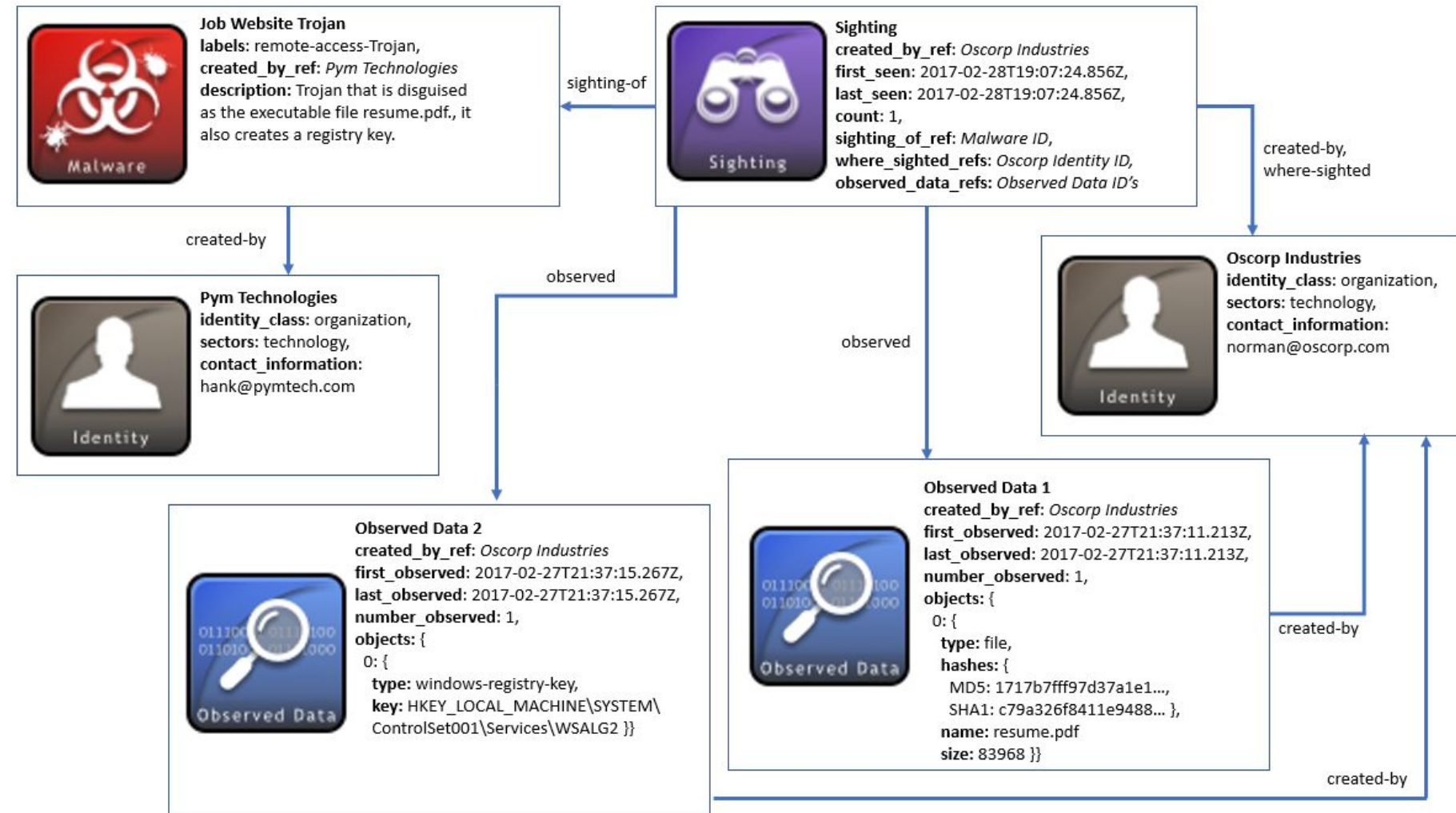
```
{  
  "type": "campaign",  
  "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",  
  "created": "2016-04-06T20:03:00.000Z",  
  "name": "Green Group Attacks Against Finance",  
  "description": "Campaign by Green Group against targets in the financial sector."  
