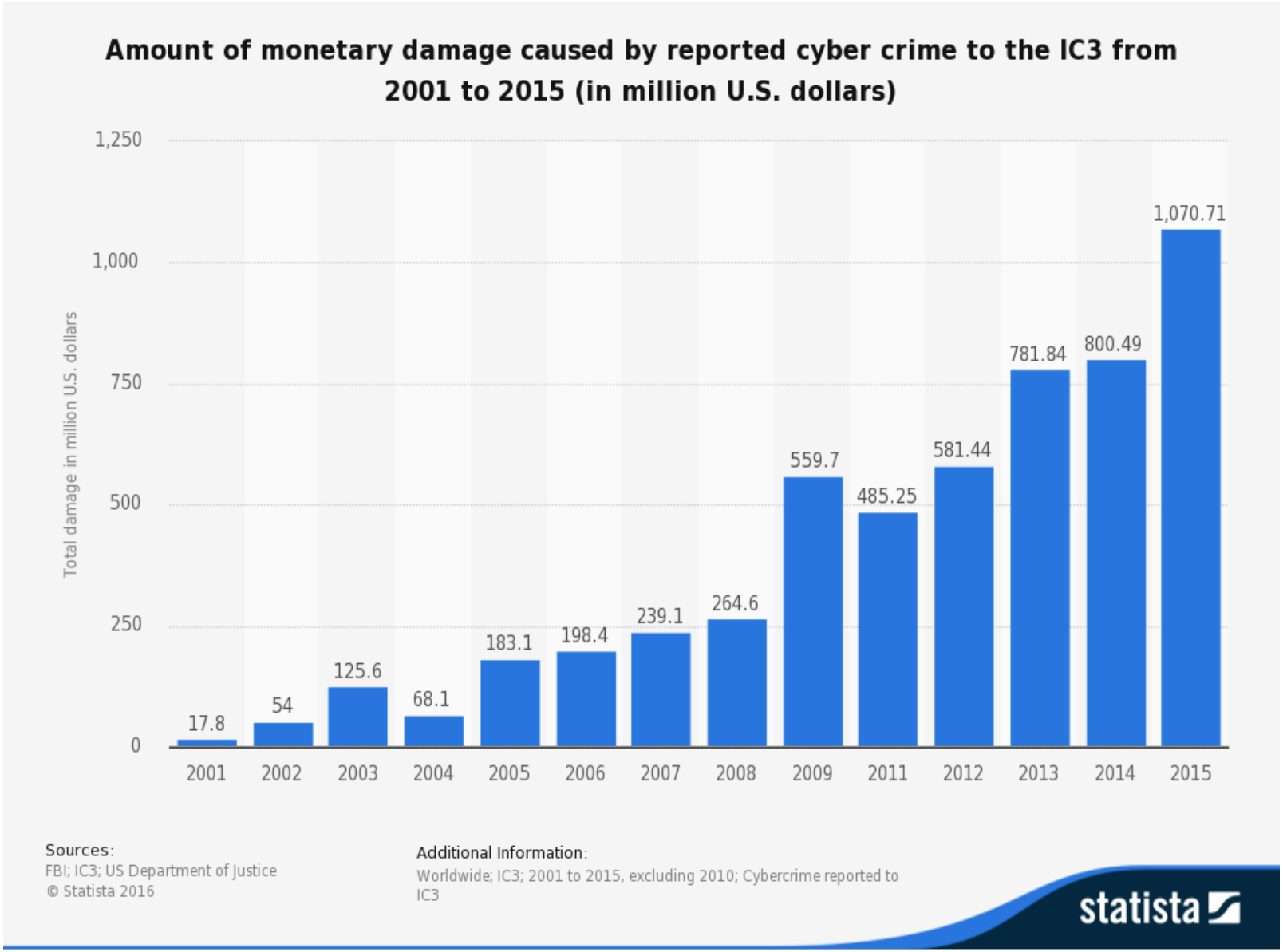
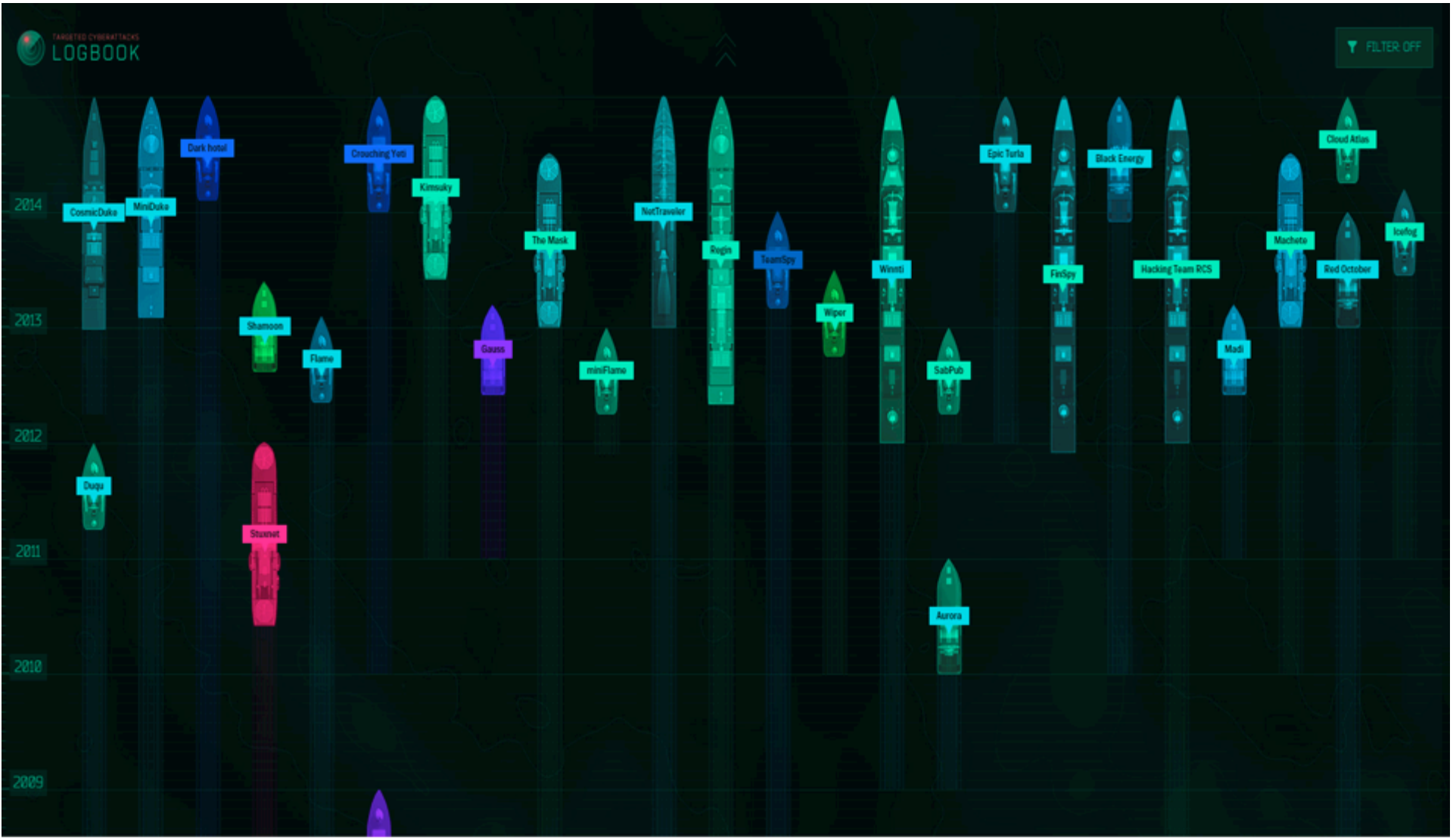
Cyberdéfense et Big Data : La Cyber Threat Intelligence

Nicolas Pierson

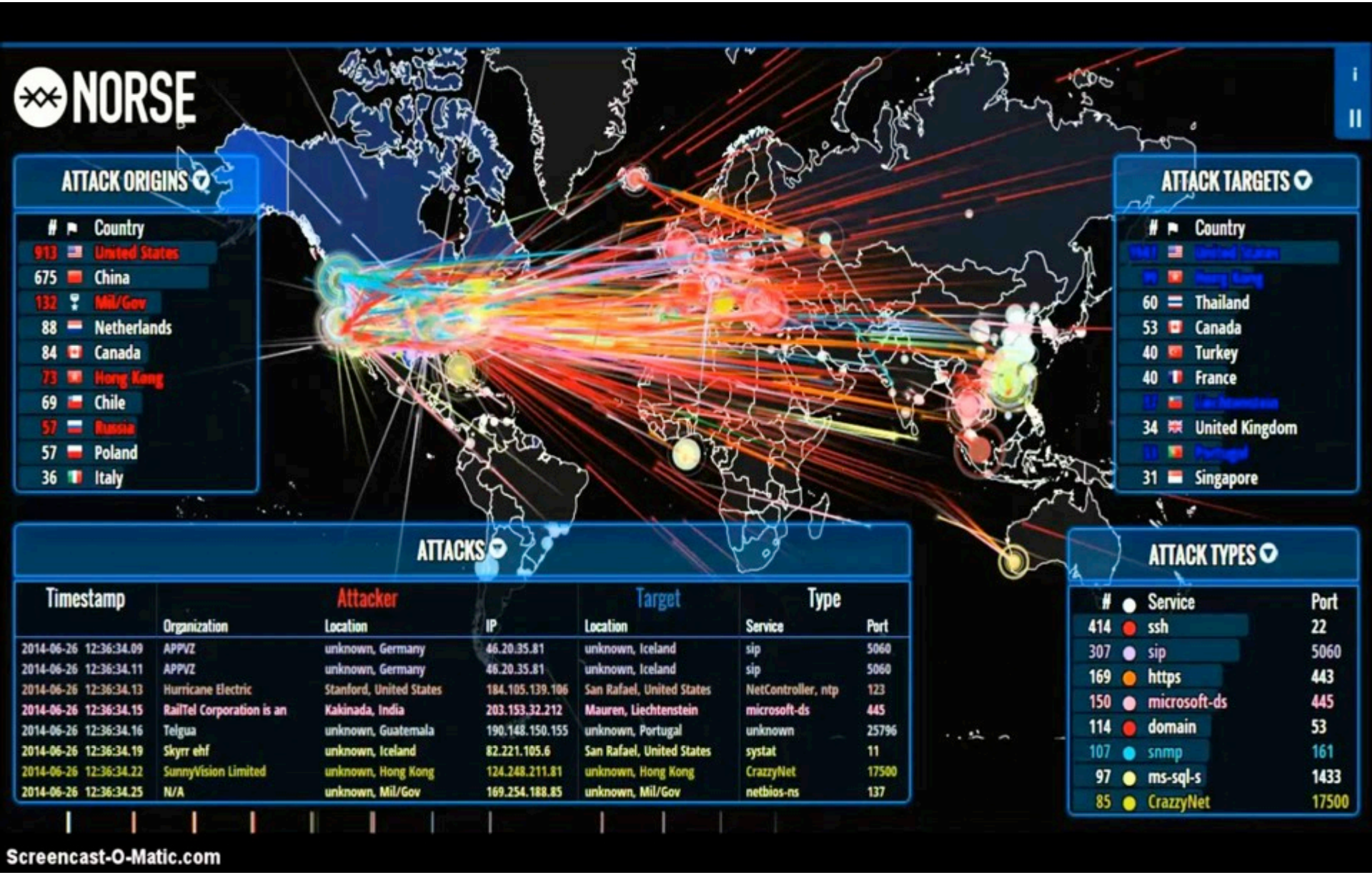
Introduction



Introduction



Introduction



Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Apports de la science des données à la cyberdéfense

Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Apports de la science des données à la cyberdéfense

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.

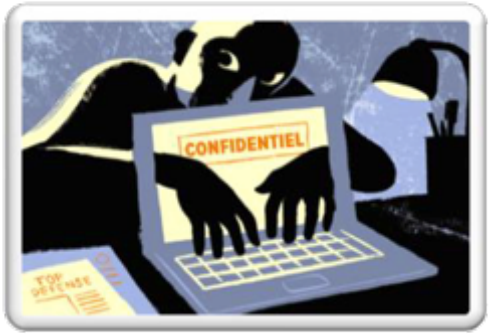
Risque :

Association d'une menace aux vulnérabilités qui permettent sa réalisation.

I. Contexte général

Menaces : les motivations

- ✓ Hackers en recherche de notoriété
- ✓ Activistes (Anonymous, éthiques)
- ✓ Criminels
- ✓ Terroristes (ex : ISIS)
- ✓ Services étatiques (ex : NSA, Russie)
- ✓ Cyber mercenaires
- ✓ Multiples



I. Contexte général

Menaces: les 10 méthodes d'attaques les plus utilisées :

1. Ingénierie sociale (réseaux sociaux)
2. Compromission de comptes (sur la base de mots de passe faibles par exemple)
3. Attaque web (injection de code/de commandes).
4. Attaque de clients de l'entreprise ciblée
5. Exploitation de vulnérabilités connues sur des serveurs non mis à jour
6. Terminaux non sécurisés
7. Intrusion physique
8. Utilisation de services personnels à des fins professionnelles (dropbox, yahoo, gmail…)
9. Attaque de prestataires de l'entreprise (consultants, administrateurs informatiques…)
10. Attaque de données hébergées dans le cloud

I. Contexte général

Menaces : les vecteurs d'attaques (exploit kit)

- ✓ « Hameçonnage » (Phishing, spearPhishing)
- ✓ Installation par support amovible
- ✓ Pièce jointe (pdf, macro…)
- ✓ « Puits numérique » (Waterhole, Malwaretising)
- ✓ Injection de code
- ✓ Force brute
- ✓ …

I. Contexte général

Menaces : Les grandes familles d'attaques actuelles (Payload)

- ✓ Ransomware
- ✓ Dénis de service DDOS
- ✓ Fraudes multiples
- ✓ Fuite/vol de données (Data Leak)
- ✓ « Défacement » de site
- ✓ Prise de contrôle à distance
- ✓ Attaque combinée
- ✓ Advanced Persistant Threat (APT)
- ✓ …

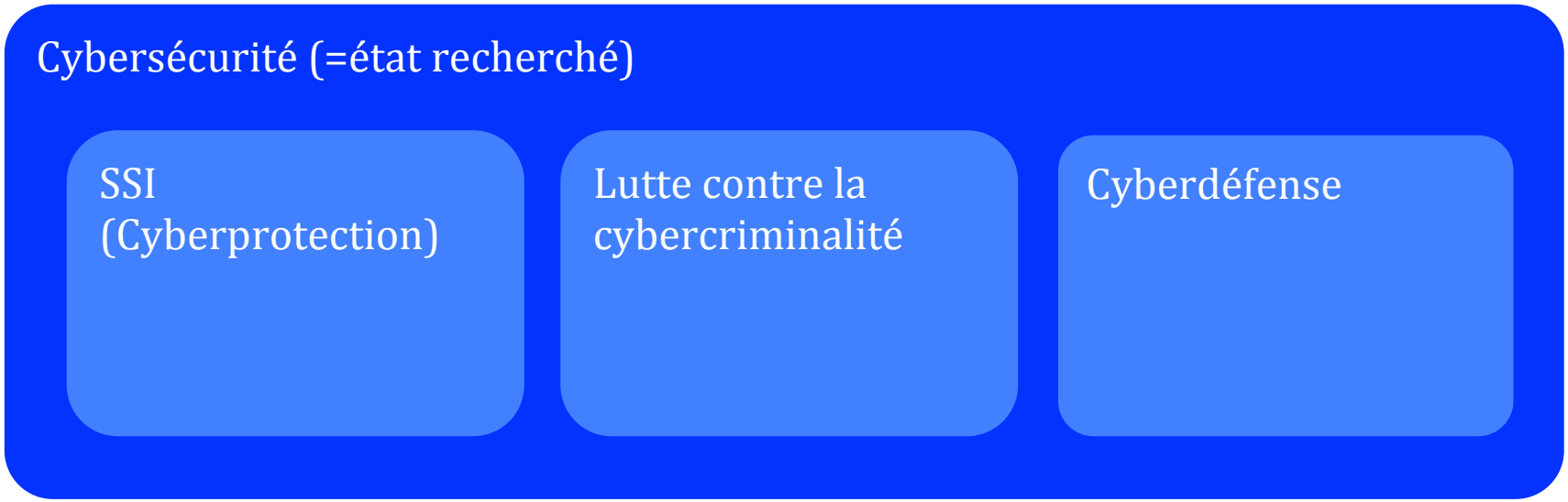
I. Contexte général

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) :



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.

