

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.



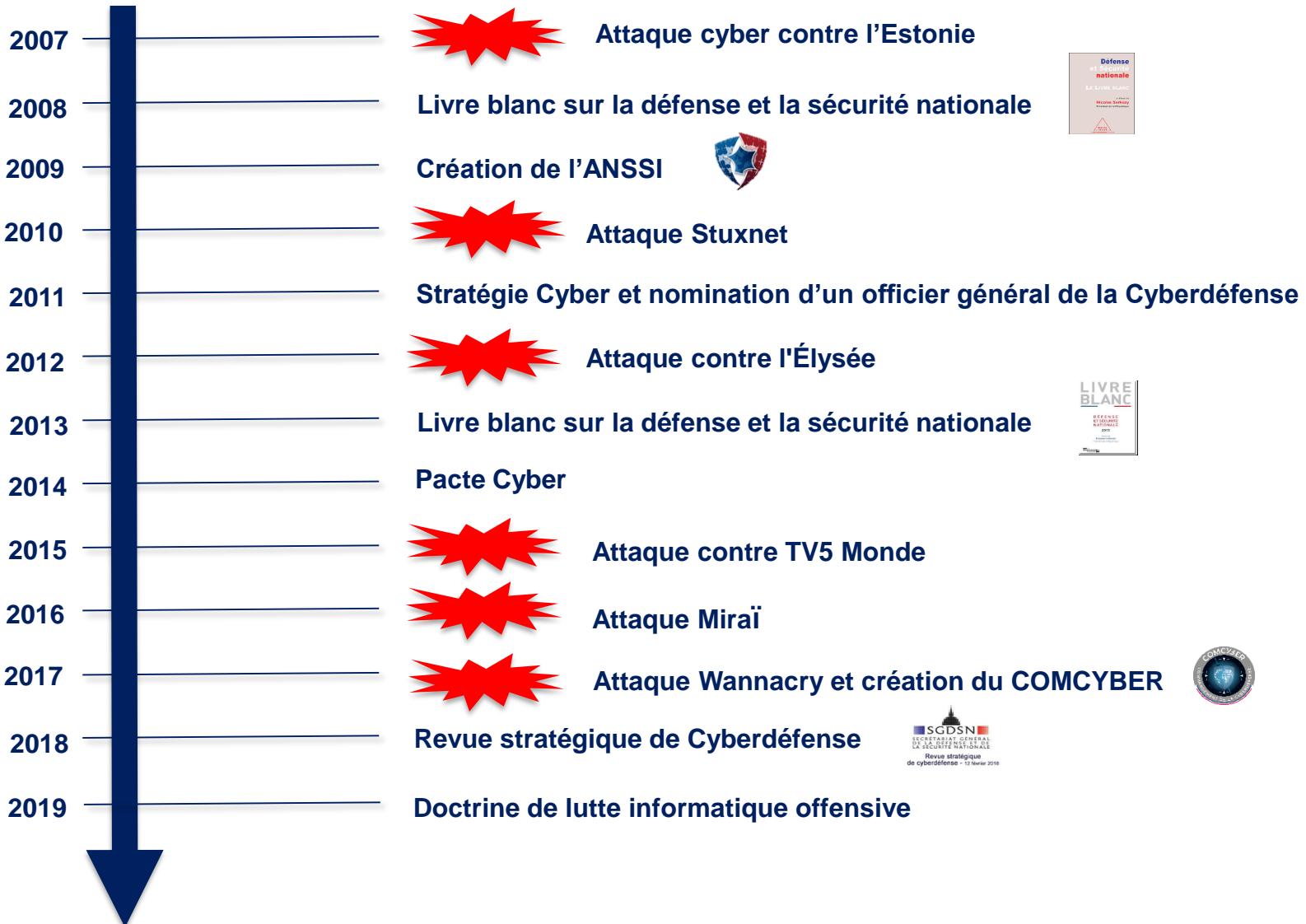
“Le cyberspace est donc désormais un champ de confrontation à part entière.”

LBDSN 2013, p45.