}
```



# STIX v2

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-29T14:09:00.000Z",
      "modified": "2016-04-29T14:09:00.000Z",
      "object_marking_refs": ["marking-definition--089a6ecb-cc15-43cc-9494-767639779123"],
      "name": "Poison Ivy Malware",
      "description": "This file is part of Poison Ivy",
      "pattern": "[file:hashes.'SHA-256' = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f']"
    },
    {
      "type": "marking-definition",
      "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",
      "created": "2016-08-01T00:00:00.000Z",
      "definition_type": "tlp",
      "definition": {
        "tlp": "green"
      }
    }
  ]
}
```

# STIX v2





# STIX v2

## Observed Data

```
{
  "type": "observed-data",
  "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
  "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "created": "2016-04-06T19:58:16.000Z",
  "modified": "2016-04-06T19:58:16.000Z",
  "first_observed": "2015-12-21T19:00:00Z",
  "last_observed": "2015-12-21T19:00:00Z",
  "number_observed": 50,
  "objects": {
    "0": {
      "type": "file",
      ...
    }
  }
}
```

Cybox v.2.1.1



# TAXII

Trusted Automated Exchange of Indicator Information

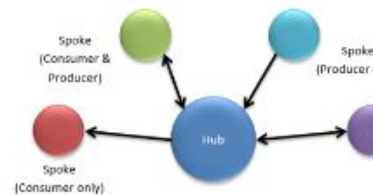
- Spécifie le partage d'informations de CTI via
  - des “endpoints” web-services nécessaires au partage
  - des formats de paramètres et de résultats exposés par ces endpoints
- Ce partage peut avoir lieu entre
  - des organisations
  - des applications
- Standard « Technique », elle ne couvre pas
  - la gestion de la confiance entre les acteurs,
  - la gouvernance...



# TAXII

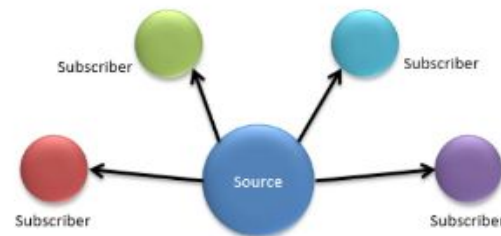
## Hub and Spoke

**Hub and Spoke** is a sharing model where one organization functions as the central clearinghouse for information, or hub, coordinating information exchange between partner organizations, or spokes. Spokes can produce and/or consume information from the Hub.



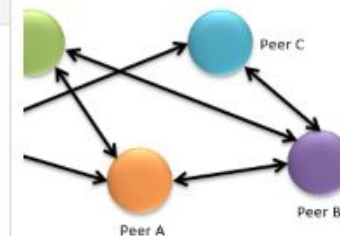
## Source/Subscriber

**Source/Subscriber** is a sharing model where one organization functions as the single source of information and sends that information to subscribers.