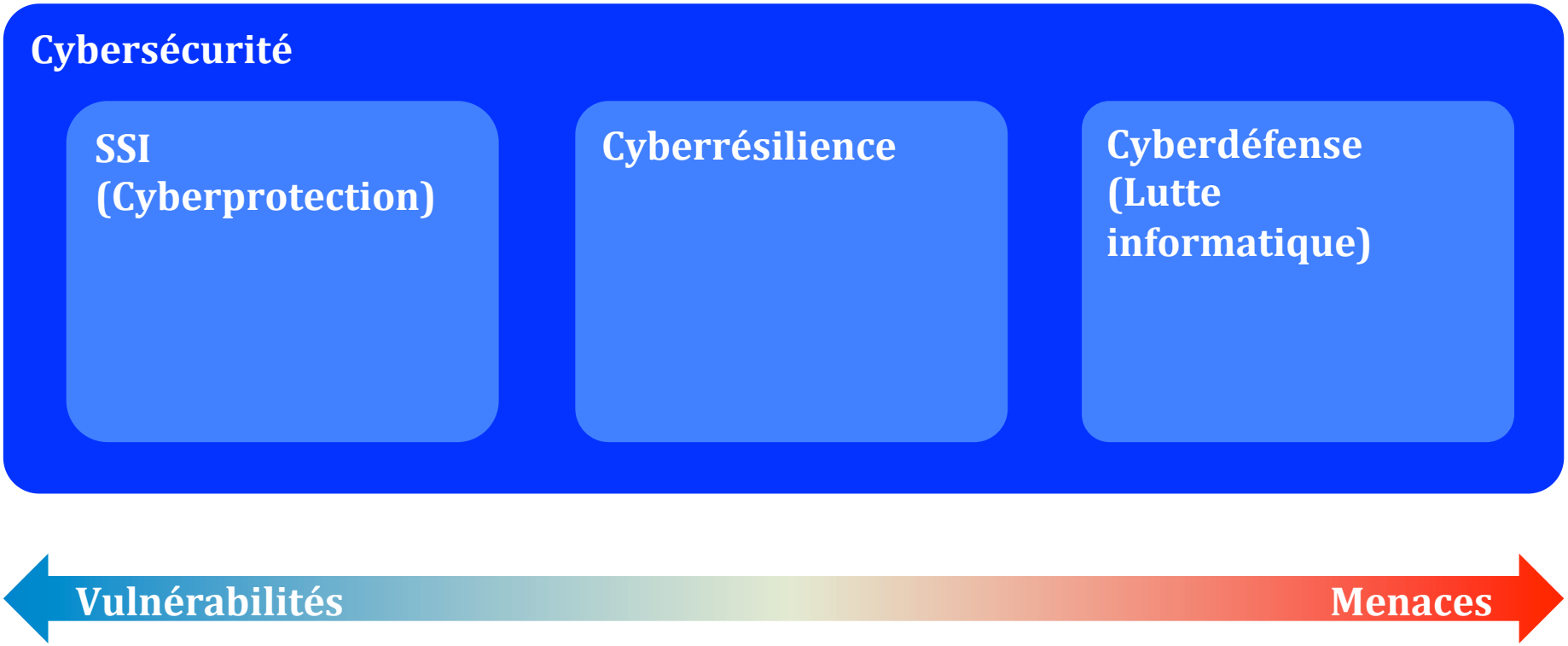
Cyberdéfense (=Etatique)

Mesures techniques

Mesures non-techniques

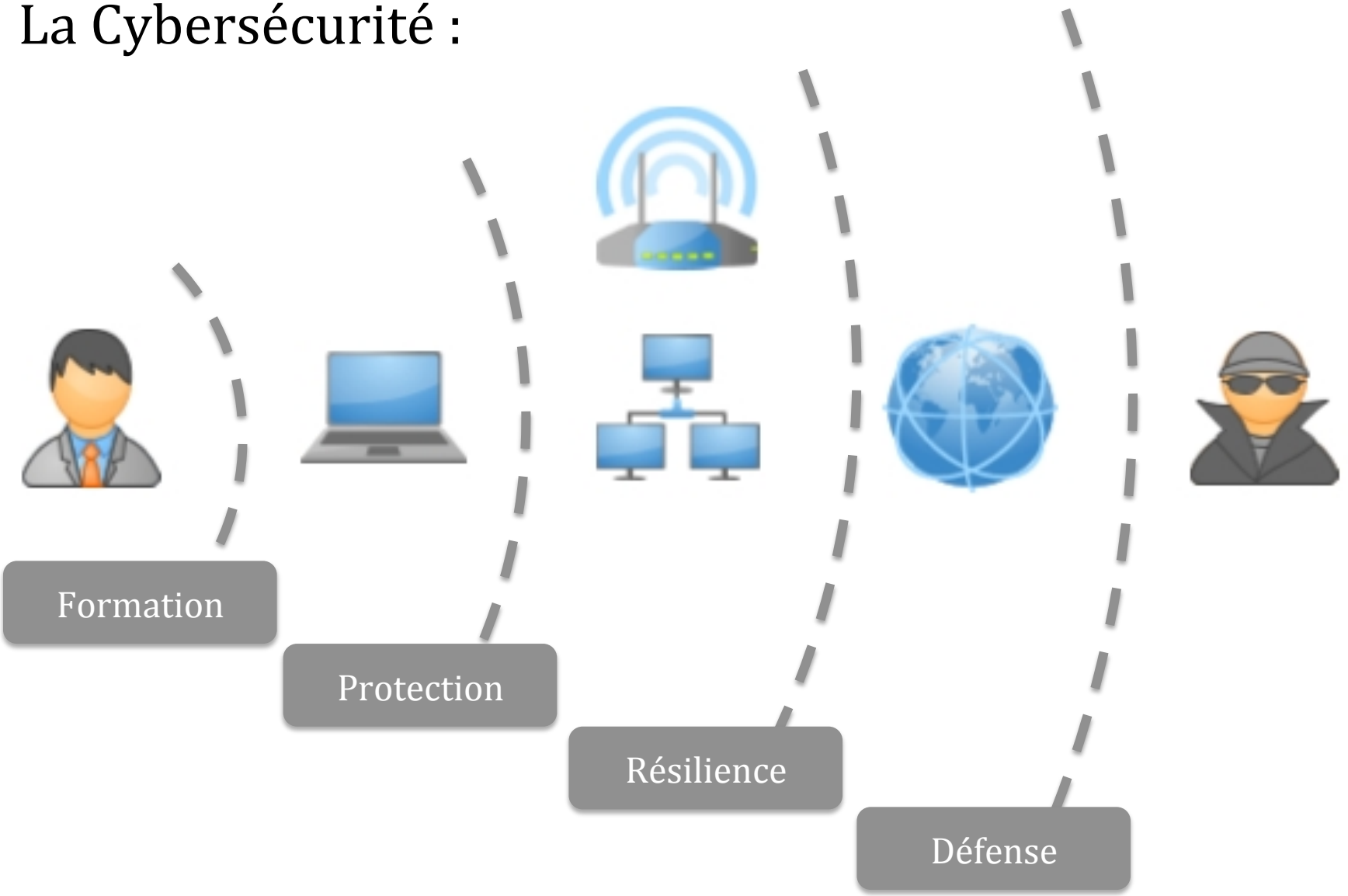
I. Contexte général

La Cybersécurité :



I. Contexte général

La Cybersécurité :



I. Contexte général

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

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

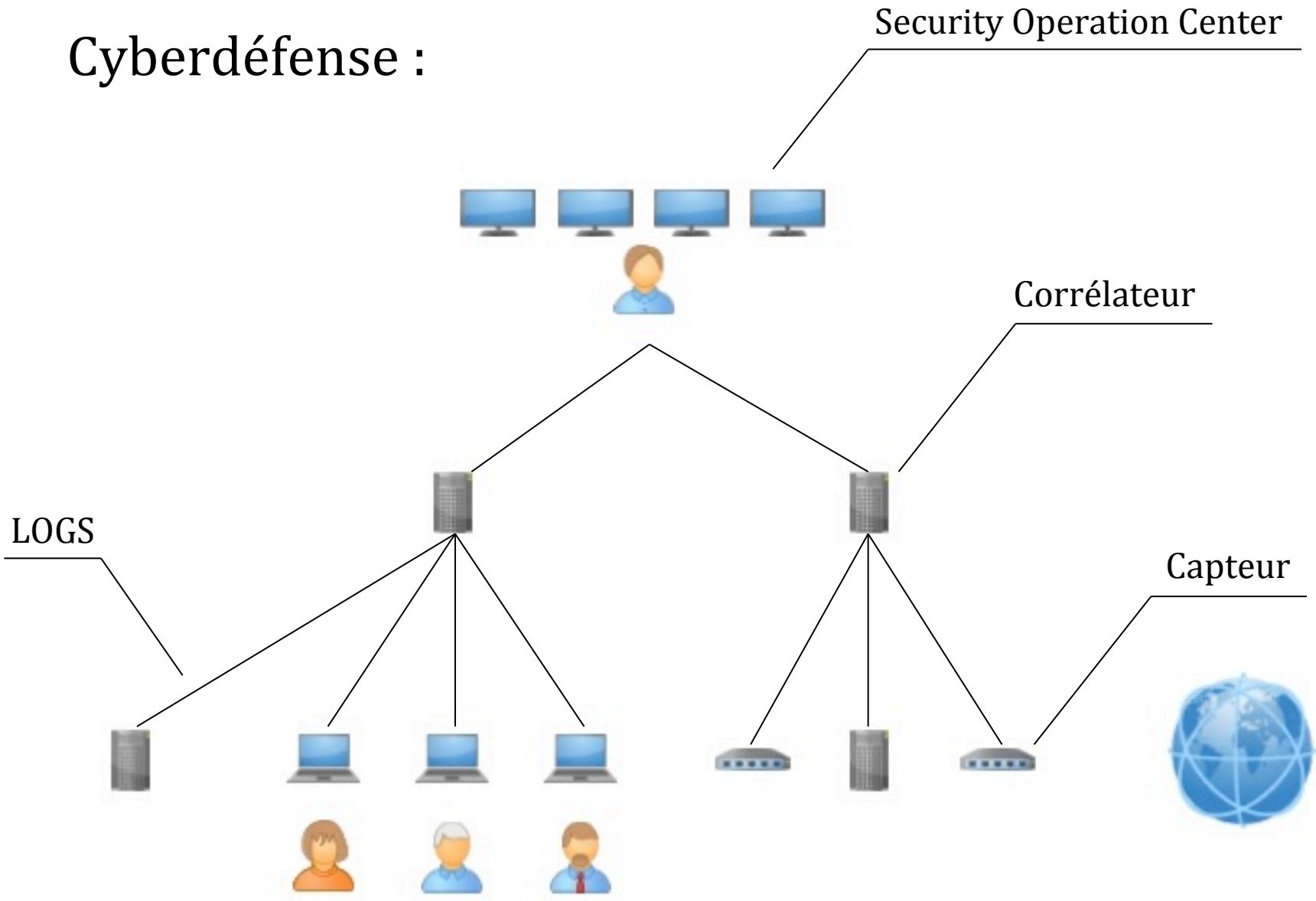
Extrait du référentiel PDIS de l'ANSSI :

« 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, qualifiées au préalable par le prestataire ;
- ✓ **les incidents de sécurité détectés auprès des éventuels autres commanditaires**. »

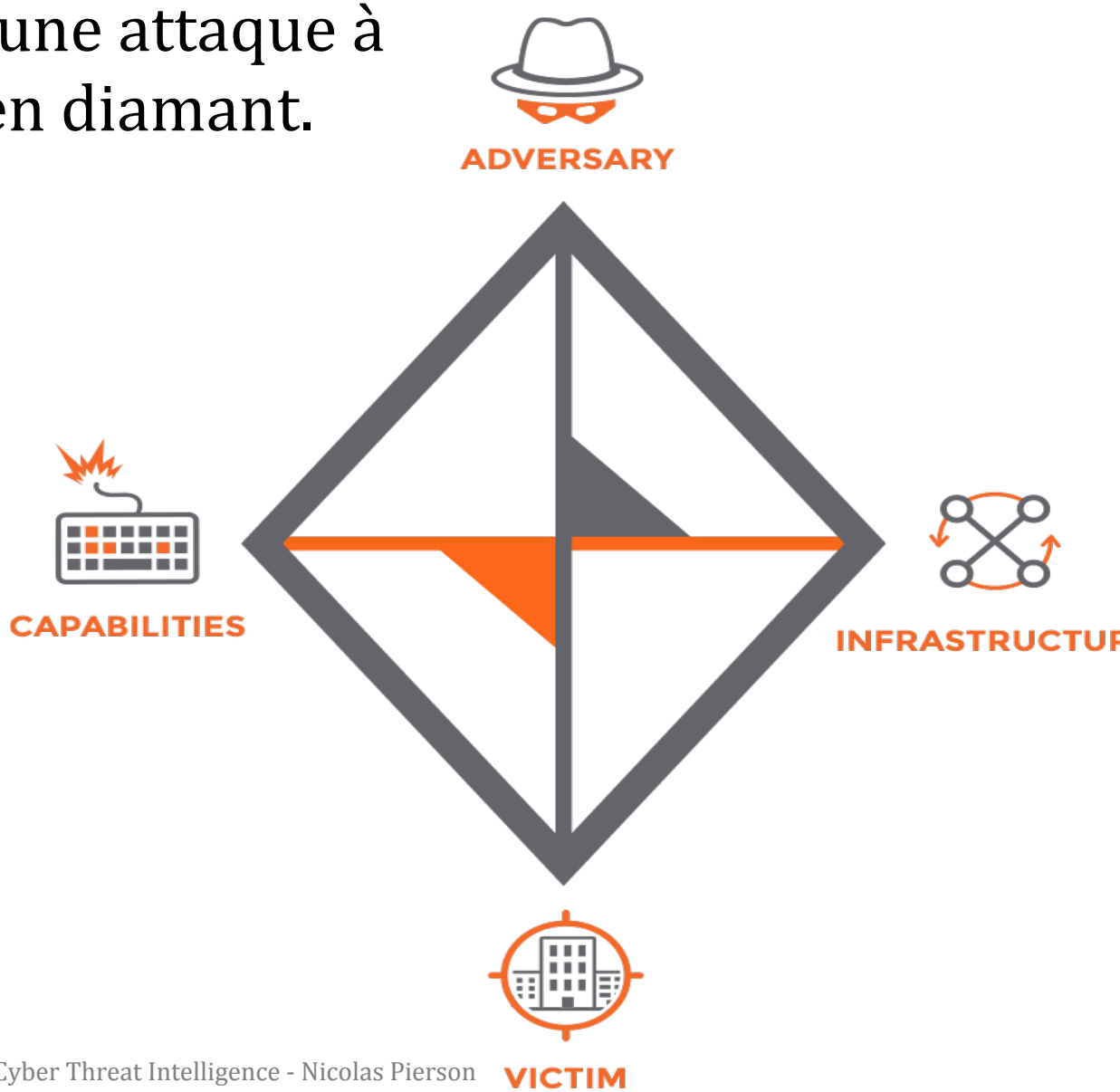
I. Contexte général

Cyberdéfense :



