Connaître les menaces : *Cyber Threat Intelligence*

Nicolas Pierson

Préambule

LE COMMANDEMENT DE LA CYBERDEFENSE

La cyberdéfense en France : une priorité nationale

Un modèle français **séparant strictement les capacités et missions défensives et les capacités et missions offensives,** contrairement au modèle anglo-saxon.

LIVRE BLANC
DÉFENSE ET SÉCURITÉ NATIONALE 2013

"Le cyberespace est donc désormais un champ de **confrontation** à part entière."

LBDSN 2013, p45.

La cyberstratégie française considère le cyberespace comme un domaine où doit s'exercer notre souveraineté nationale.

Montée en puissance

2007 — Attaque cyber contre l'Estonie

2008 — Livre blanc sur la défense et la sécurité nationale

2009 — Création de l'ANSSI

2010 — Attaque Stuxnet

2011 — Stratégie Cyber et nomination d'un officier général de la Cyberdéfense

2012 — Attaque contre l'Élysée

2013 — Livre blanc sur la défense et la sécurité nationale

2014 — Pacte Cyber

2015 — Attaque contre TV5 Monde

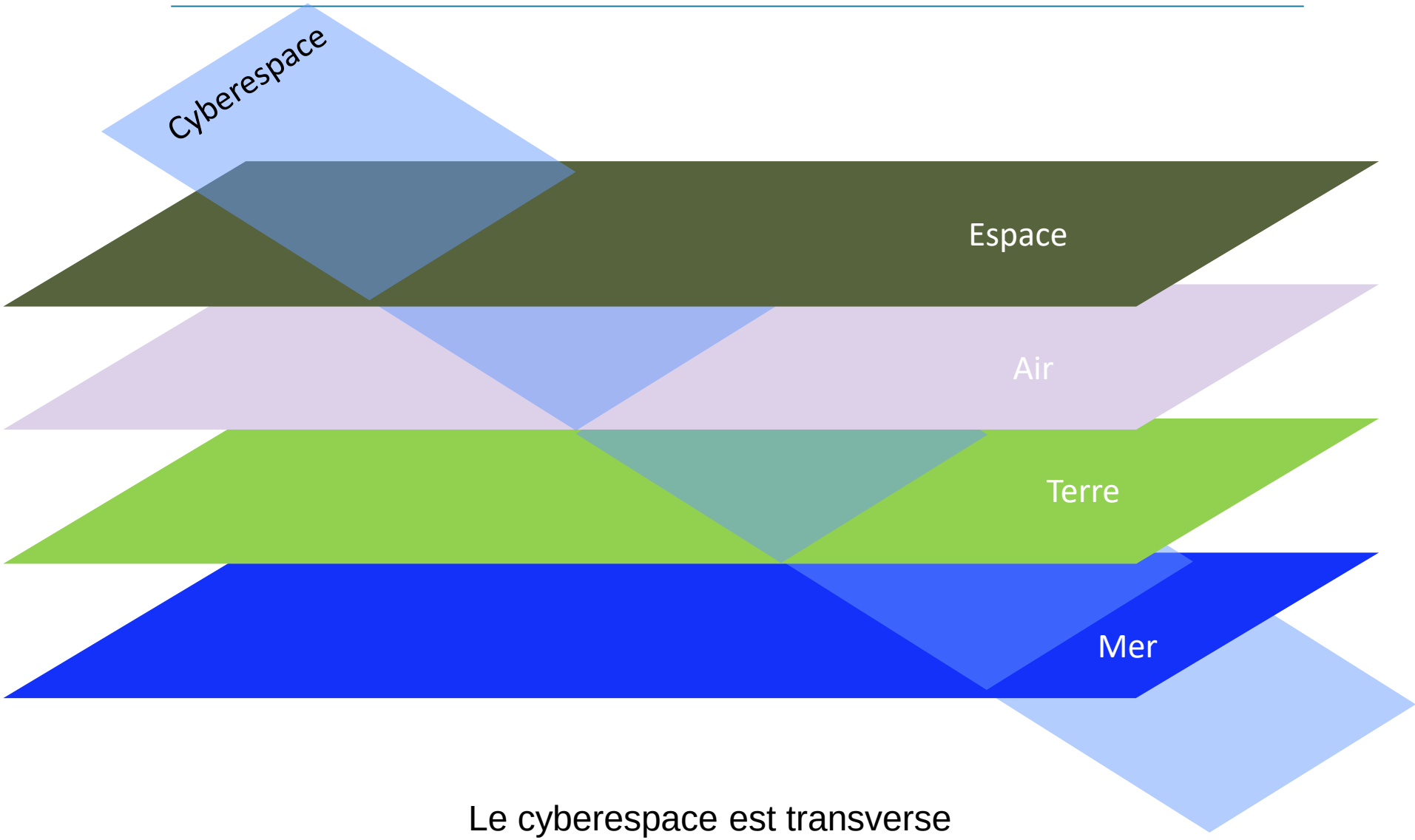
2016 — Attaque Miraï

2017 — Attaque Wannacry et création du COMCYBER

2018 — Revue stratégique de Cyberdéfense

2019 — Doctrine de lutte informatique offensive

Cyberdéfense dans les opérations



Le cyberespace est transverse
à tous les champs de confrontation.

L'organisation de la cyber au niveau national

Autorité Nationale

- LID au niveau national.
- Production des normes au niveau national.
- Protection des OIV.

PM

ANSSI

Délégation pour les opérations militaires

MinArm

- Protection des SI du CEMA.
- Défense des réseaux du MinArm.
- Planification et conduite des opérations cyber militaire sous la responsabilité du SCOPS.
- Préparer le futur.

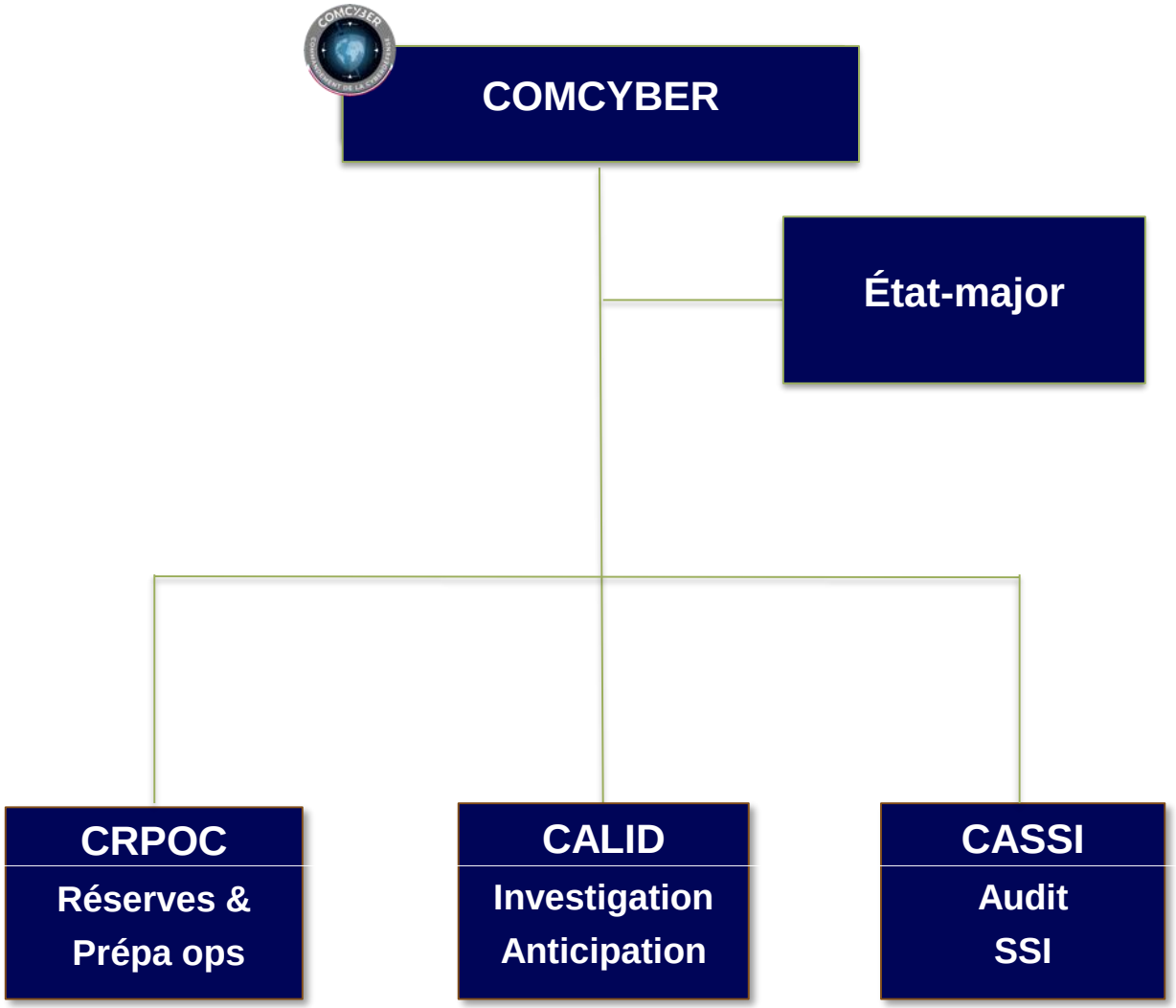
Commande

Gov-CERT (SDO)

Mil-CERT (CALID)

Colocalisés pour une plus grande efficacité

Organisation du COMCYBER



Cyberespace

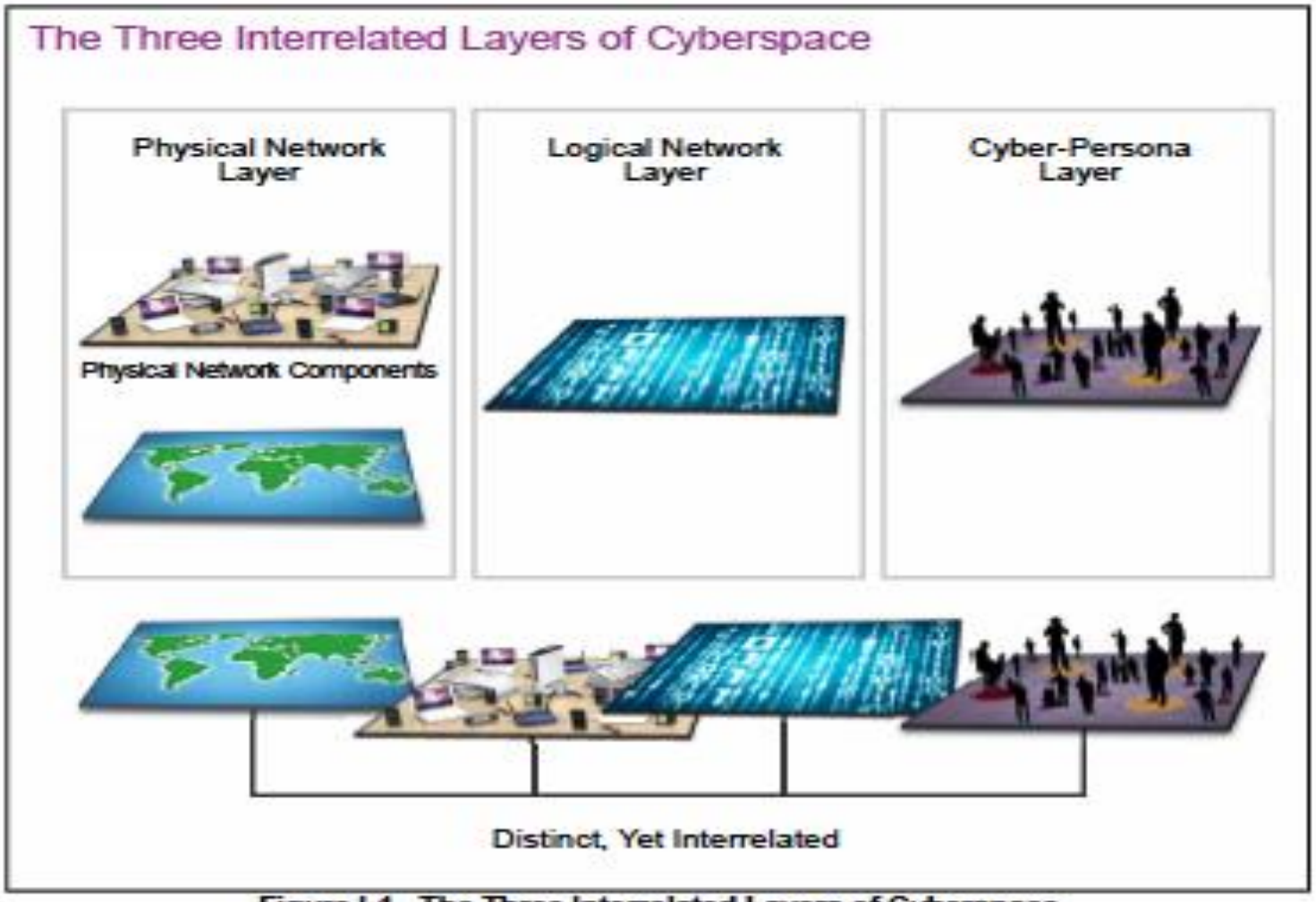


Figure I-1. The Three Interrelated Layers of Cyberspace

Source : Joint publication 3-12 – cyberspace operation

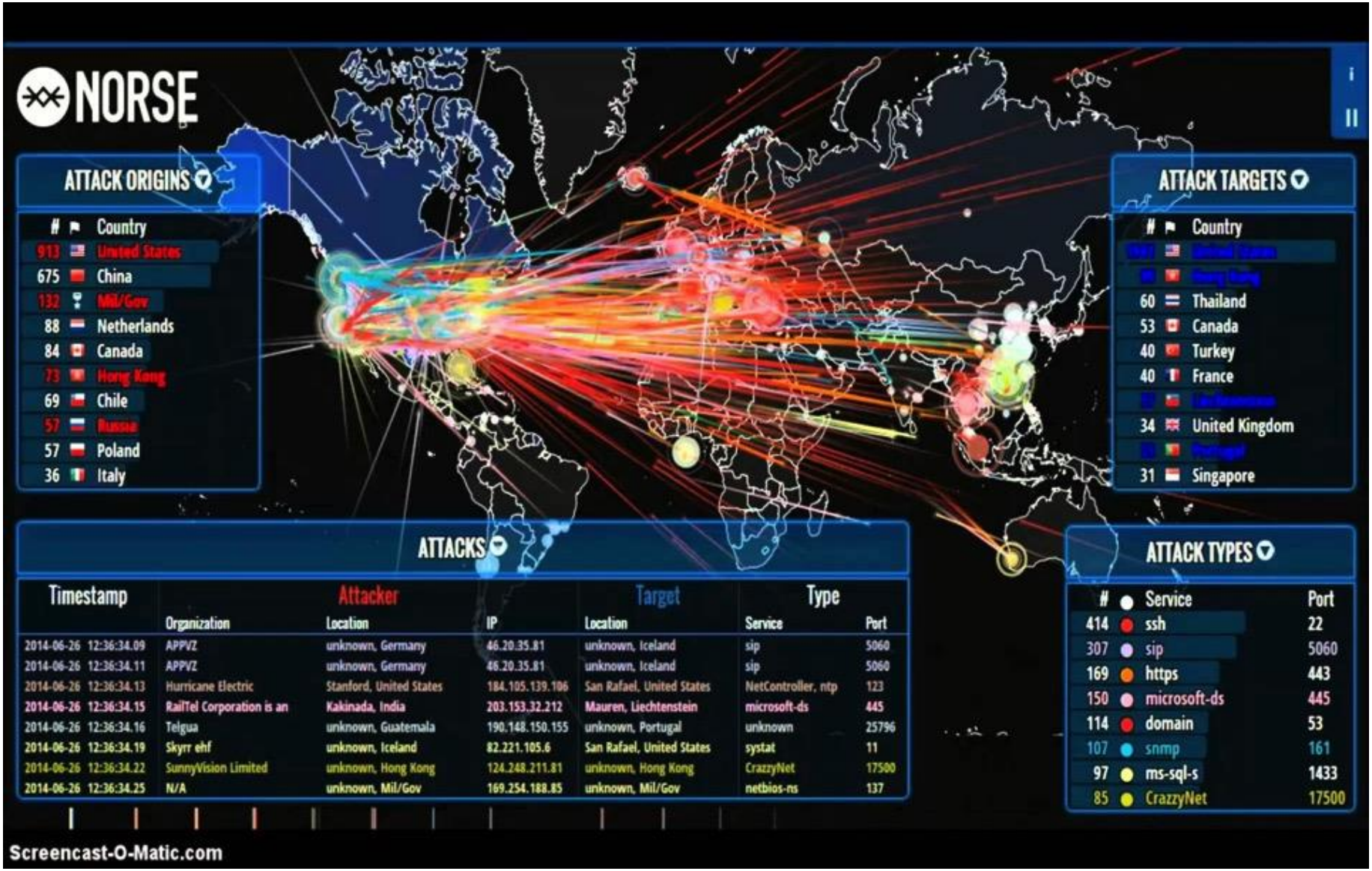
Introduction

Guillaume Poupard | FIC 2020 :

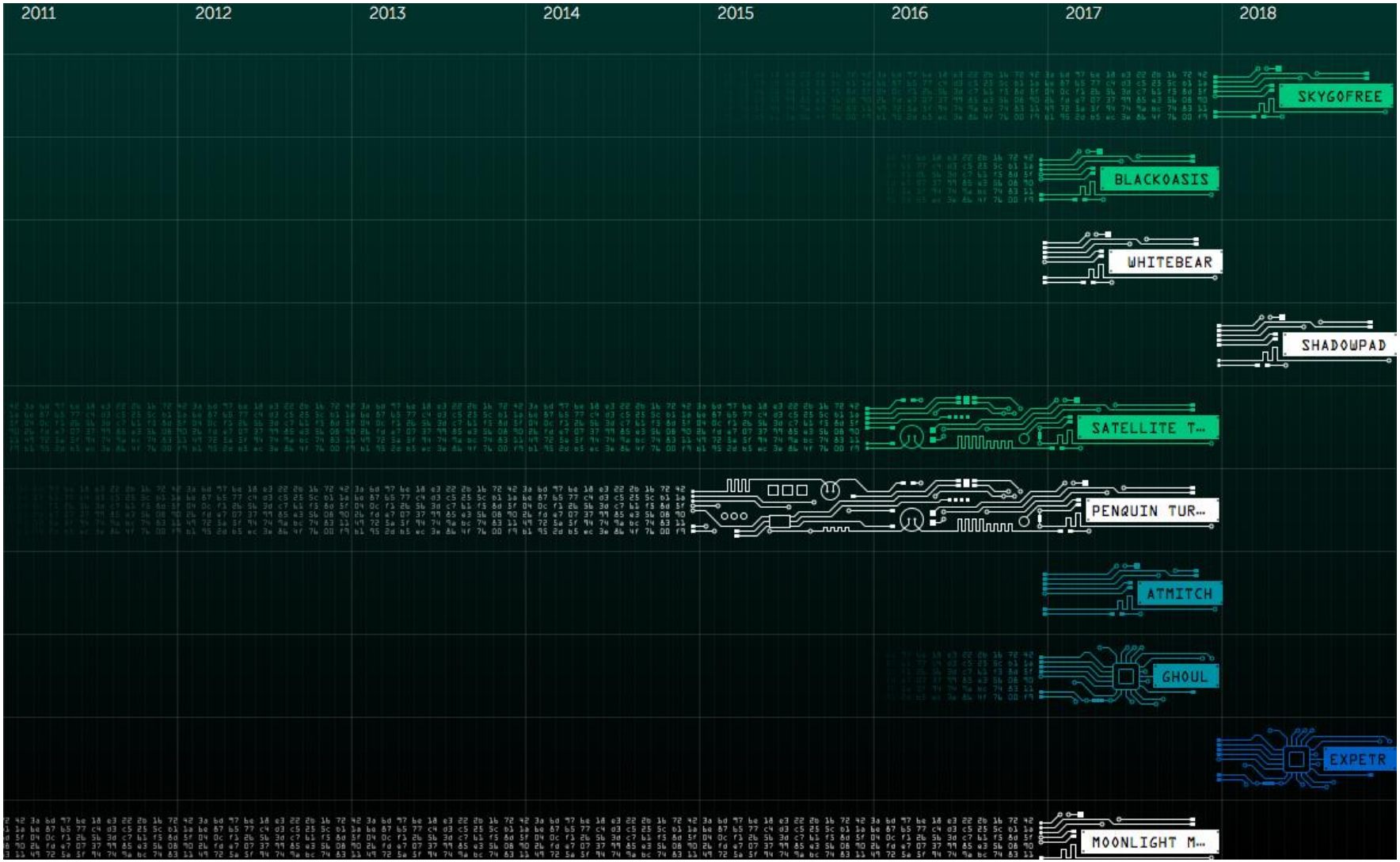
« Si vous voulez vous faire peur, dites vous que si vous prenez la somme de ce que vous trouvez en source ouverte en terme d'attaques et de victimes, vous êtes probablement à moins de 10% de la réalité. »