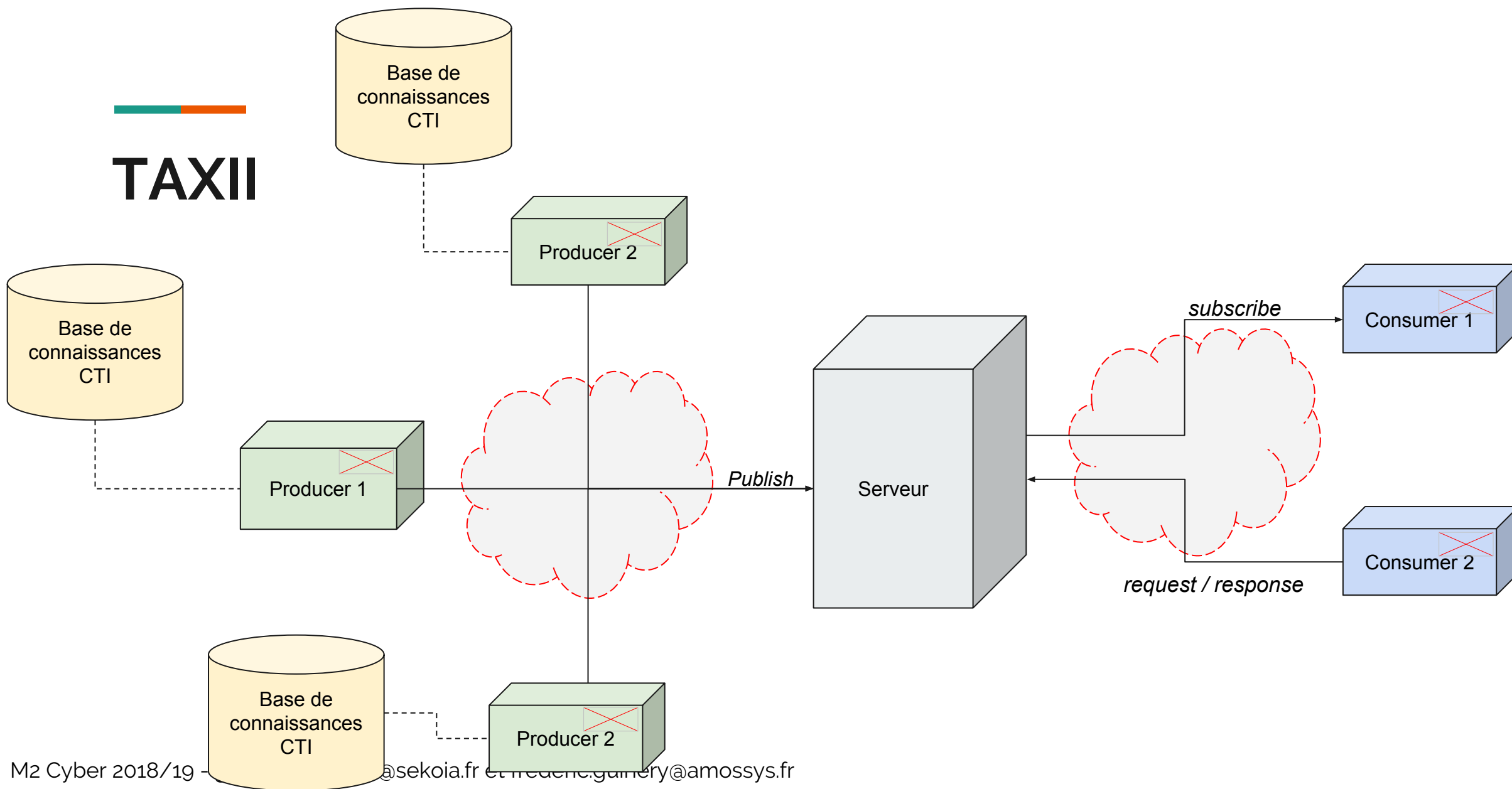


## Peer to Peer

**Peer to Peer** is a sharing model where two or more organizations share information directly with one another. A Peer to Peer sharing model may be ad-hoc, where information exchange is not coordinated ahead of time and is done on an as-needed basis, may be well defined with legal agreements and established procedures, or somewhere in the



# TAXII





# TAXII v2

- Définition d'une API RESTFul pour gérer des **Racines** de
  - **Collections**
    - Organisation des données dans un référentiel
    - Modèle Request - Response
    - Définition de filtres de recherches
  - **Channels**
    - Modèle publish-subscribe
    - Un channel = un flux
      - Un producteur de données peut « pousser » des données à plusieurs consommateurs
- Un serveur peut exposer plusieurs racines
  - Une racine ~ une URL ~ un groupe logique de collections et de channels
- Un serveur peut
  - s'enregistrer via les DNS Services records
  - expose des Endpoints de Découvertes pour lister ses racines

**Des questions ?**

—