

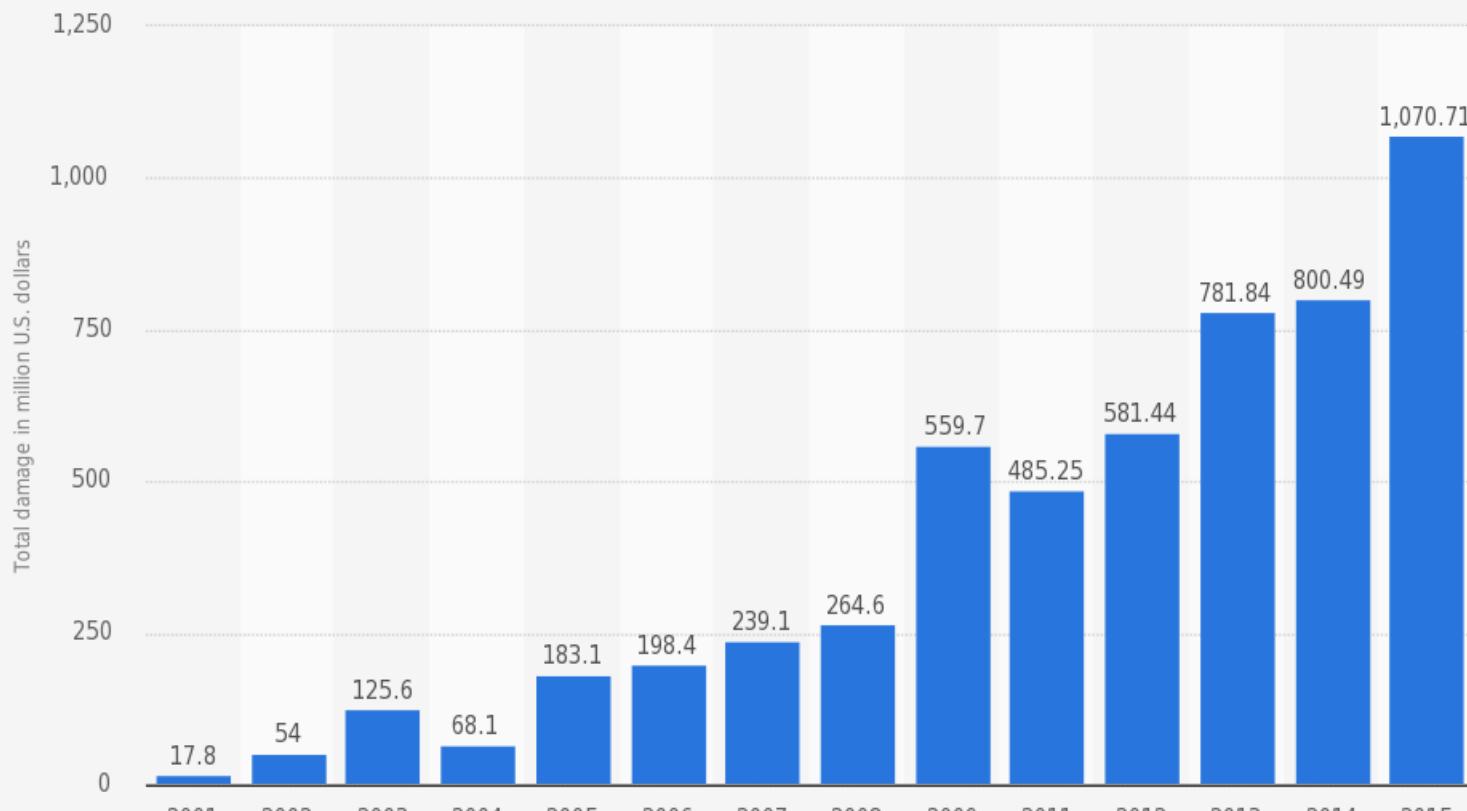
Cyberdéfense et Big Data : La Cyber Threat Intelligence



Nicolas Pierson

Introduction

Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2015 (in million U.S. dollars)



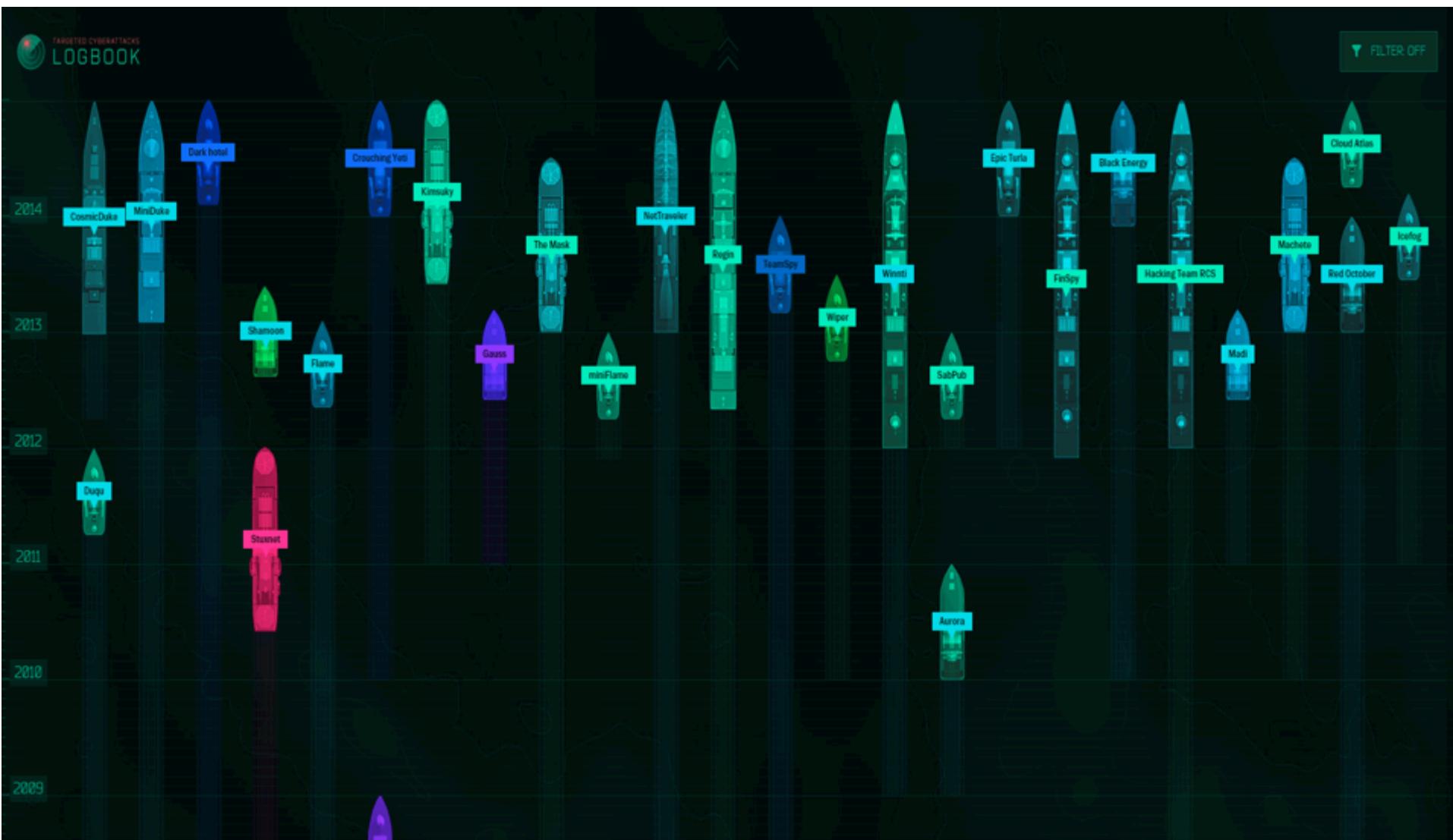
Sources:

FBI; IC3; US Department of Justice
© Statista 2016

Additional Information:

Worldwide; IC3; 2001 to 2015, excluding 2010; Cybercrime reported to IC3

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

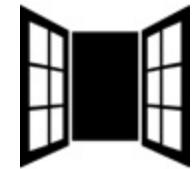
III

- 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) :

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 cyberspace les systèmes d'information jugés essentiels.

Cyberdéfense (=Etatique)

Mesures techniques

Mesures non-techniques

I. Contexte général

La Cybersécurité :

Cybersécurité

SSI
(Cyberprotection)

Cyberrésilience

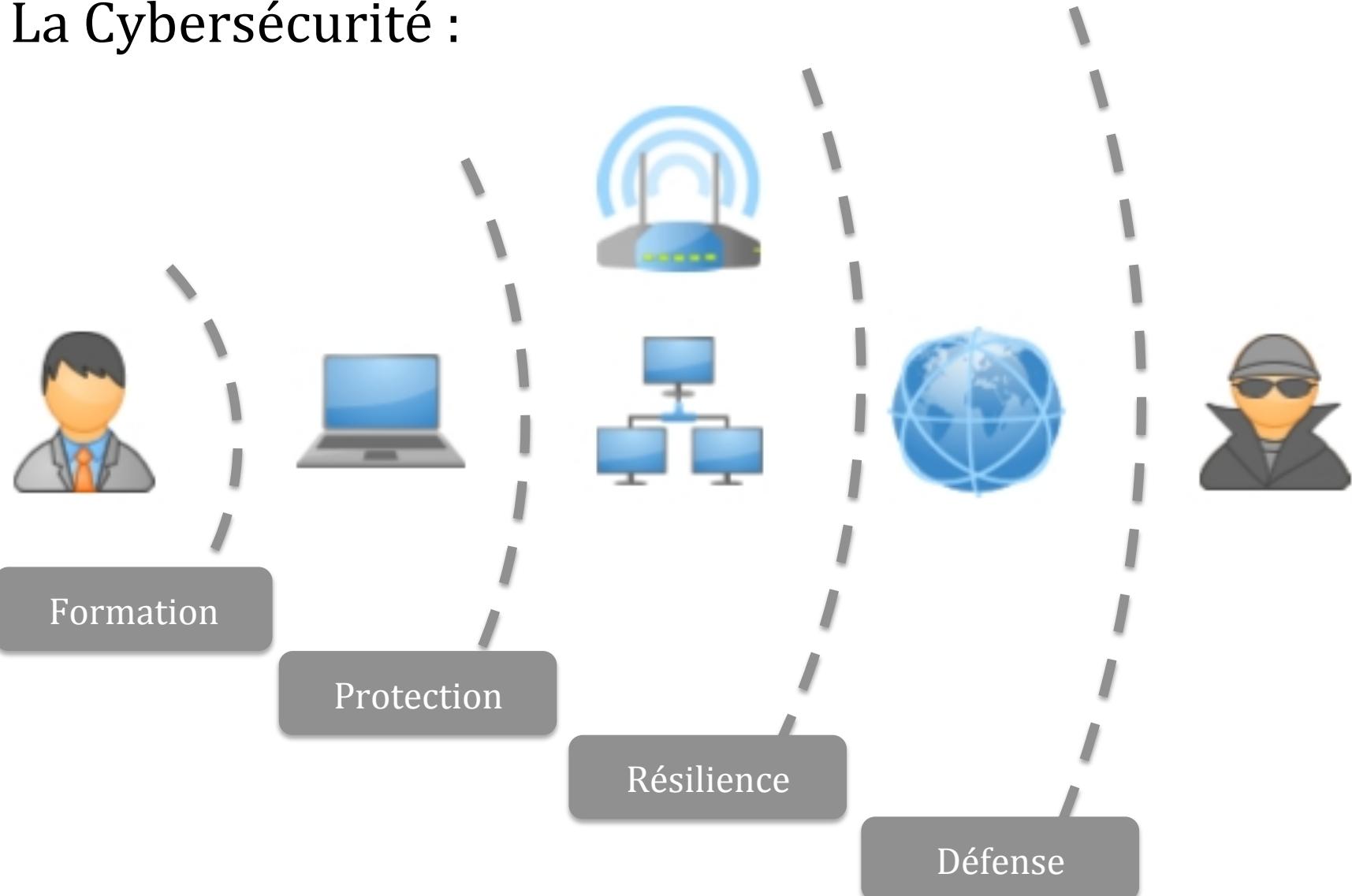
Cyberdéfense
(Lutte
informatique)