Vidéo complète sur : https://youtu.be/kSBZhgrFNZA

Introduction

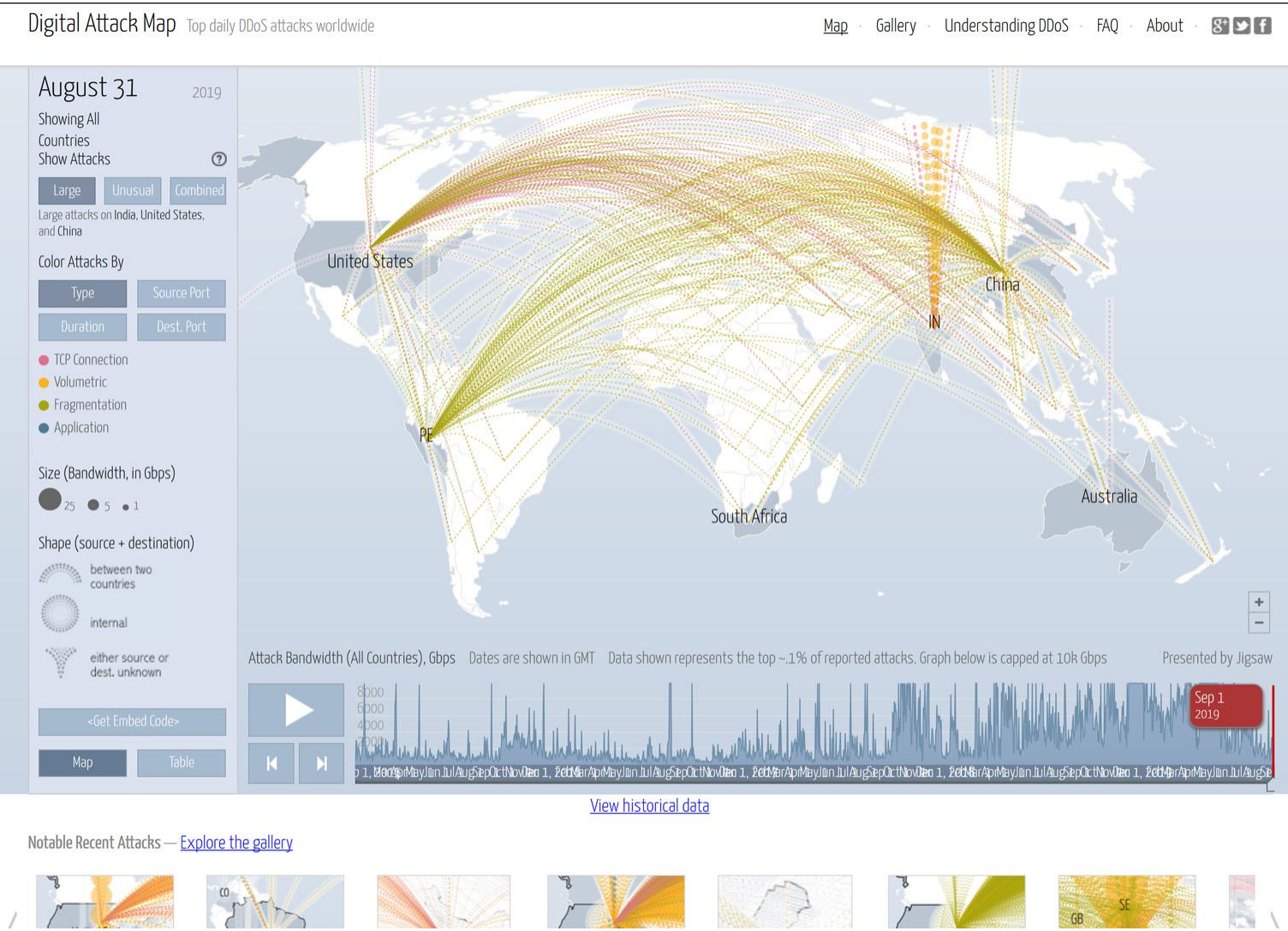


Introduction



Source : https://apt.securelist.com/#!/threats/

Introduction



Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Perspectives

Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Perspectives

I. Contexte général

Vulnérabilité :

Faiblesse dans le système, qui peut être exploitée par une menace.

Menace :

Évènement, d'origine accidentelle ou délibérée, capable s'il se réalise de causer un dommage au sujet étudié.

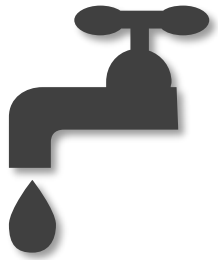
Risque :

Possibilité qu'une menace donnée exploite les vulnérabilités d'un bien ou d'un groupe de biens et nuise donc à l'organisation. (ISO 27005)

I. Contexte général

Motivations :

- Profit financier,
- Espionnage industriel,
- Activisme (ANONYMOUS, hackeurs éthiques),
- Terrorisme (ISIS),
- Services étatiques (NSA),
- Recherche de notoriété,
- Multiples.

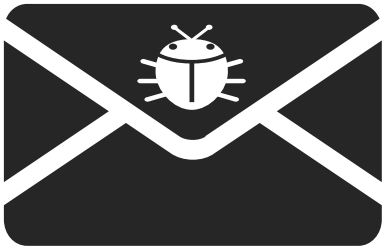


Tendance : industrialisation de la menace.

I. Contexte général

Vecteurs d'attaque *(exploit kit)* :

- "Hameçonnage" (*phishing*, *spear phishing*),
- Exploitation de vulnérabilités sur les processeurs,
- Installation par support amovible,
- Pièce jointe (pdf, macro…),
- "Puit numérique" (*waterhole*, *malwaretising*),
- Injection de code,
- Logiciel piraté,
- Force brute…



I. Contexte général

Grandes familles d'attaques actuelles (charge : *payload*) :

- Prise de contrôle à distance (minage de monnaies virtuelles, *botnet*)
- Rançongiciel *(Ransomware),*
- Déni de service DDOS,
- Fraudes multiples,
- Fuite/vol de données,
- Défiguration de sites web,
- Attaque combinée,
- Menace avancée *(APT).*

I. Contexte général

Cybersécurité (ANSSI) :

État recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la **disponibilité, l'intégrité ou la confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de **sécurité des systèmes d'information (SSI)** et s'appuie sur la **lutte contre la cybercriminalité** et sur la mise en place d'une **cyberdéfense**.

I. Contexte général

Cybersécurité (ANSSI) :

Cybersécurité (=état recherché)

- SSI (Cyberprotection)
- Lutte contre la cybercriminalité
- Cyberdéfense

I. Contexte général

CyberDéfense (ANSSI) :

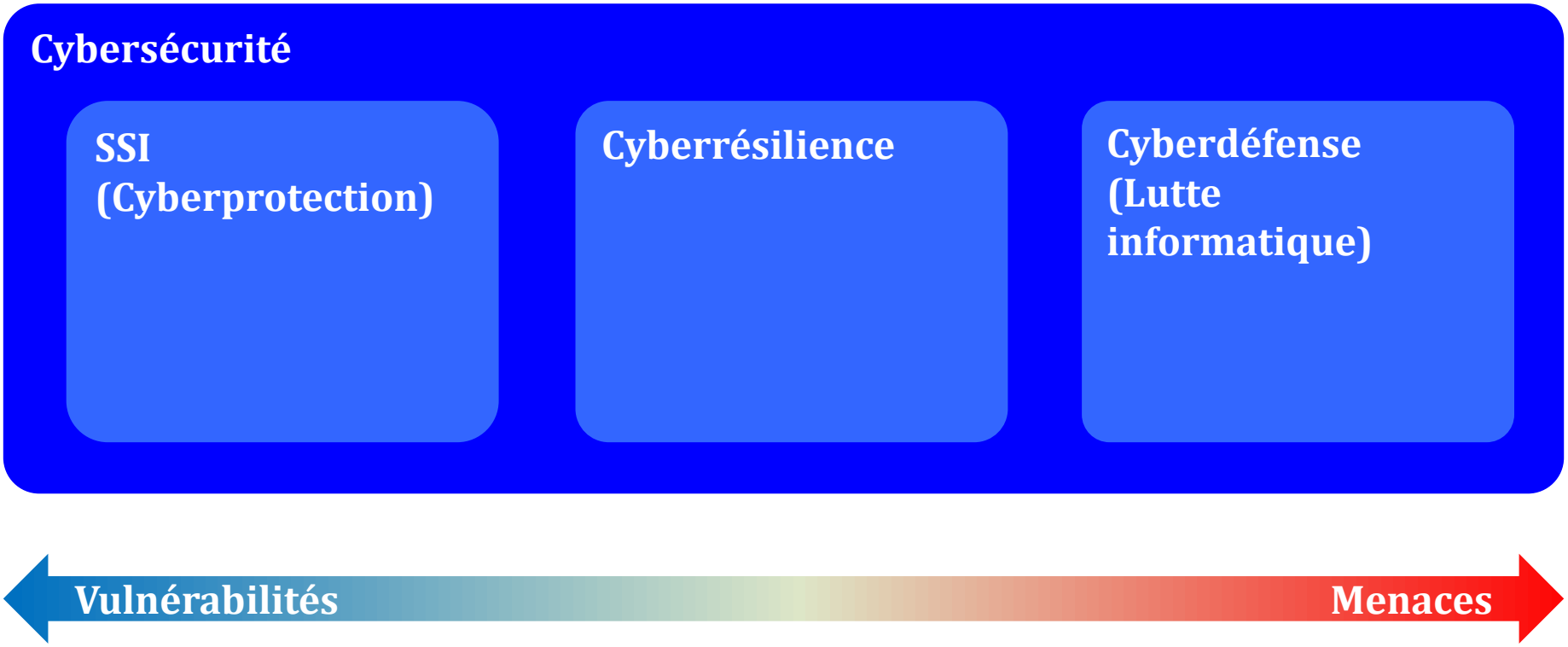
Ensemble des mesures techniques et non techniques permettant **à un État** de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cyberdéfense (=Etatique)

Mesures techniques	Mesures non-techniques

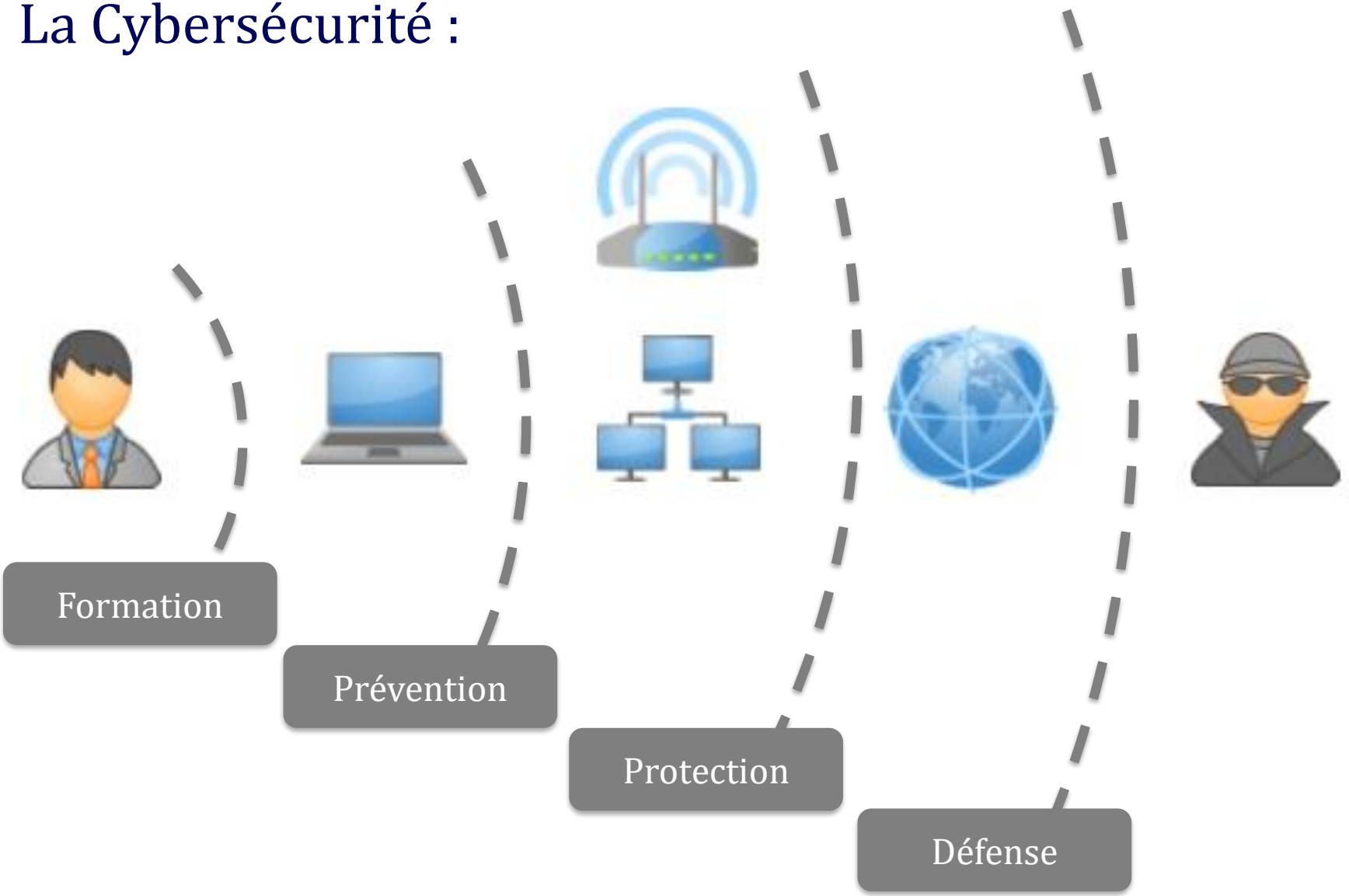
I. Contexte général

La Cybersécurité :

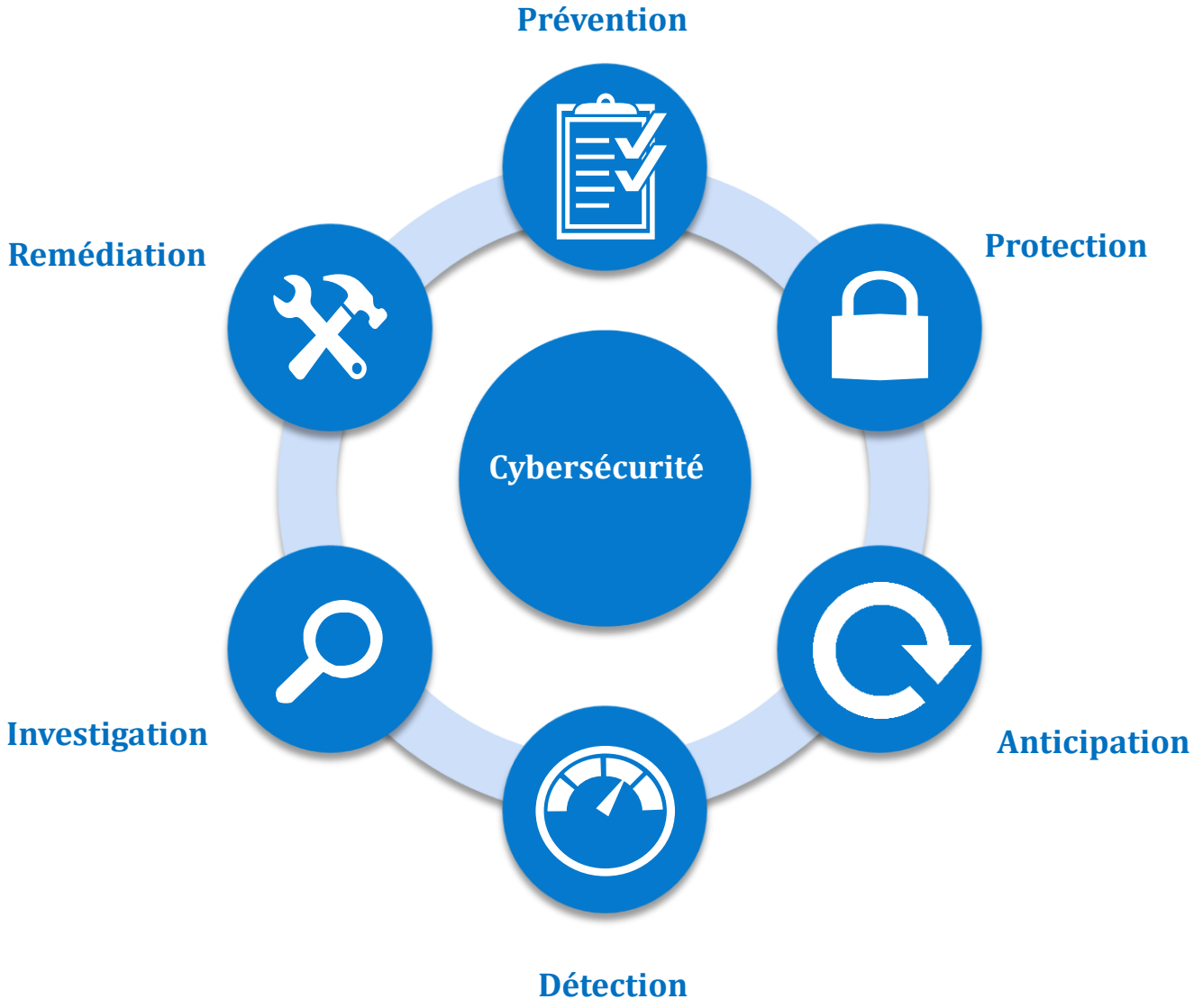


I. Contexte général

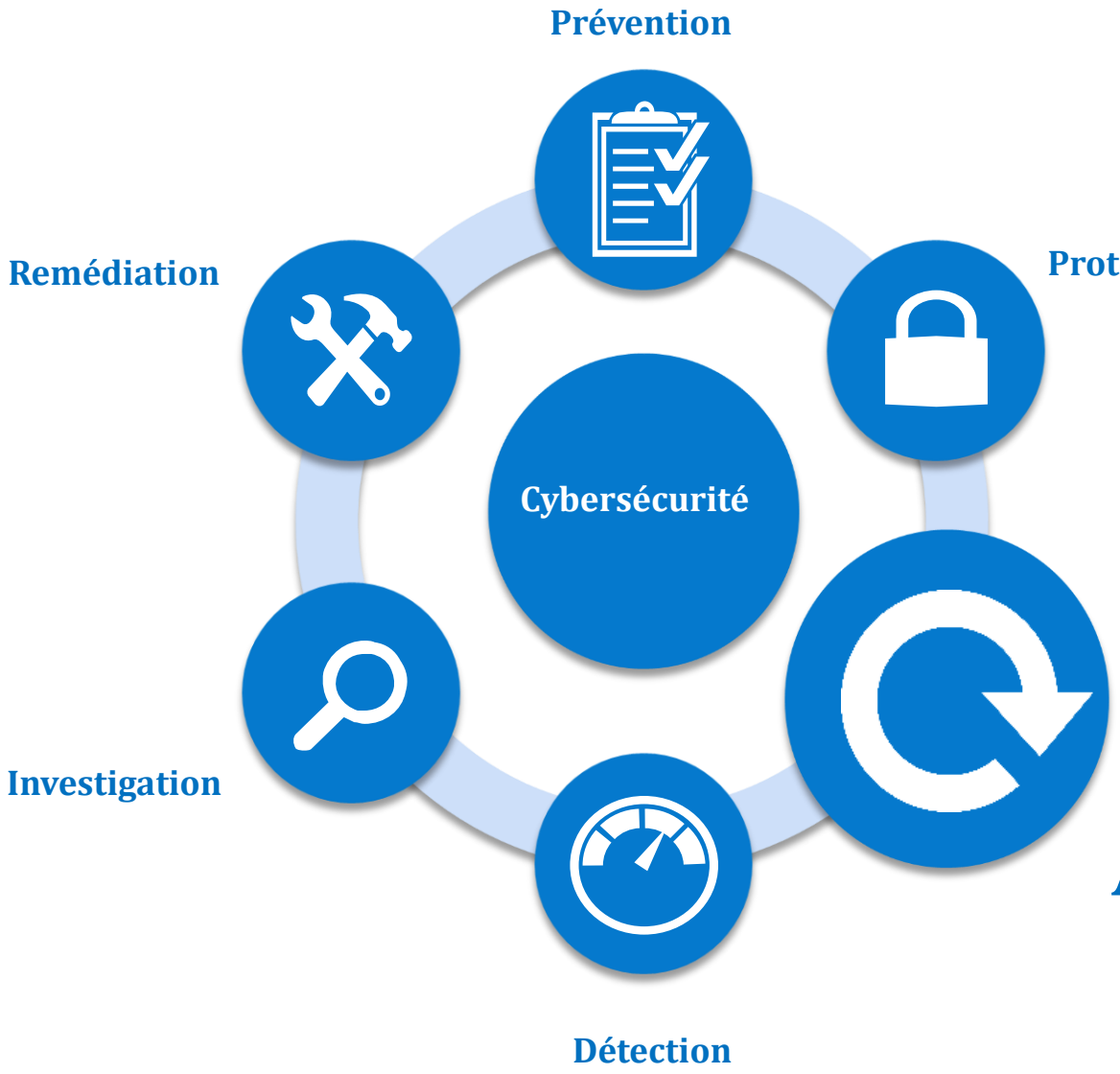
La Cybersécurité :