I. Contexte général

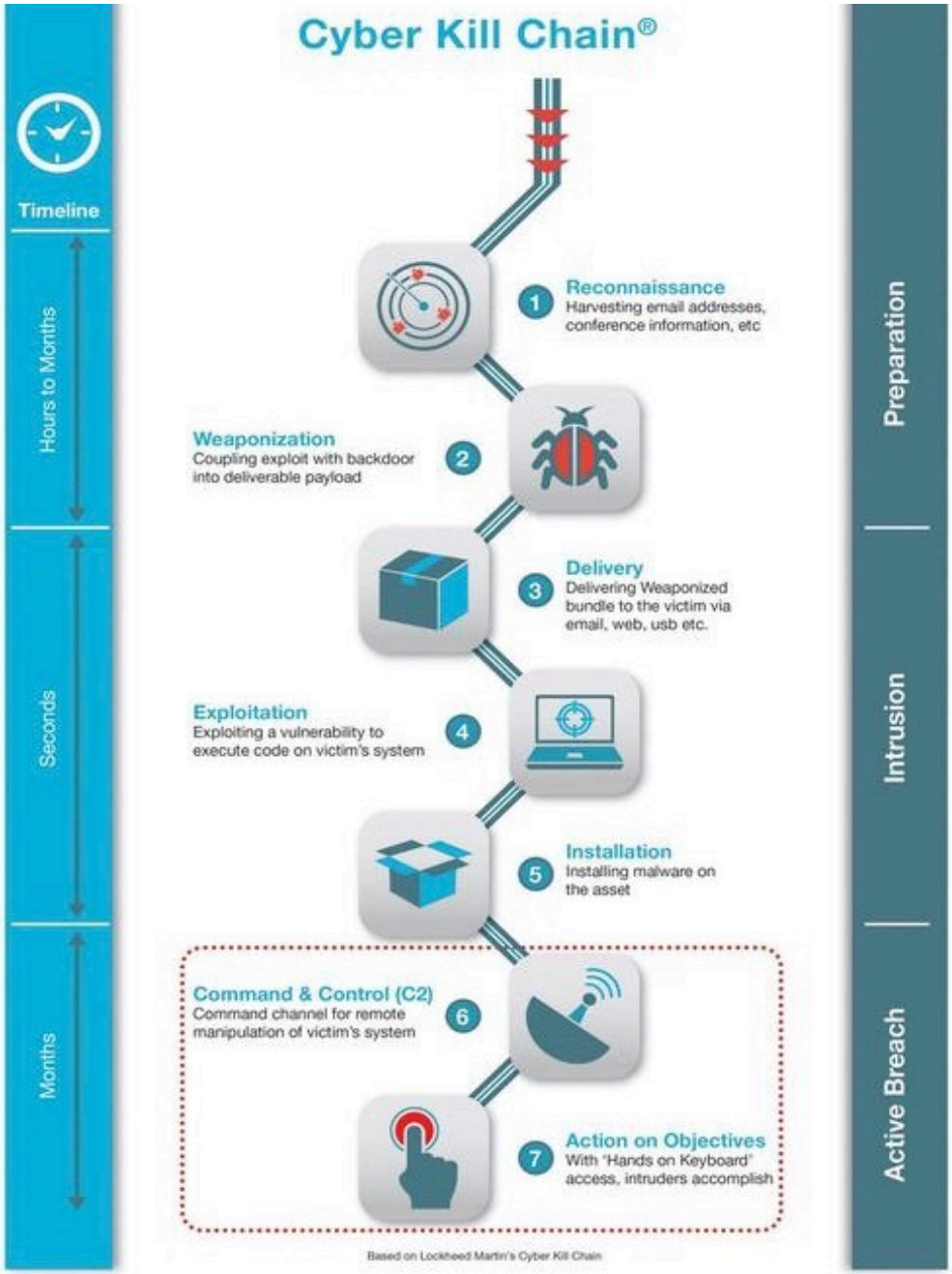
Caractérisation d'une attaque à l'aide du modèle en diamant.



I. Contexte général

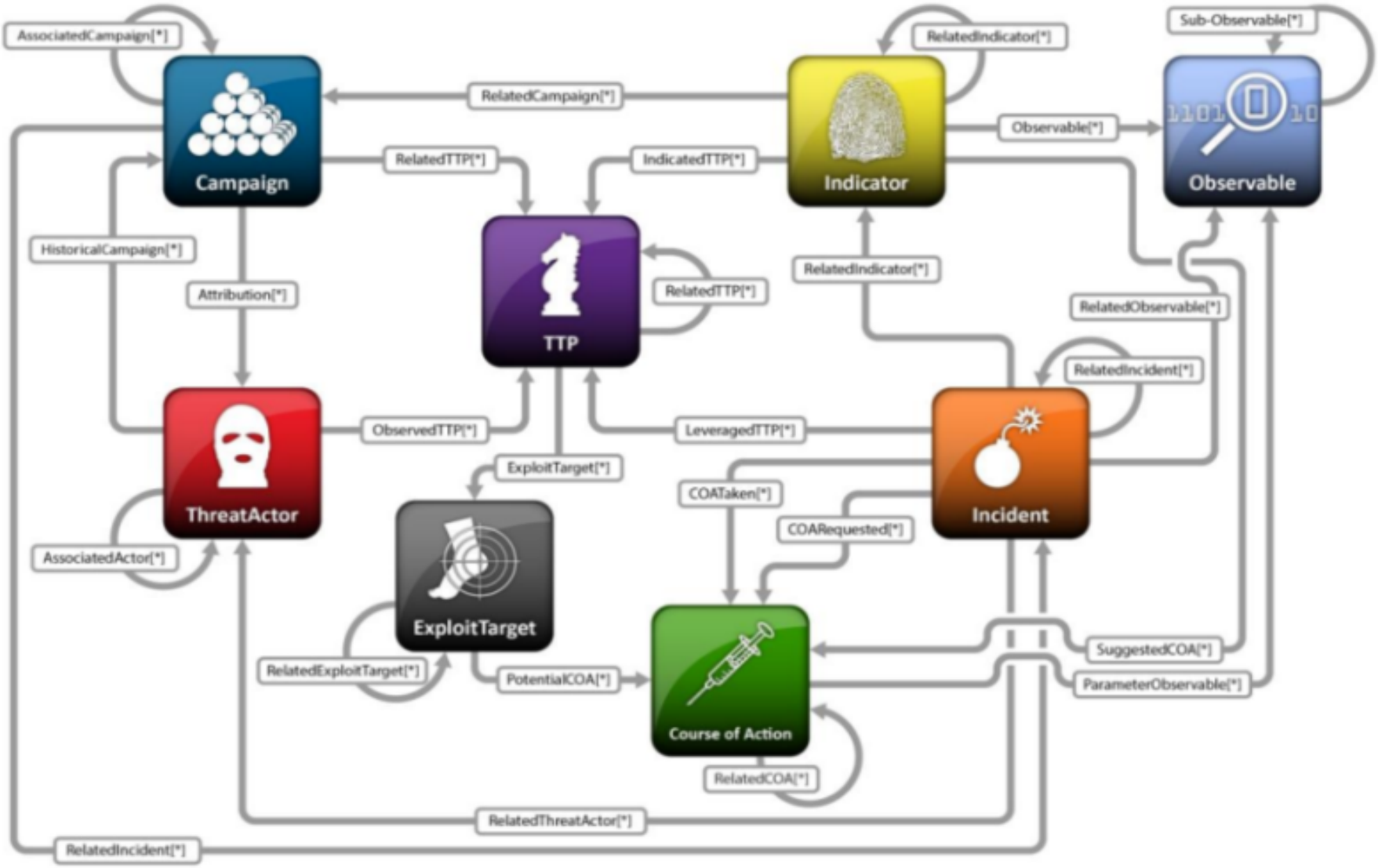
Cyber Kill Chain :

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

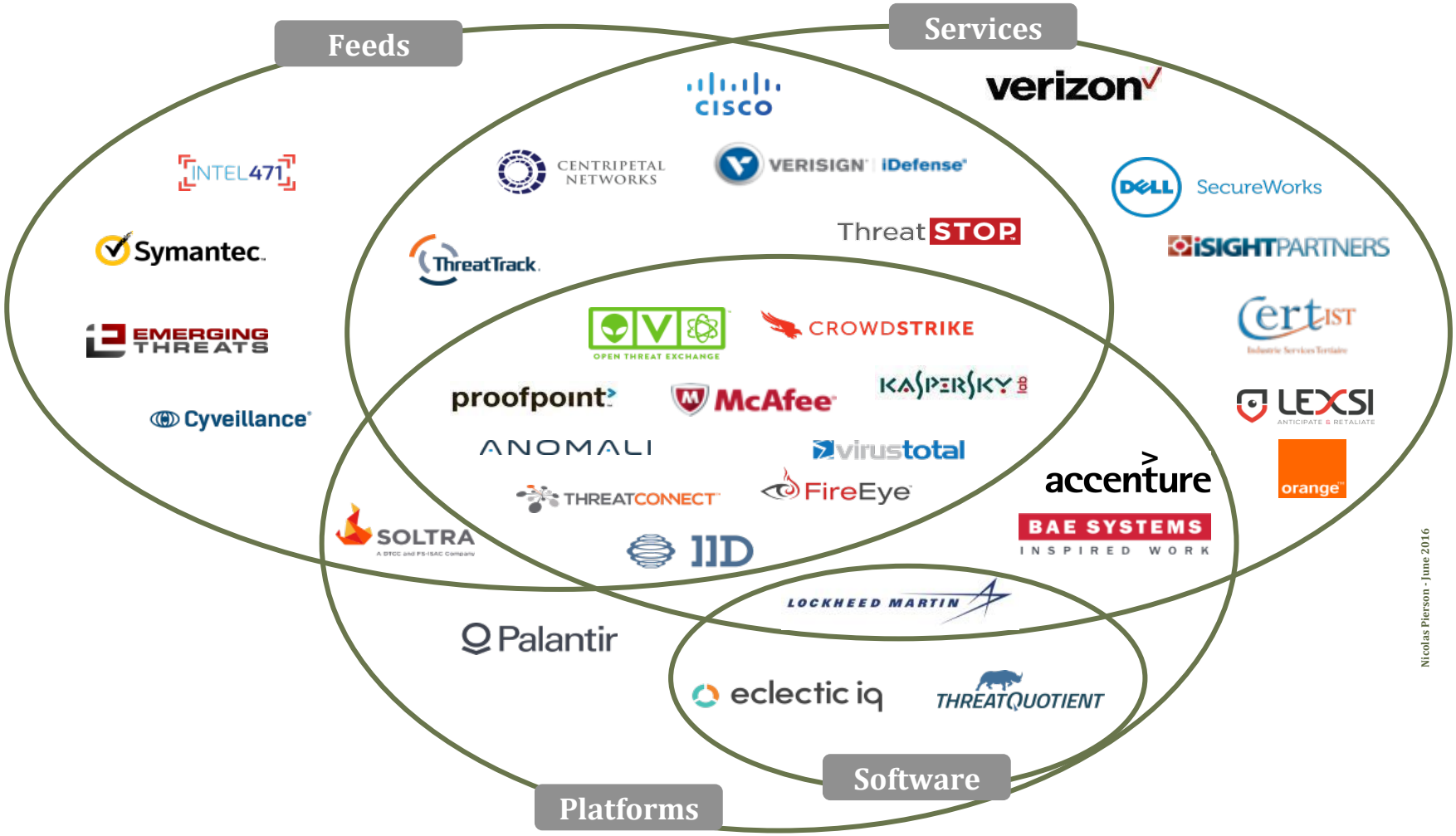


I. Contexte général

STIX : Structured Threat Information eXpression (MITRE)



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

- Apports de la science des données à la cyberdéfense

II. Cyber Threat Intelligence

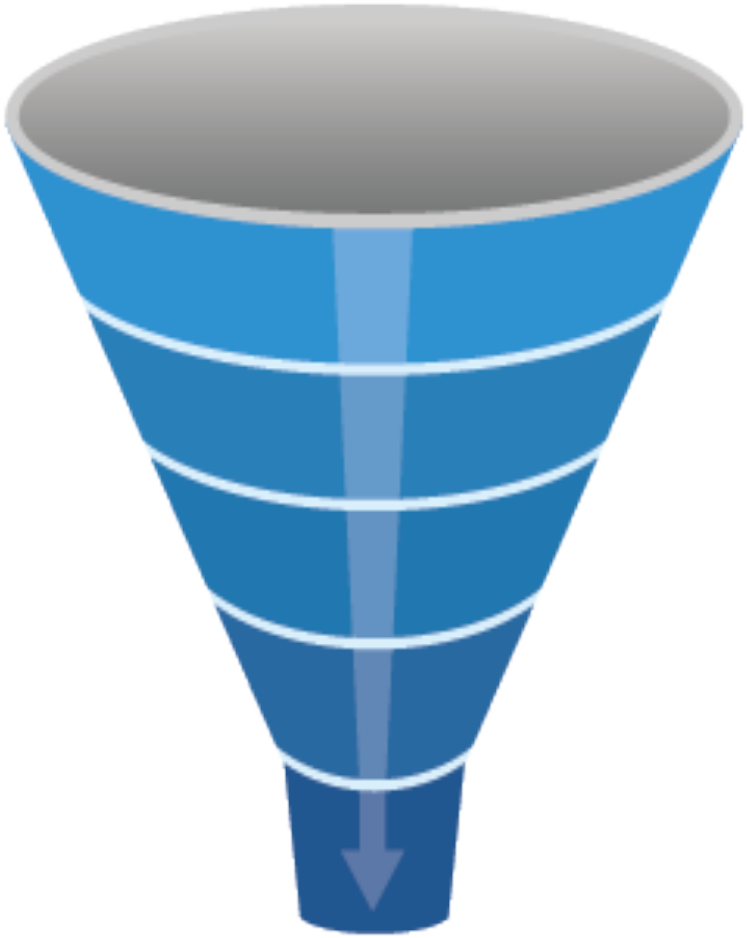
Définition de la Threat Intelligence :

Ensemble des informations et des actions de renseignement sur les 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.

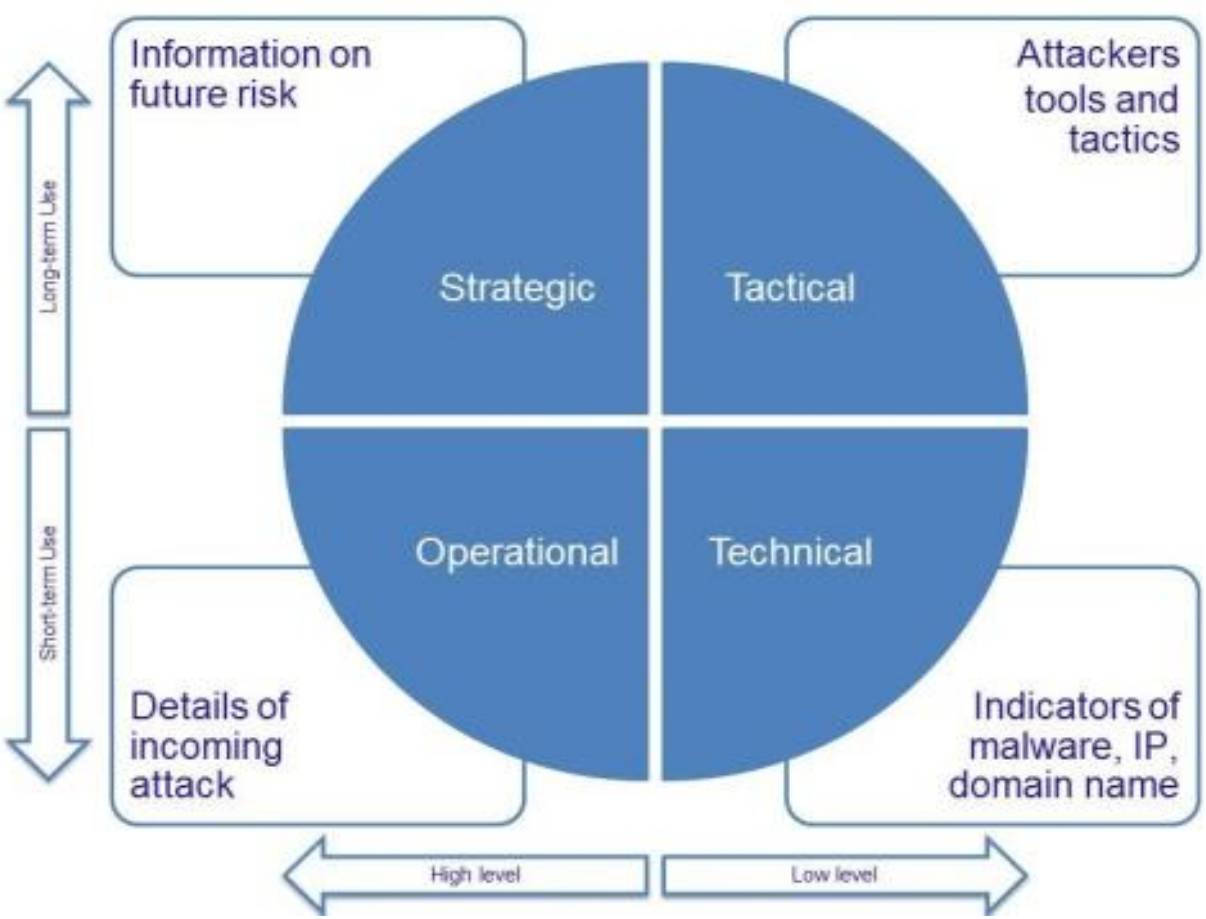
Information is data with a purpose. Once it is assigned a purpose it becomes information.