Vulnérabilités

Menaces

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

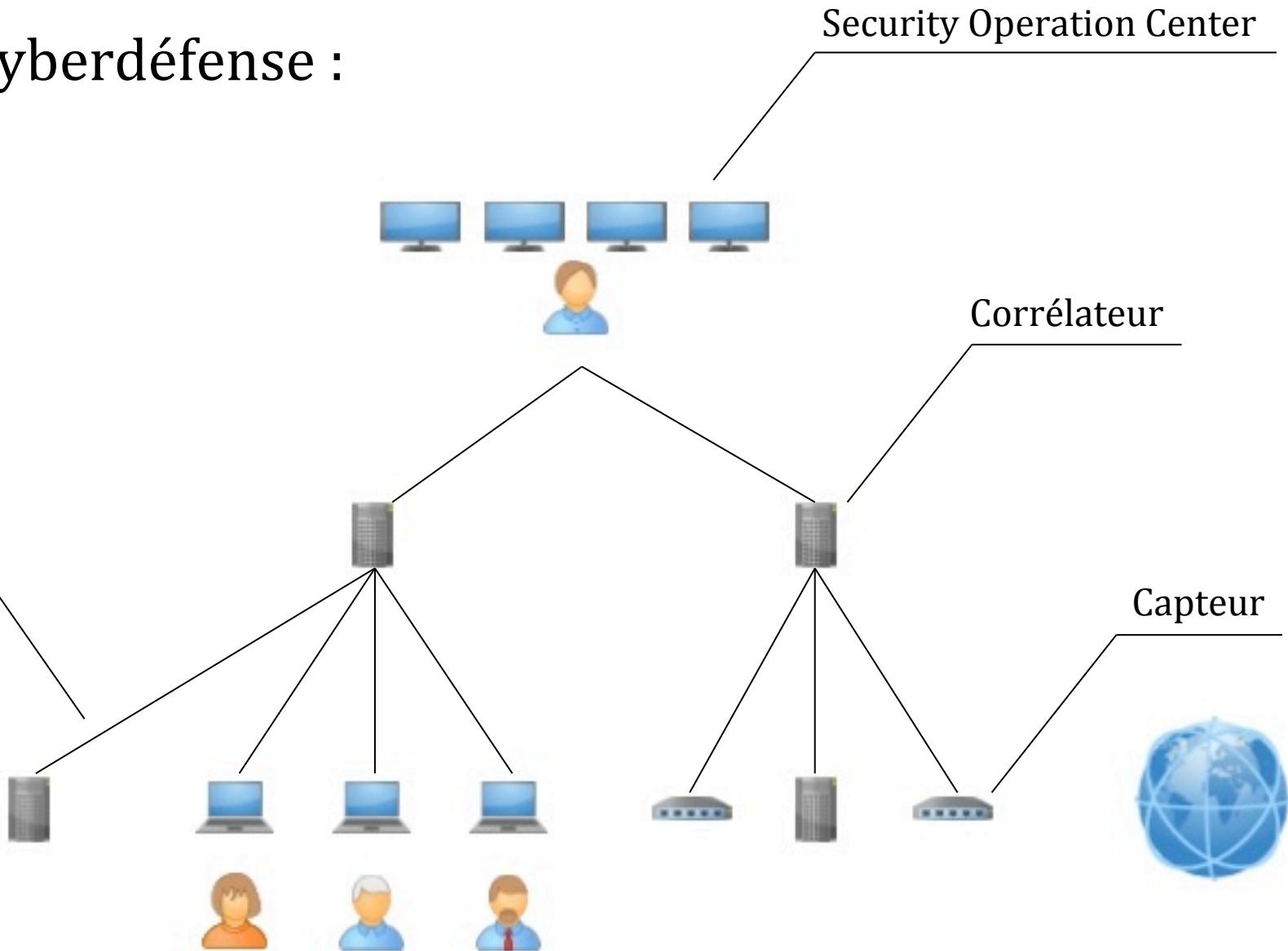
Extrait du référentiel PDIS de l'ANSSI :

« 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. »**

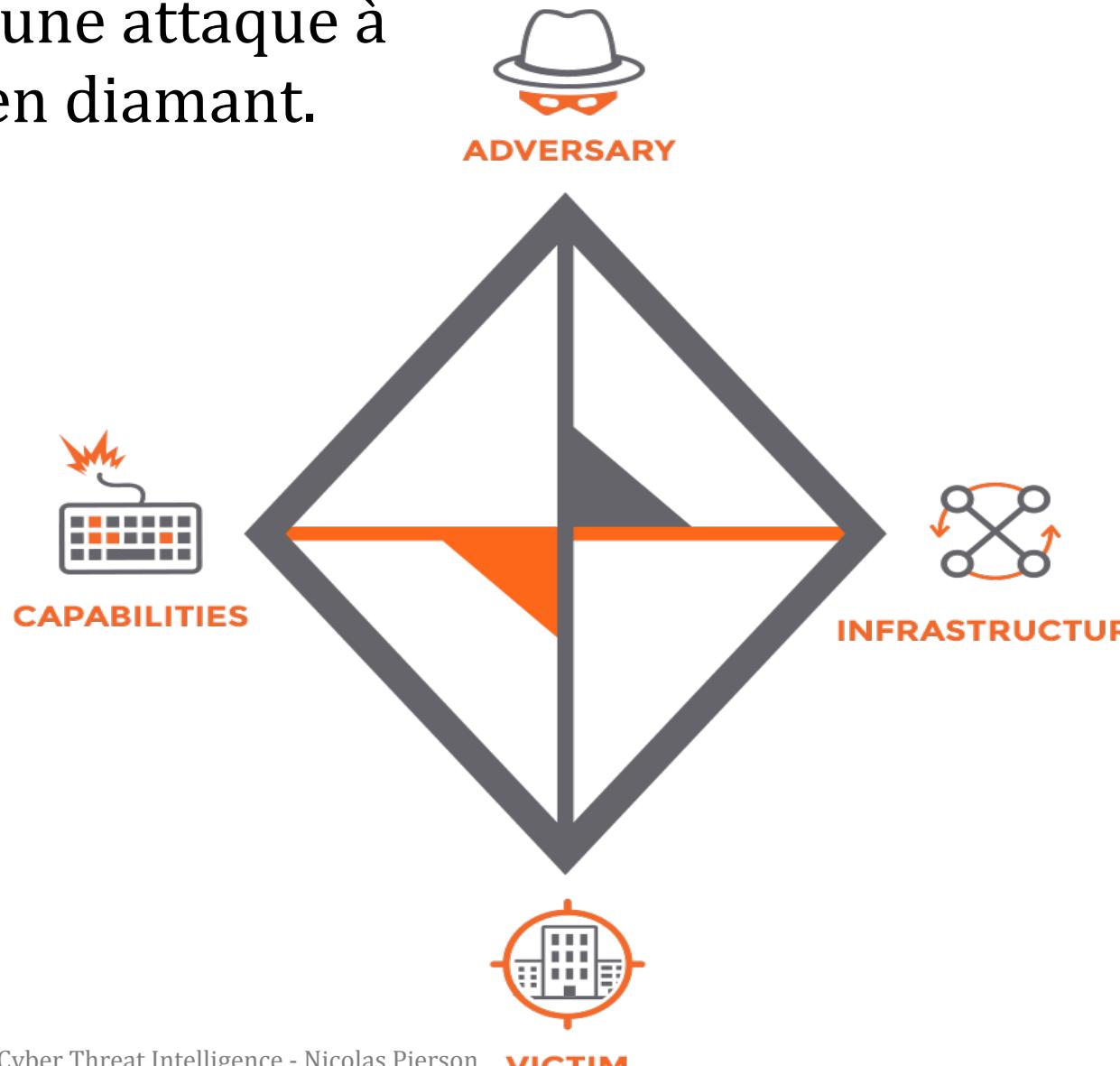
I. Contexte général

Cyberdéfense :



I. Contexte général

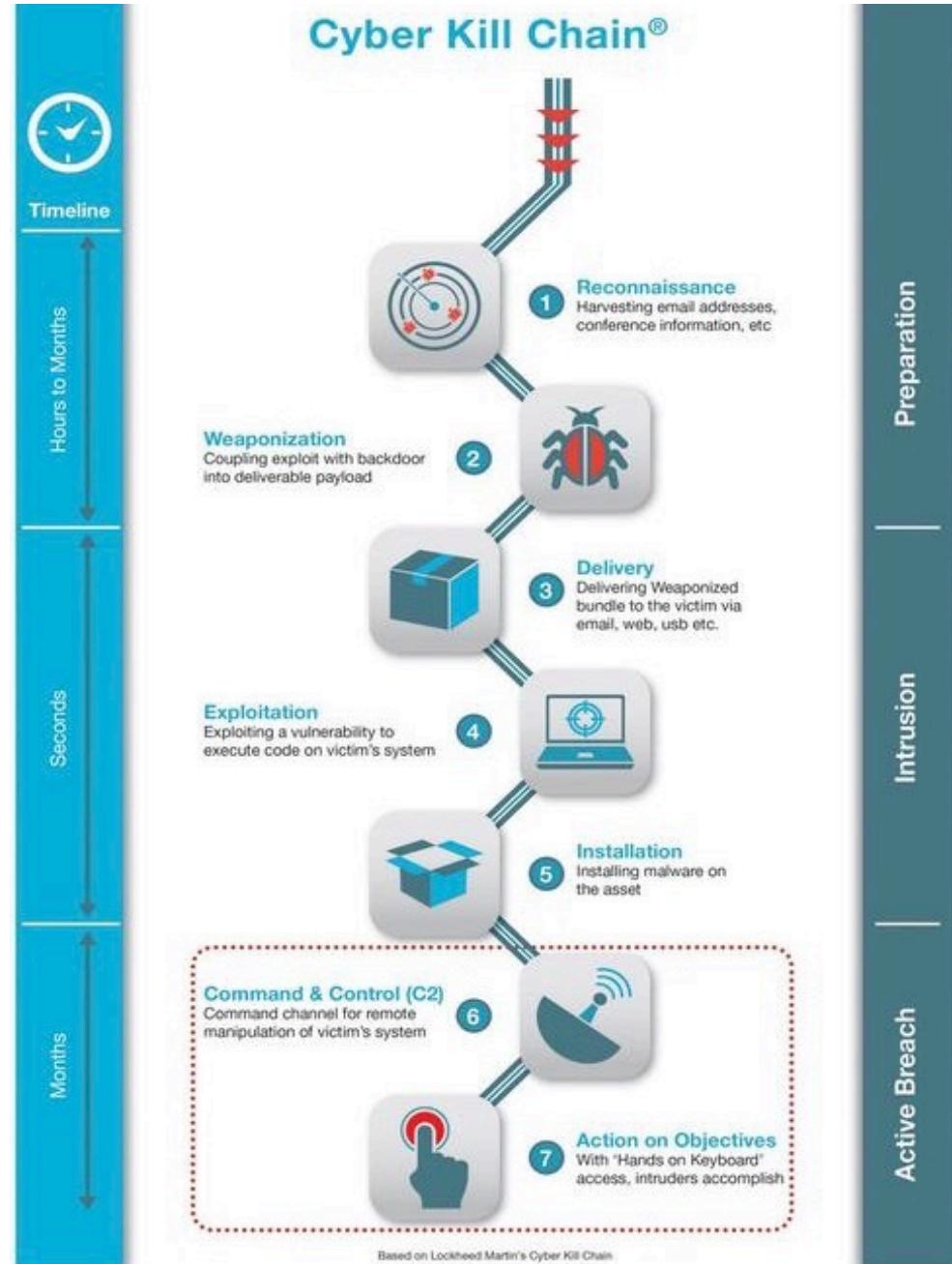
Caractérisation d'une attaque à l'aide du modèle en diamant.



I. Contexte général

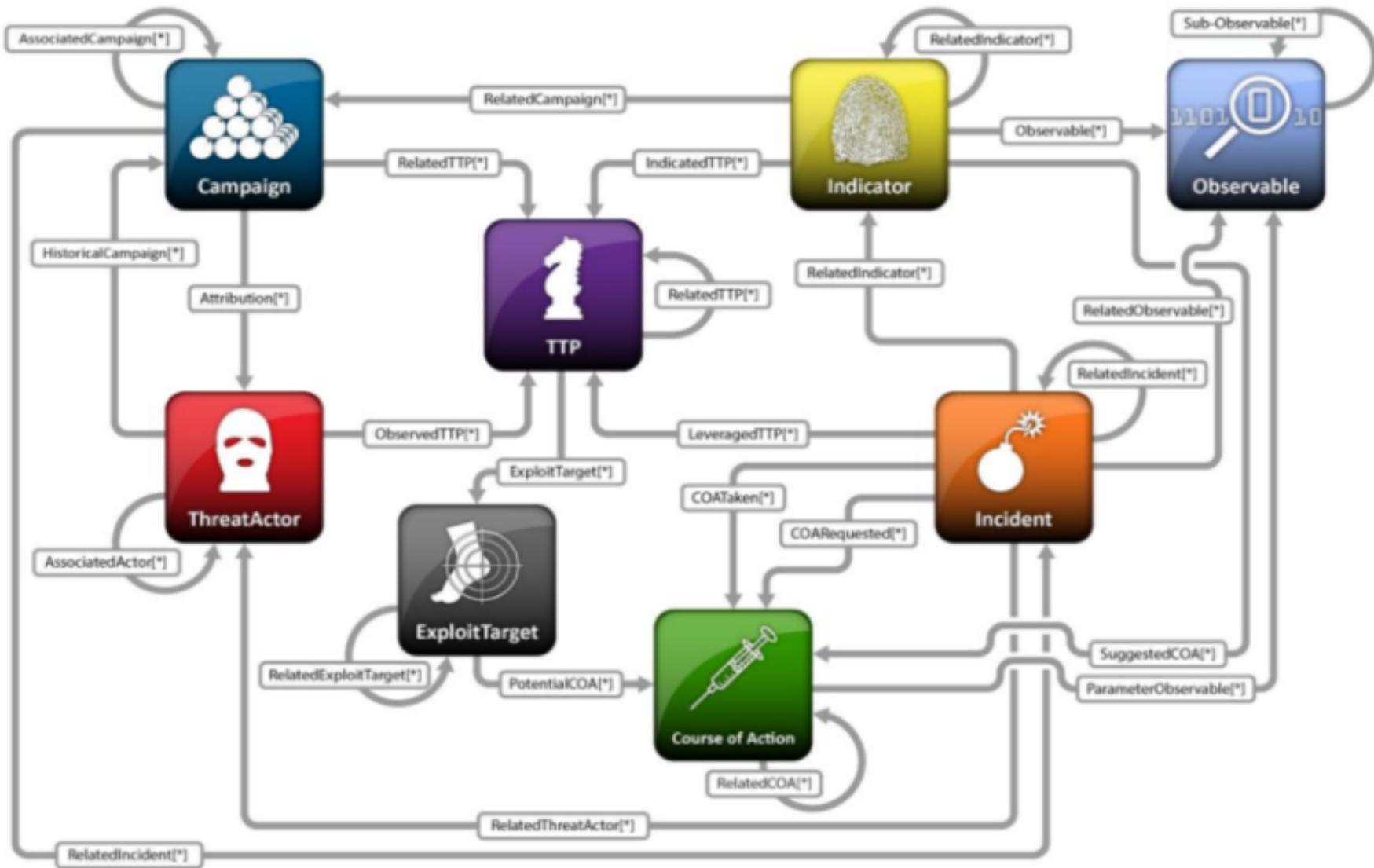
Cyber Kill Chain :