I. Contexte général

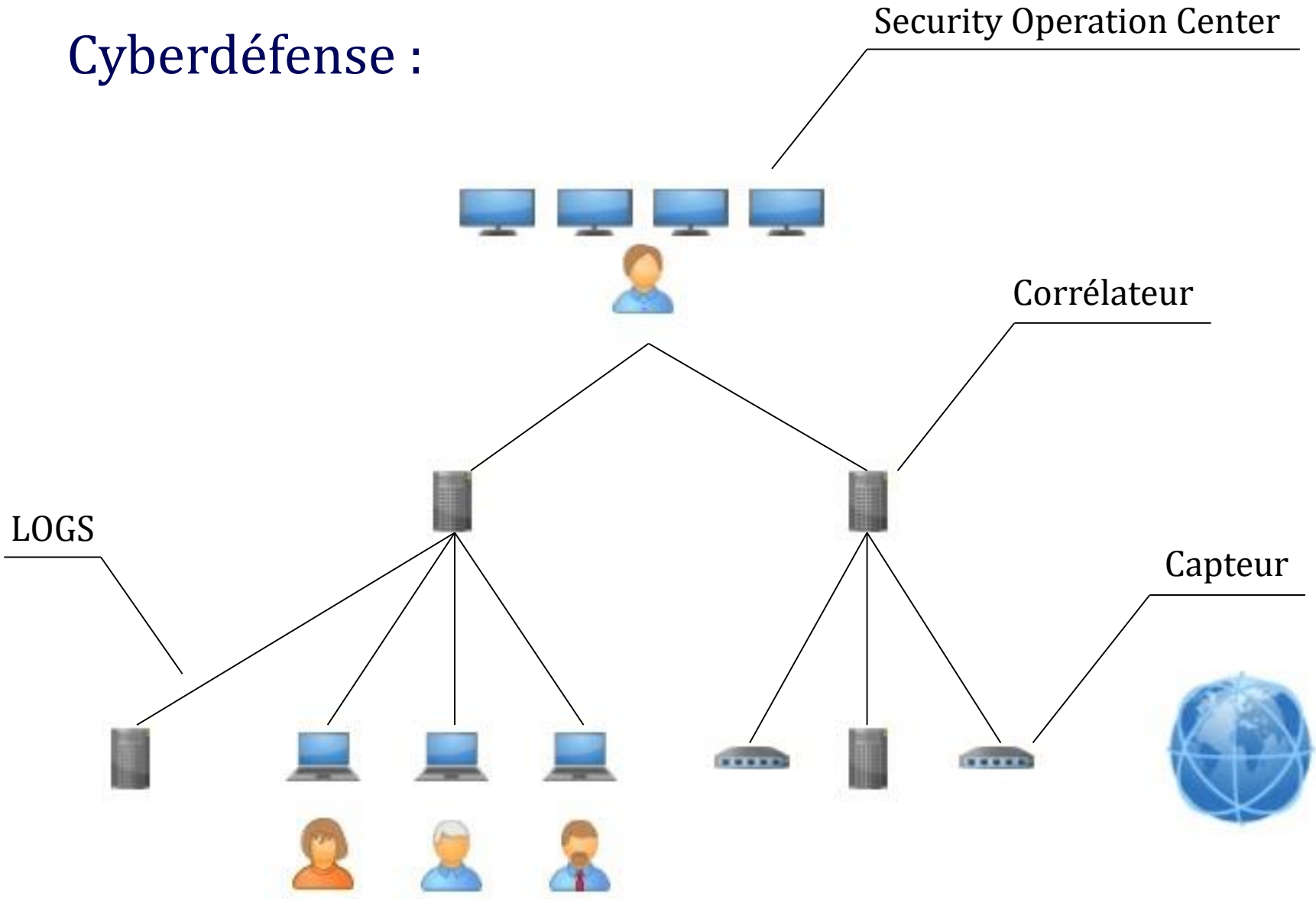


I. Contexte général



I. Contexte général

Cyberdéfense :



I. Contexte général

SOC (*Security Operation Center*) ou centre opérationnel de sécurité ou service de détection des incidents de sécurité (PDIS) :

Dispositif de supervision et d'administration de la sécurité des systèmes d'information permettant de détecter et d'analyser les menaces internes et externes et de répondre aux intrusions dans le SI.

I. Contexte général

Extrait du référentiel PDIS de l'ANSSI :

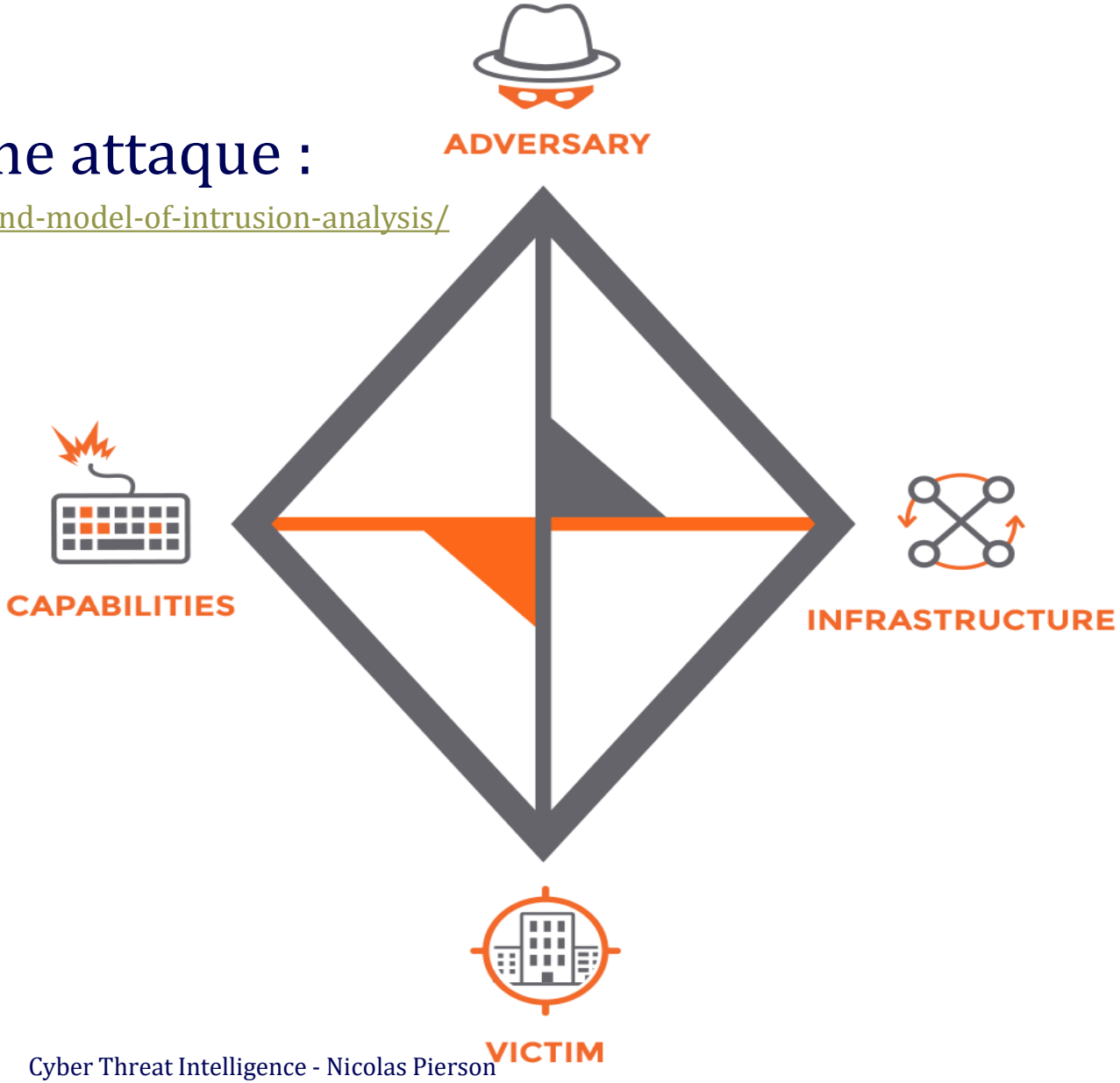
« Le prestataire doit créer des règles de détection en s'appuyant sur :

- ✓ la liste des incidents de sécurité redoutés du commanditaire ;
- ✓ **des bases de connaissances acquises auprès d'éditeurs et de sociétés spécialisées en sécurité des systèmes d'information ;**
- ✓ des bases de connaissances internes issues de l'expertise du prestataire :
    - veille et qualification de vulnérabilités, en priorité celles relatives à l'exécution de code arbitraire, localement ou à distance ;
    - veille et qualification de protocoles de contrôle commande ;
    - **veille sur les modes opératoires d'attaque et les codes malveillants .**
- ✓ les éléments de contexte spécifiques du commanditaire ;
- ✓ les règles provenant directement du commanditaire, évaluées au préalable par le prestataire (bon fonctionnement par rapport au comportement à détecter, impact sur les performances, correction des alertes, exploitabilité des alertes produites , etc.) ;
- ✓ **les incidents de sécurité détectés auprès des éventuels autres commanditaires.** »

I. Contexte général

Caractérisation d'une attaque :

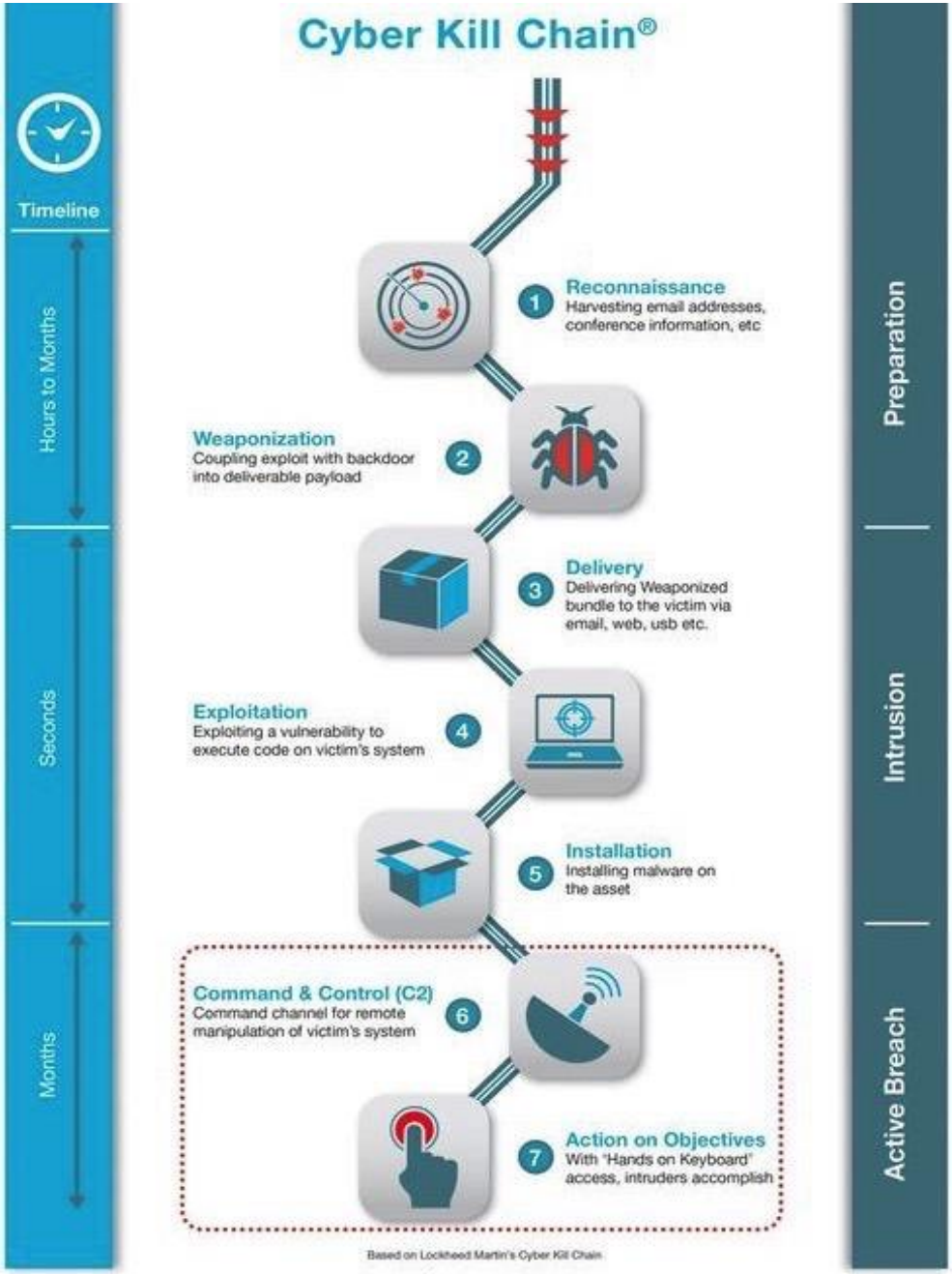
https://threatconnect.com/tag/diamond-model-of-intrusion-analysis/



I. Contexte général

Cyber Kill Chain :

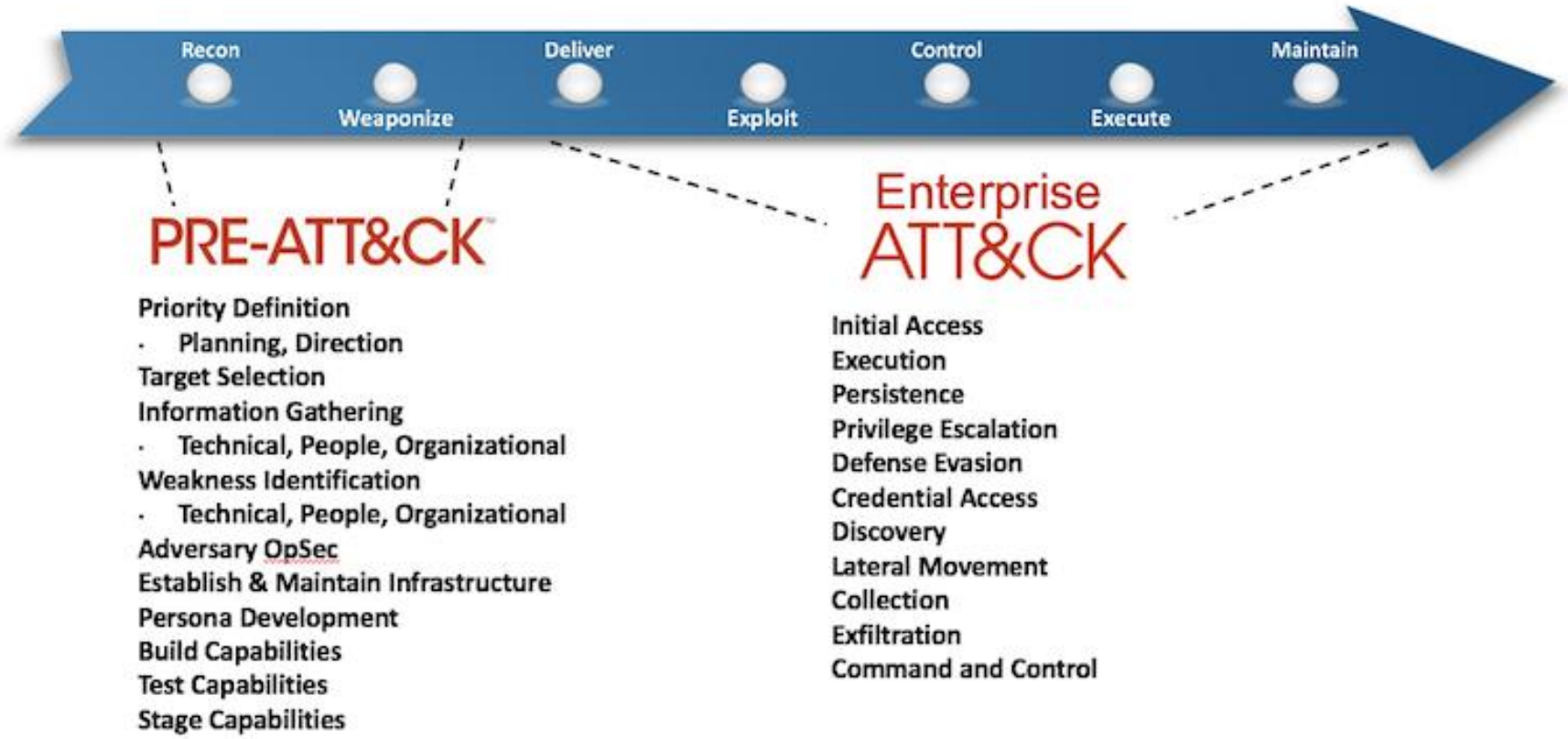
- ✓ Reconnaissance
- ✓ Préparation
- ✓ Livraison
- ✓ Exploitation
- ✓ Installation
- ✓ Contrôle
- ✓ Action