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 de renseignement :



II. Cyber Threat Intelligence

Atomic

What threat activity are we seeing?

Tactical

What threats should I look for on my networks and systems and why?

Operational

Where has this threat been seen?

What can I do about it?

What weaknesses does this threat exploit?

Strategic

Who is responsible for this threat?

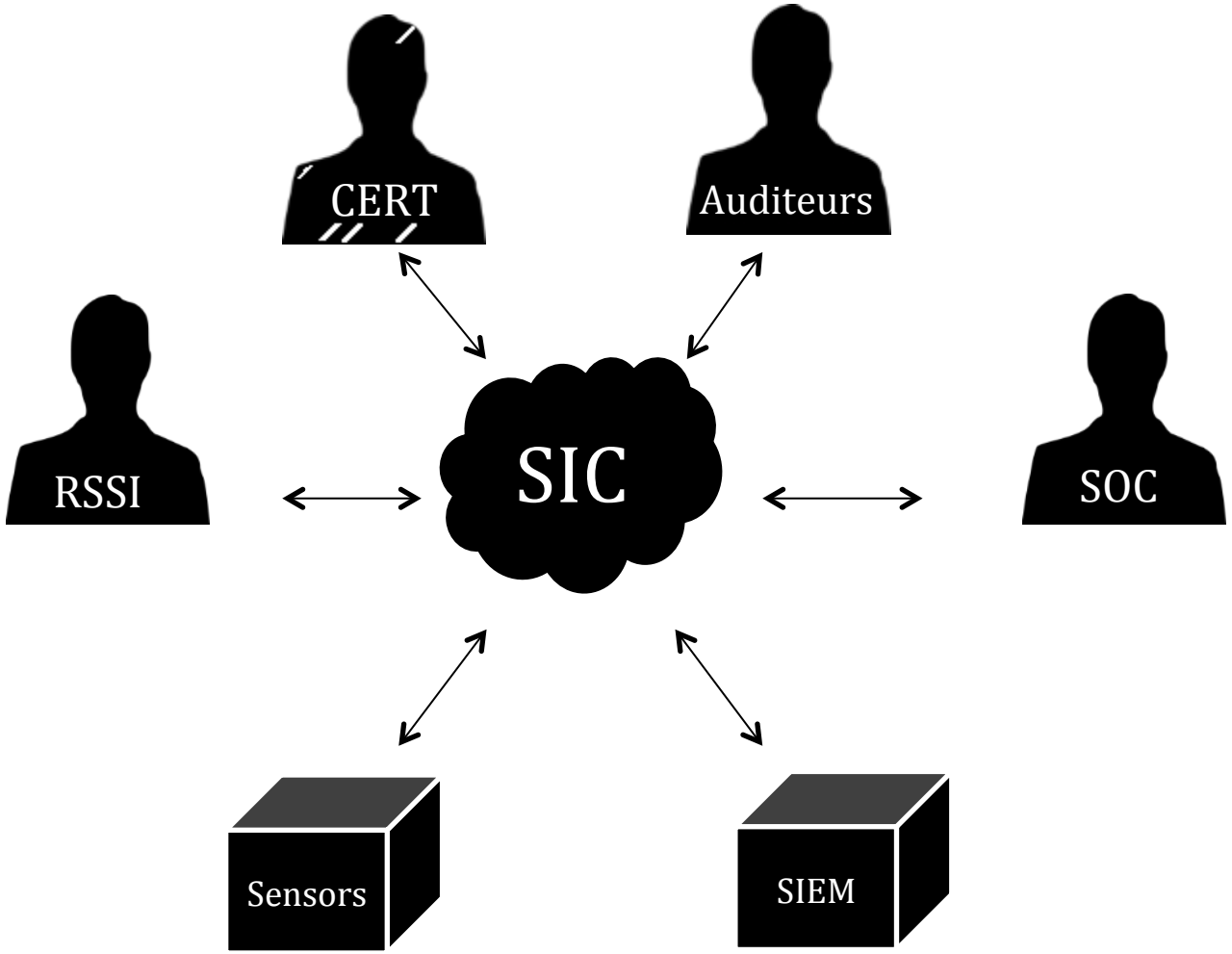
Why do they do this?

What do they do?

II. Cyber Threat Intelligence

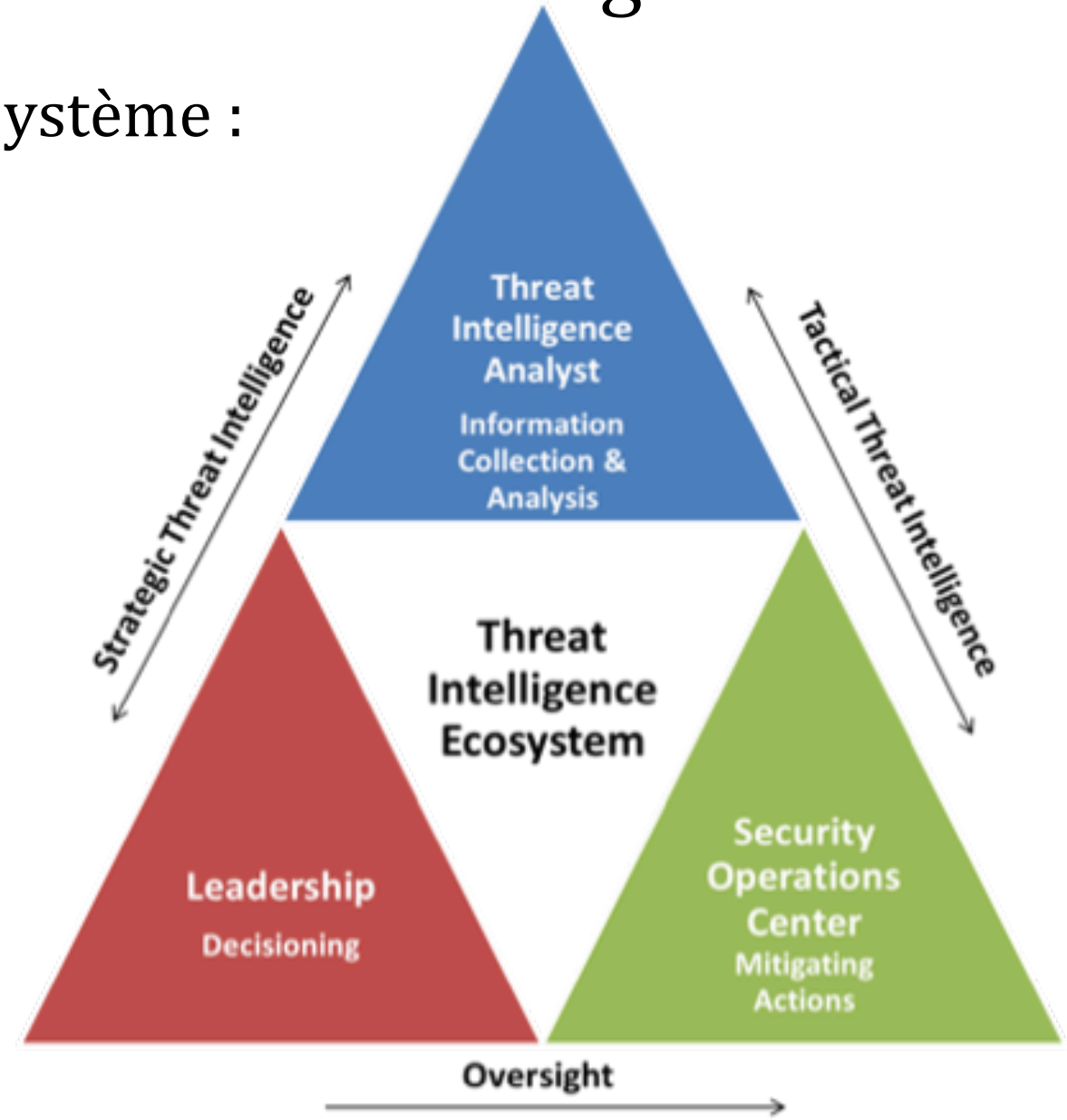
SIC: Security Intelligence Center

Des destinataires multiples :



II. Cyber Threat Intelligence

Un écosystème :



II. Cyber Threat Intelligence

Cyber threat intelligence :

✓Temps réel (Firewall, IPS)

✓Détection (Sonde, SOC)

✓A posteriori (« Hunting »)

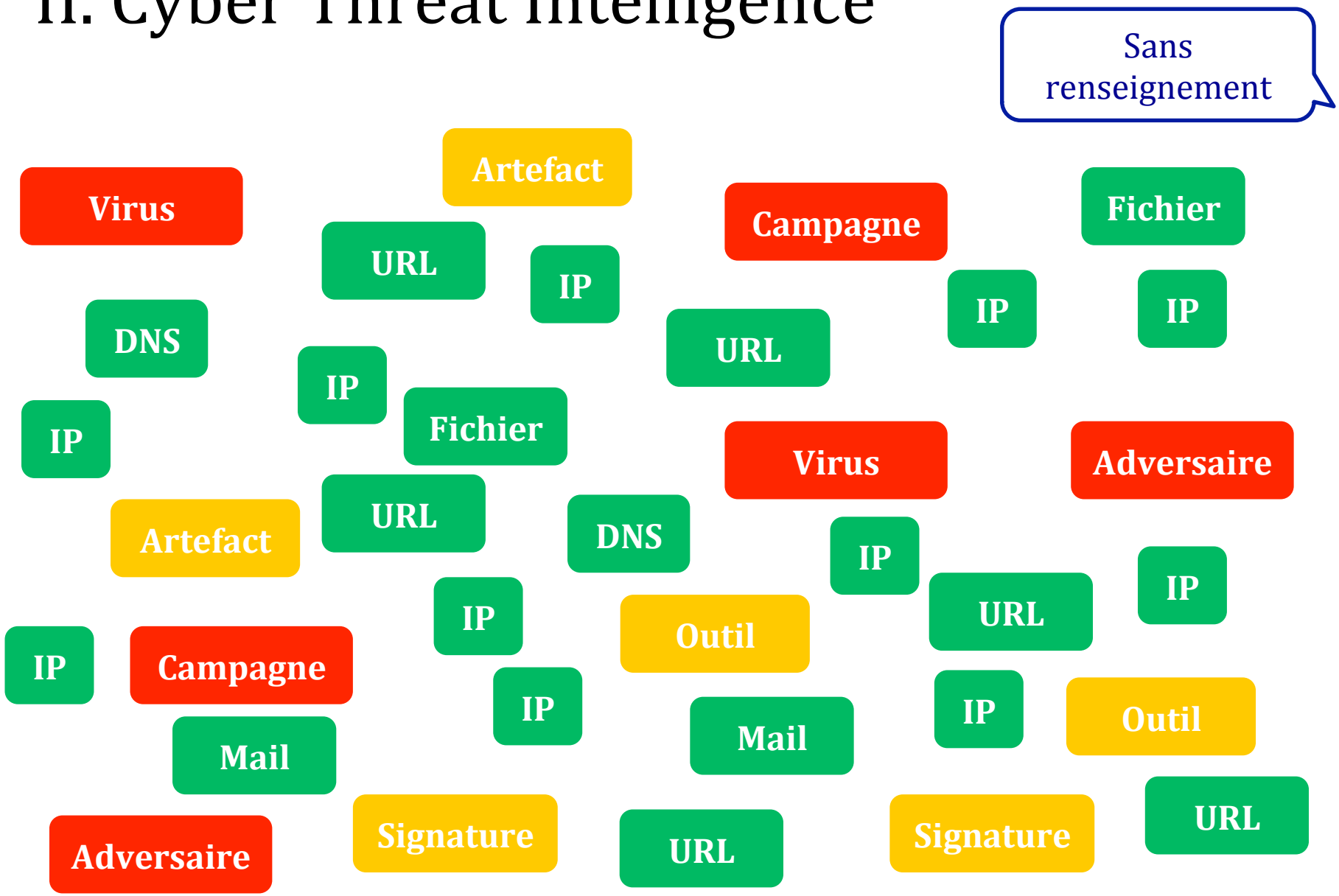
L'*ART* du renseignement :

✓ *Accurate* (Précis)

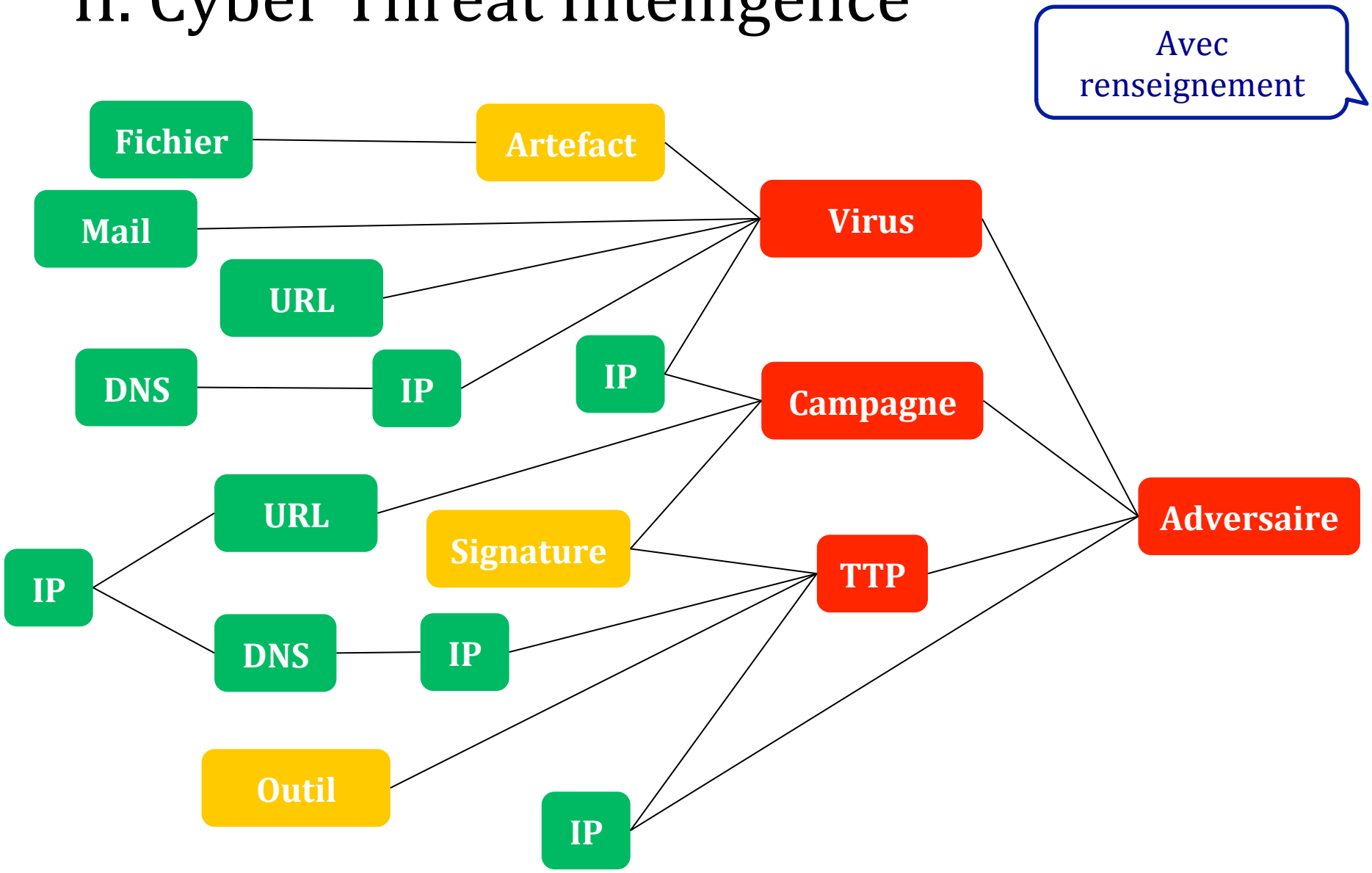
✓ *Relevant* (Pertinent)