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

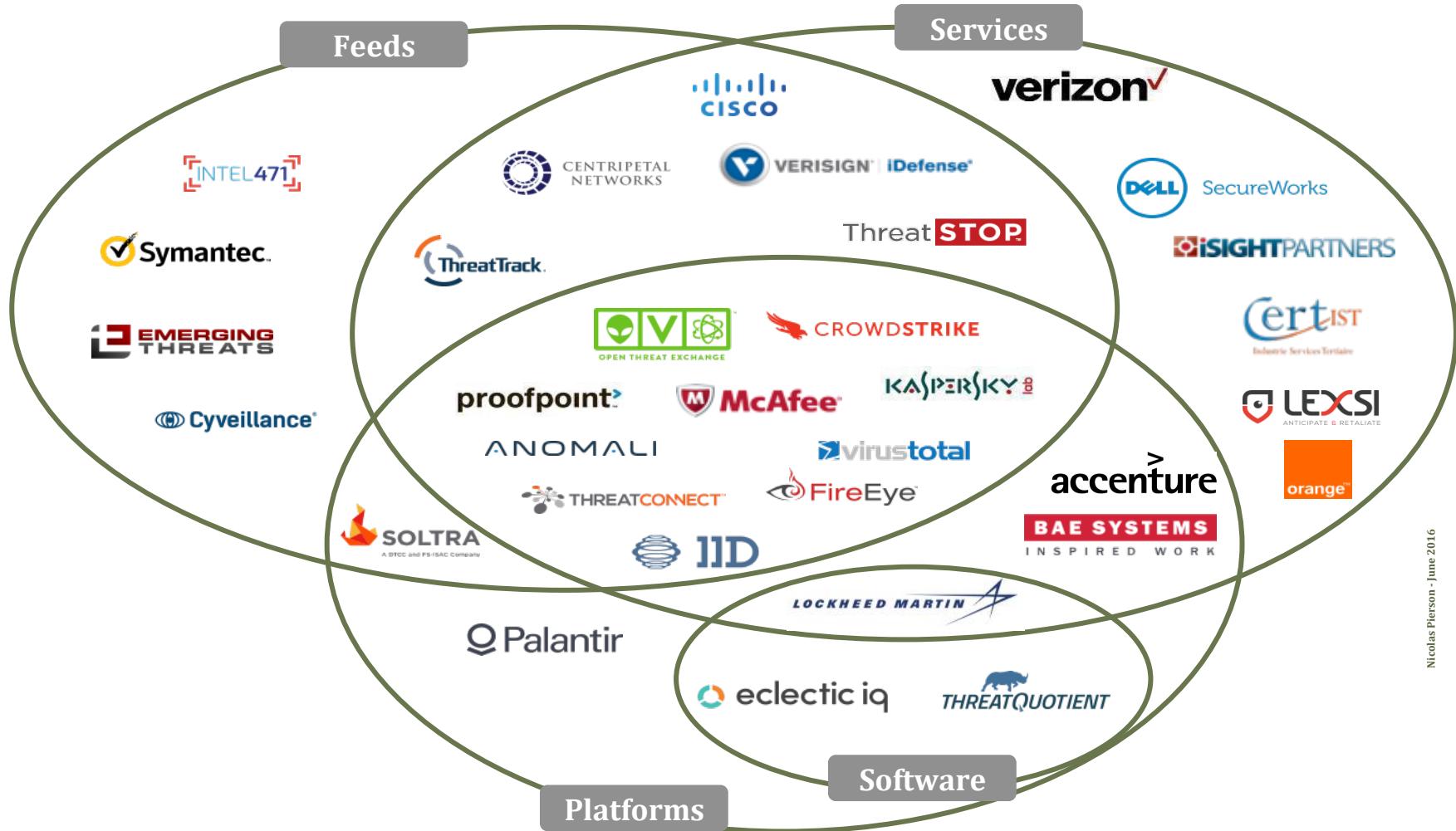


I. Contexte général

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

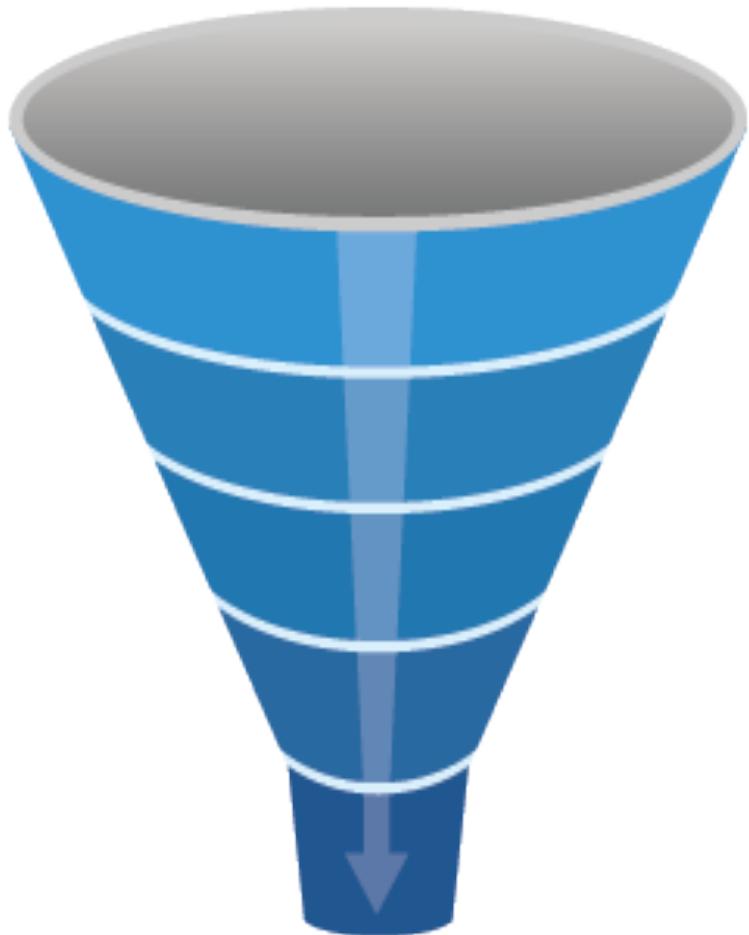
Définition de la Threat Intelligence :

Ensemble des informations et des actions de renseignement sur les menaces en provenance du cyberspace.

L'objectif de la Threat Intelligence est de connaître 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.

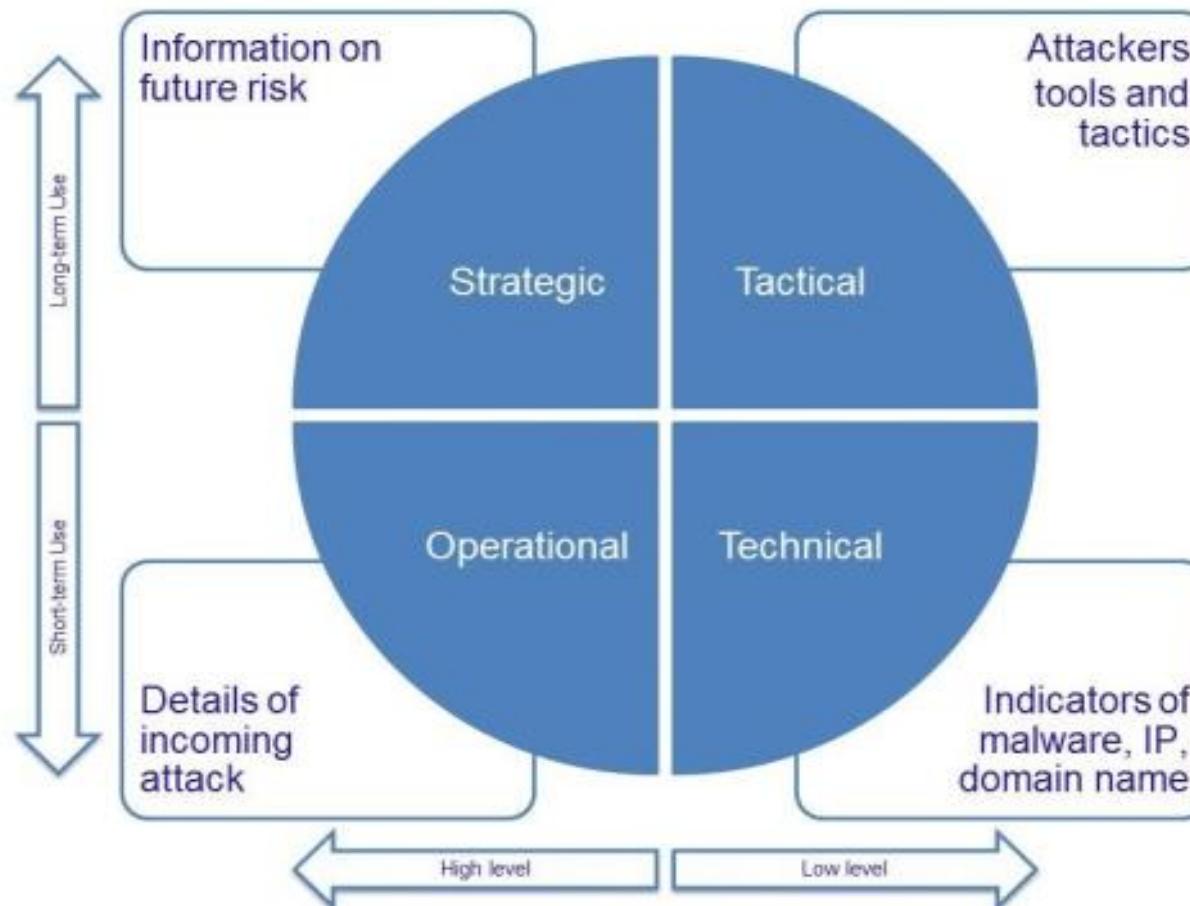
Information is data with a purpose. Once it is assigned a purpose it becomes information.

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?

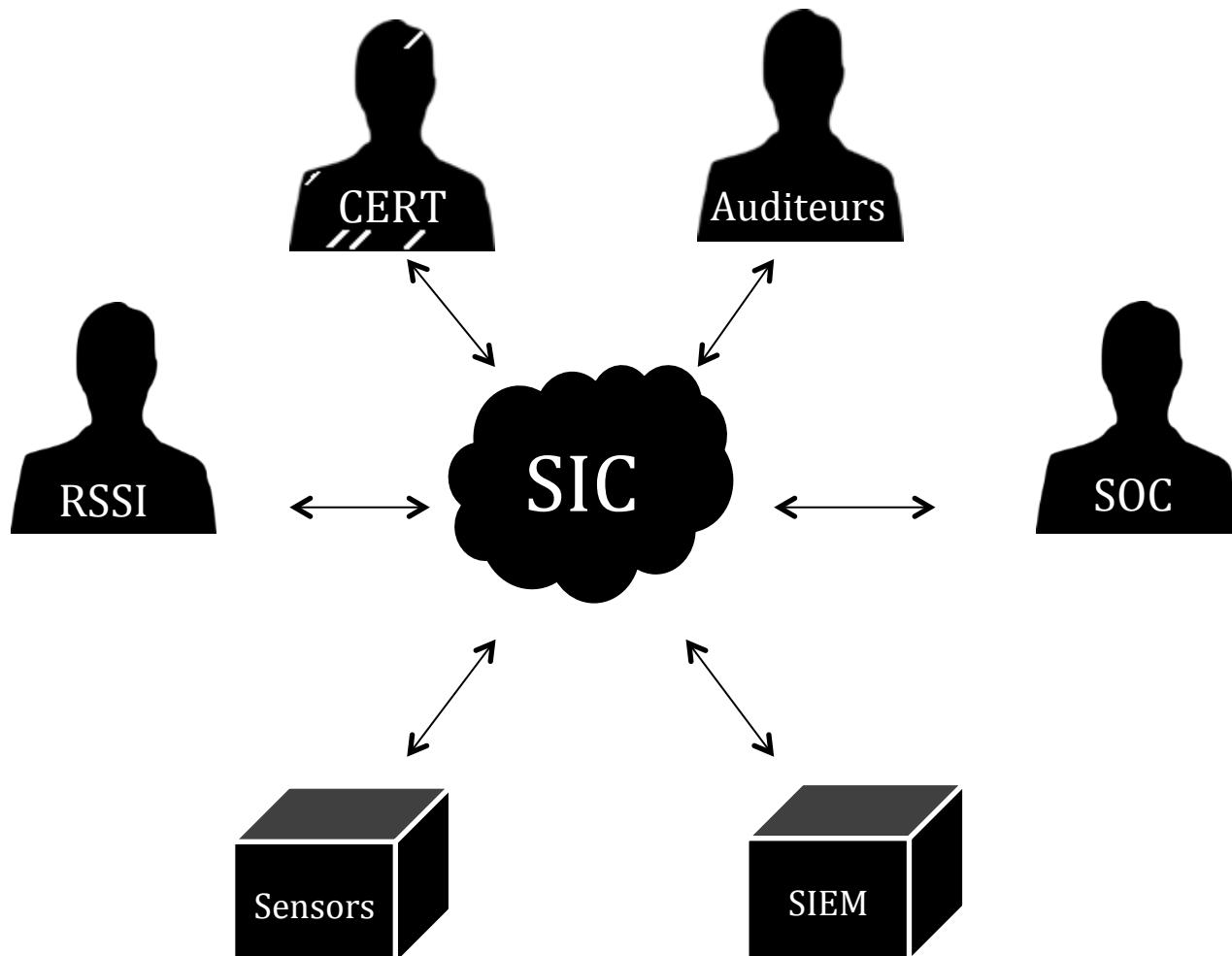


What do they do?