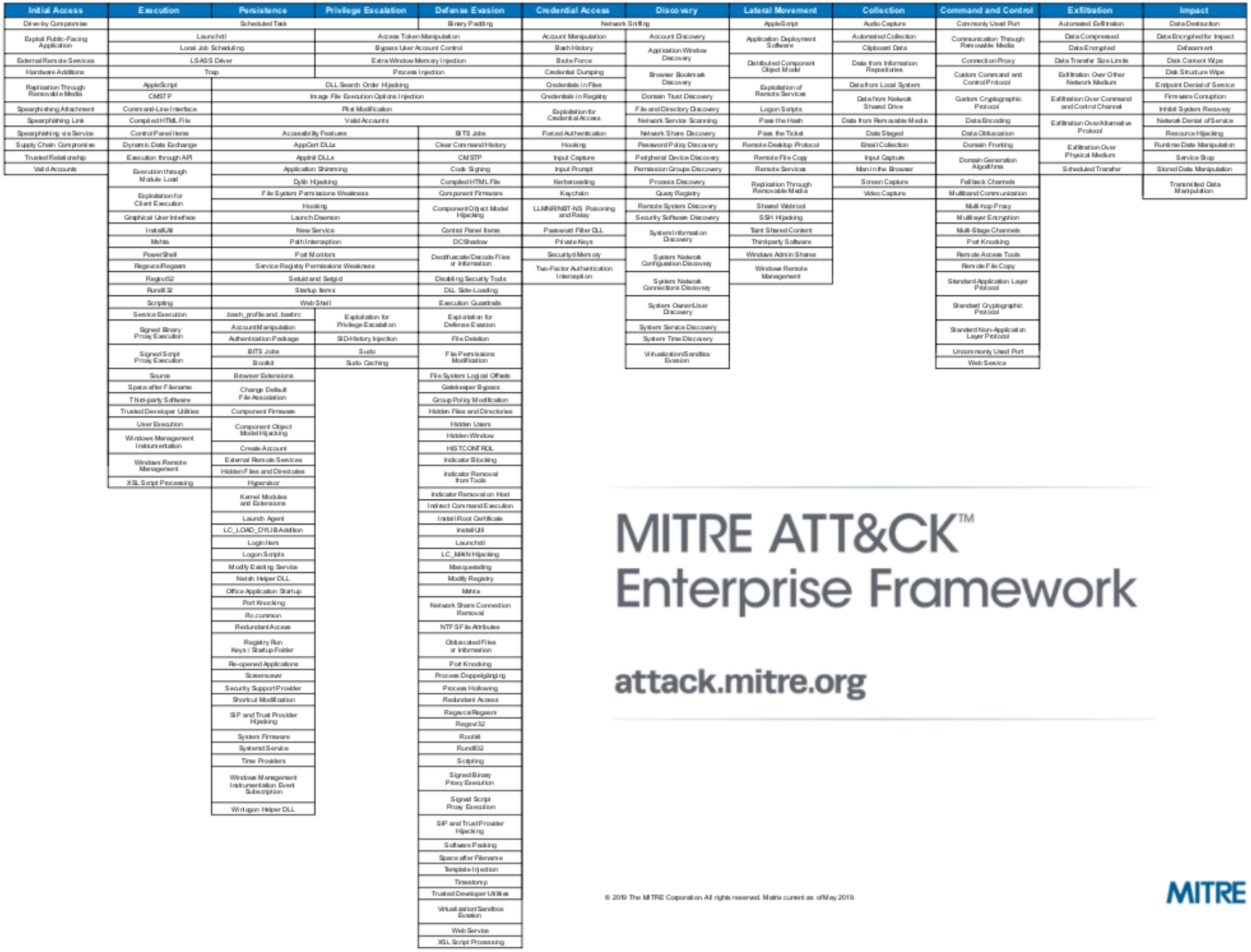
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

I. Contexte général

MITRE ATT&CK :



I. Contexte général

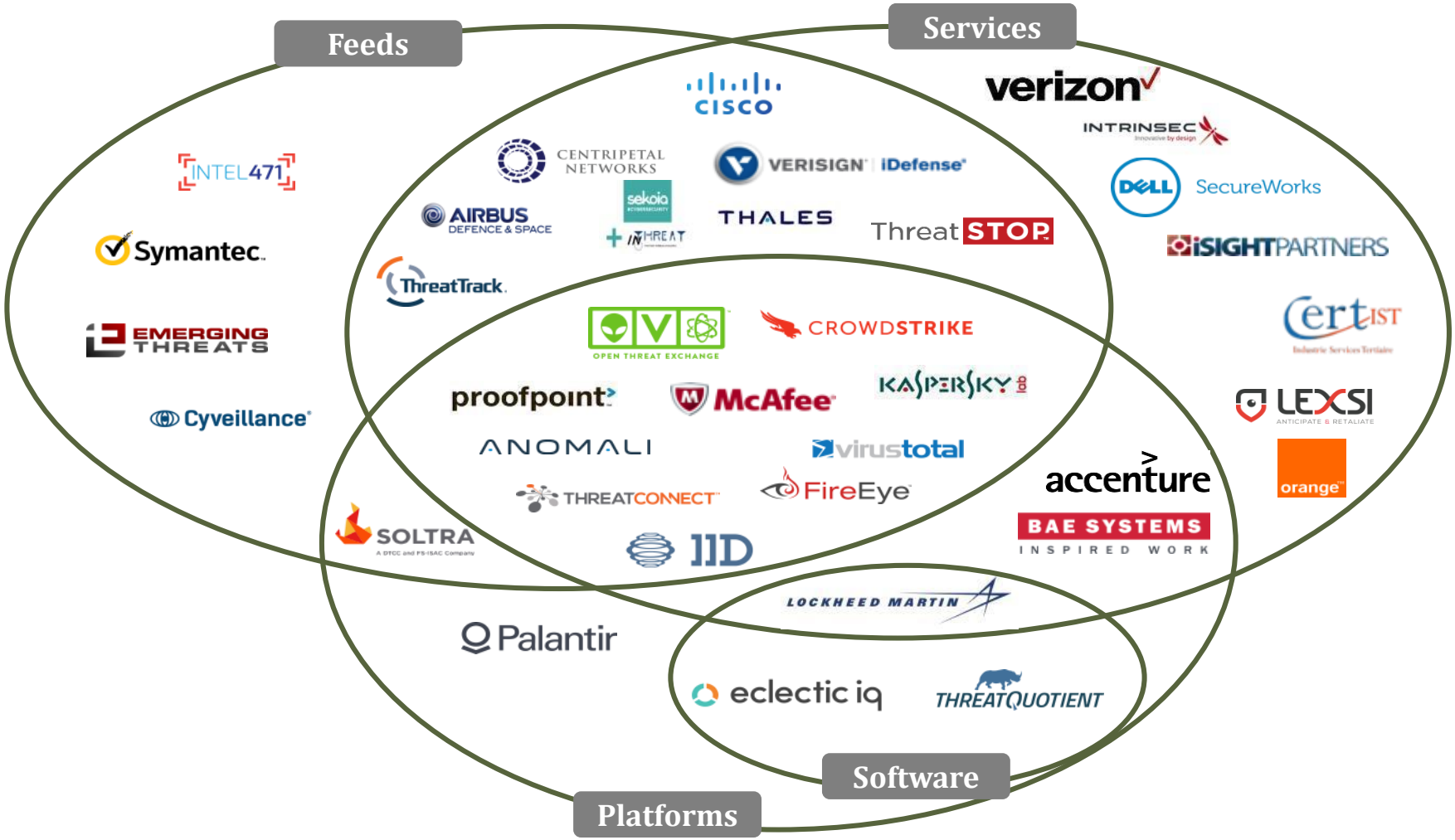


I. Contexte général

STIX : Structured Threat Information eXpression (MITRE)

Object	Name	Description
	Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
	Course of Action	An action taken to either prevent an attack or respond to an attack.
	Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
	Malware	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
	Observed Data	Conveys information observed on a system or network (e.g., an IP address).
	Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
	Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
	Tool	Legitimate software that can be used by threat actors to perform attacks.
	Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.

I. Contexte général



I. Contexte général

Définition :

Indicateur de compromission (IOC) : informations structurées sur les indices d'activité malveillante

Pas de format unique mais plusieurs types de données structurées :

- ✓ IOC
- ✓ STIX
- ✓ JSON
- ✓ CSV

Signatures :
- ✓ Yara
- ✓ Bro
- ✓ Snort
- ✓ Suricata

Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Perspectives

II. Cyber Threat Intelligence

Quoi ?

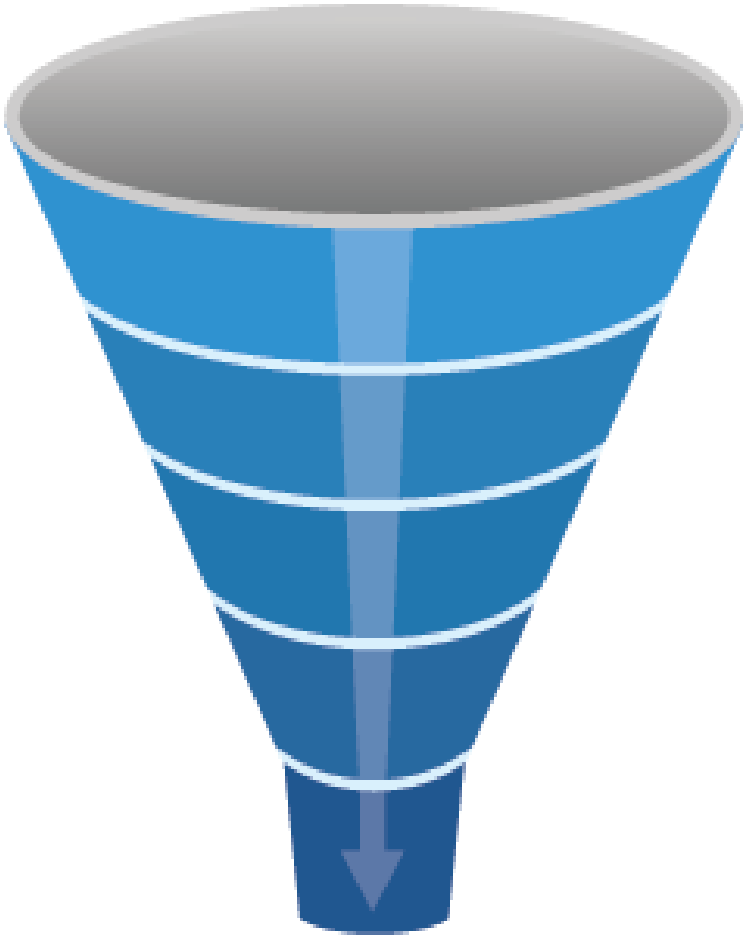
Définition de la Threat Intelligence :

Ensemble des informations et des actions issues de la collecte et de l'analyse des menaces en provenance du cyberespace.

L'objectif de la Threat Intelligence est de connaitre les menaces pour s'en défendre efficacement.

II. Cyber Threat Intelligence

Réduire le bruit et produire des données utiles, « *actionable* »



Noise is comprised of everything that is collected according to the Priority Intelligence Requirements (PIR).

Data remains after noise is filtered and non-applicable items are removed (scrubbed). Remaining artifacts are grouped according to defining characteristics.

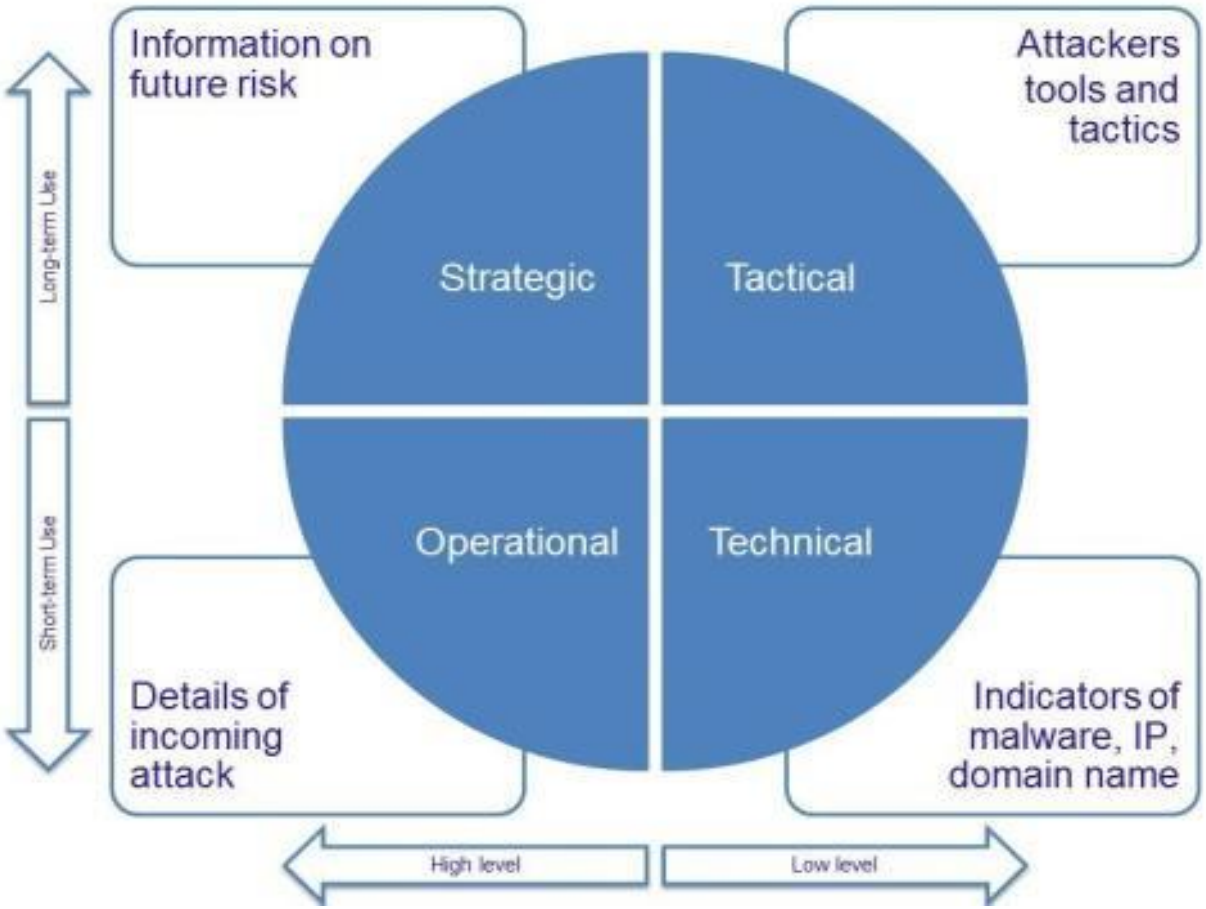
Information is data with a purpose. Once it is assigned a purpose it becomes information.

Intelligence is information with a strategic purpose that can be used to gain an advantage. Intelligence development is exclusively a human centered activity.

Actionable Intelligence is intelligence-led, evidence-based assessments which can be initiated, acted upon and provide clear results, supporting the PIR.

II. Cyber Threat Intelligence

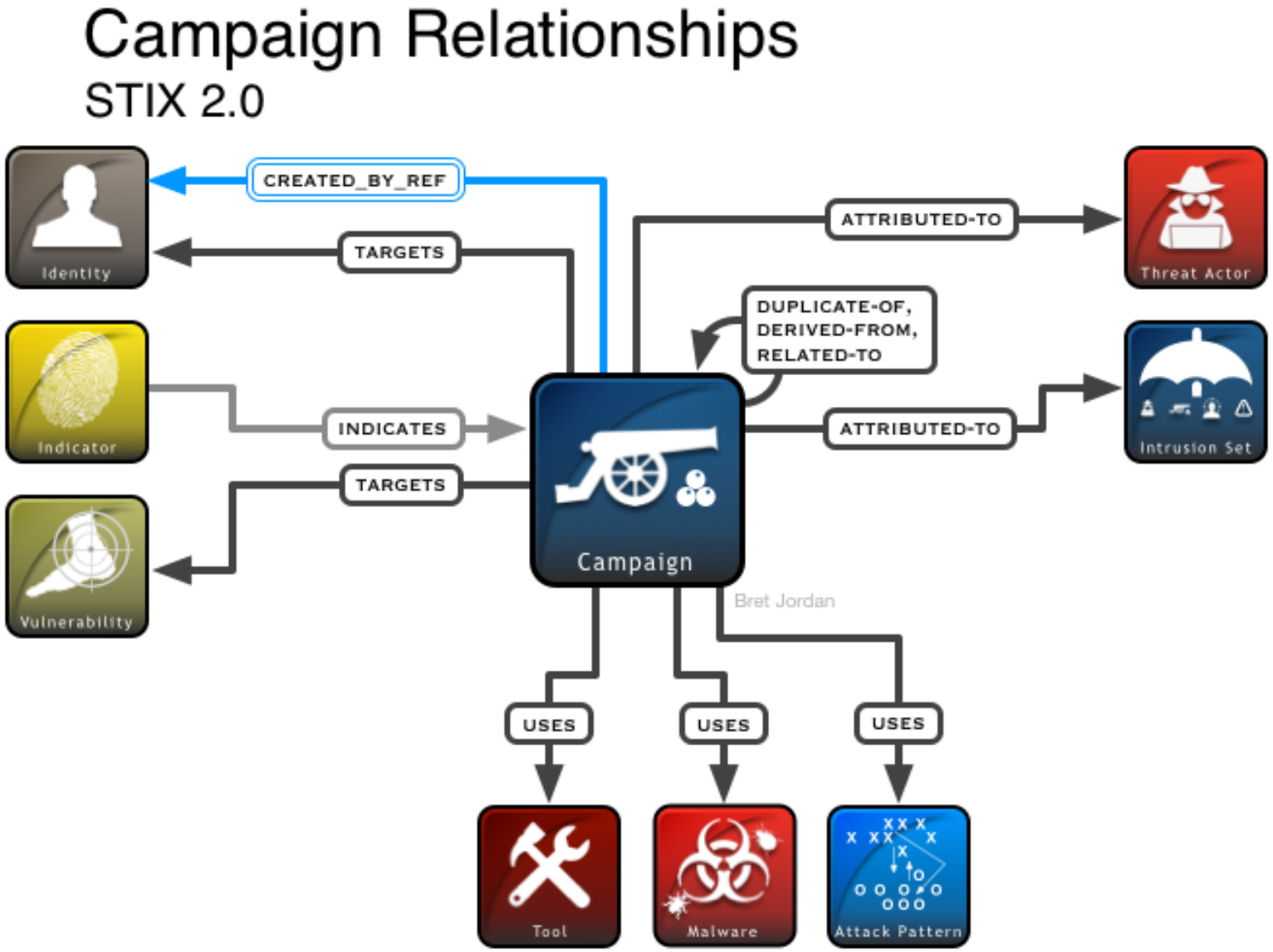
Quatre niveaux :



II. Cyber Threat Intelligence

Technique	  
Tactique	  
Opérationnelle	  
Stratégique	

II. Cyber Threat Intelligence

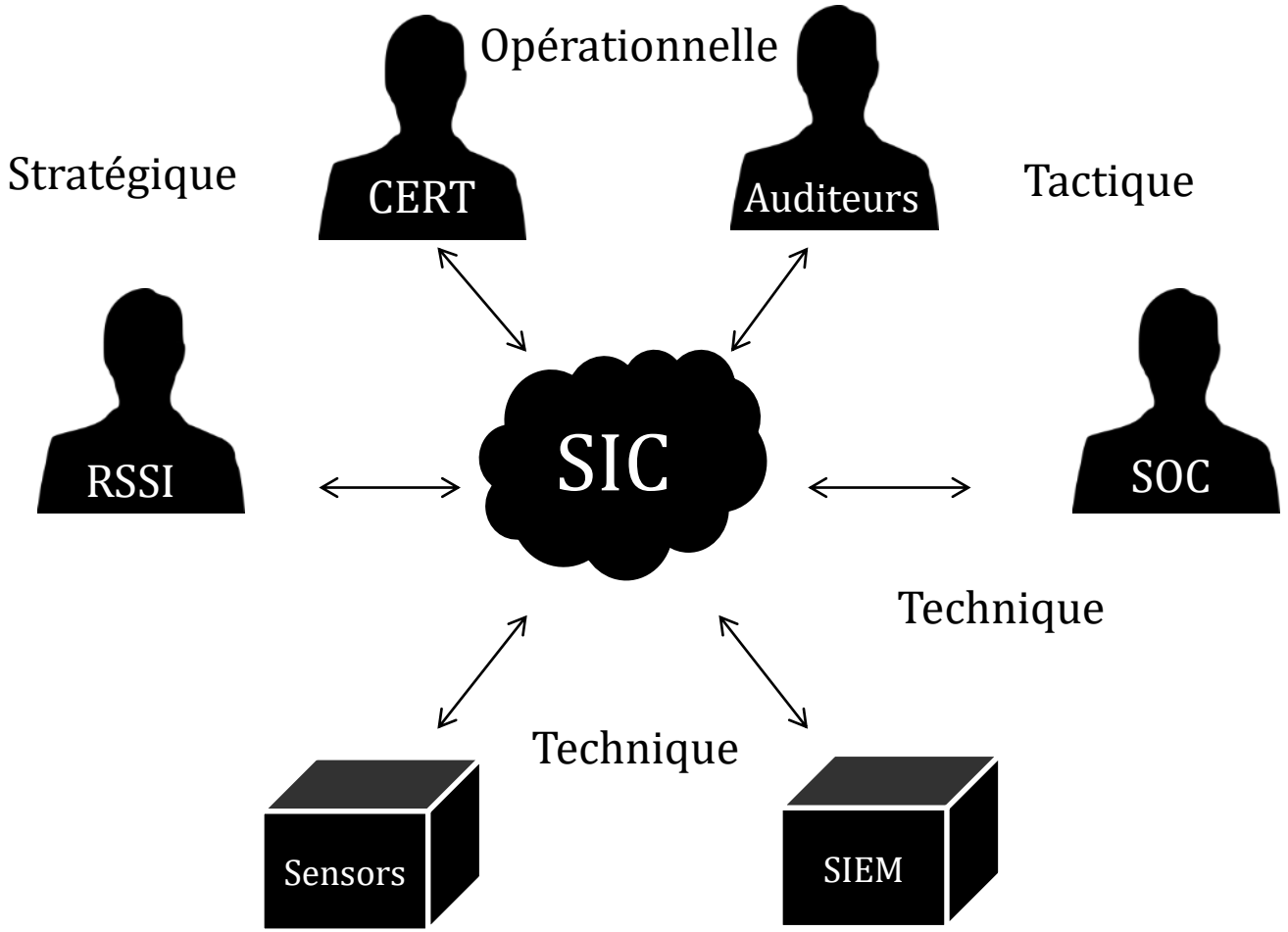


II. Cyber Threat Intelligence

SIC: Security Intelligence Center

Pour qui ?