✓ *Timely* (A temps)

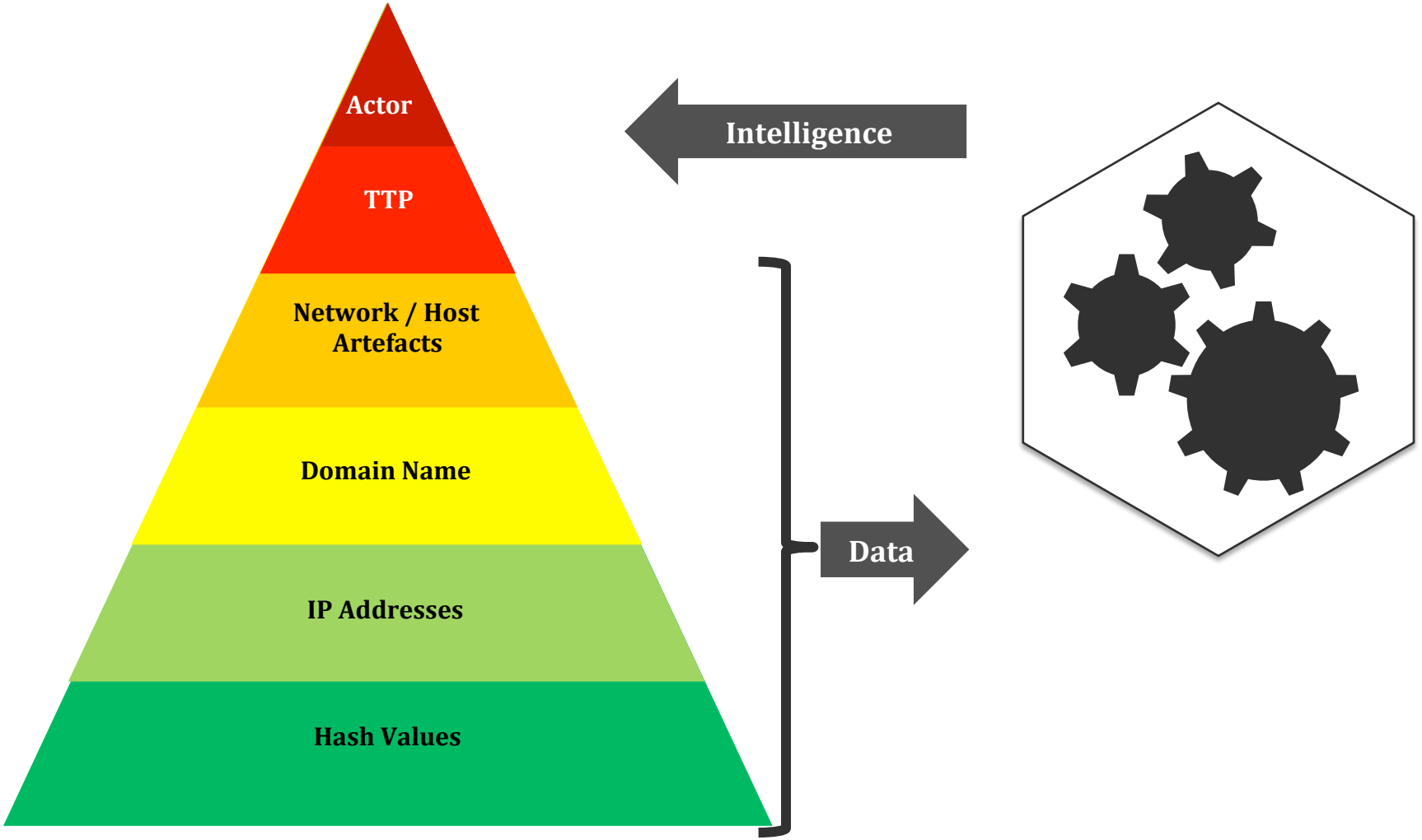
II. Cyber Threat Intelligence



II. Cyber Threat Intelligence

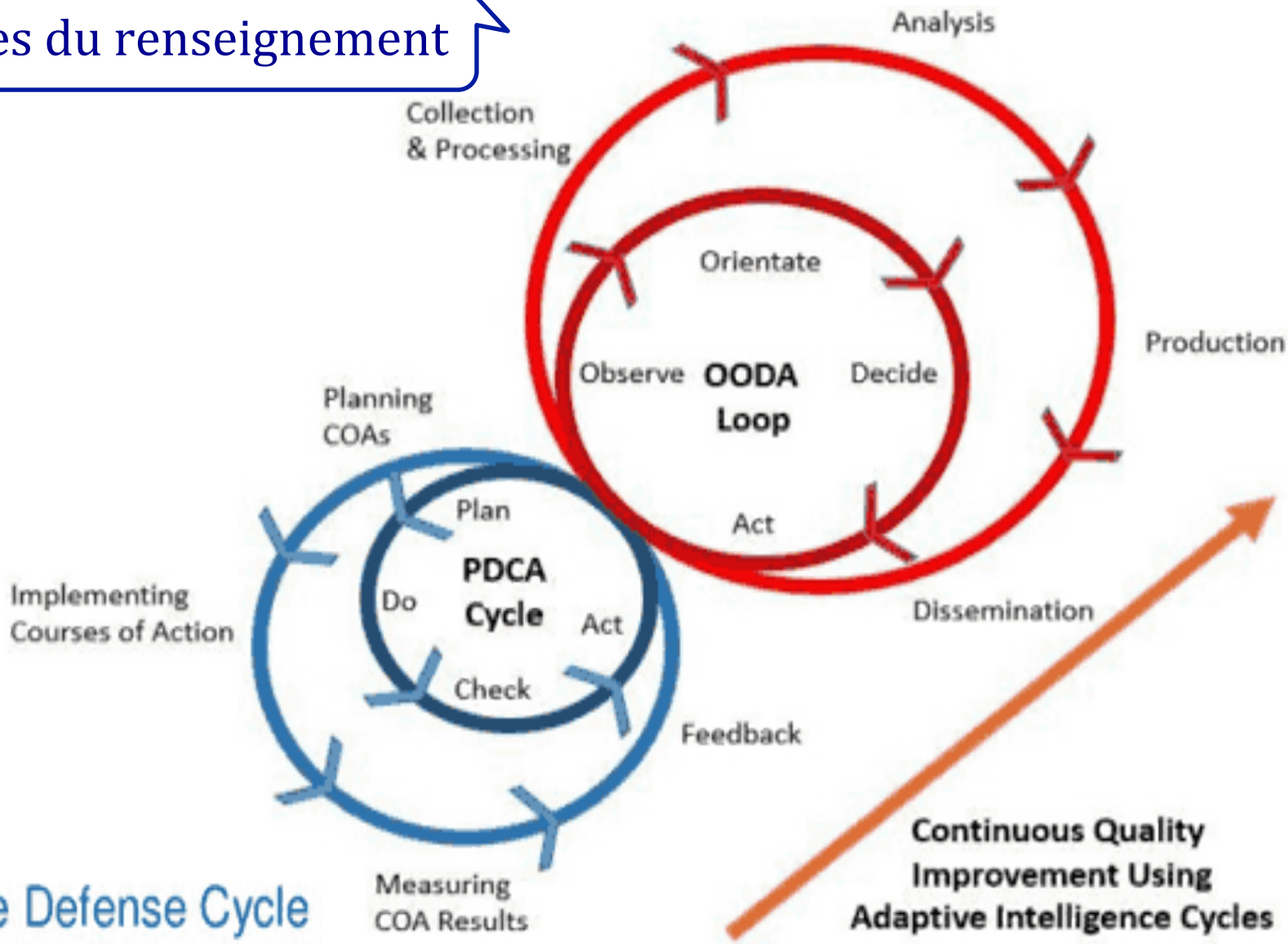


II. Cyber Threat Intelligence

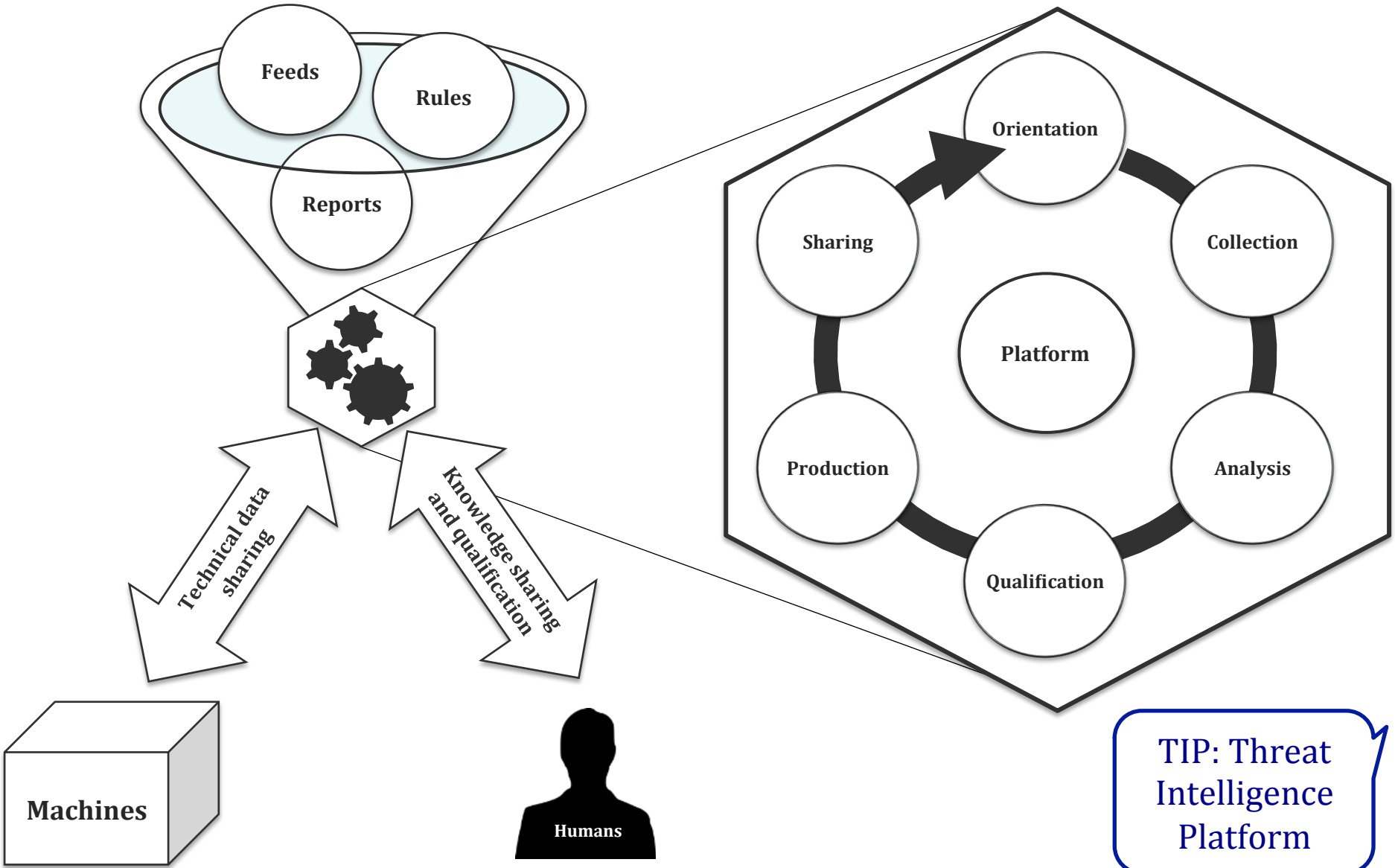


II. Cyber Threat Intelligence

Cycles du renseignement



II. Cyber Threat Intelligence



TIP: Threat Intelligence Platform

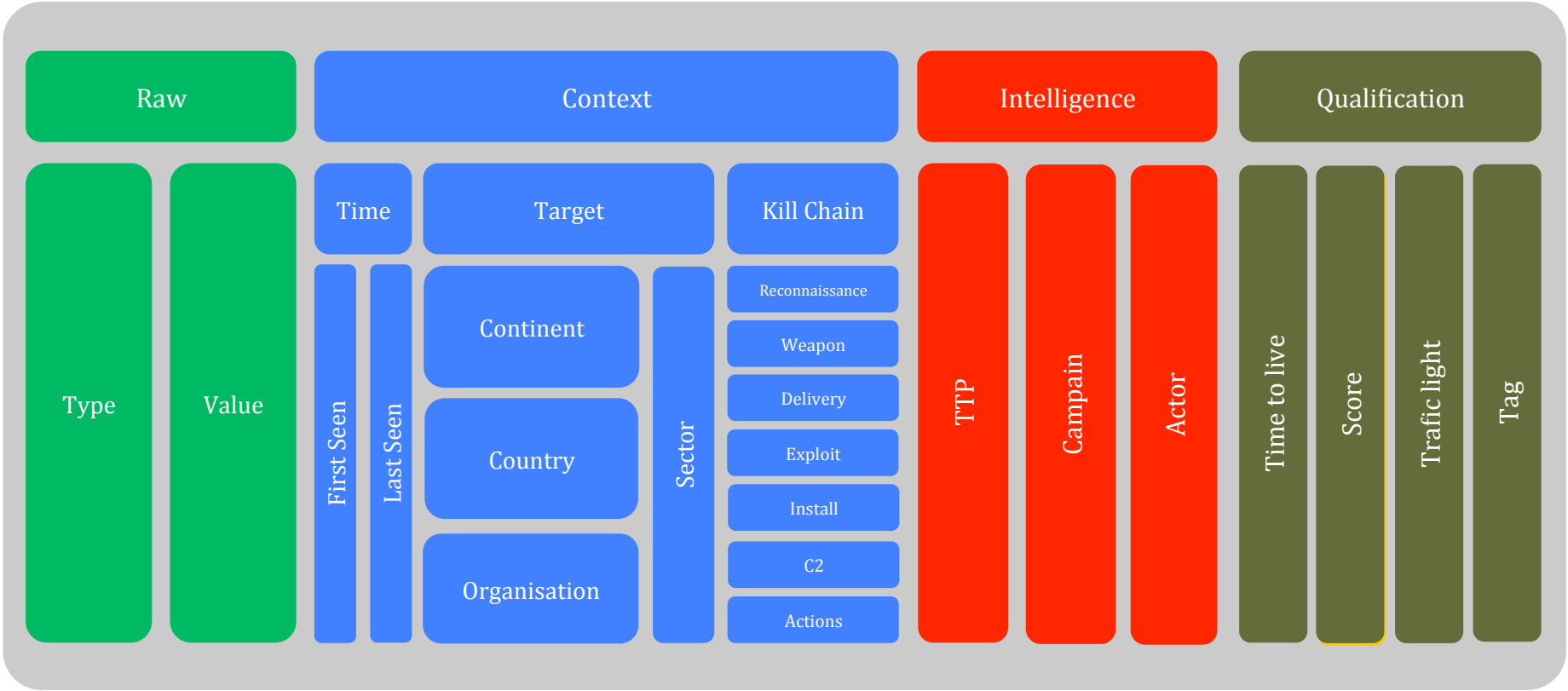
II. Cyber Threat Intelligence

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 :