II. Cyber Threat Intelligence

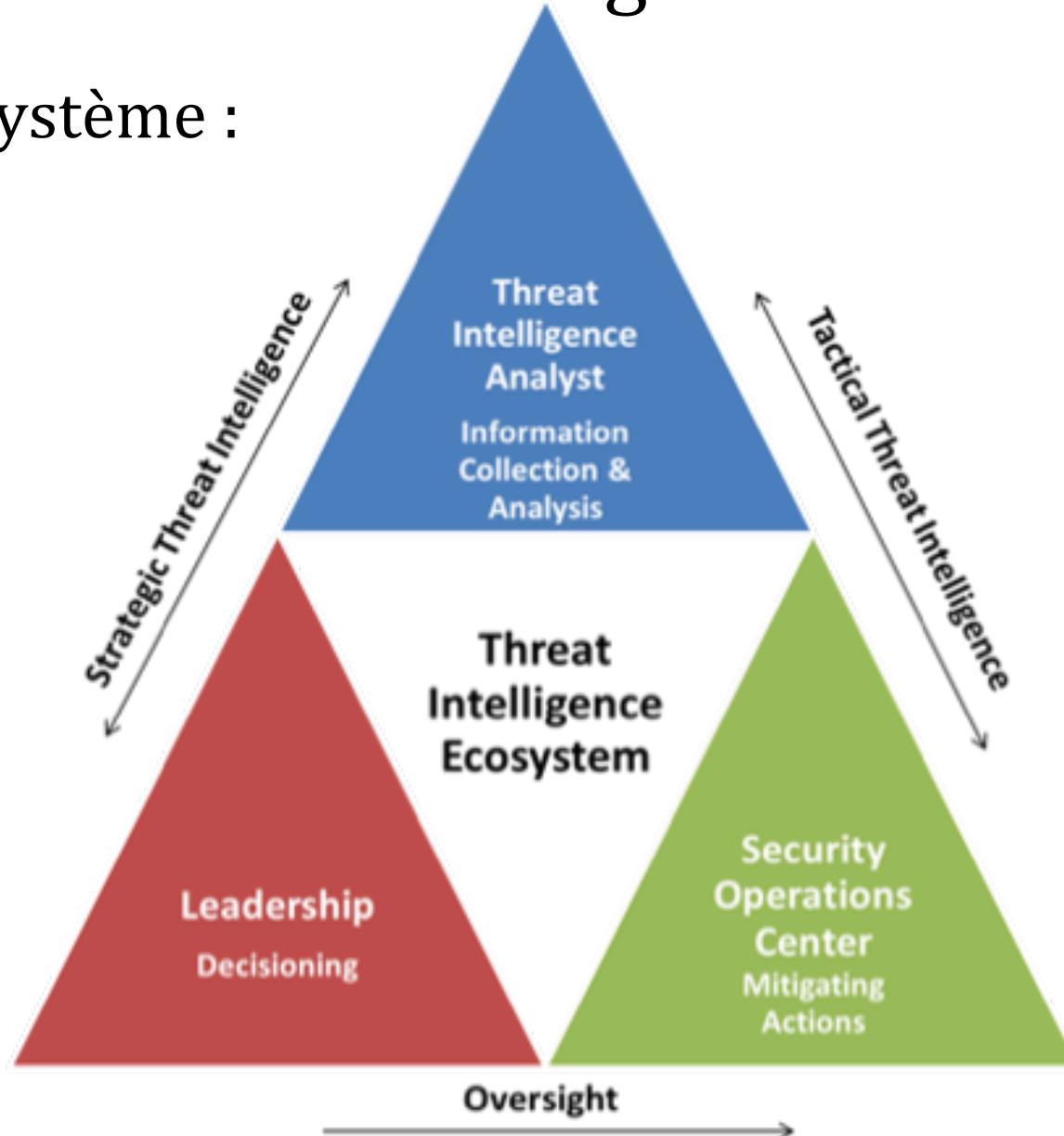
Des destinataires multiples :

SIC: Security
Intelligence
Center



II. Cyber Threat Intelligence

Un écosystème :



II. Cyber Threat Intelligence

Cyber threat intelligence :

- ✓ Temps réel (Firewall, IPS)
- ✓ Détection (Sonde, SOC)
- ✓ A posteriori (« Hunting »)

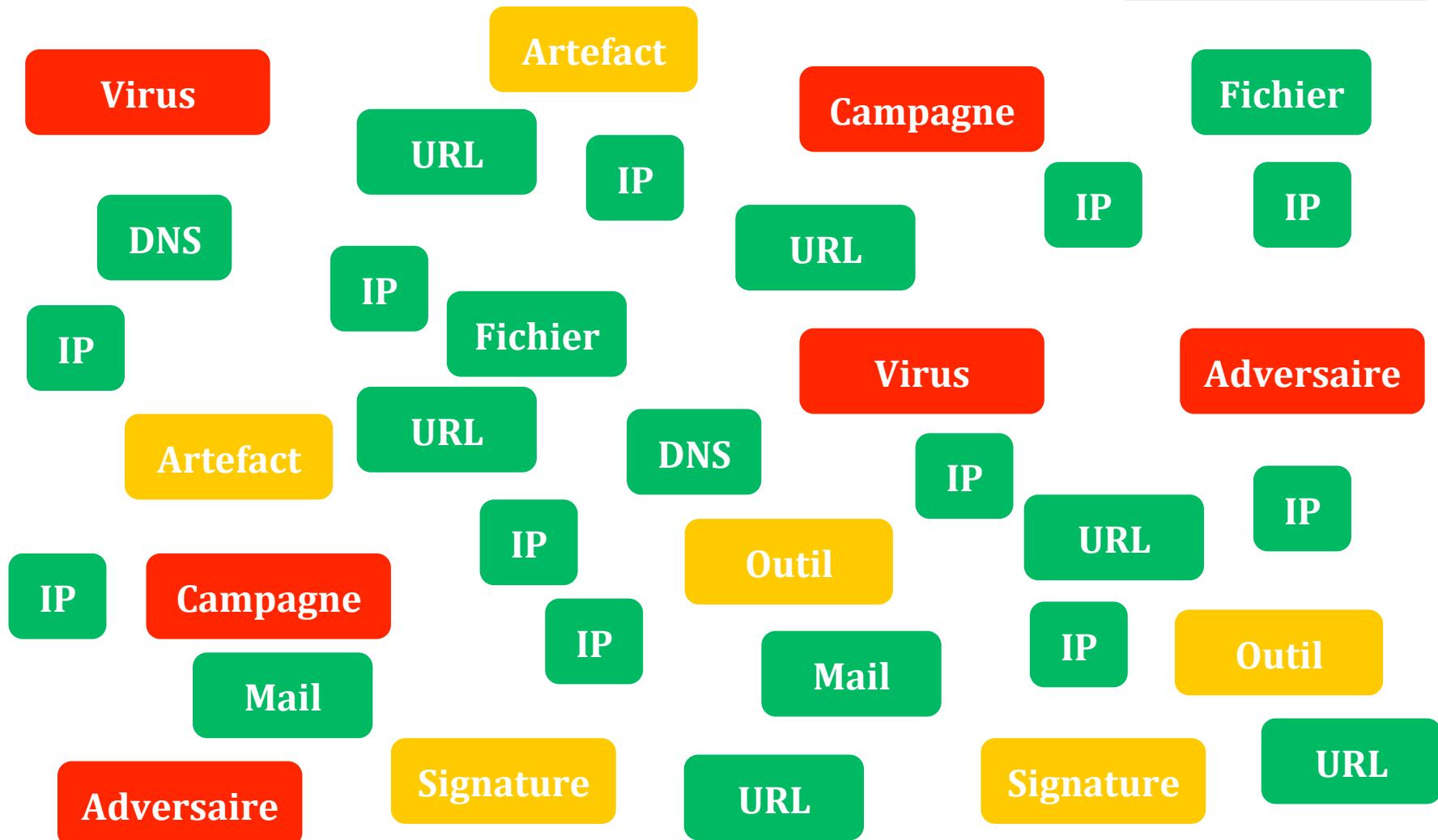


L'ART du renseignement :

- ✓ *Accurate* (Précis)
- ✓ *Relevant* (Pertinent)
- ✓ *Timely* (A temps)