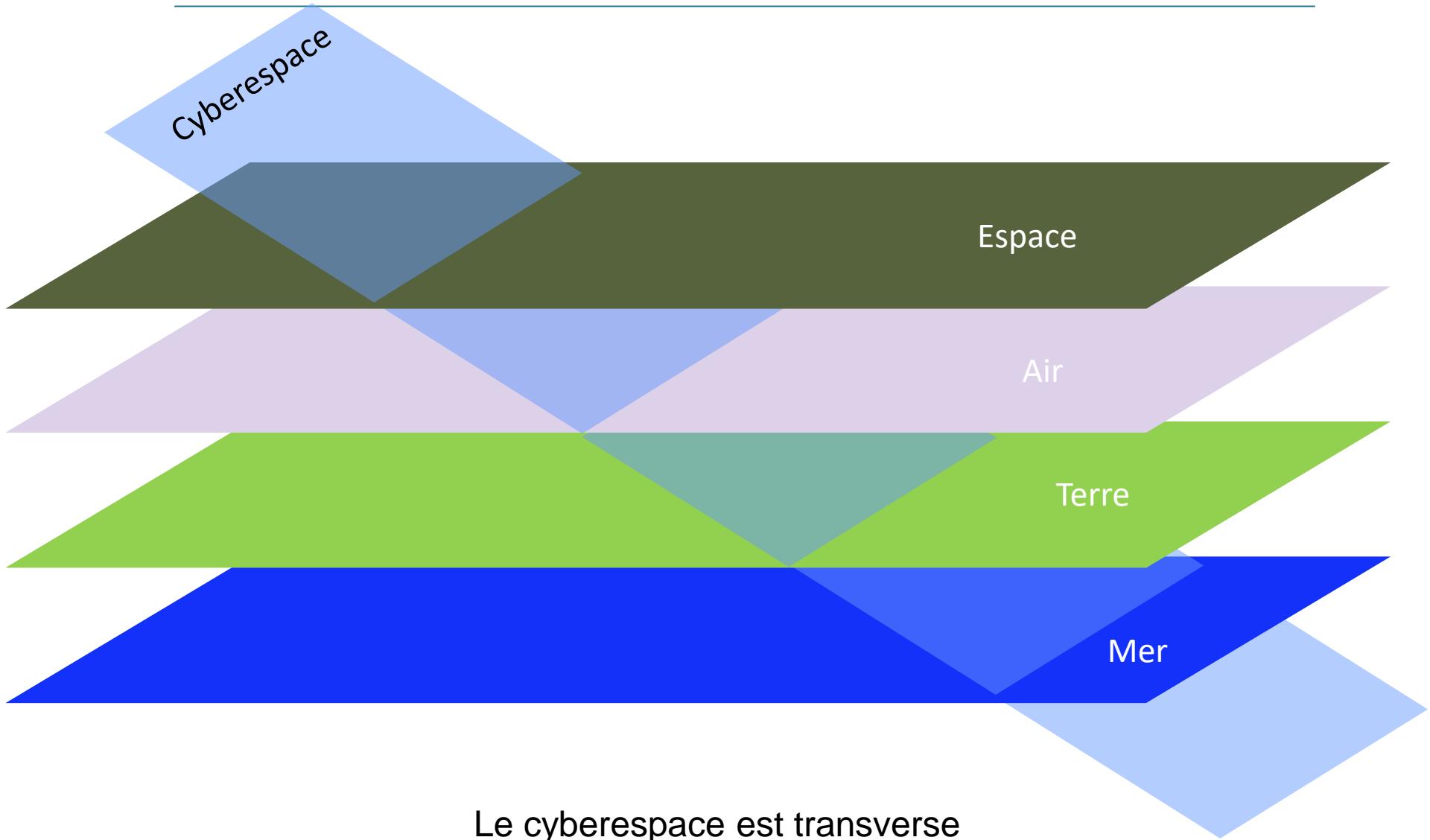
La cyberstratégie française considère le cyberspace comme un domaine où doit s'exercer notre souveraineté nationale.