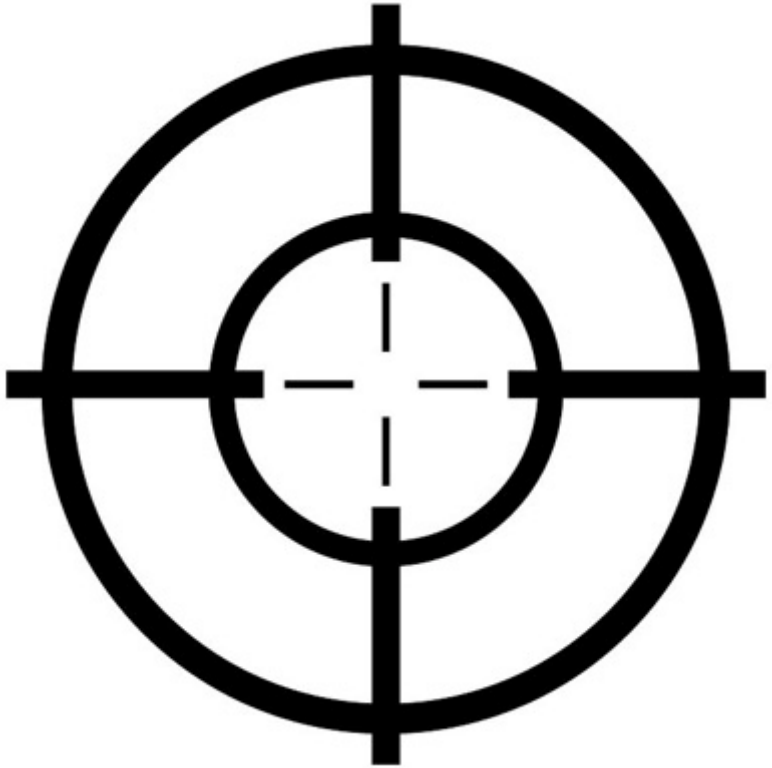
Base de travail essentielle

II. Cyber Threat Intelligence

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

- ✓ Type d'acteur (étatique/privé)
- ✓ Renommée des sources
- ✓ Contexte géopolitique
- ✓ Situation économique
- ✓ Zone géographique
- ✓ Secteur d'activité
- ✓ Incidents
- ✓ Coûts
- ✓ …

Orientation



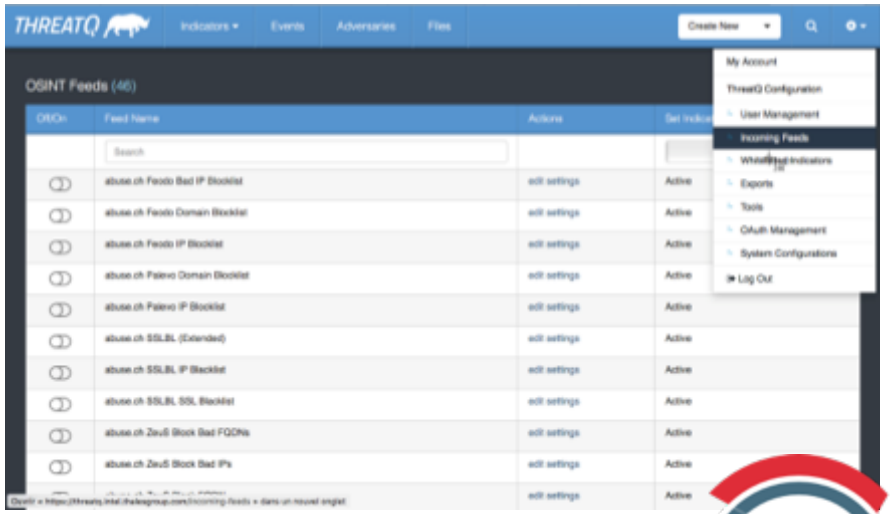
PIR : Priority Intelligence Requirements

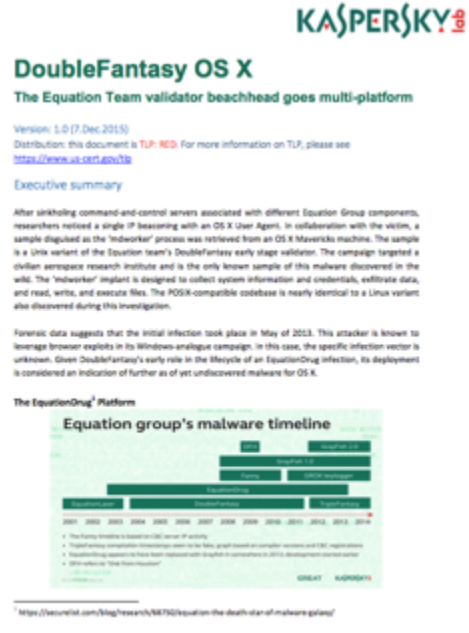
II. Cyber Threat Intelligence

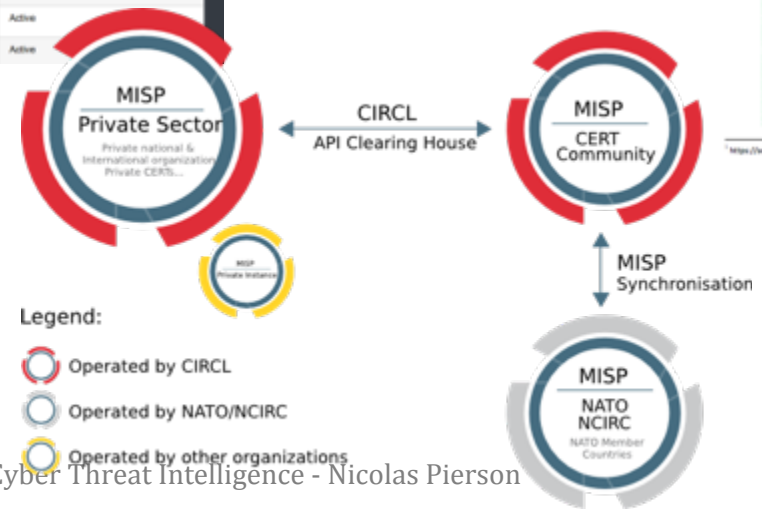
Collecte

Automatique
(Feeds, rapports, connecteurs)

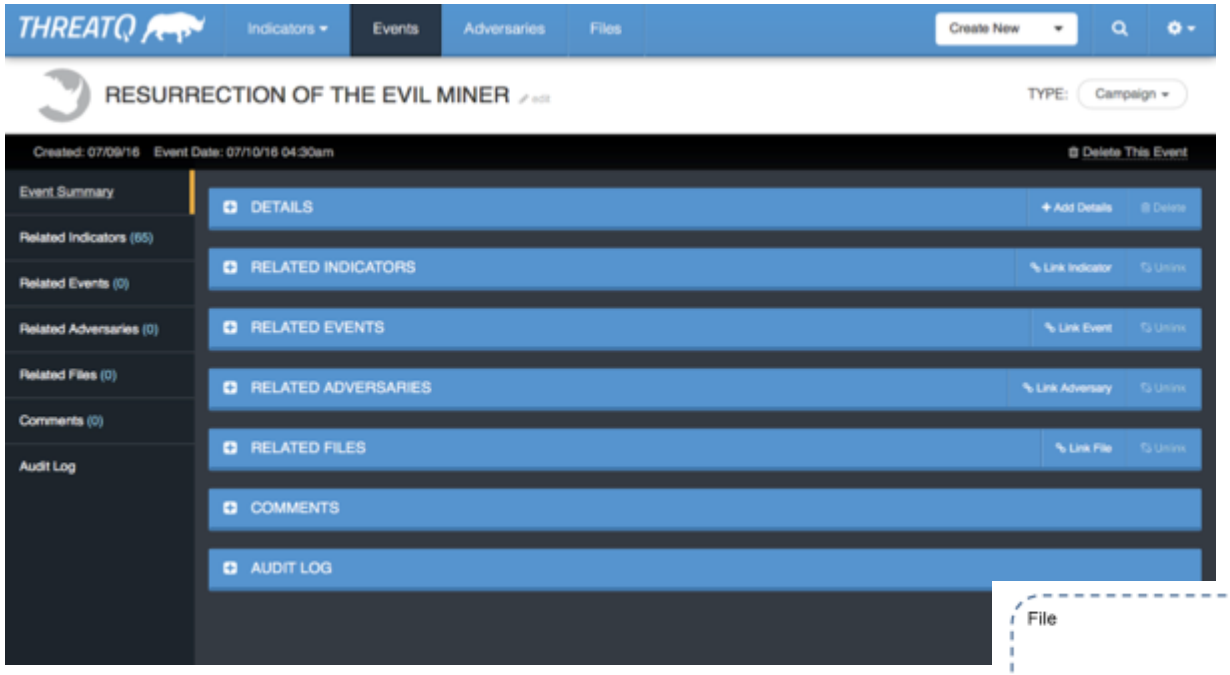
Manuelle
(rapport incident, mail, pdf, doc, csv…)