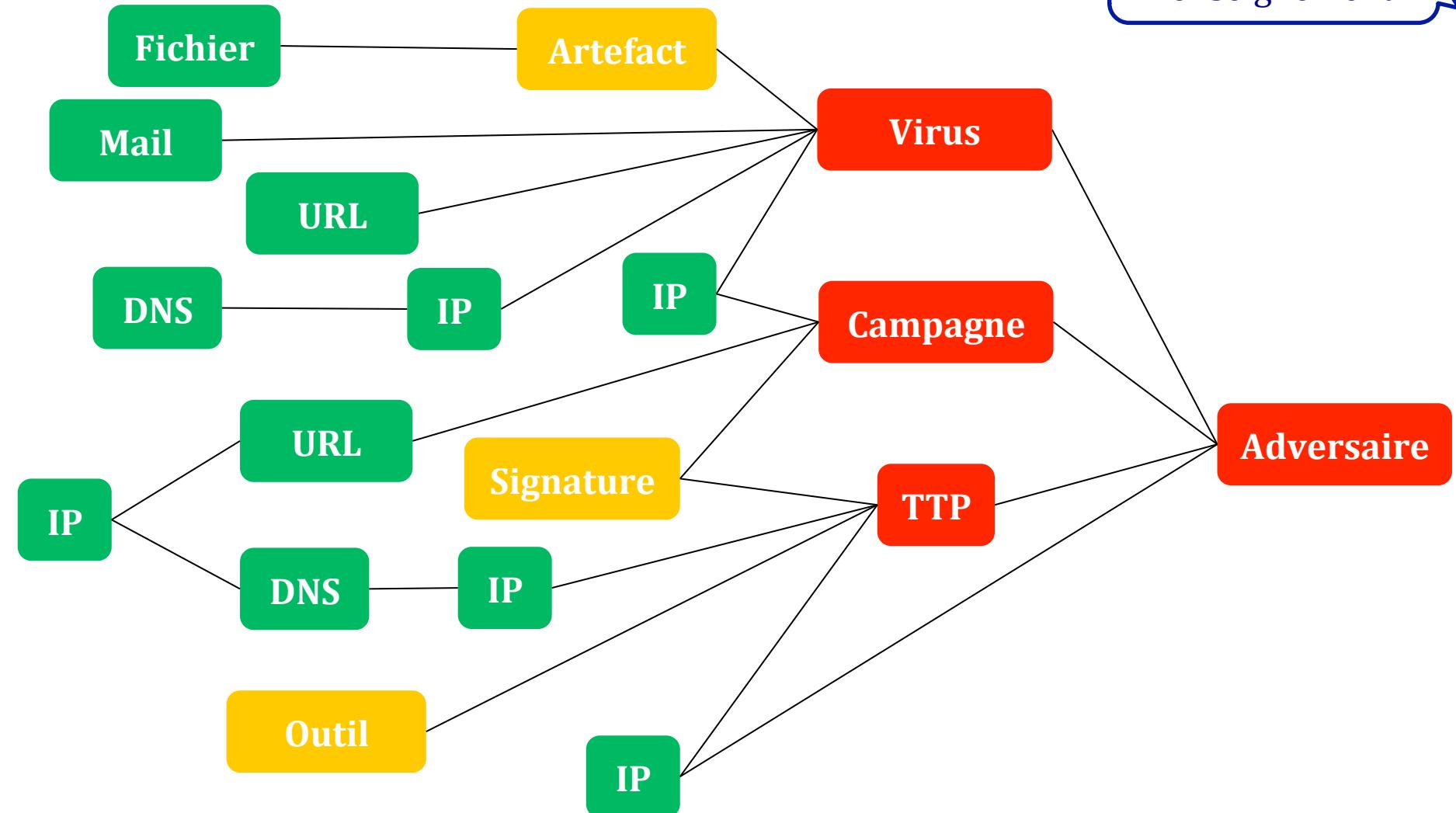
II. Cyber Threat Intelligence

Sans renseignement

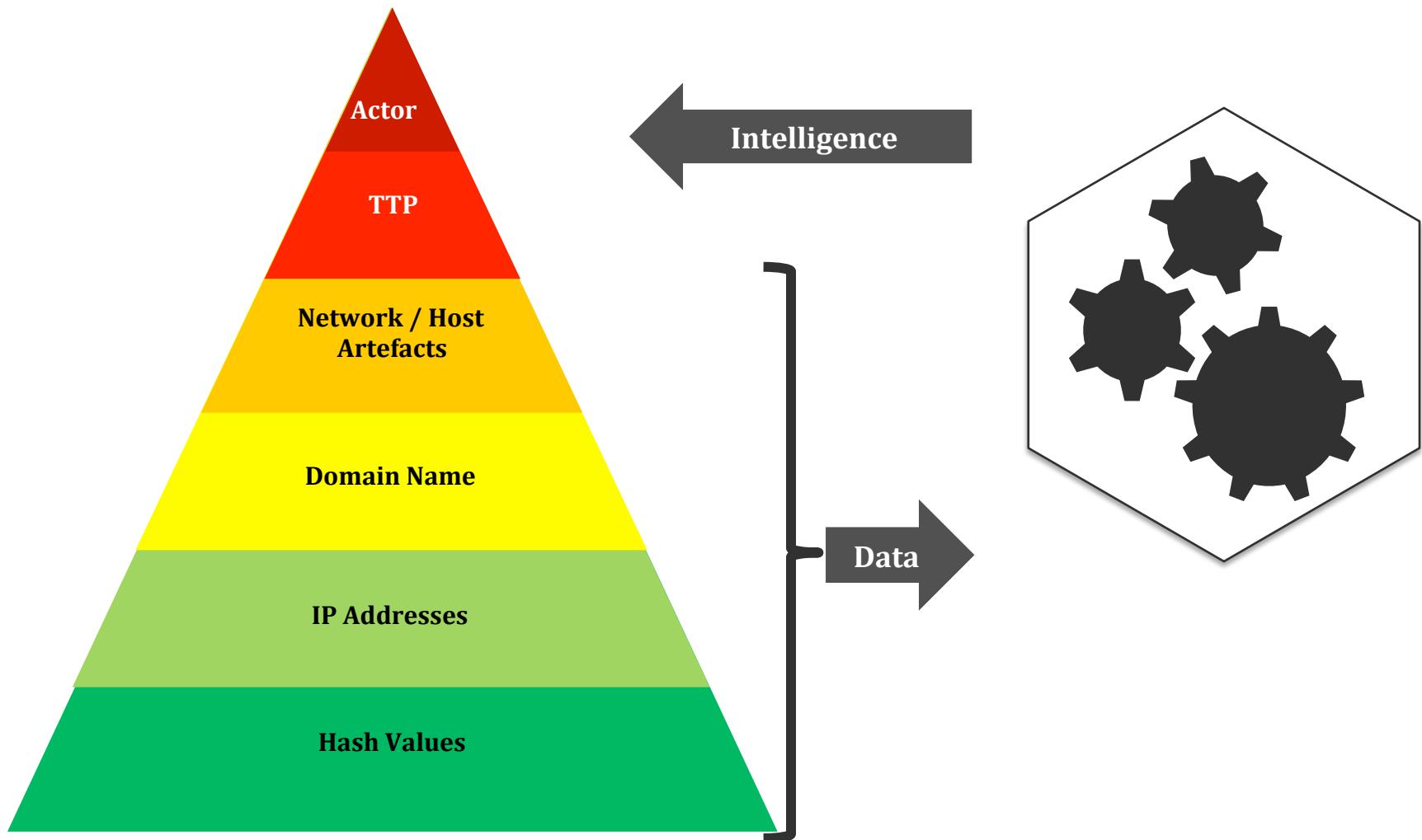


II. Cyber Threat Intelligence

Avec
renseignement

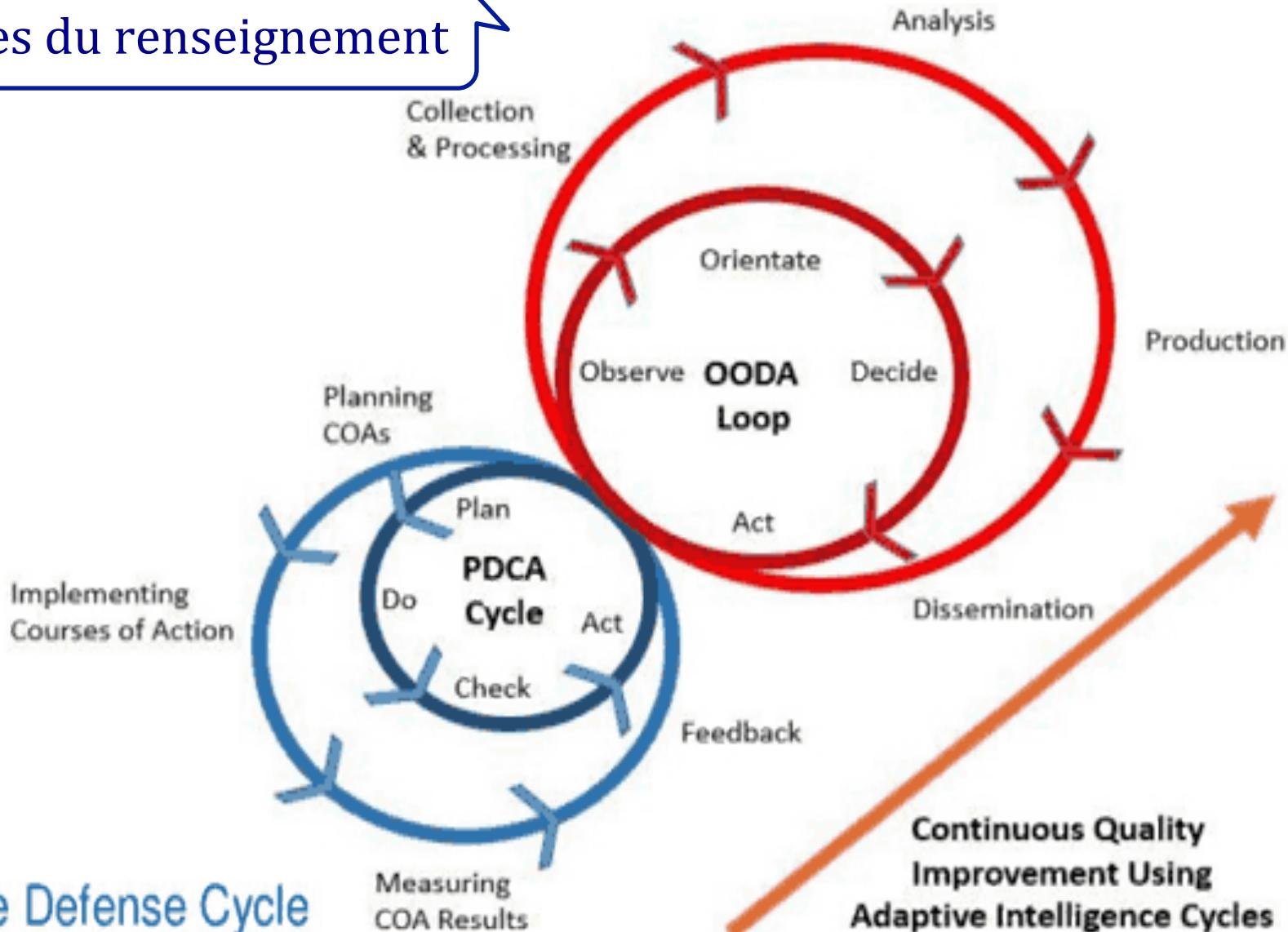


II. Cyber Threat Intelligence



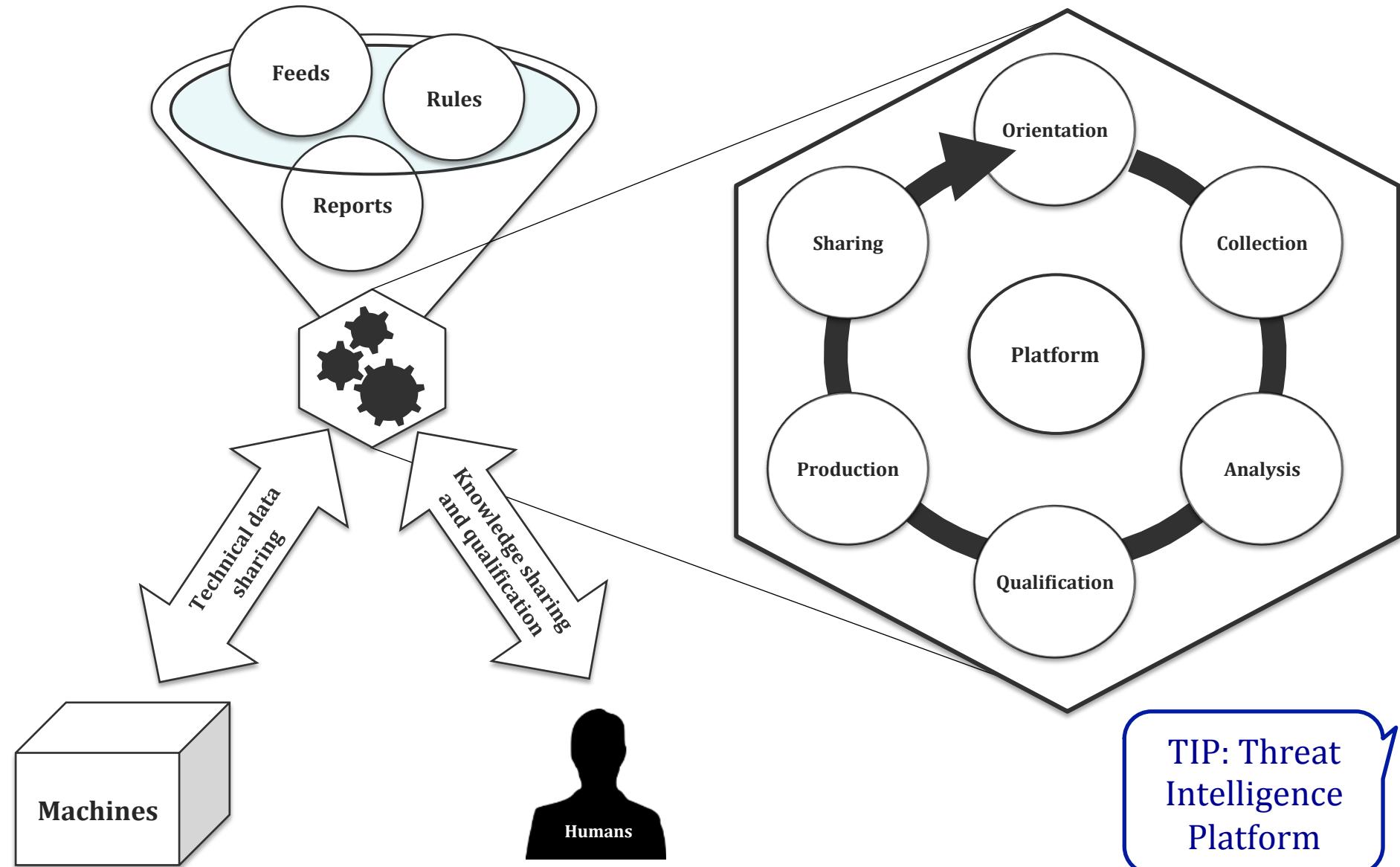
II. Cyber Threat Intelligence

Cycles du renseignement



Active Defense Cycle

II. Cyber Threat Intelligence



II. Cyber Threat Intelligence

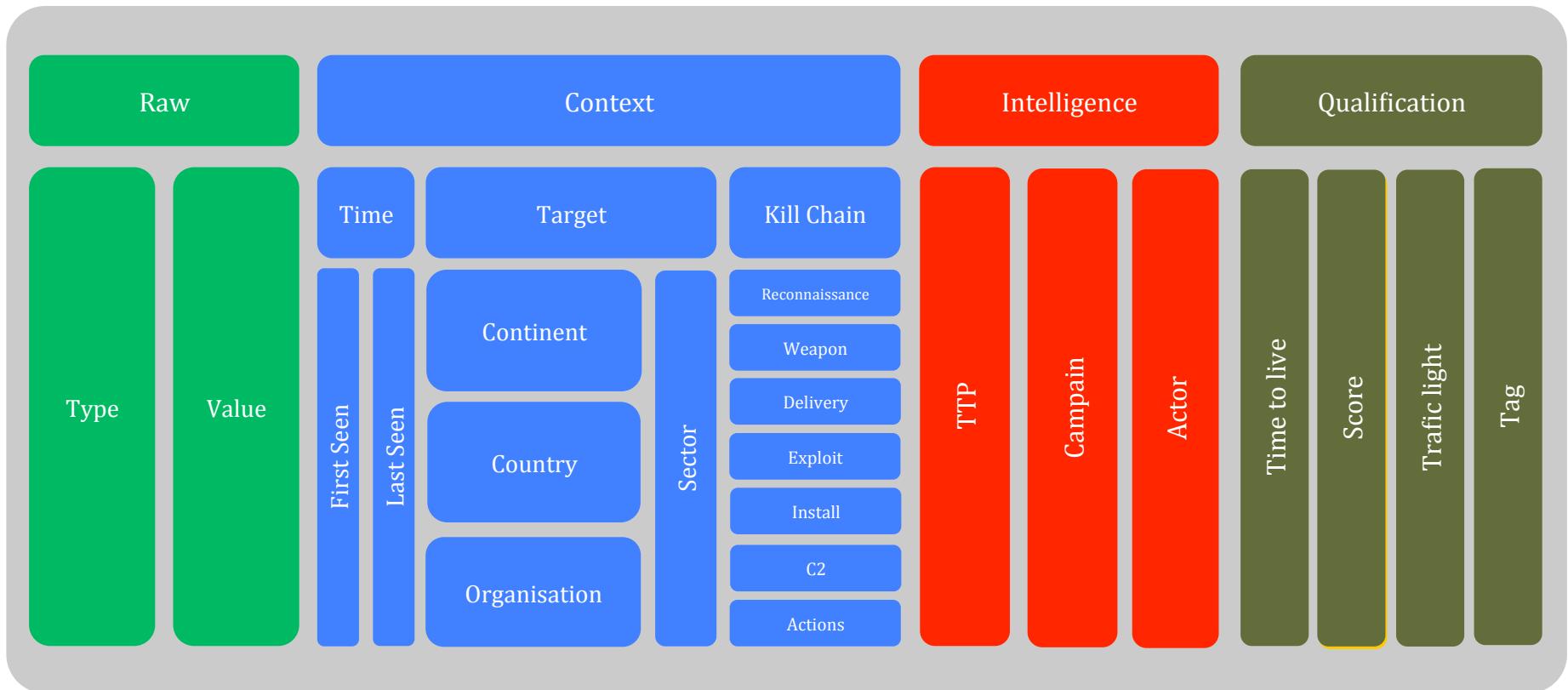


Fonctions d'une plateforme de Threat Intelligence :