Des destinataires multiples :



II. Cyber Threat Intelligence

Un écosystème :

II. Cyber Threat Intelligence

Pourquoi ?

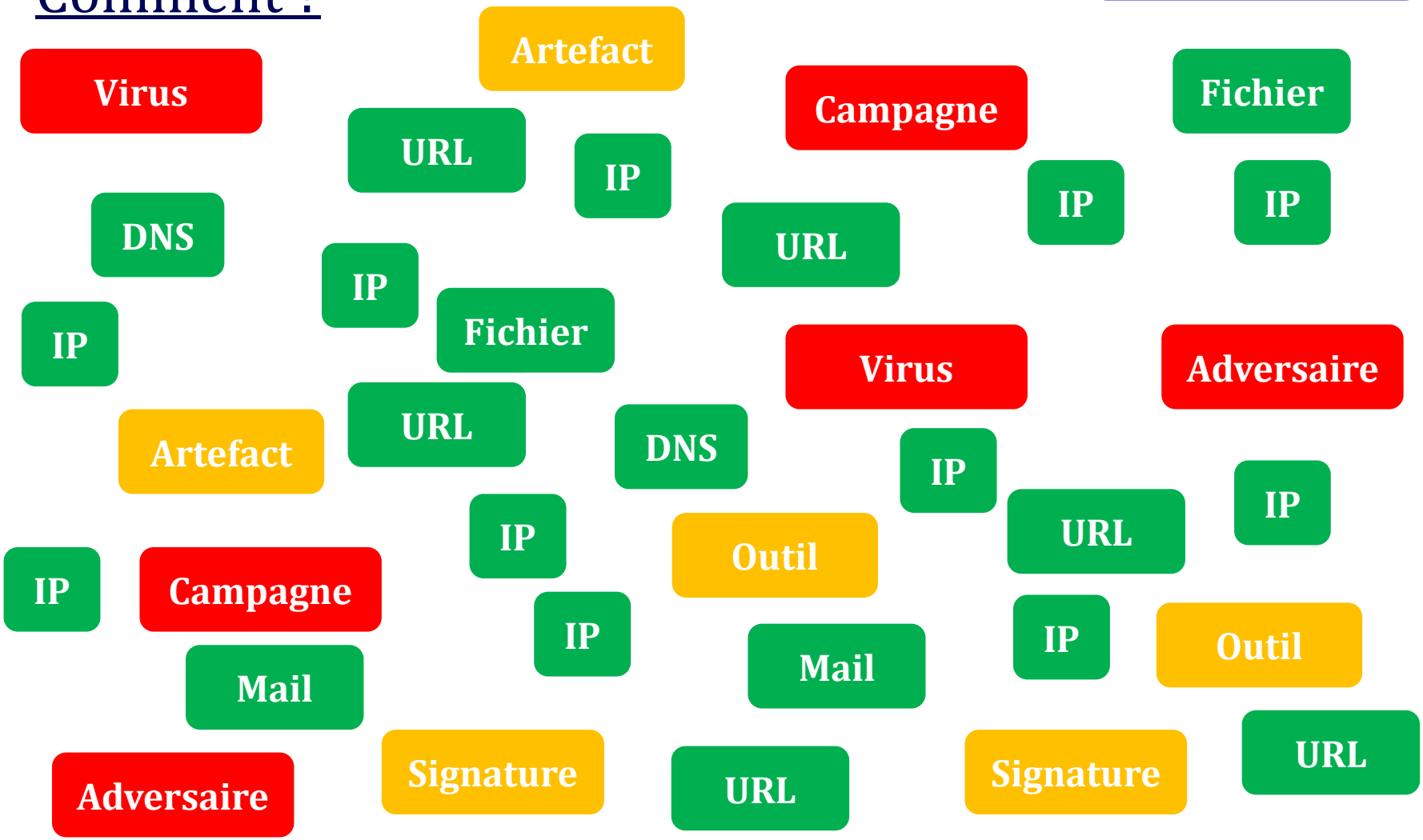
Utilisation de la CTI Technique :

- ✓Blocage en temps réel (*Firewall*, IPS)
- ✓Détection (IDS, Sonde, SOC)
- ✓Recherche *a posteriori* (« *Hunting* »)

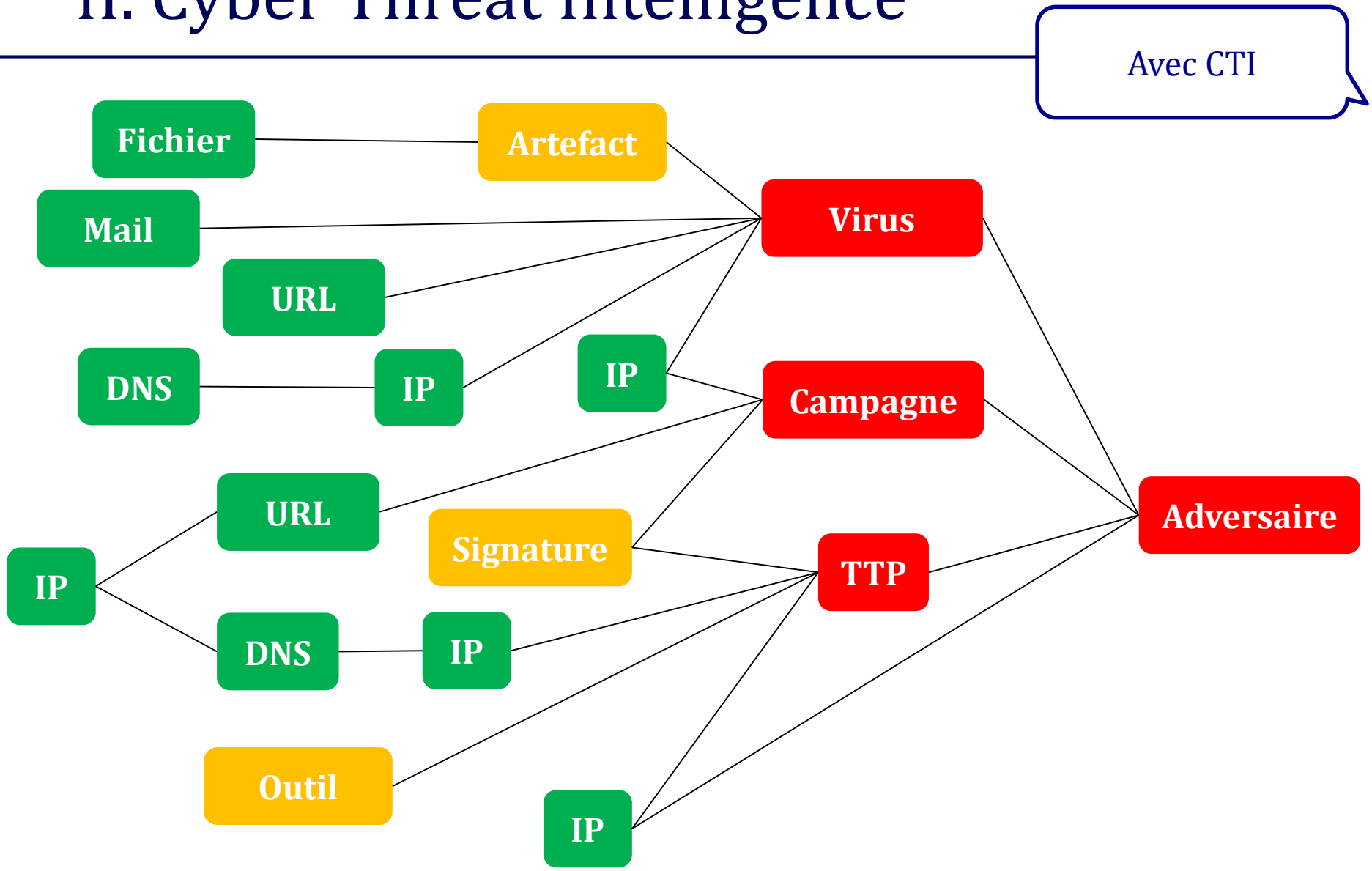
II. Cyber Threat Intelligence

Sans CTI

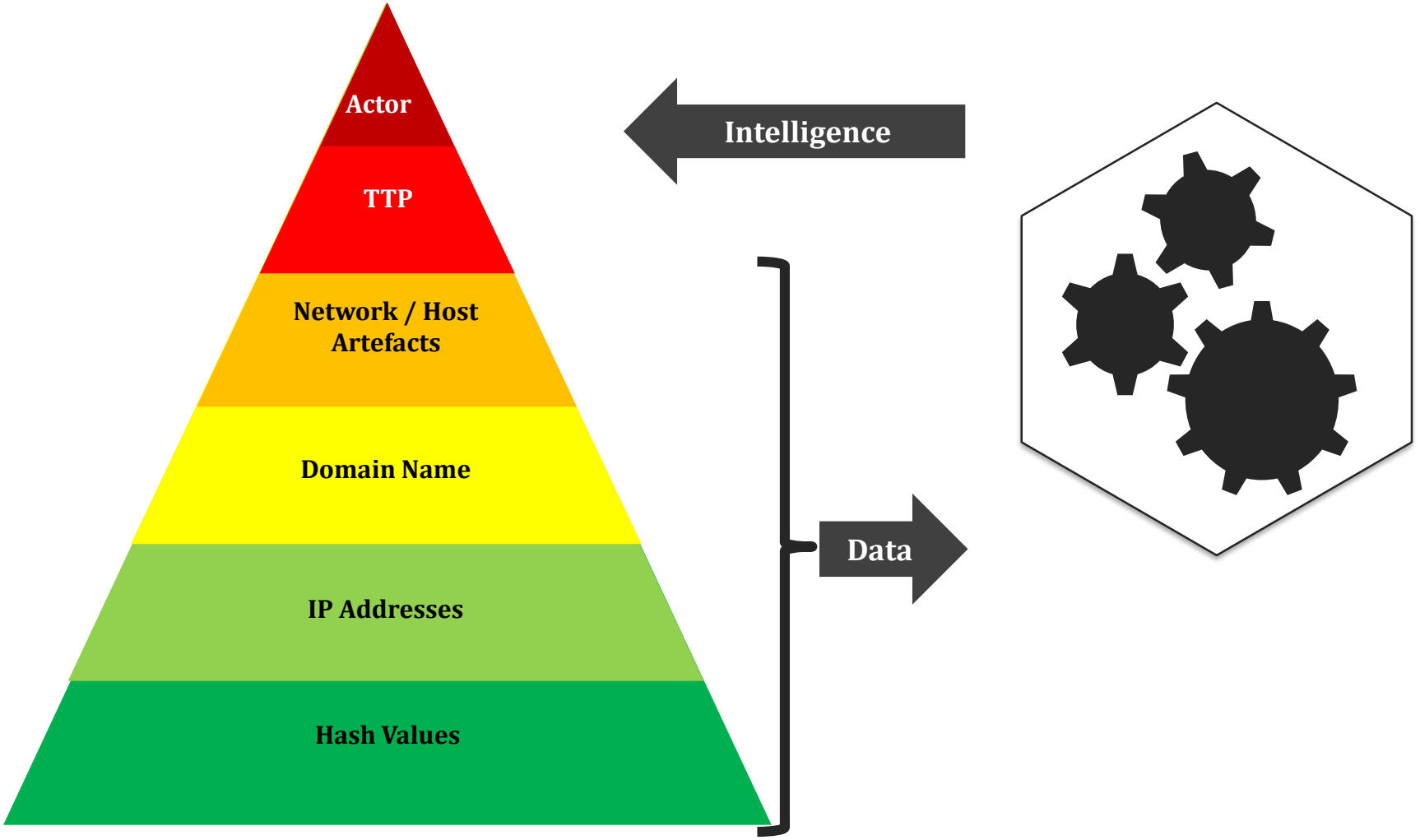
Comment ?