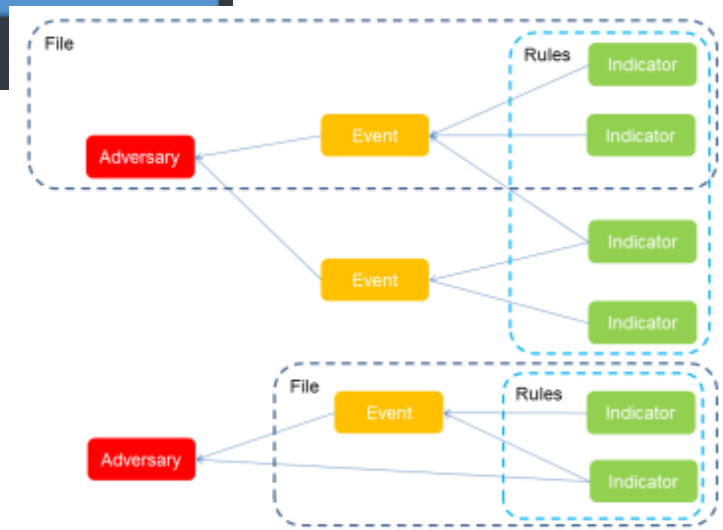




II. Cyber Threat Intelligence

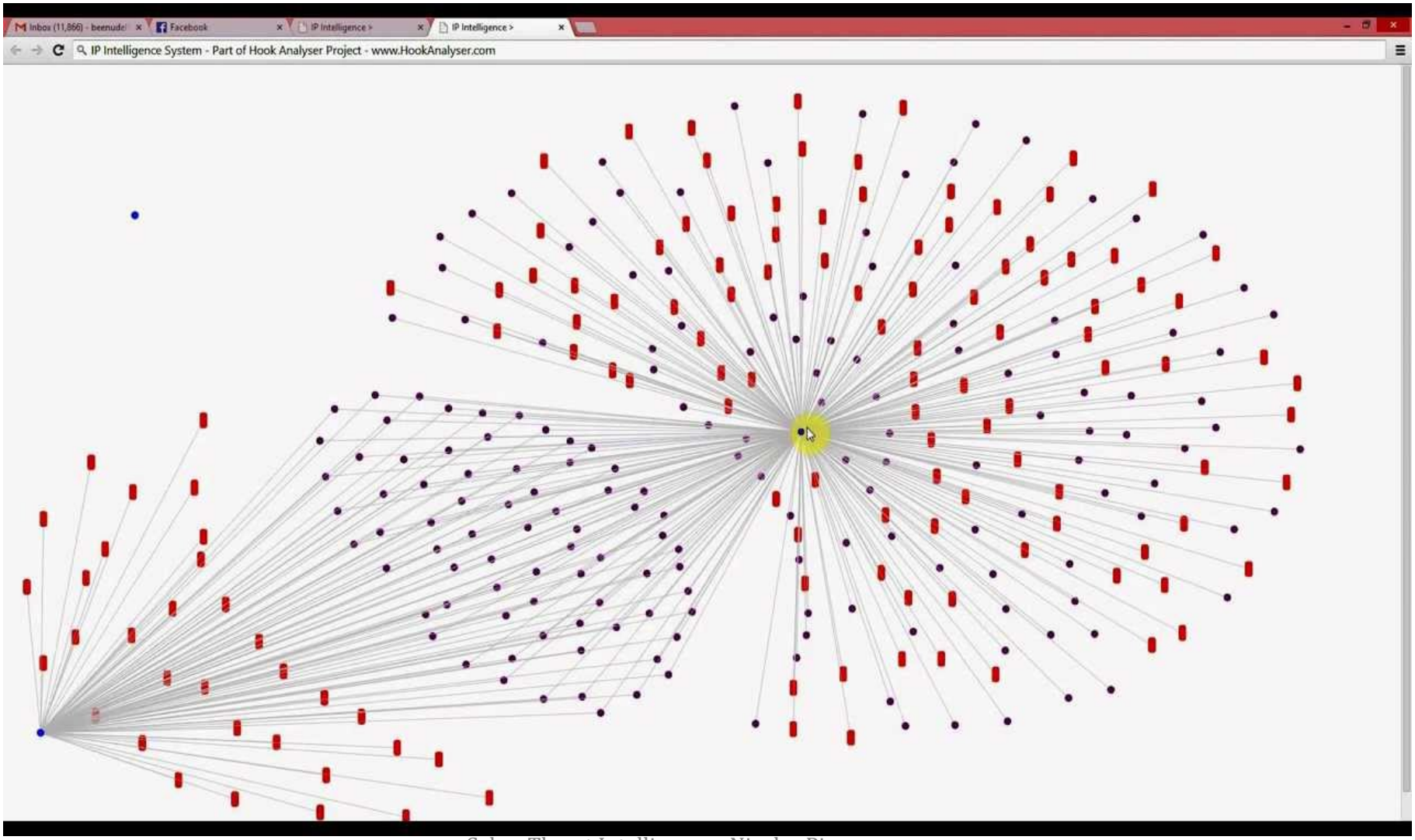


Analyse



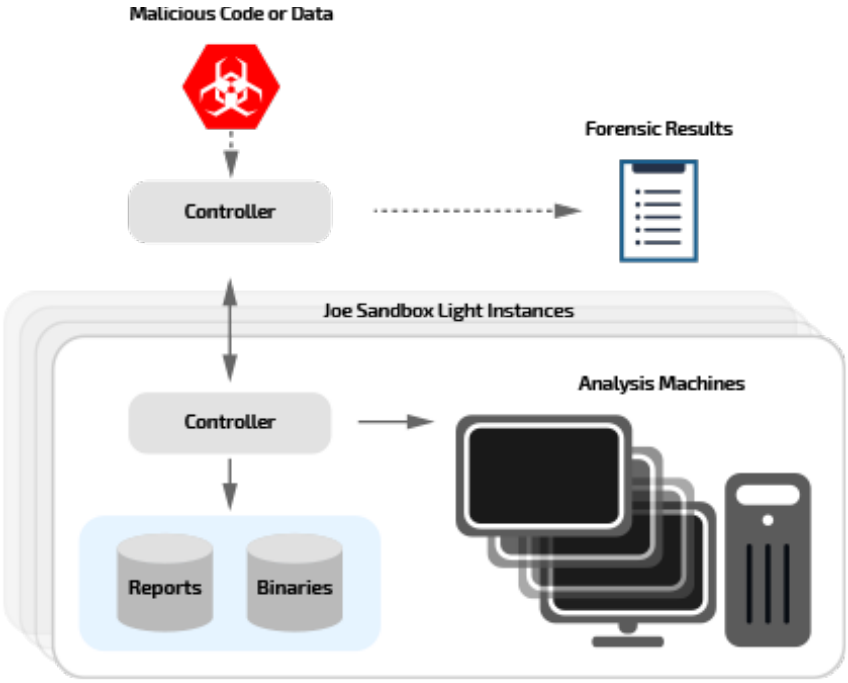
II. Cyber Threat Intelligence

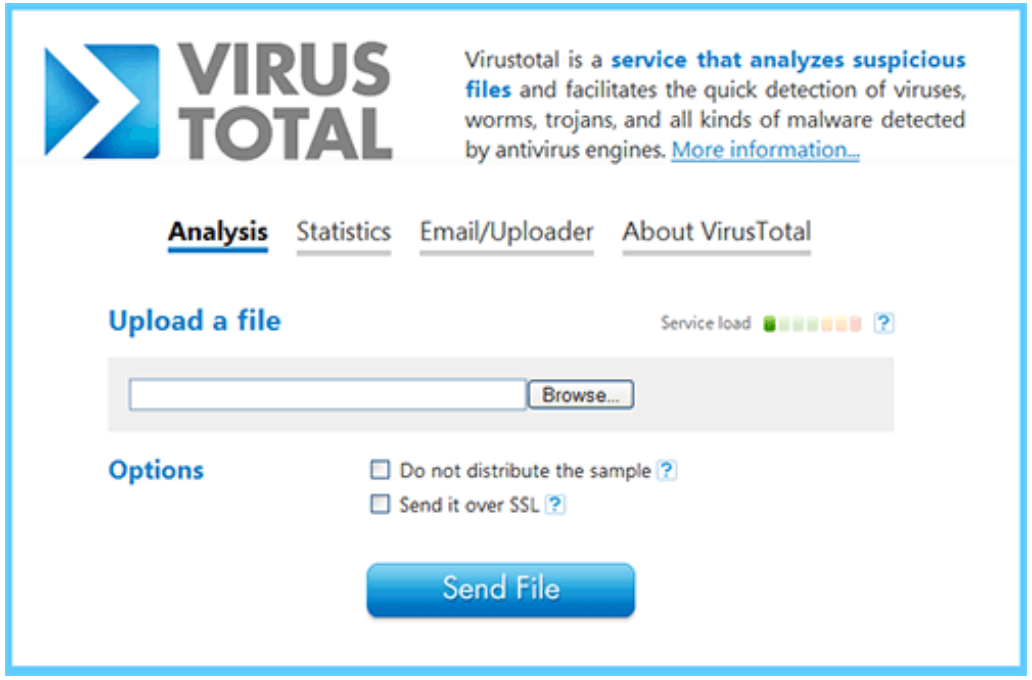
Analyse



II. Cyber Threat Intelligence

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





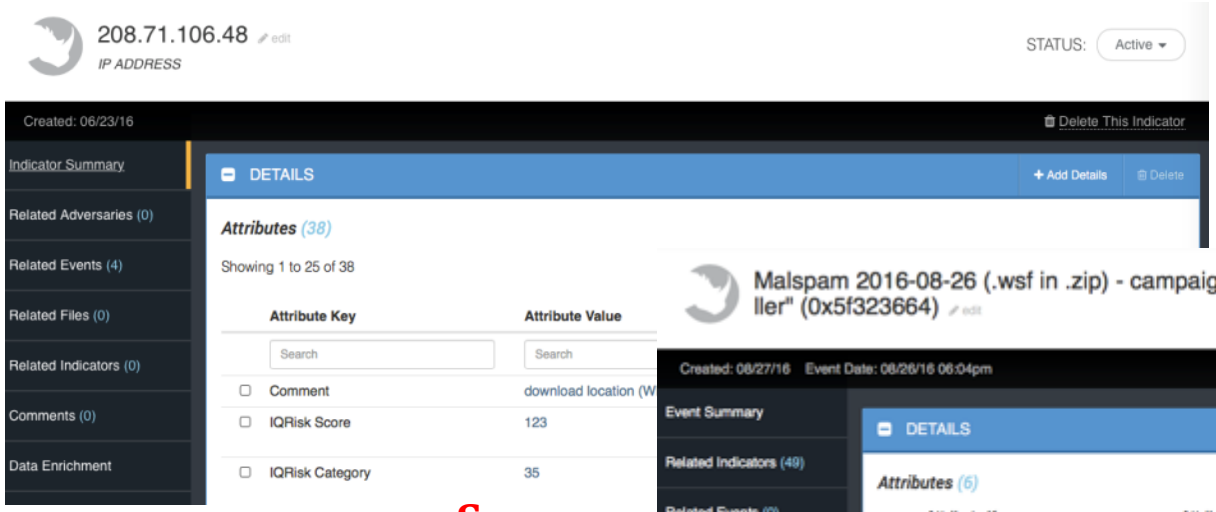
Analyse

II. Cyber Threat Intelligence

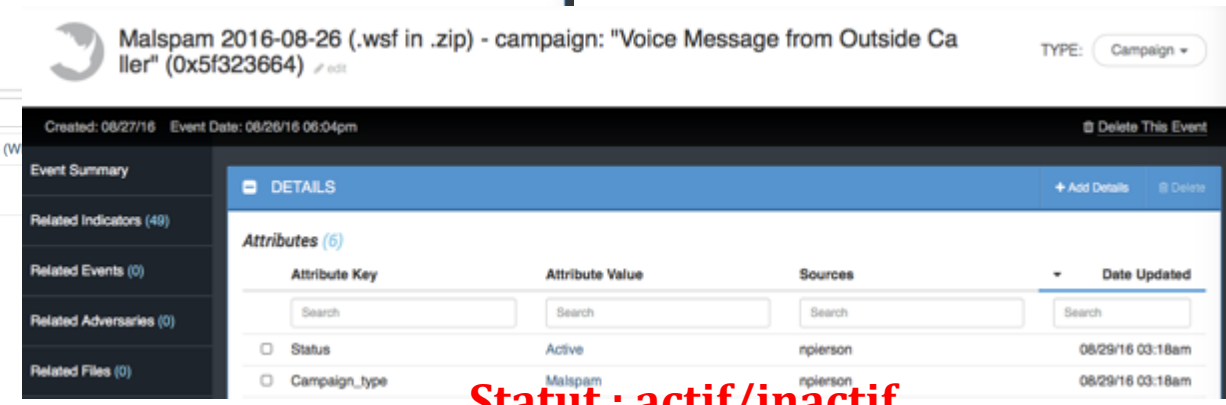
Qualifier pour :

- ✓ 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

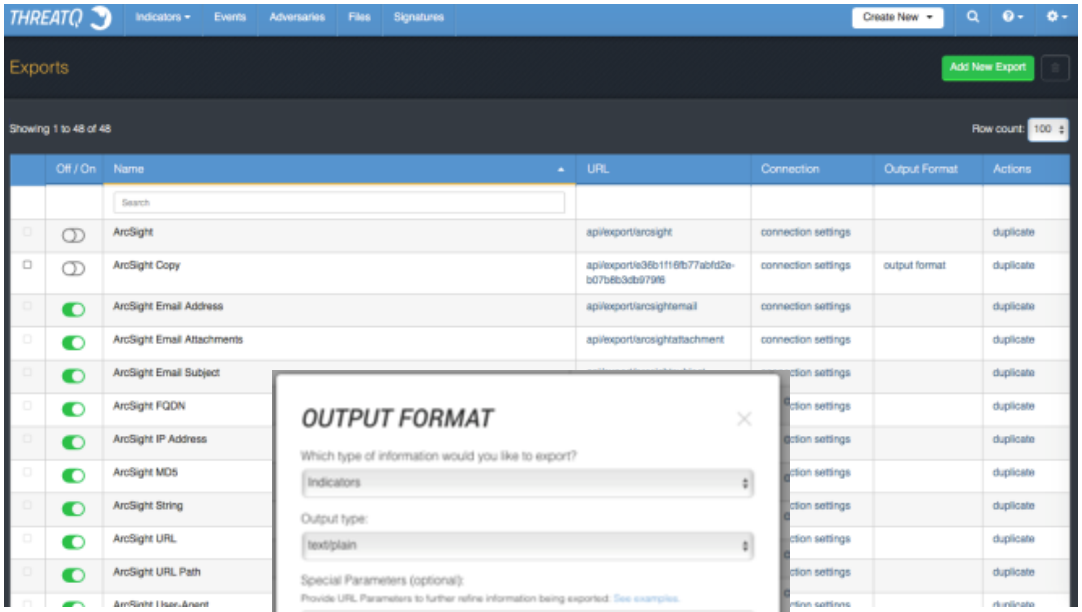


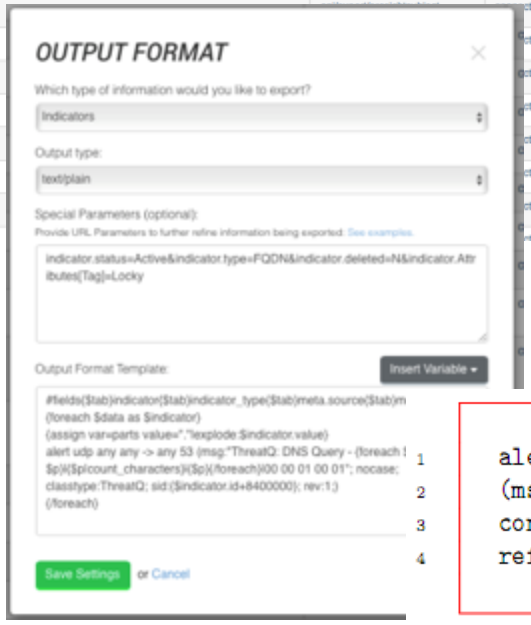
Statut : actif/inactif

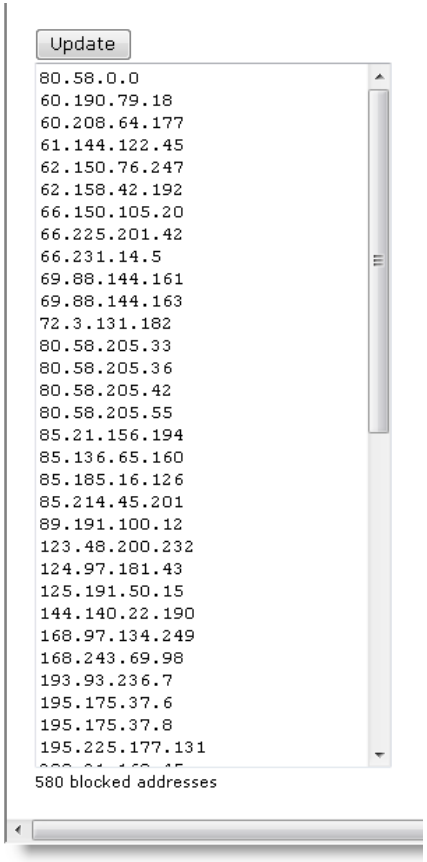
II. Cyber Threat Intelligence

Production

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

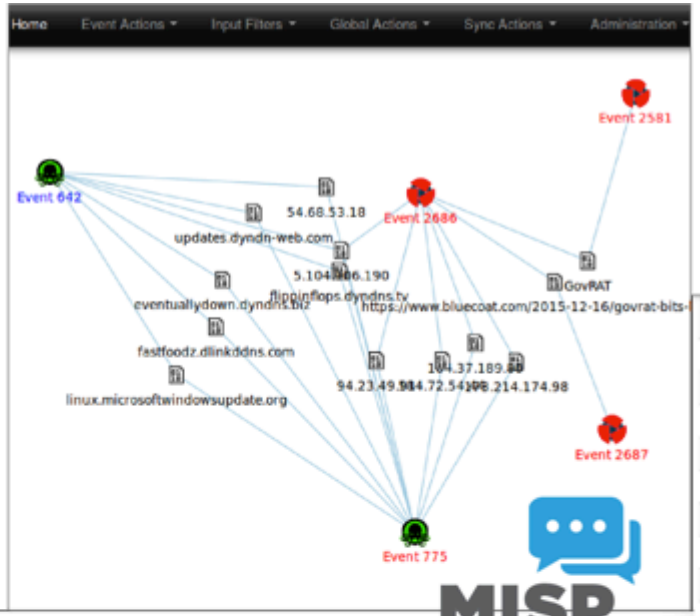







```
alert tcp $EXTERNAL_NET any -> $HOME_NET 6000
(msg:"X11 MIT Magic Cookie detected"; flow:established;
content:"MIT-MAGIC-COOKIE-1";
reference:arachnids,396; classtype:attempted-user; sid:1225; rev:4;)
```

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 confidantialité
- ✓ Communautés de confiance

Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Apports de la science des données à la cyberdéfense

III. Apports de la science des données

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

Threat Intelligence

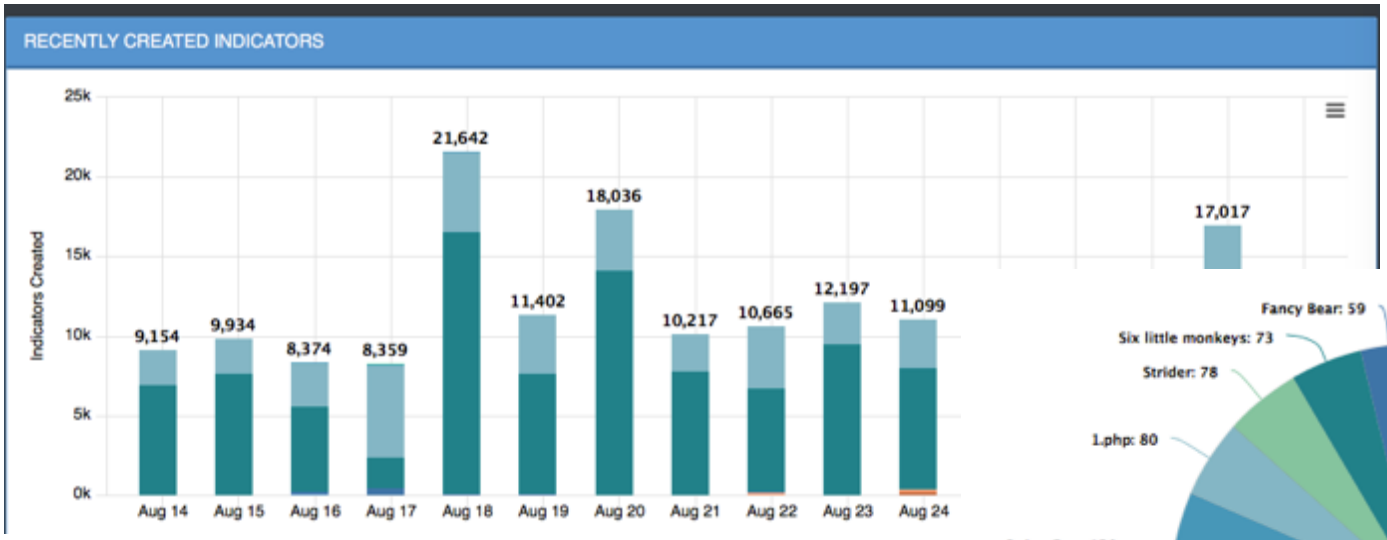
Mais aussi :