- ✓ 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 :



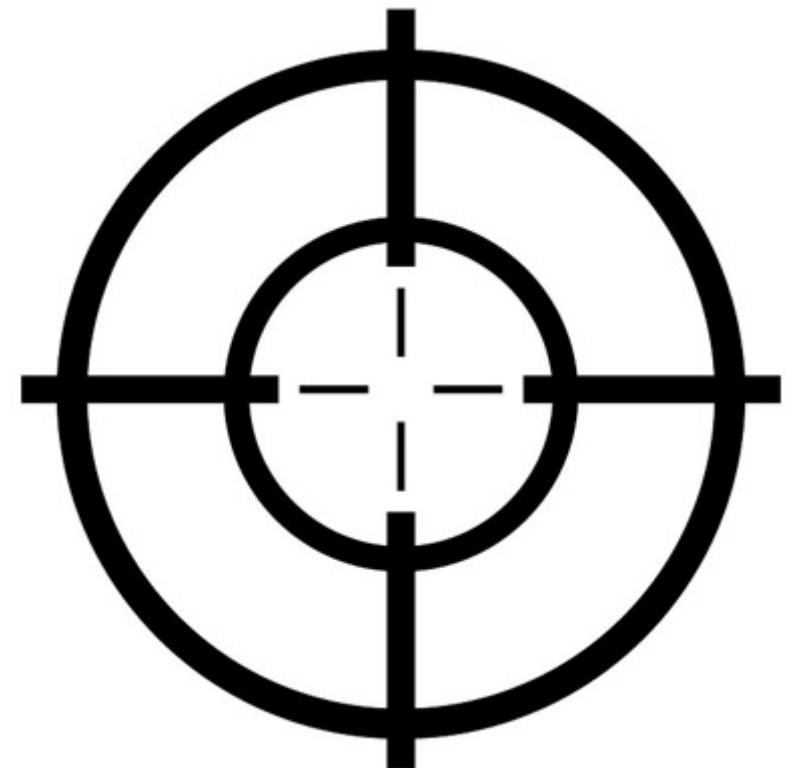
Base de travail essentielle

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



The screenshot shows the ThreatQ web interface. At the top, there are tabs for Indicators, Events, Adversaries, and Files. A search bar and a 'Create New' button are also present. A dropdown menu is open, showing options like User Management, Incoming Feeds, Whitelisted Indicators, Exports, Tools, OAuth Management, and System Configurations. The main area displays a table titled 'OSINT Feeds (46)' with columns for ID, Feed Name, Actions, and Set Indicator. The feed names listed include abuse.ch Feodo Bad IP Blocklist, abuse.ch Feodo Domain Blocklist, abuse.ch Feodo IP Blocklist, abuse.ch Pateno Domain Blocklist, abuse.ch Pateno IP Blocklist, abuse.ch SSLBL (Extended), abuse.ch SSLBL IP Blocklist, abuse.ch SSLBL SSL Blocklist, abuse.ch ZeuS Block Bad FQDNs, and abuse.ch ZeuS Block Bad IPs.



DoubleFantasy OS X

The Equation Team validator beachhead goes multi-platform

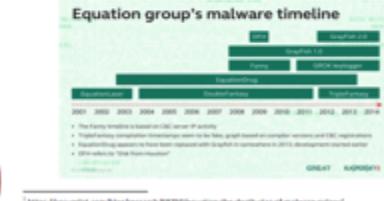
Version: 1.0 (7 Dec 2015)
Distribution: this document is TLP:RED. For more information on TLP, please see <http://www.us-cert.gov/tlp>

Executive summary

After sinkholing command-and-control servers associated with different Equation Group components, researchers noticed a single IP bearing with an OS X User Agent. In collaboration with the victim, a sample disguised as the 'Equation' process was retrieved from an OS X Mavericks machine. The sample is a variant of the Equation's DoubleFantasy exploit stage loader. The malware targeted a certain公益 research institute and is the only known sample of this malware discovered in the wild. The 'infowork' implant is designed to collect system information and credentials, extract data, and read, write, and execute files. The POSIX-compatible codebase is nearly identical to a Linux variant also discovered during this investigation.

Forensic data suggests that the initial infection took place in May of 2013. This attacker is known to leverage browser exploits in its Windows-analogue campaign. In this case, the specific infection vector is unknown. Given DoubleFantasy's early role in the lifecycle of an EquationDrug infection, its deployment is considered an indicator of further as yet undiscovered malware for OS X.

The EquationDrug[®] Platform



Legend:

- Operated by CIRCL
- Operated by NATO/NCIRC
- Operated by other organizations

II. Cyber Threat Intelligence

THREATQ

Indicators Events Adversaries Files Create New Search Settings

RESURRECTION OF THE EVIL MINER

Created: 07/09/16 Event Date: 07/10/16 04:30am

Event Summary

Related Indicators (65)

Related Events (0)

Related Adversaries (0)

Related Files (0)

Comments (0)

Audit Log

DETAILS

RELATIONSHIPS

RELATED INDICATORS

RELATED EVENTS

RELATED ADVERSARIES

RELATED FILES

COMMENTS

AUDIT LOG

Delete This Event

+ Add Details

% Link Indicator

% Link Event

% Link Adversary

% Link File

% Unlink

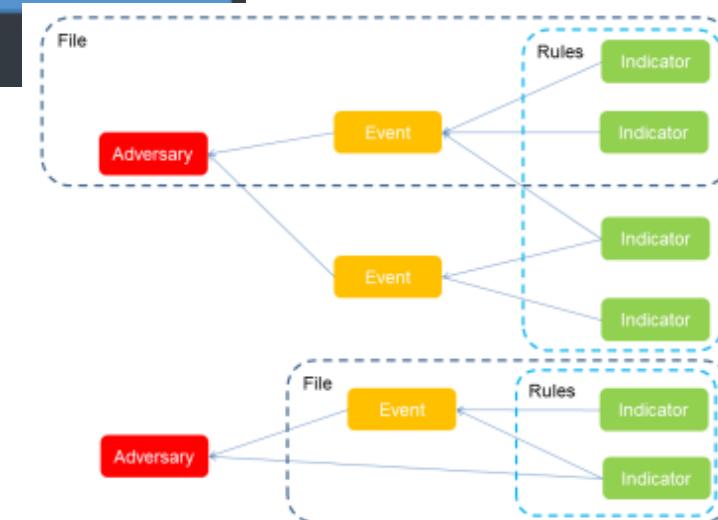
% Unlink

% Unlink

% Unlink

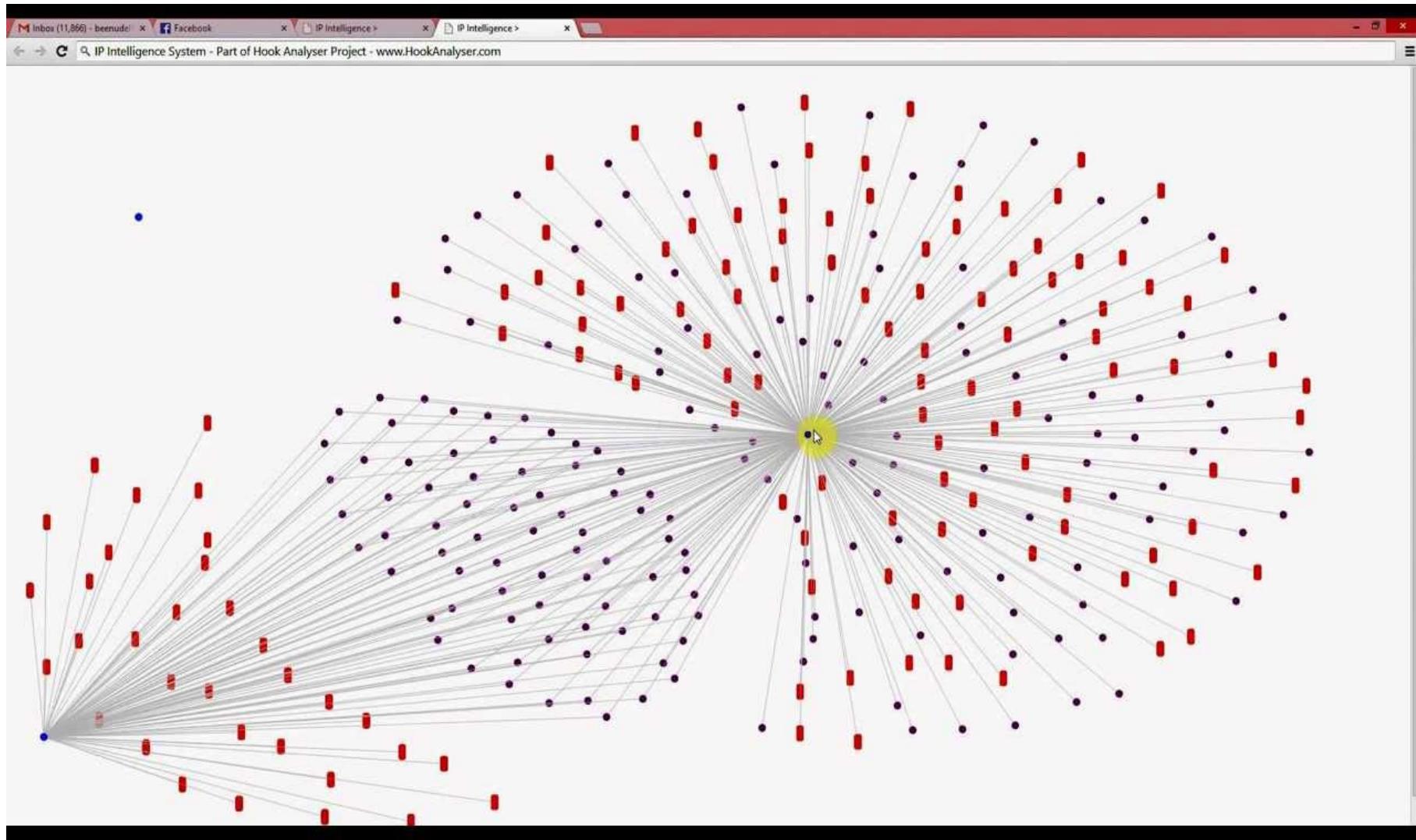


Analyse



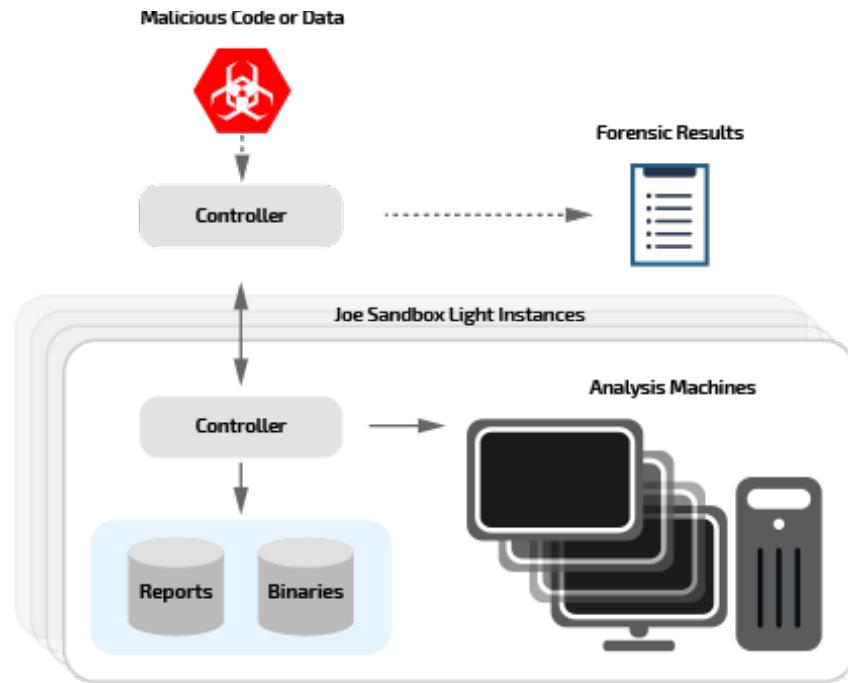
II. Cyber Threat Intelligence

Analyse



II. Cyber Threat Intelligence

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



VIRUS TOTAL

Virustotal is a [service that analyzes suspicious files](#) and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

[Analysis](#) [Statistics](#) [Email/Uploader](#) [About VirusTotal](#)

Upload a file

Service load

[Browse...](#)

Options

Do not distribute the sample [?](#)
 Send it over SSL [?](#)

Send File

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

The screenshot displays a Cyber Threat Intelligence interface. On the left, there's a sidebar with navigation links: 'Indicator Summary', 'Related Adversaries (0)', 'Related Events (4)', 'Related Files (0)', 'Related Indicators (0)', 'Comments (0)', and 'Data Enrichment'. The main area shows an IP address record for '208.71.106.48' (IP ADDRESS). The 'DETAILS' tab is selected, showing the status as 'Active'. Below this, the 'Attributes (38)' section lists various key-value pairs. Two related indicators are listed under 'Related Indicators':

1. Malspam 2016-08-26 (.wsf in .zip) - campaign: "Voice Message from Outside Caller" (0x5f323664)
 - Attribute Key: Comment
 - Attribute Value: download location (W...
 - Attribute Key: IQRisk Score
 - Attribute Value: 123
 - Attribute Key: IQRisk Category
 - Attribute Value: 35

2. Malspam 2016-08-26 (.wsf in .zip) - campaign: "Voice Message from Outside Caller" (0x5f323664)
 - Attribute Key: Status
 - Attribute Value: Active
 - Attribute Key: Campaign_type
 - Attribute Value: Malspam

A large red 'Score' label is overlaid on the left side of the interface. A red 'Statut : actif/inactif' label is overlaid at the bottom right.