II. Cyber Threat Intelligence

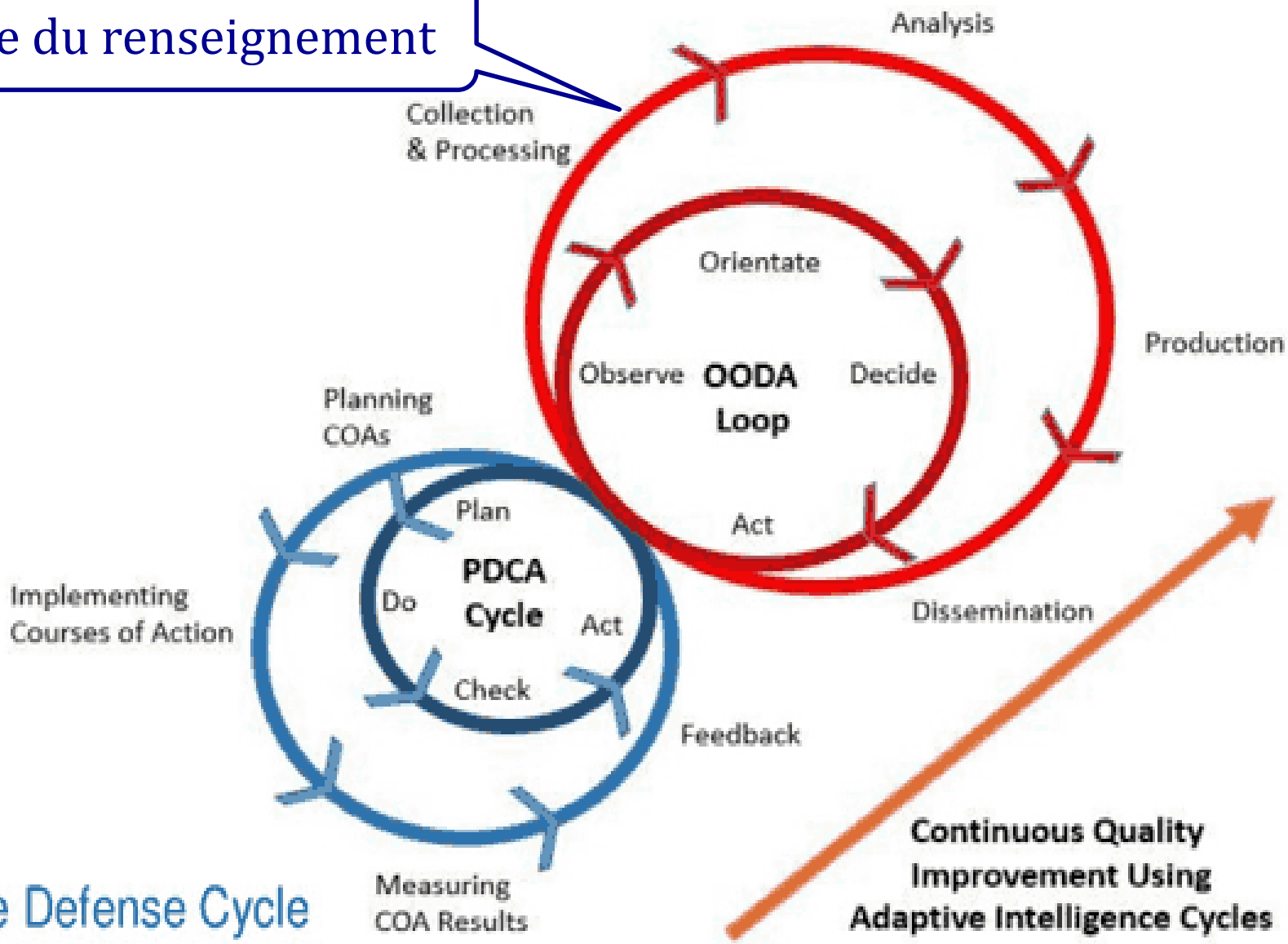


II. Cyber Threat Intelligence



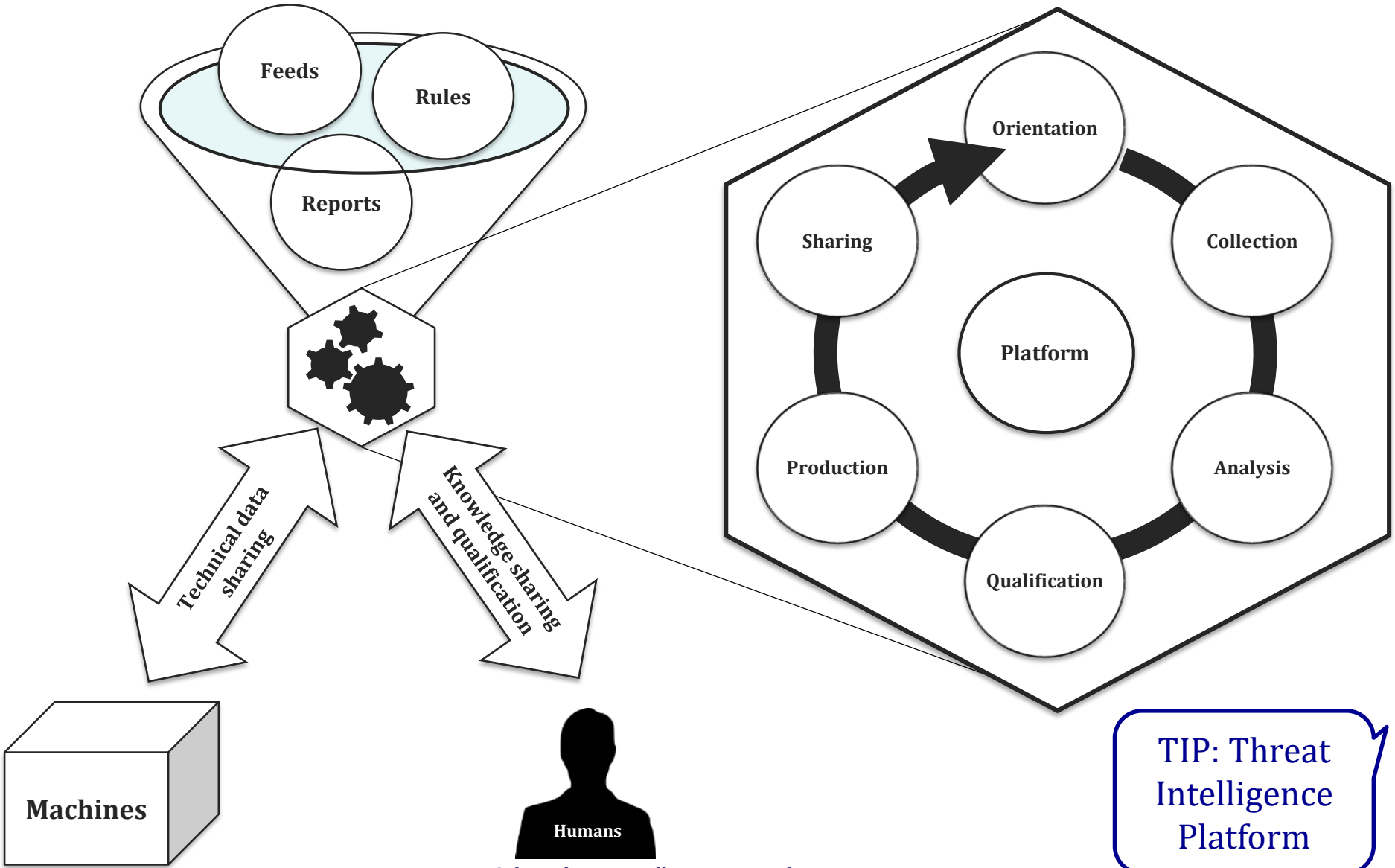
II. Cyber Threat Intelligence

Cycle du renseignement



Active Defense Cycle

II. Cyber Threat Intelligence



TIP: Threat Intelligence Platform

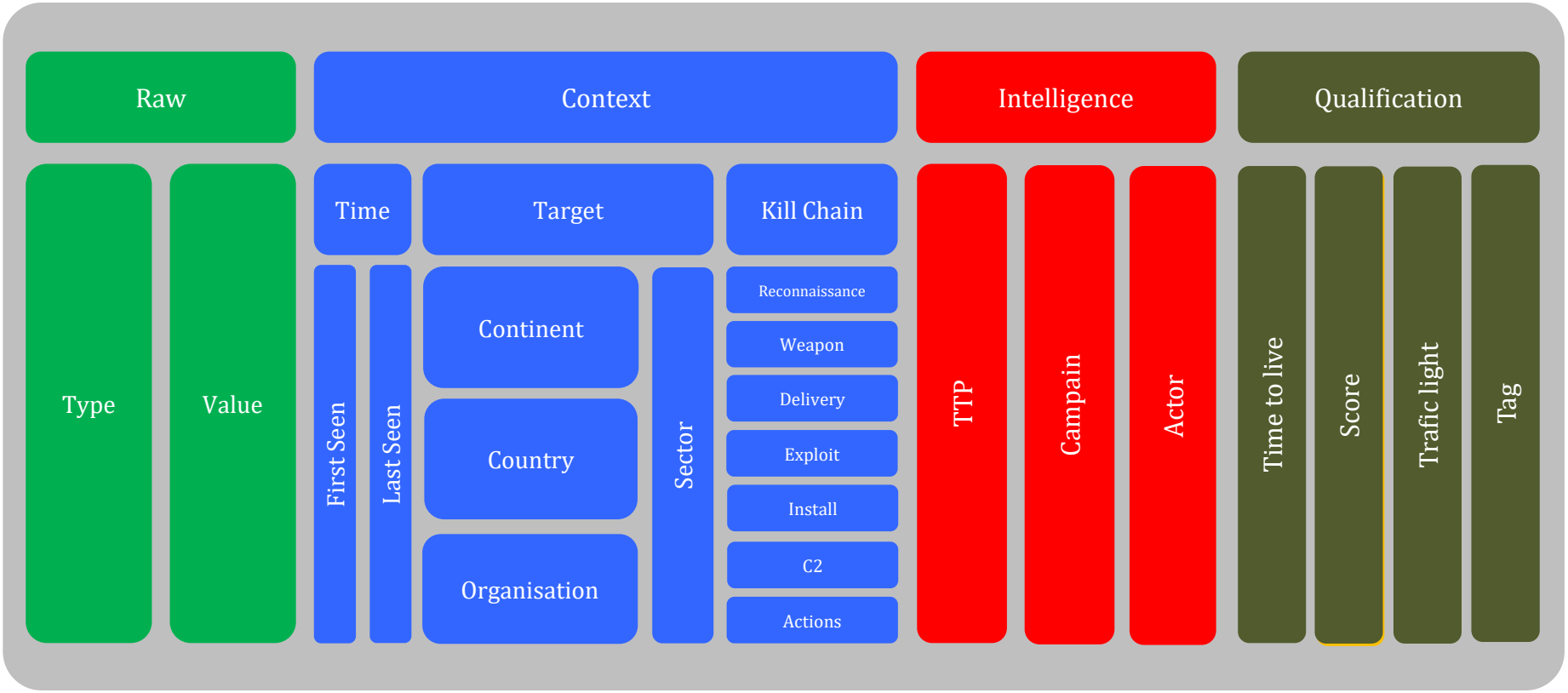
II. Cyber Threat Intelligence

Fonctions d'une plateforme de Threat Intelligence :

- ✓ Collecter un grand nombre de données automatiquement et manuellement
- ✓ Fournir un espace de travail aux analystes
- ✓ Fournir des outils de visualisation et de mise en relation
- ✓ Permettre la qualification des données et leur gestion dans le temps
- ✓ Enrichir les données
- ✓ Permettre le partage et le travail collaboratif

II. Cyber Threat Intelligence

Modèle de données :



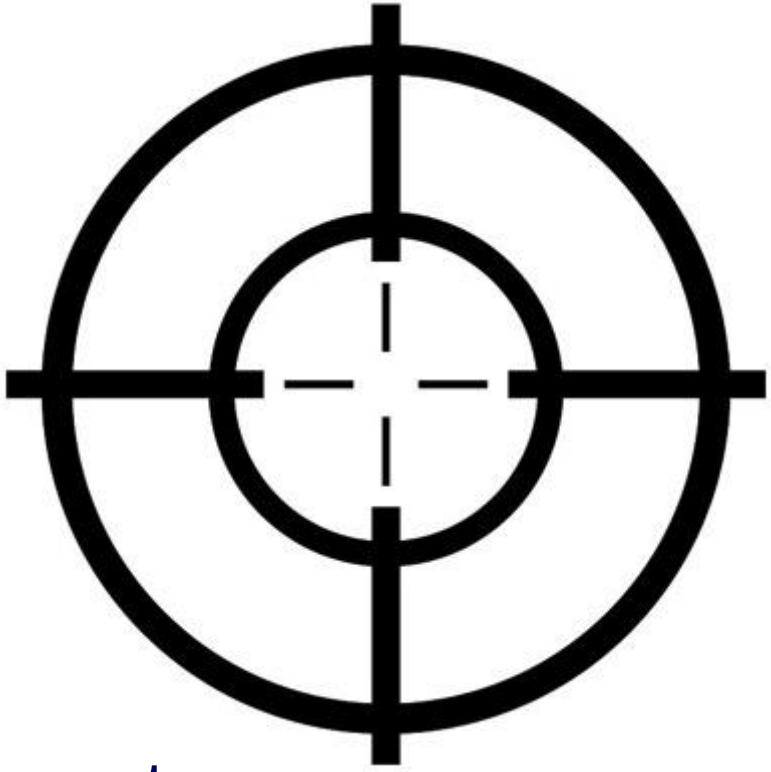
Base de travail

II. Cyber Threat Intelligence

La collecte et l'analyse se font en fonction de :

- ✓ Type d'acteur
- ✓ Secteur d'activité
- ✓ Contexte géopolitique
- ✓ Situation économique
- ✓ Zone géographique
- ✓ Type de menaces
- ✓ Historique
- ✓ Renommée des sources
- ✓ Coûts
- ✓ …

Orientation



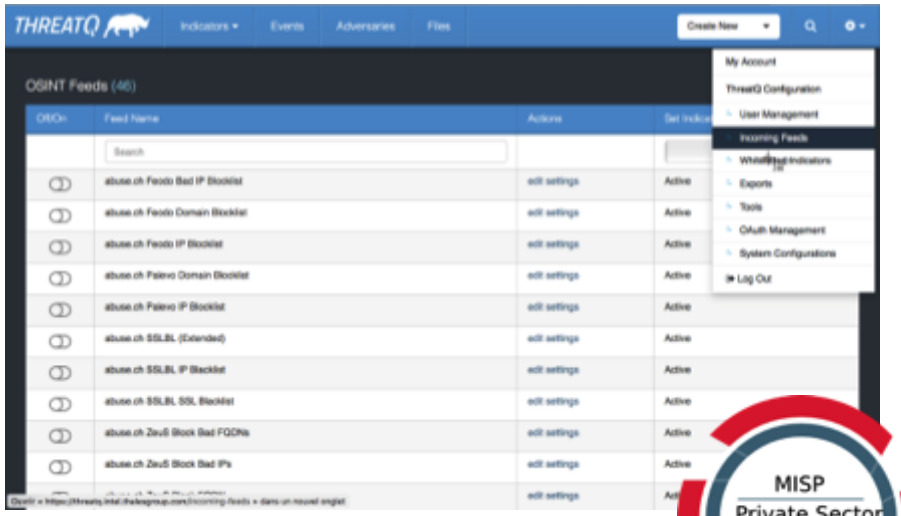
PIR : Priority Intelligence Requirements

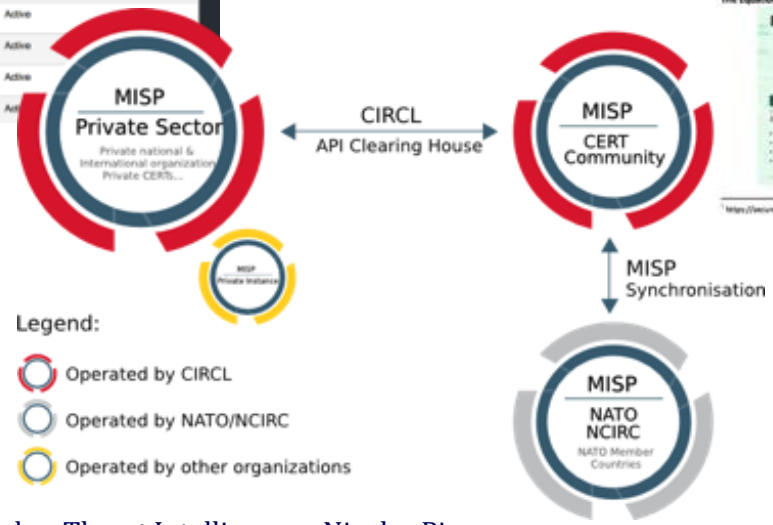
II. Cyber Threat Intelligence

Collecte

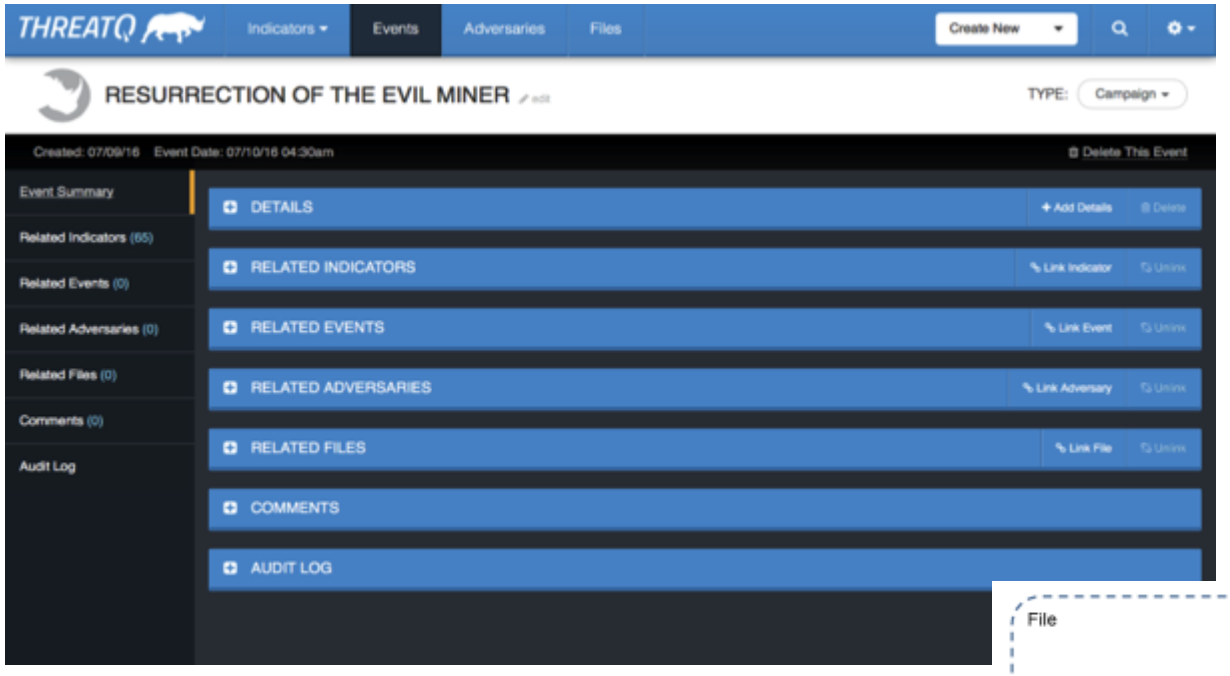
Automatique
(Feeds, rapports, connecteurs)

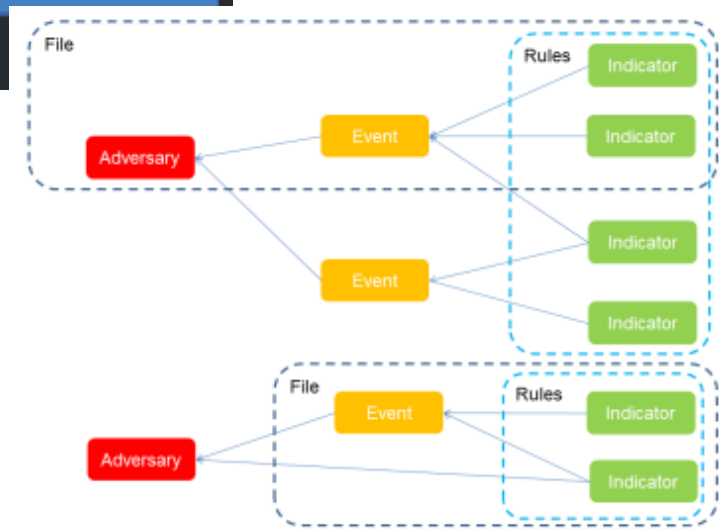
Manuelle
(rapport incident, mail, pdf, doc, csv…)