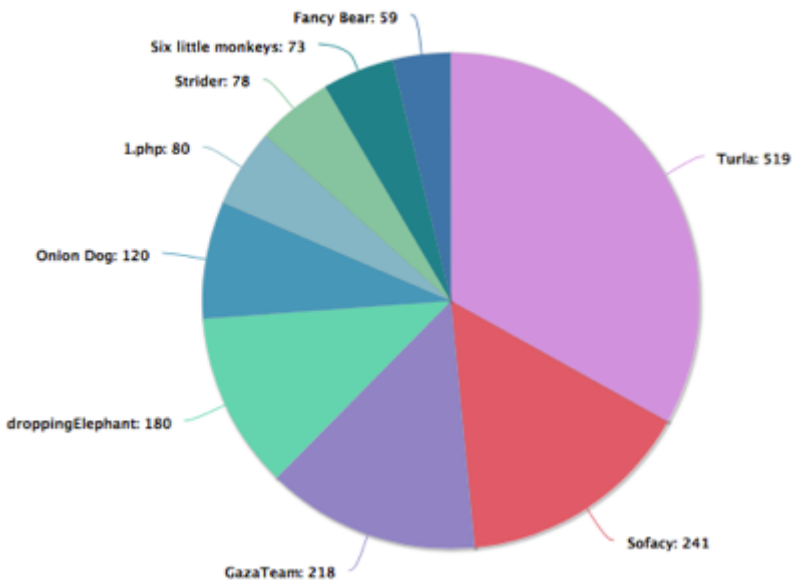
- ✓ Corrélation
- ✓ Détection
- ✓ Analyse comportementale
- ✓ Recherche de signaux faibles

Cyberdéfense

III. Apports de la science des données

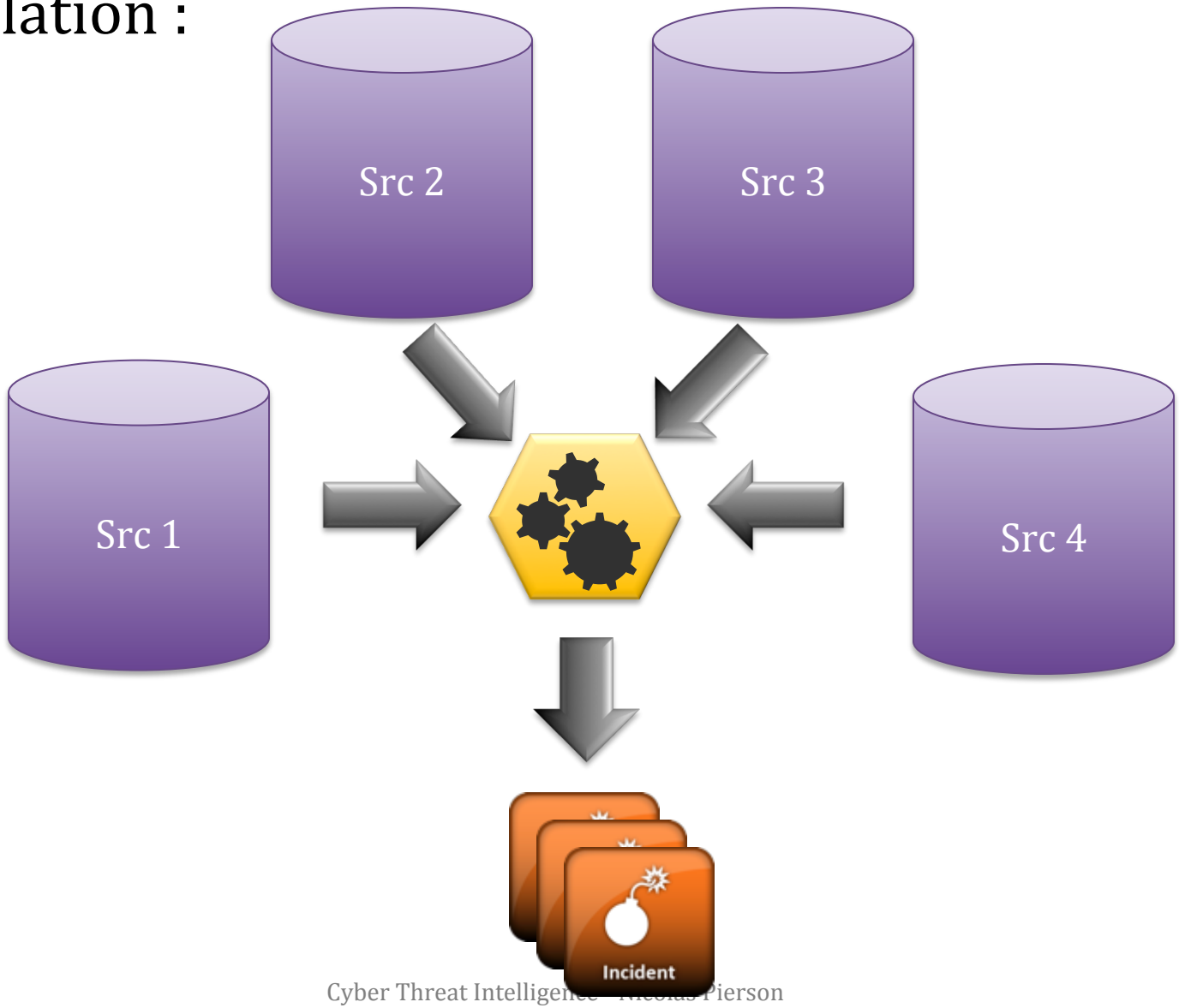
Collecte, stockage, gestion dans le temps, manipulation, recherche et visualisation des indicateurs :





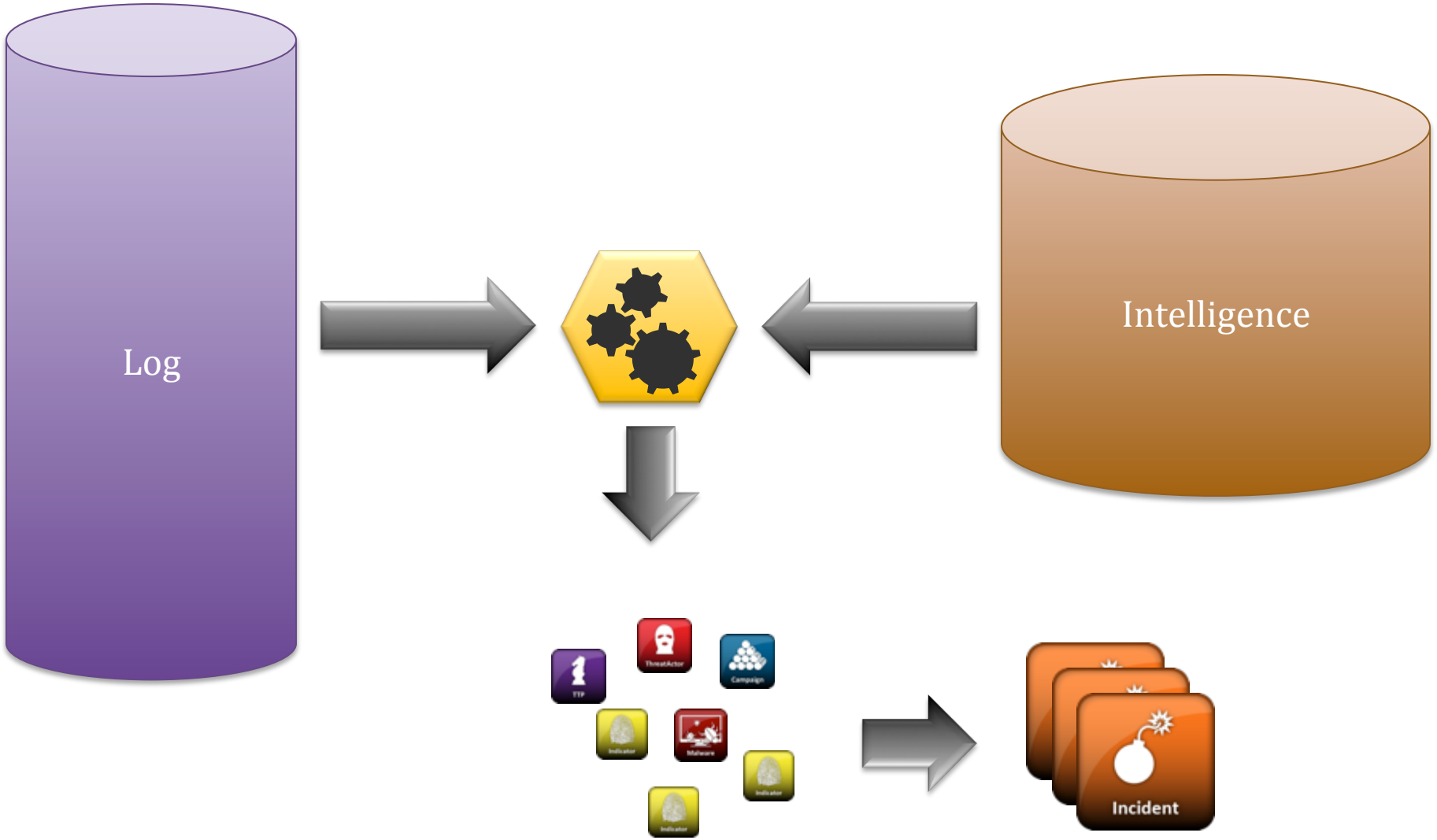
III. Apports de la science des données

Correlation :



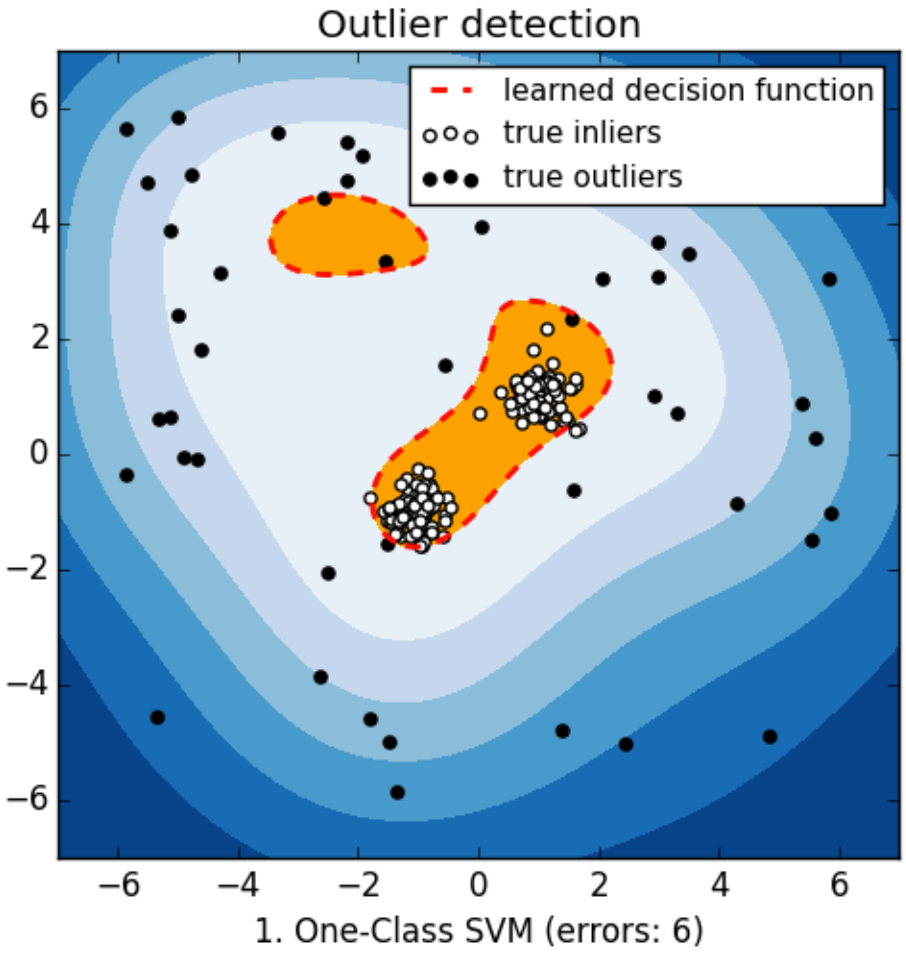
III. Apports de la science des données

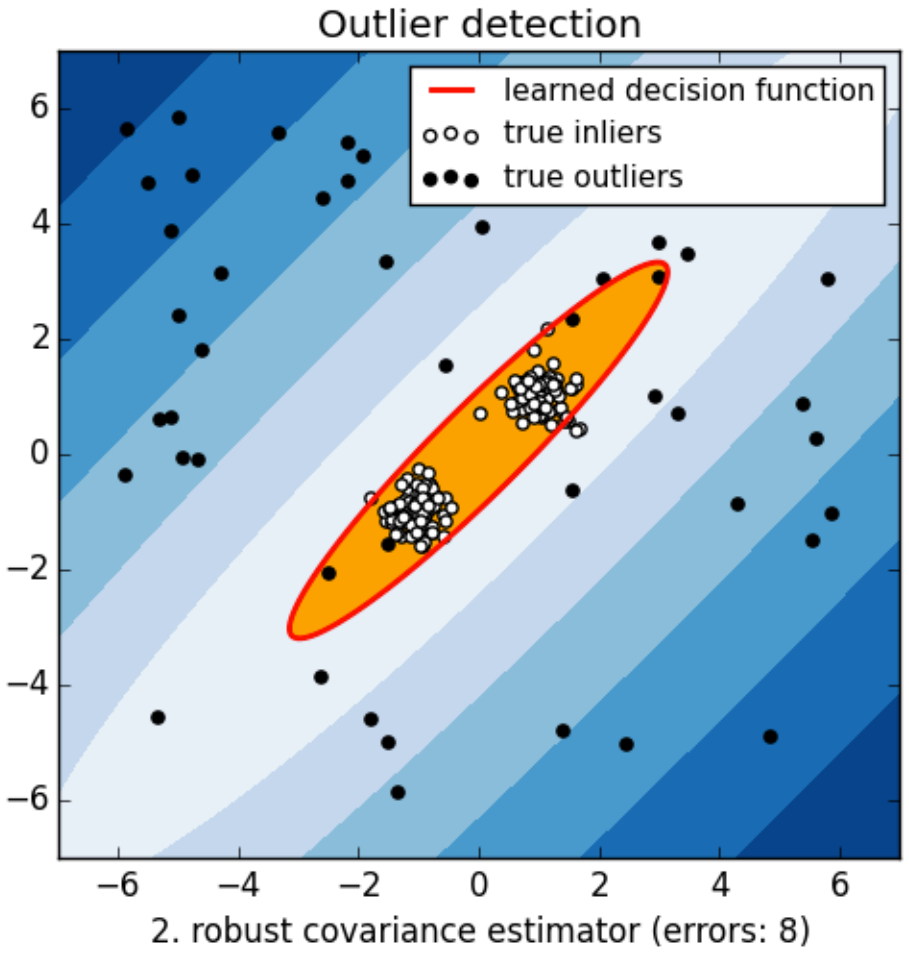
Recherche/hunting :



III. Apports de la science des données

Analyse comportementale :





III. Apports de la science des données

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. Apports de la science des données

Perspectives :

- ✓ Intelligence artificielle
- ✓ Cyberdéfense prédictive

III. Apports de la science des données

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

- ✓ ART :
  - Accurate
  - Reliable
  - Timely

- ✓ Data scientist = ressource rare et chère

- ✓ Cybersecurity specialist = ressource rare et chère

- ✓ Data & Cybersecurity specialist = ressource très rare et très chère

TP du 8 mars de 8h30 à 11h45

Objectif :

Mener à l'aide de Splunk ou ELK une investigation numérique par étape pour comprendre et contrer une attaque.

Réalisation :

- Par Binôme
- Livrable pdf à rendre
- Restitution de deux binômes en fin de séance
- Utilisation de Splunk (Mise à disposition) ou autre outils (ex: ELK, à installer par les élèves)

Contact : nicolas.pierson@for-cyb.com

Engagez vous !

Contact recrutement : cyber.contact@defense.gouv.fr
Contact réserve : rcd@defense.gouv.fr