II. Cyber Threat Intelligence

Production

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

The screenshot shows the THREATQ web application. At the top, there's a navigation bar with links for Indicators, Events, Adversaries, Files, and Signatures. Below the navigation is a search bar and a 'Create New' dropdown. A large table titled 'Exports' lists various export configurations. An 'Add New Export' button is at the top right of the table area. The table has columns for 'Off / On', 'Name', 'URL', 'Connection', 'Output Format', and 'Actions'. A modal window titled 'OUTPUT FORMAT' is open, asking 'Which type of information would you like to export?'. It shows 'Indicators' selected in the dropdown. Below that, 'Output type:' is set to 'text/plain'. There's a 'Special Parameters (optional)' section containing the URL parameter 'indicator.status=Active&indicator.type=FQDN&indicator.deleted=N&indicator.Attributes[Tag]=Locky'. At the bottom of the modal is an 'Output Format Template' text area with some code, and buttons for 'Save Settings' and 'Cancel'.

Update	
80.58.0.0	
60.190.79.18	
60.208.64.177	
61.144.122.45	
62.150.76.247	
62.158.42.192	
66.150.105.20	
66.225.201.42	
66.231.14.5	
69.88.144.161	
69.88.144.163	
72.3.131.182	
80.58.205.33	
80.58.205.36	
80.58.205.42	
80.58.205.55	
85.21.156.194	
85.136.65.160	
85.185.16.126	
85.214.45.201	
89.191.100.12	
123.48.200.232	
124.97.181.43	
125.191.50.15	
144.140.22.190	
168.97.134.249	
168.243.69.98	
193.93.236.7	
195.175.37.6	
195.175.37.8	
195.225.177.131	
200.21.160.15	
580 blocked addresses	

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

II. Cyber Threat Intelligence

MISP Threat Sharing

The MISP Threat Sharing interface displays a network graph where nodes represent events and edges represent relationships between them. Nodes are color-coded: green for Event 642, red for Event 2581, Event 2686, Event 2687, and Event 775, and blue for other nodes like 54.68.53.18, 5.104.886.190, GovPAT, and various IP addresses.

TLP Taxonomy Library

ID	Namespace	Name	Taxonomy	Tagged events	Actions
6	tp	APT		31	<input type="checkbox"/> <input type="checkbox"/>
7	tp	Actionable: NO		5	<input type="checkbox"/> <input type="checkbox"/>
3	tp	TLP:AMBER		131	<input type="checkbox"/> <input type="checkbox"/>
8	tp	TLP:EX:CHR		11	<input type="checkbox"/> <input type="checkbox"/>
5	tp	TLP:GREEN		550	<input type="checkbox"/> <input type="checkbox"/>
4	tp	TLP:RED		3	<input type="checkbox"/> <input type="checkbox"/>
2	tp	TLP:WHITE		531	<input type="checkbox"/> <input type="checkbox"/>
10		TO:HIDE		2	<input type="checkbox"/> <input type="checkbox"/>
9		TODO		9	<input type="checkbox"/> <input type="checkbox"/>
11		TODO:VT-ENRICHMENT		8	<input type="checkbox"/> <input type="checkbox"/>
1		Type:OSINT		832	<input type="checkbox"/> <input type="checkbox"/>
18	admiralty-scale	admiralty-scale:information-credibility="1"	admiralty-scale	0	<input type="checkbox"/> <input type="checkbox"/>
19	admiralty-scale	admiralty-scale:information-credibility="2"	admiralty-scale	0	<input type="checkbox"/> <input type="checkbox"/>
20	admiralty-scale	admiralty-scale:information-credibility="3"	admiralty-scale	0	<input type="checkbox"/> <input type="checkbox"/>
21	admiralty-scale	admiralty-scale:information-credibility="4"	admiralty-scale	0	<input type="checkbox"/> <input type="checkbox"/>
22	admiralty-scale	admiralty-scale:information-credibility="5"	admiralty-scale	0	<input type="checkbox"/> <input type="checkbox"/>
23	admiralty-scale	admiralty-scale:information-credibility="6"	admiralty-scale	0	<input type="checkbox"/> <input type="checkbox"/>

Filter

Tag	Expanded	Events	Tag	Action
tip:red	(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	<input type="checkbox"/>
tip:amber	(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	<input type="checkbox"/>
tip:green	(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	<input type="checkbox"/>
tip:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	<input type="checkbox"/>
tip:ex:chr	(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	<input type="checkbox"/>

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

Partage

II. Cyber Threat Intelligence

TLP : Trafic Light Protocol

✓ Outils de gestion du partage

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

- 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

Mais aussi :

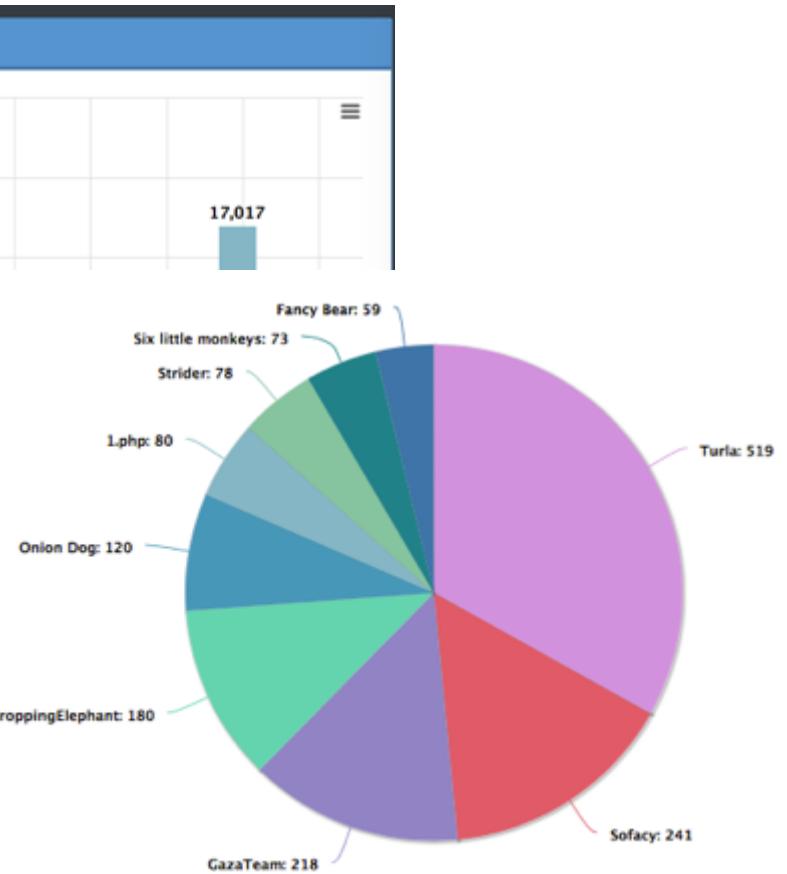
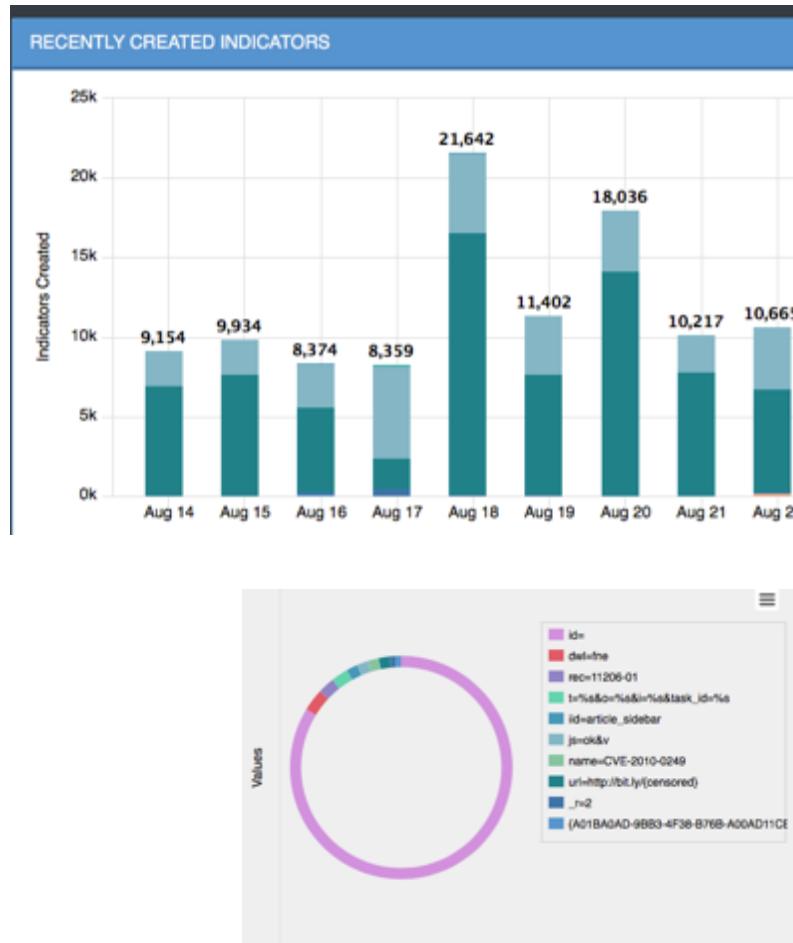
- ✓ Corrélation
- ✓ Détection
- ✓ Analyse comportementale
- ✓ Recherche de signaux faibles