II. Cyber Threat Intelligence

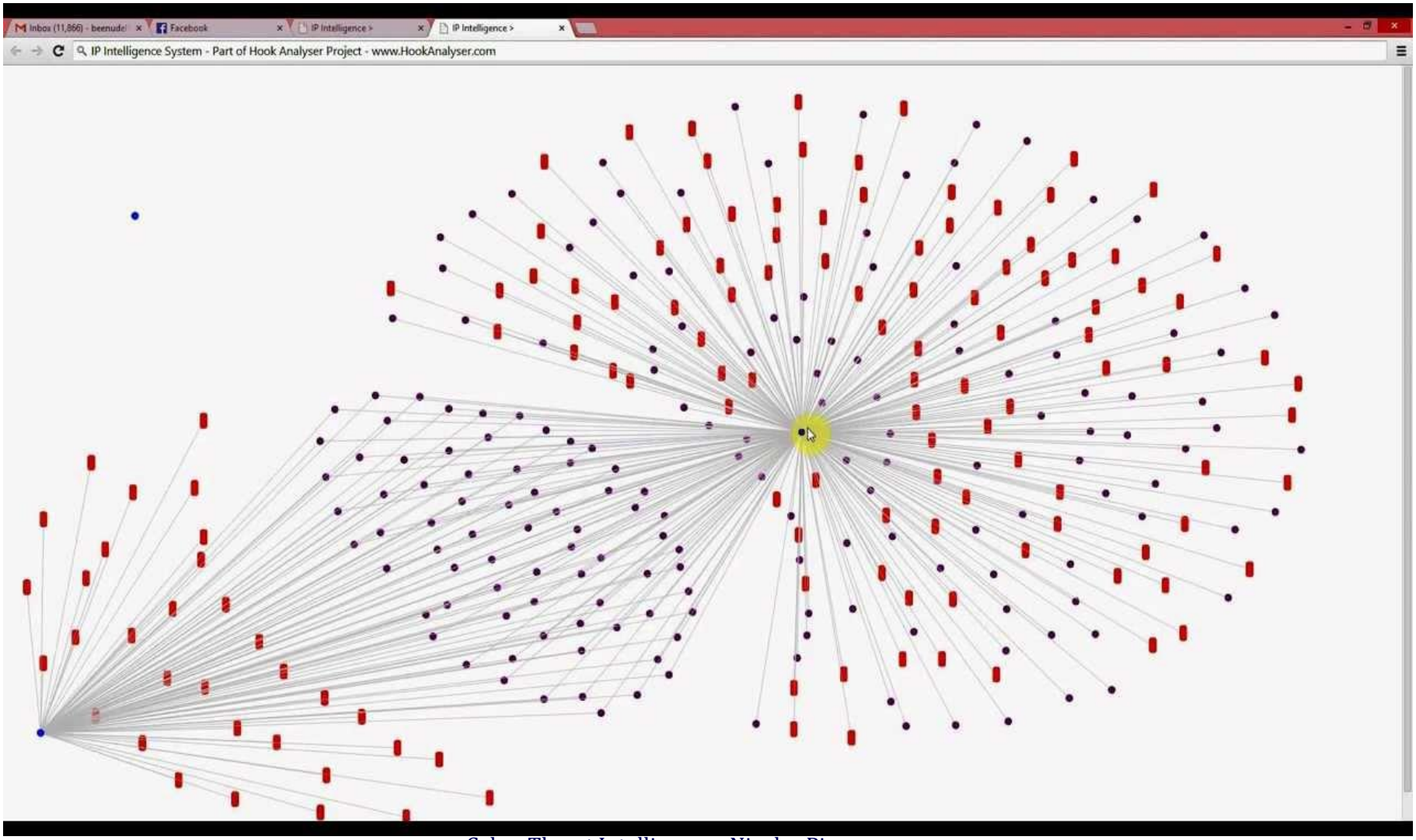




Analyse

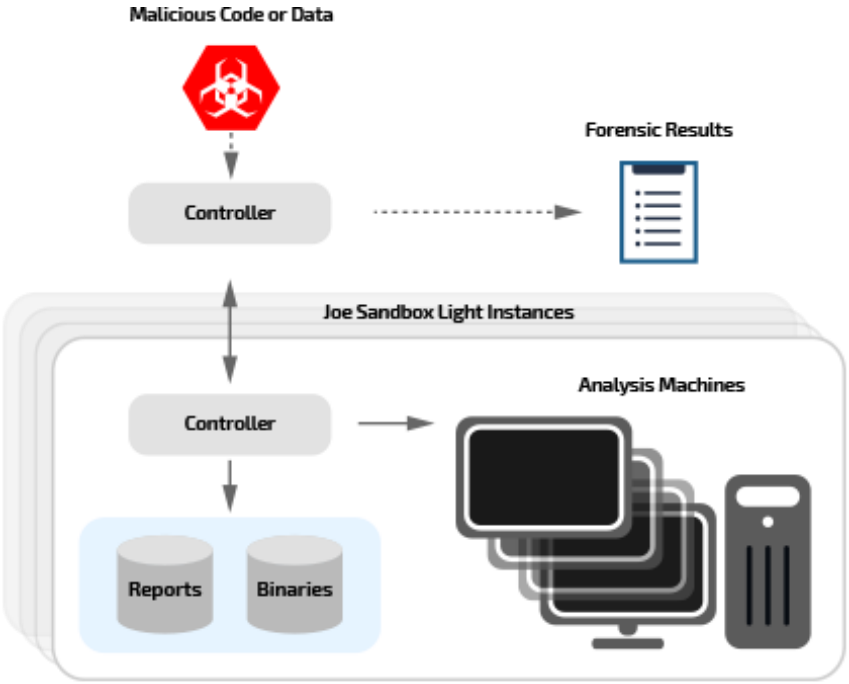
II. Cyber Threat Intelligence

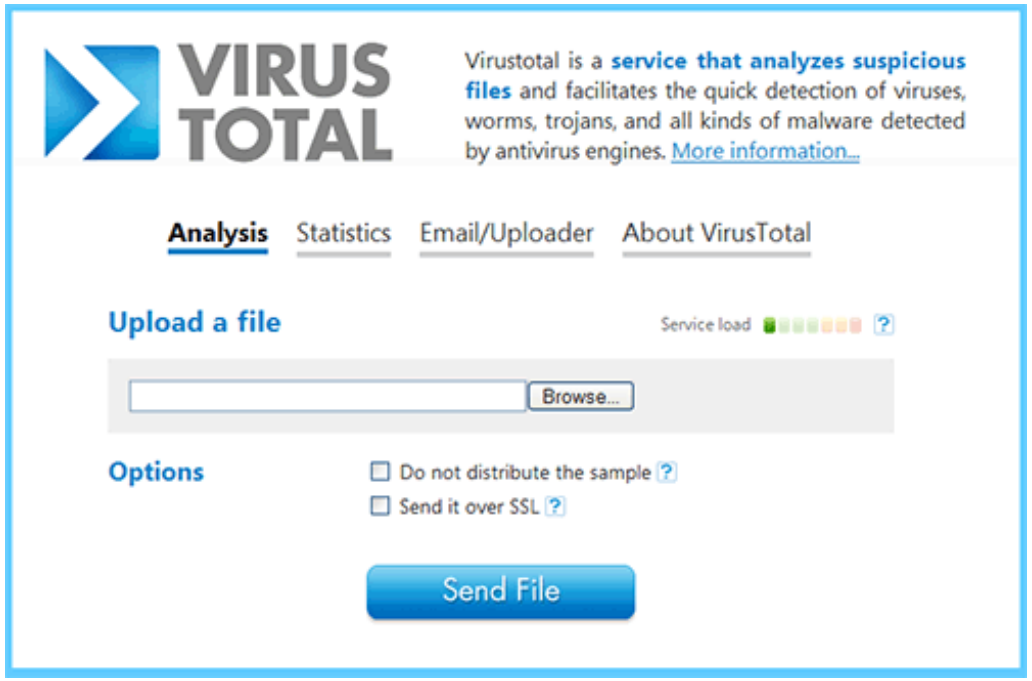
Analyse



II. Cyber Threat Intelligence

- ✓ Analyse complémentaire
- ✓ Sandboxing
- ✓ Incubation
- ✓ Honey pot





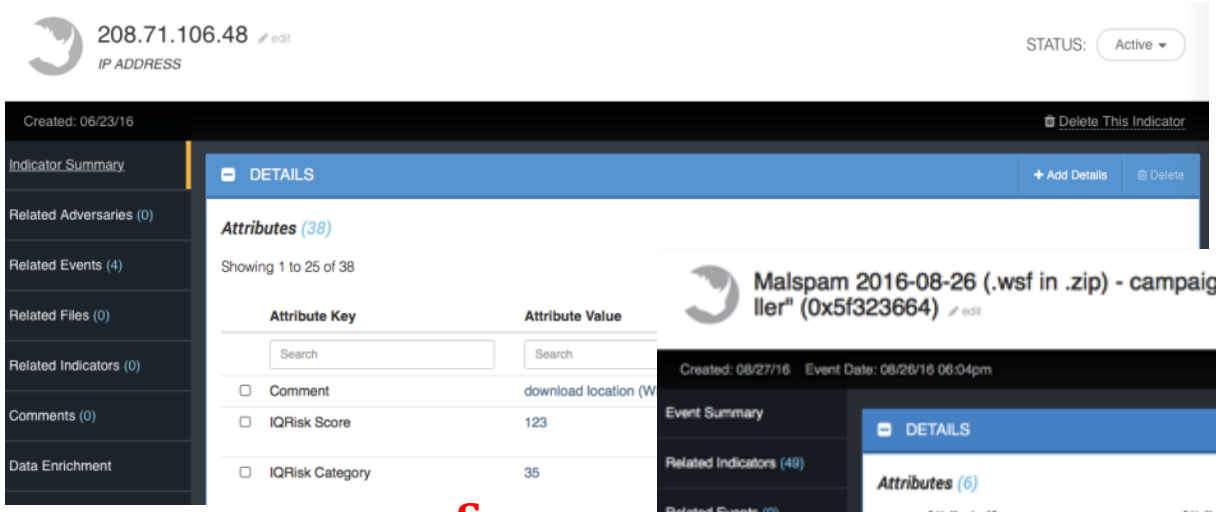
Analyse

II. Cyber Threat Intelligence

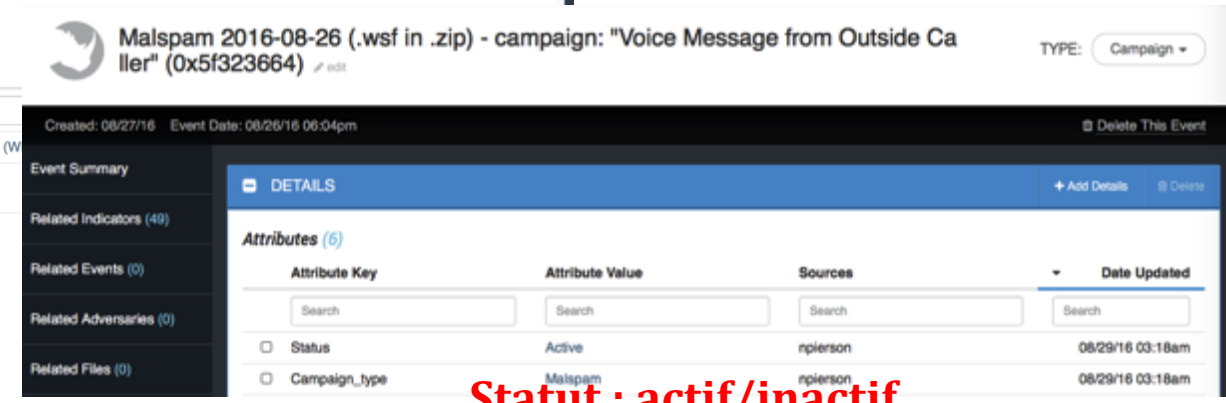
Qualifier pour :

- ✓ Traiter les menaces récentes et à risque
- ✓ Gérer les indicateurs et les campagnes dans le temps (TTL)
- ✓ In fine, s'adapter aux performances des capteurs (IDS, FW) et réduire les faux positifs

Qualification



Score

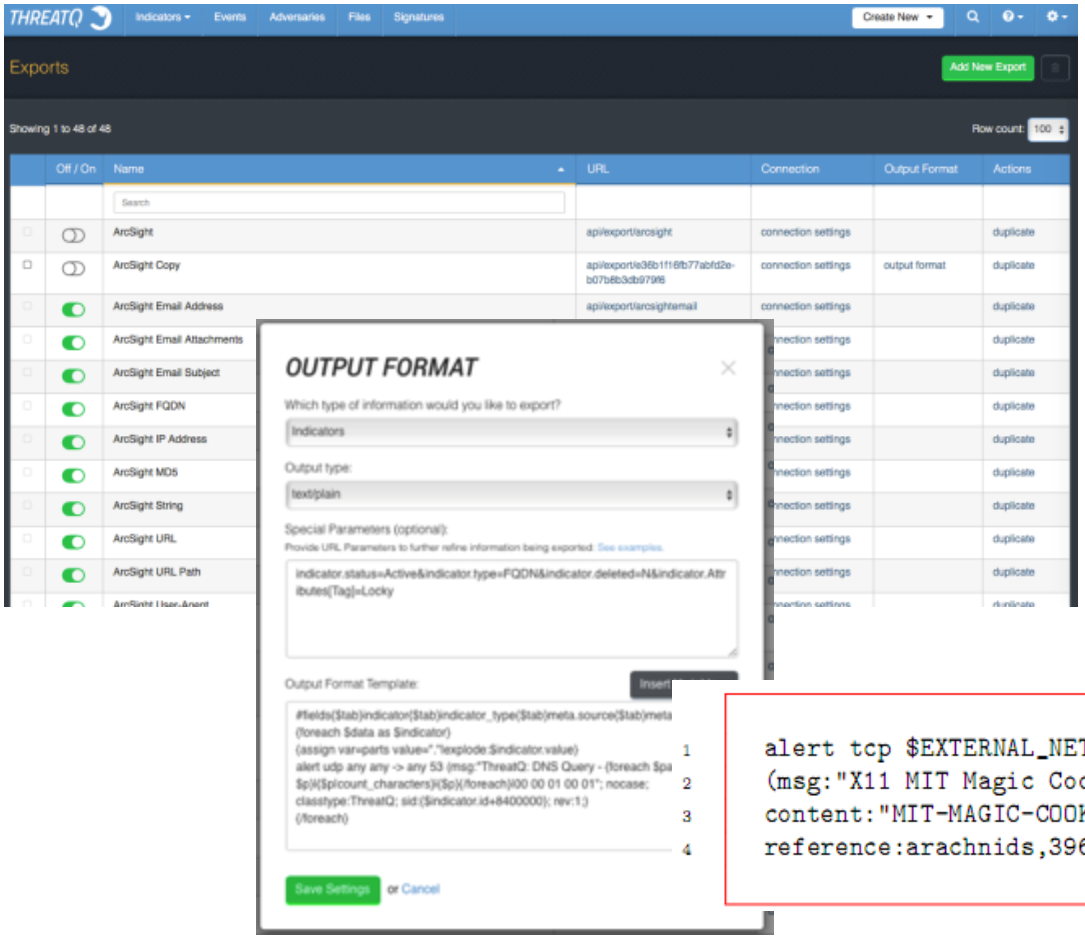


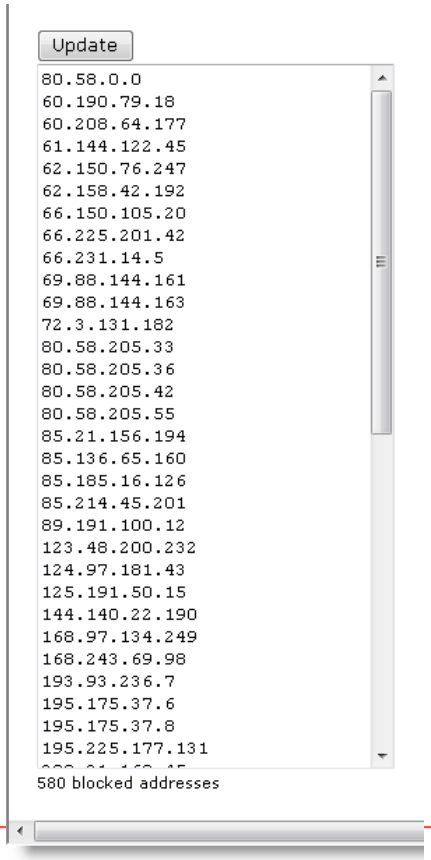
Statut : actif/inactif

II. Cyber Threat Intelligence

Production

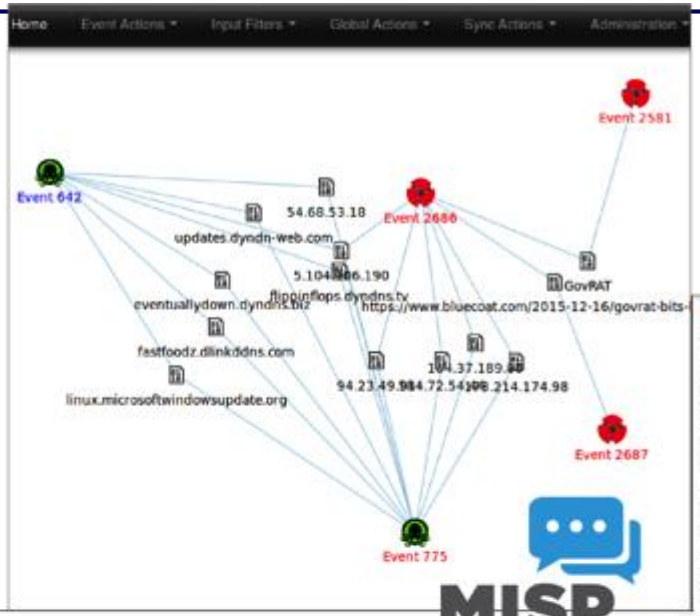
Création de listes, de règles, de notifications et de rapports.






```
alert tcp $EXTERNAL_NET any -> $HOME_NET 6000
(msg:"X11 MIT Magic Cookie detected"; flow:established;
content:"MIT-MAGIC-COOKIE-1";
reference:arachnids,396; classtype:attempted-user; sid:1225; rev:4;)
```

II. Cyber Threat Intelligence



Id	Exportable	Name	Taxonomy	Tagged events	Actions
6	✖	APT		31	
7	✖	Actionable:NO		5	
3	✖	TLP:AMBER	tlp	131	
8	✖	TLP:EX:CHR	tlp	11	
5	✖	TLP:GREEN	tlp	550	
4	✖	TLP:RED	tlp	3	
2	✖	TLP:WHITE	tlp	531	
10	✖	TO:HIDE		2	
9	✖	TODO		9	
11	✖	TODO:VT-ENRICHMENT		8	
1	✖	Type:OSINT		832	
18	✔	admiralty-scale:information-credibility="1"	admiralty-scale	0	
19	✔	admiralty-scale:information-credibility="2"	admiralty-scale	0	
20	✔	admiralty-scale:information-credibility="3"	admiralty-scale	0	
21	✔	admiralty-scale:information-credibility="4"	admiralty-scale	0	
22	✔	admiralty-scale:information-credibility="5"	admiralty-scale	0	
23	✔	admiralty-scale:information-credibility="6"	admiralty-scale	0	

Partage

II. Cyber Threat Intelligence

Partage

TLP : Trafic Light Protocol

✓ Outils de gestion du partage

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

II. Cyber Threat Intelligence

Partage

- ✓ Essentiel
- ✓ …mais délicat
- ✓ Besoin de confidentialité
- ✓ Communautés de confiance

Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Perspectives

III. Perspectives

Apport de la « science des données » :

- ✓ Collecte
- ✓ Stockage
- ✓ Indexation
- ✓ Gestion dans le temps
- ✓ Manipulation
- ✓ Recherche
- ✓ Visualisation

Threat Intelligence

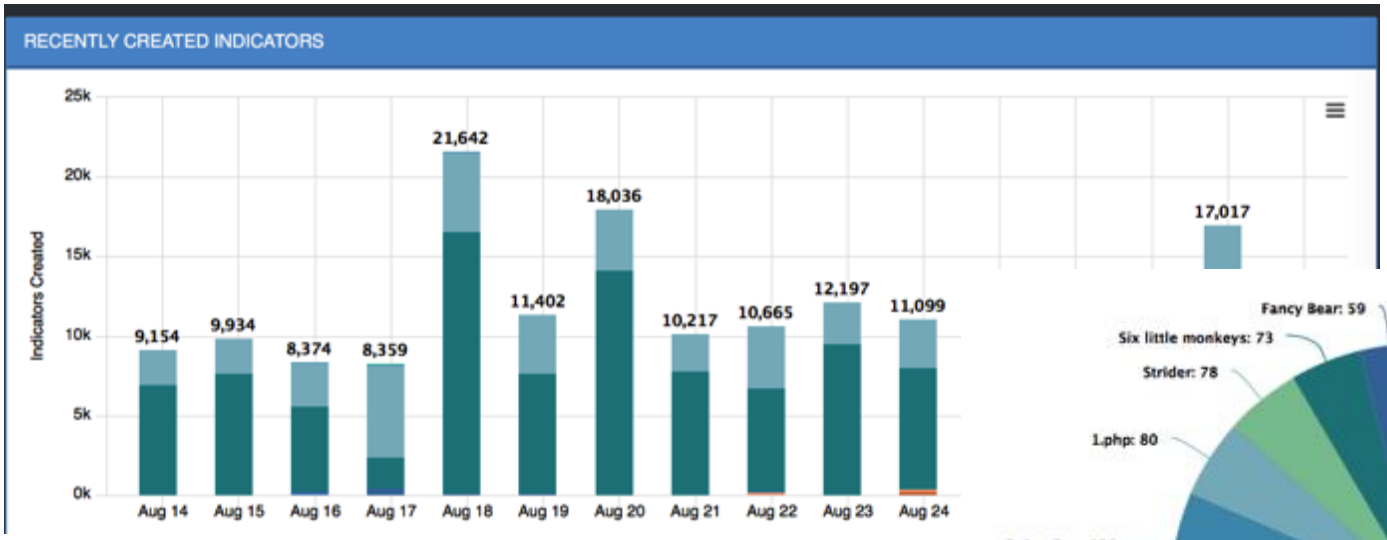
Mais aussi :

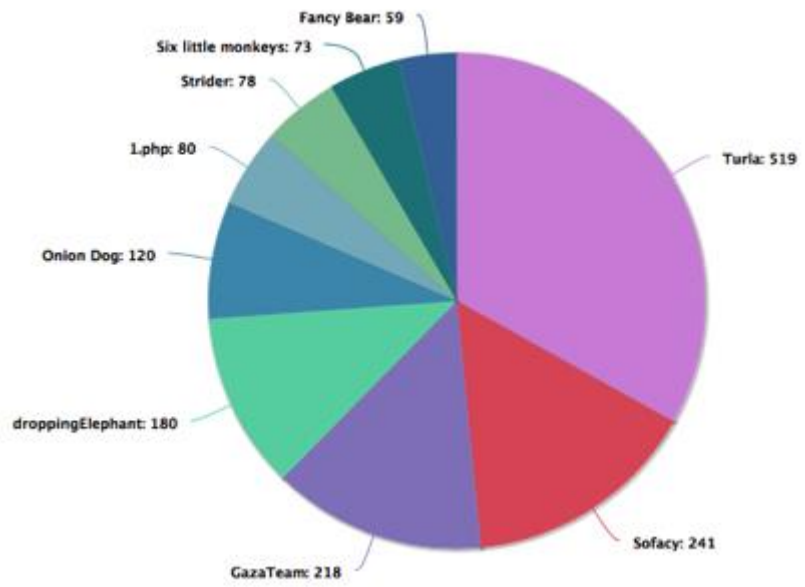
- ✓ Corrélation
- ✓ Détection
- ✓ Analyse comportementale
- ✓ Recherche de signaux faibles

Cyberdéfense

III. Perspectives

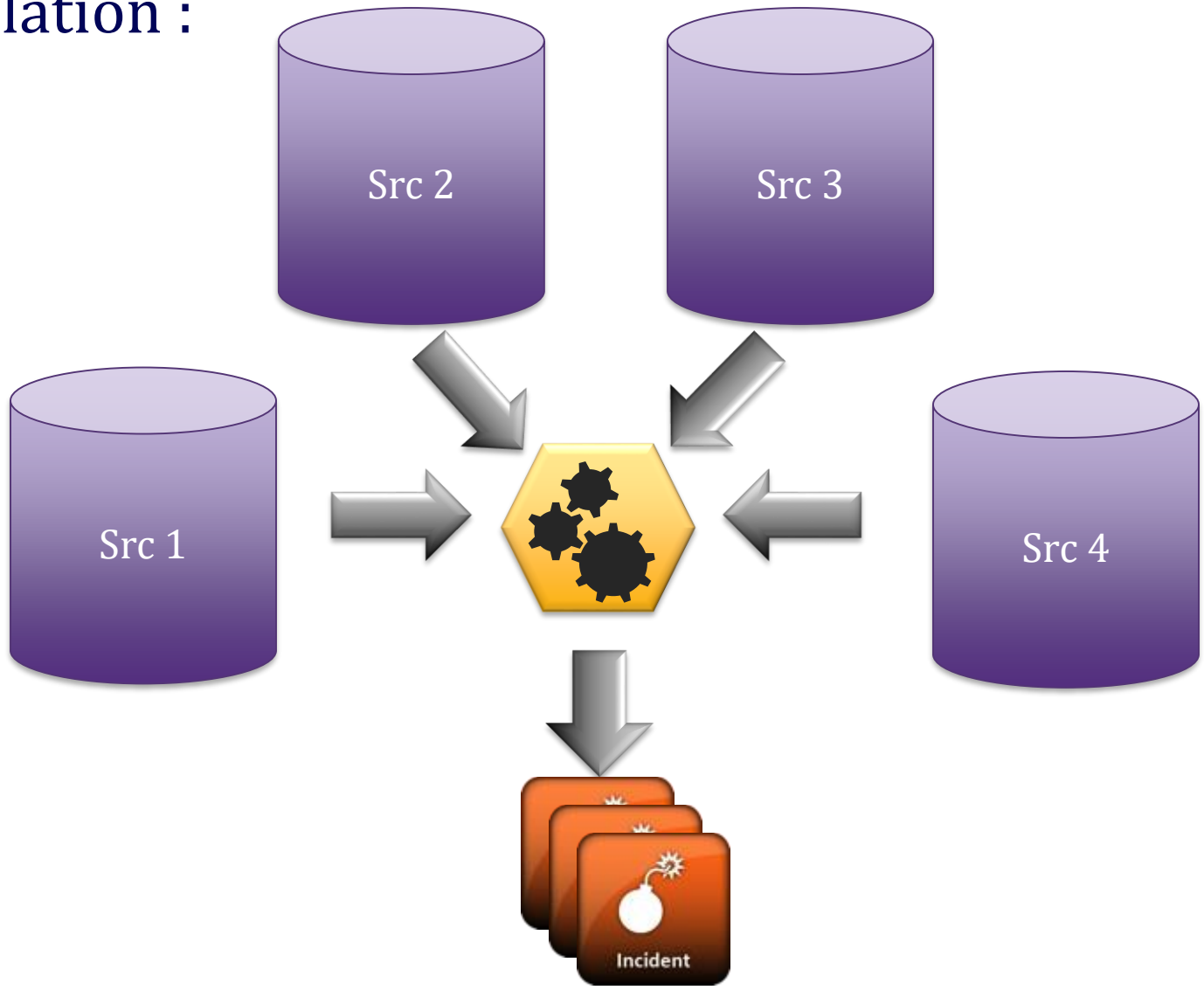
Collecte, stockage, gestion dans le temps, manipulation, recherche et visualisation des indicateurs :





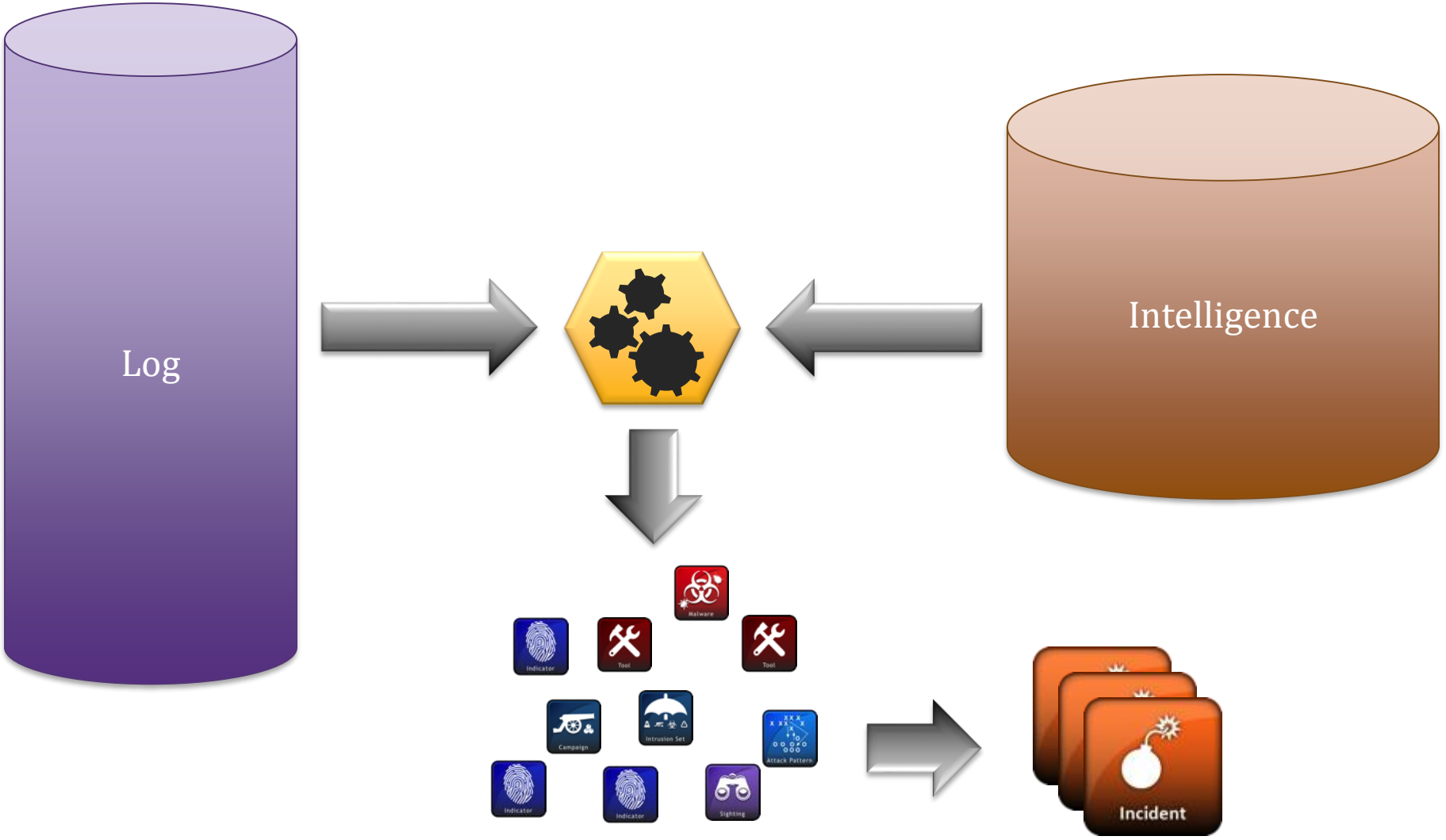
III. Perspectives

Corrélation :



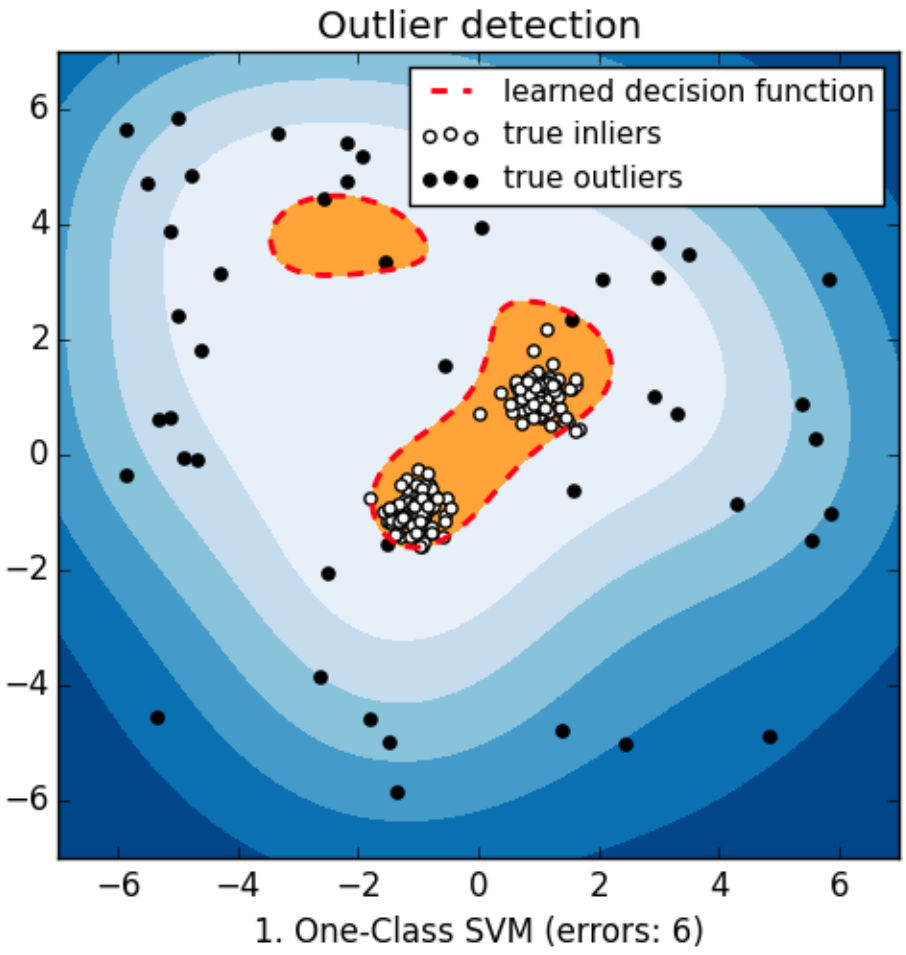
III. Perspectives

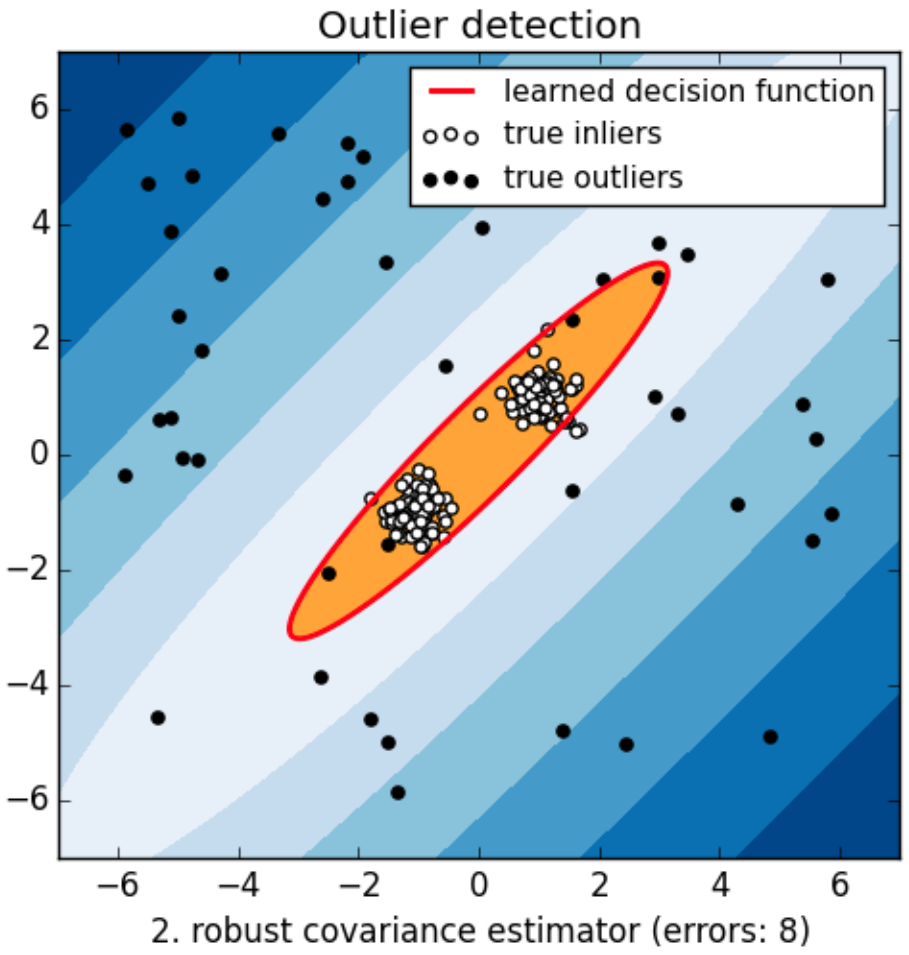
Recherche/hunting :



III. Perspectives

Analyse comportementale :





III. Perspectives

Recherche de signaux faibles :

```
12/30 01:42:32 23.75.345.200 example.com /index.php?2346354=-349087 WordPress/3.7.2
12/30 01:42:31 23.75.345.200 example.com /index.php?7231344=4454226 WordPress/3.3.1
12/30 01:42:25 23.75.345.200 example.com /index.php?1243847=9161112 WordPress/3.7.2
12/30 01:42:23 23.75.345.200 example.com /index.php?8809549=4423410 WordPress/3.3.1
12/30 01:42:21 23.75.345.200 example.com /index.php?1834306=3447145 WordPress/3.5.1
12/30 01:42:16 23.75.345.200 example.com /index.php?-234069=6121852 WordPress/3.3.3
12/30 01:42:16 23.75.345.200 example.com /index.php?-152536=6922268 WordPress/3.3.1
12/30 01:42:14 23.75.345.200 example.com /index.php?3433701=7147876 WordPress/3.4.2
12/30 01:42:14 23.75.345.200 example.com /index.php?6732828=-106444 WordPress/3.2.2
```

« Trouver une cyber aiguille dans une botte de foin »

III. Perspectives

Futur proche :

- ✓ Intelligence artificielle
- ✓ Cyberdéfense prédictive

III. Perspectives

TOUTE L'ACTUALITÉ / SÉCURITÉ / **INTRUSION, HACKING ET PARE-FEU**

Cybersécurité : IBM injecte la puissance de Watson dans les SOC

Maryse Gros, publié le 13 Février 2017

Pendant un an, la technologie d'apprentissage machine Watson d'IBM a digéré des dizaines de milliers de documents sur la cybersécurité. Elle est aujourd'hui intégrée à la plateforme Cognitive SOC pour permettre aux équipes de sécurité d'accélérer le traitement des cybermenaces.

IBM met du Watson dans la cybersécurité

par Guillaume Périssat, le 15 février 2017 16:29

L'IA de Big Blue se décline désormais dans le domaine de la sécurité informatique. Watson for Cybersecurity se destine à assister les équipes sécurité des entreprises à faire le tri entre menaces réelles et faux positifs.

Lundi, à la conférence RSA, IBM a annoncé mettre Watson au service de la cybersécurité. Watson for Cybersecurity veut mettre à disposition des RSSI et de leurs équipes les technologies cognitives concoctées par Big Blue. L'intelligence arrtificielle doit permettre aux chercheurs de réduire les faux positifs et de faciliter la détection et la réponses aux attaques.

Selon une étude d'IBM, les équipes en charge de la sécurité dans les entreprises ont à gérer 200 000 alertes de sécurité par jour. Elles passeraient ainsi 20 000 heures par an sur des faux positifs. Watson for Cybersecurity pourrait les aider à déterminer quels évènements, parmi les 200 000 journaliers, méritent vraiment leur attention immédiate. En d'autres termes, l'IA fait gagner du temps et, par extension, permet de mieux répondre (et plus vite) aux véritables menaces.

Un million de documents ingérés

Mais le multitâche Watson n'est pas devenu « expert » en sécurité informatique du jour au lendemain. Il a étudié ces douze derniers mois plus d'un million de documents relatif à la cybersécurité. Et travaille en version bêta dans 40 entreprises et organisations à l'instar d'Avnet, de l'université de New Brunswick ou encore de Sopra Steria, apprenant de ces équipes qu'il assiste.

Conclusion

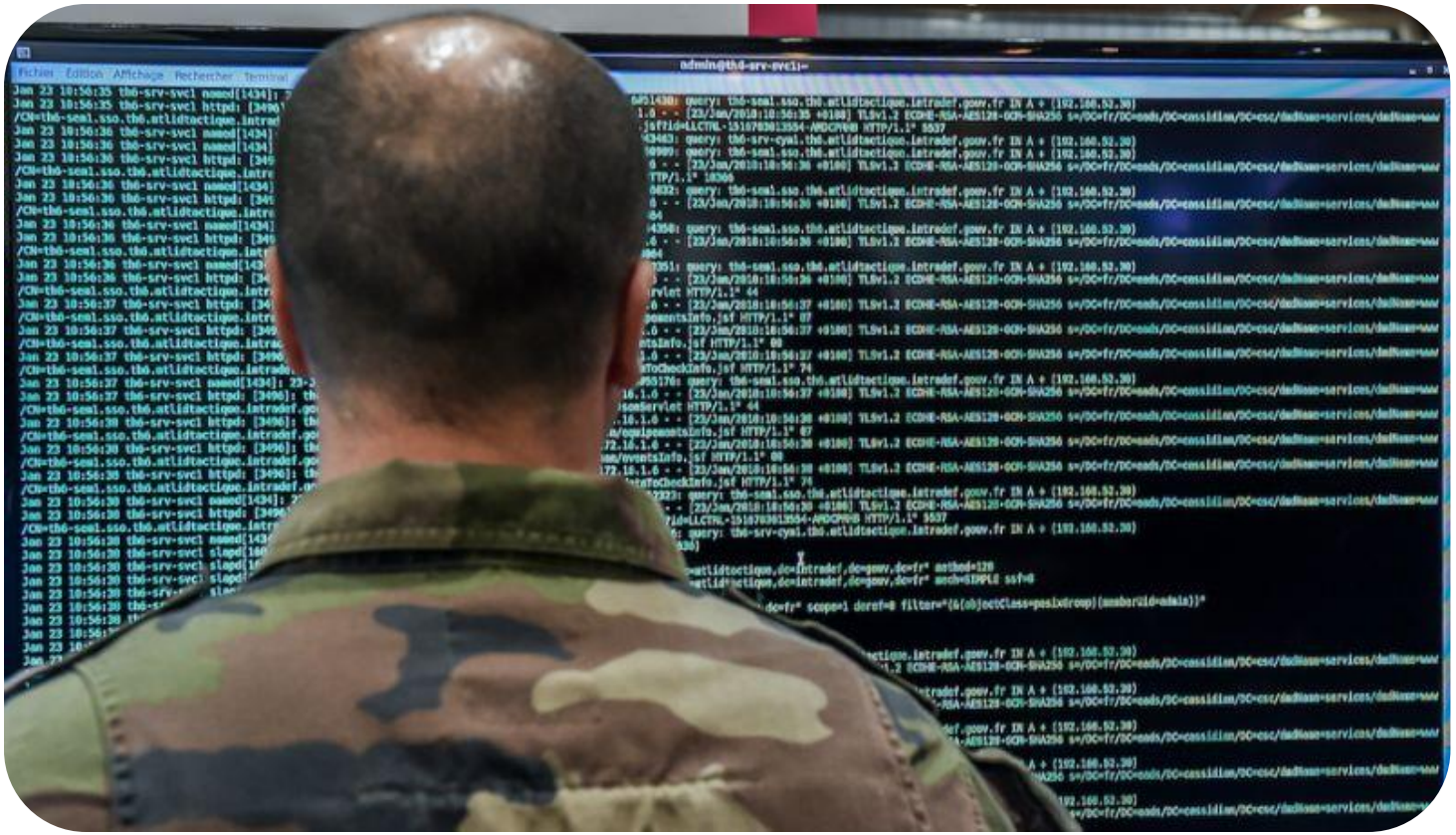
- ✓ **Cyber Threat Intelligence =**

Des outils + des hommes + des processus

- ✓ **Cyber Threat Intelligence = ART :**
  - Accurate
  - Reliable
  - Timely

- ✓ **19 mars | TP noté :**
  - Par binôme
  - Accès à l'aide d'un poste connecté à Internet

Engagez vous !



Contact recrutement : sga-cyber.contact.fct@def.gouv.fr
Contact pour la réserve : crpoc.cer.fct@intradef.gouv.fr

Mais aussi : DGSE, DRM, DRSD, ANSSI, DGSI…

Contact : nicolas.pierson@for-cyb.com