Threat Intelligence

Cyberdéfense

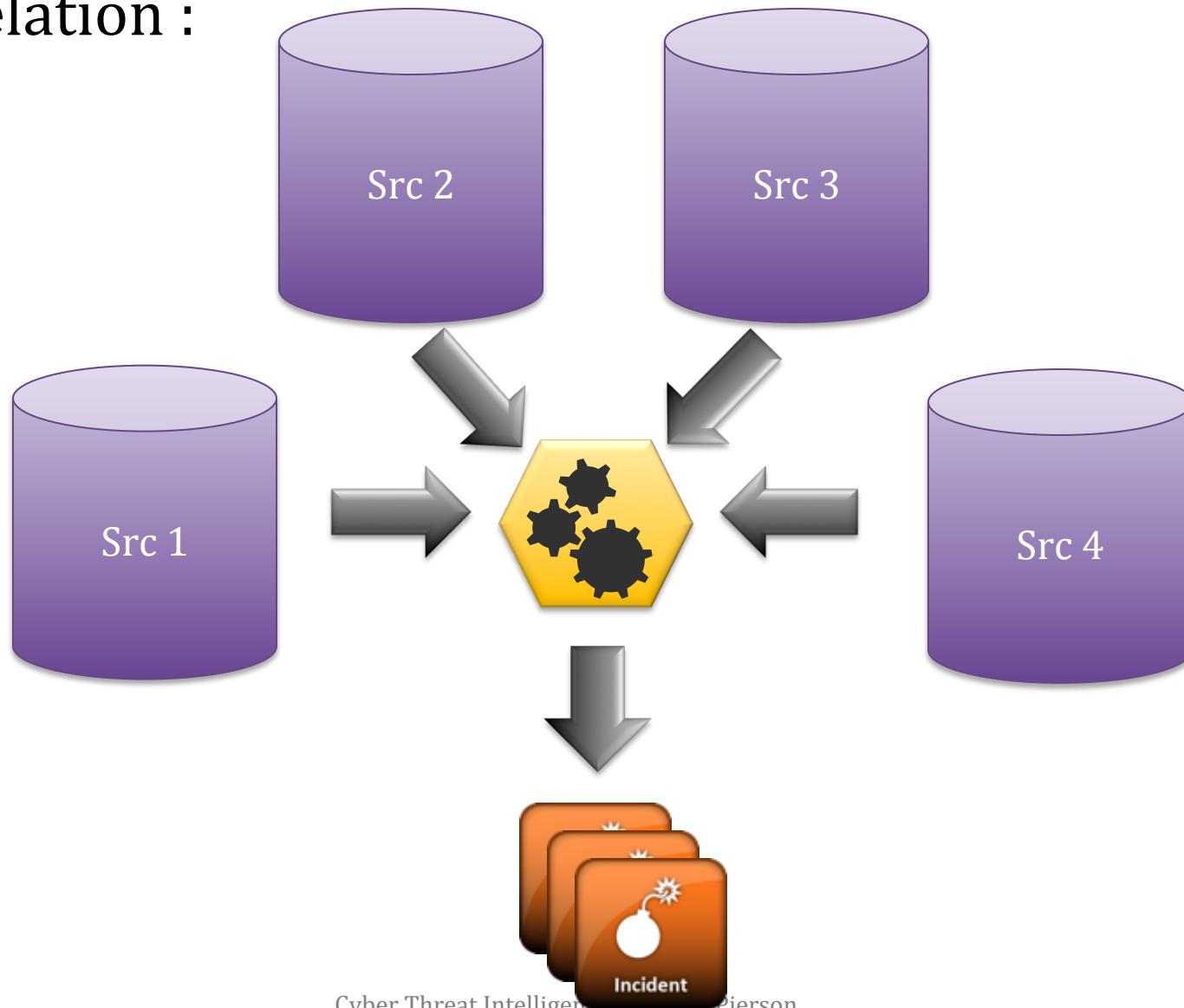
III. Apports de la science des données

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



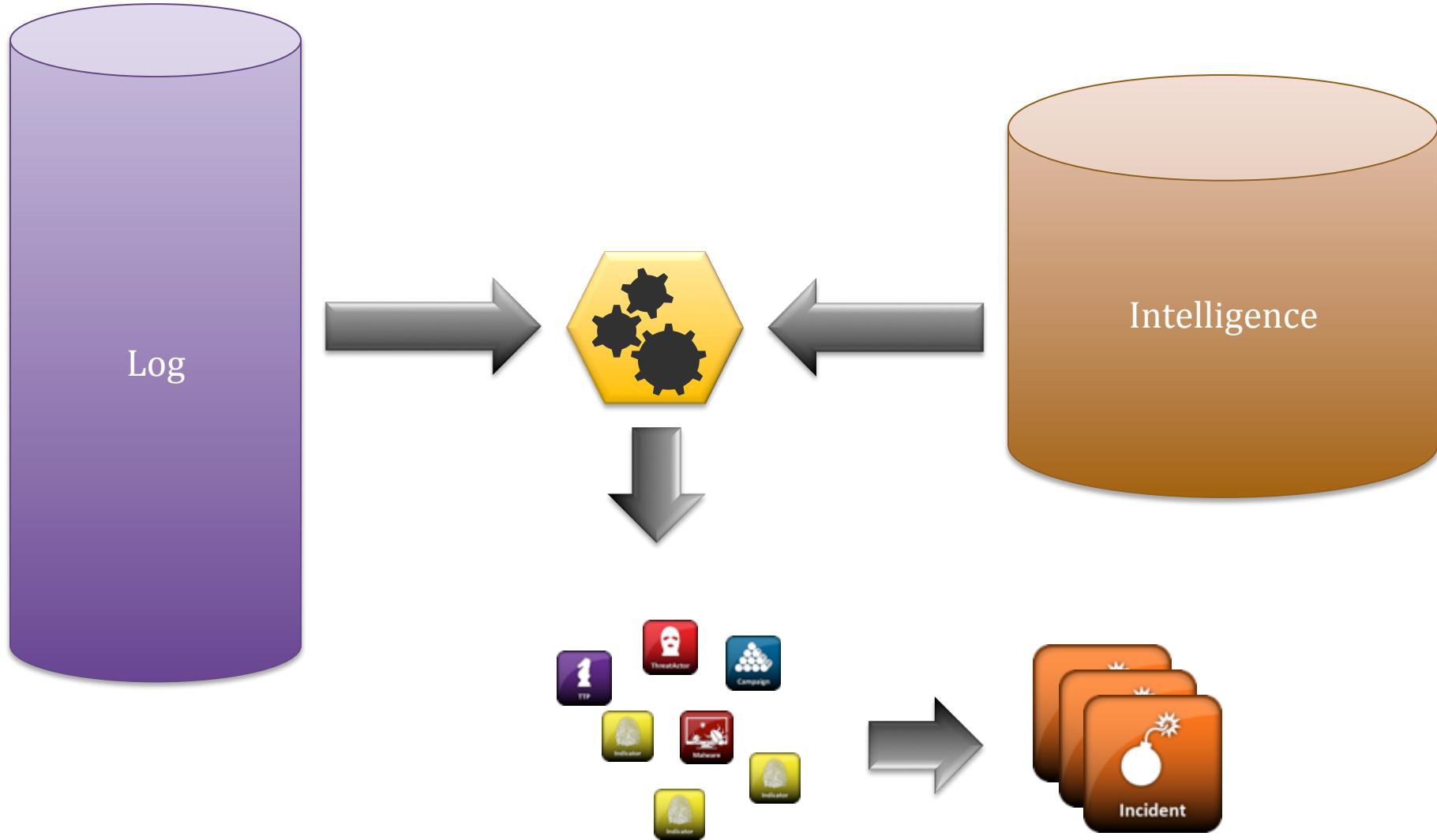
III. Apports de la science des données

Correlation :



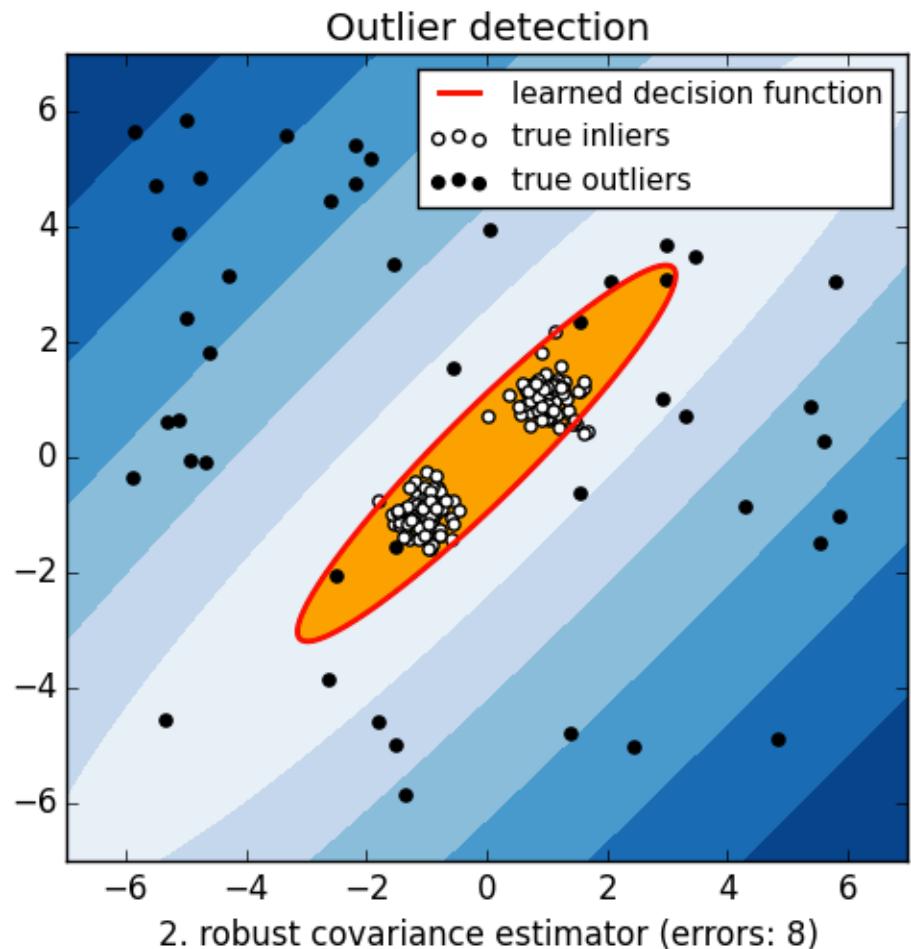
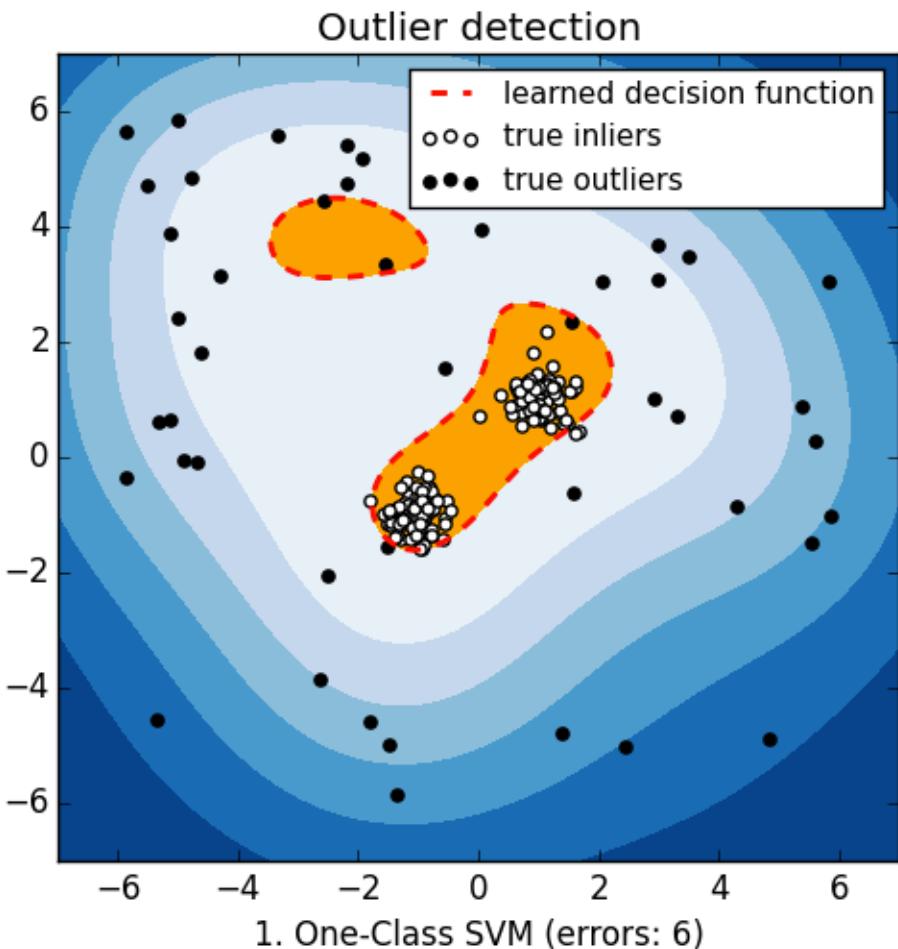
III. Apports de la science des données

Recherche/hunting :



III. Apports de la science des données

Analyse comportementale :



III. Apports de la science des données

Recherche de signaux faibles :

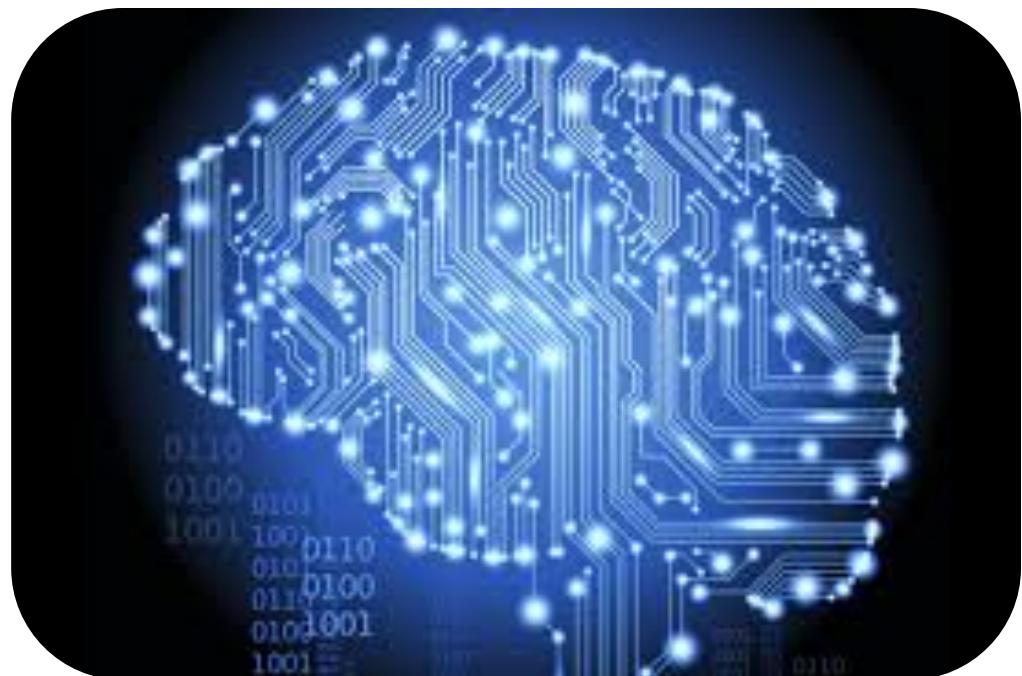
```
12/30 01:42:32 23.75.345.200 example.com /index.php?2346354=-349087 WordPress/3.7.2
12/30 01:42:31 23.75.345.200 example.com /index.php?7231344=4454226 WordPress/3.3.1
12/30 01:42:25 23.75.345.200 example.com /index.php?1243847=9161112 WordPress/3.7.2
12/30 01:42:23 23.75.345.200 example.com /index.php?8809549=4423410 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 Périsat, 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 artificielle 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 événements, 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

Cyber Threat Intelligence - Nicolas Pierson



Engagez vous !



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