Montée en puissance



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



Commande

Gov-CERT
(SDO)

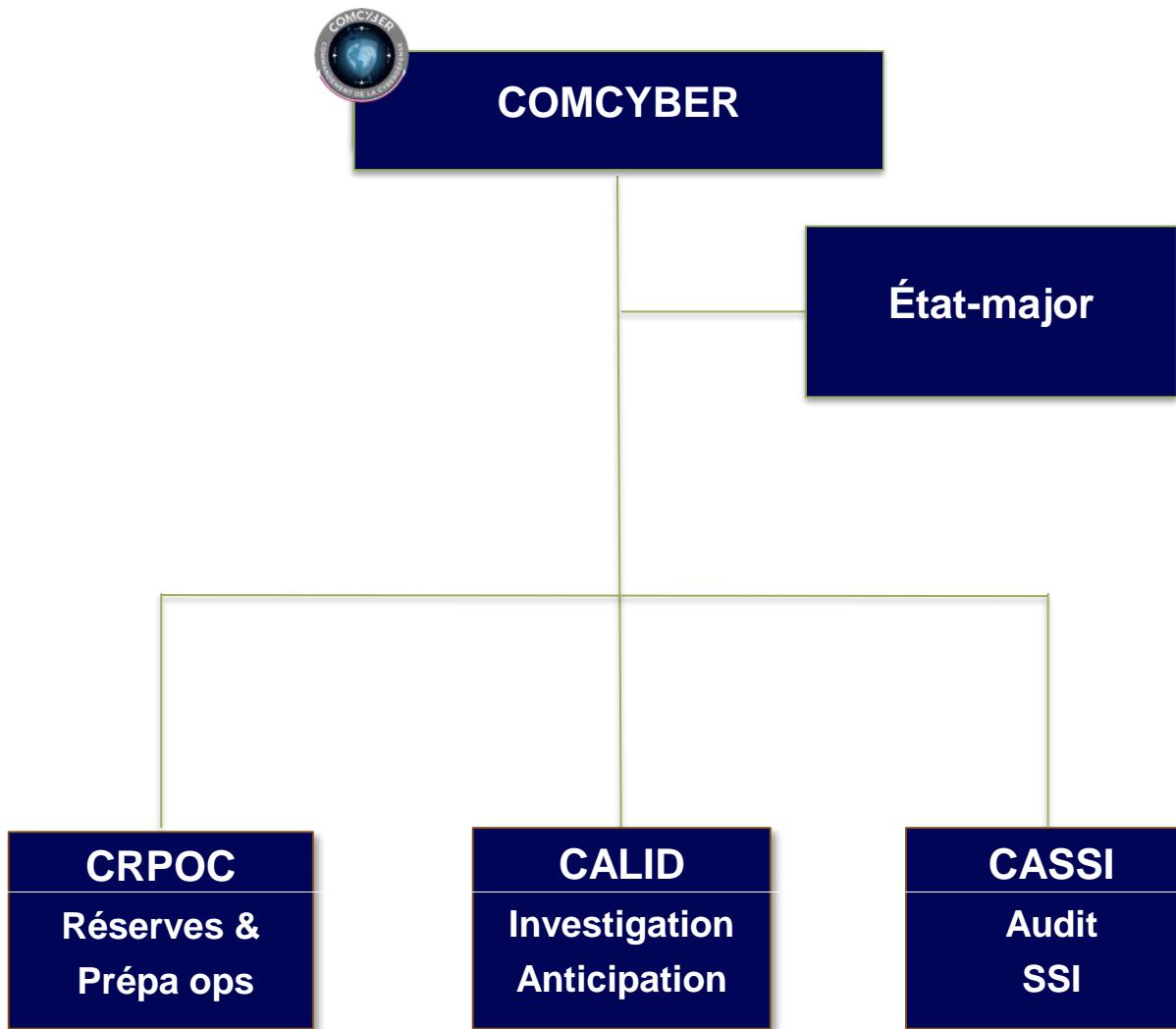
Mil-CERT
(CALID)

- 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.

Colocalisés pour une plus grande efficacité



Organisation du COMCYBER



Cyberespace

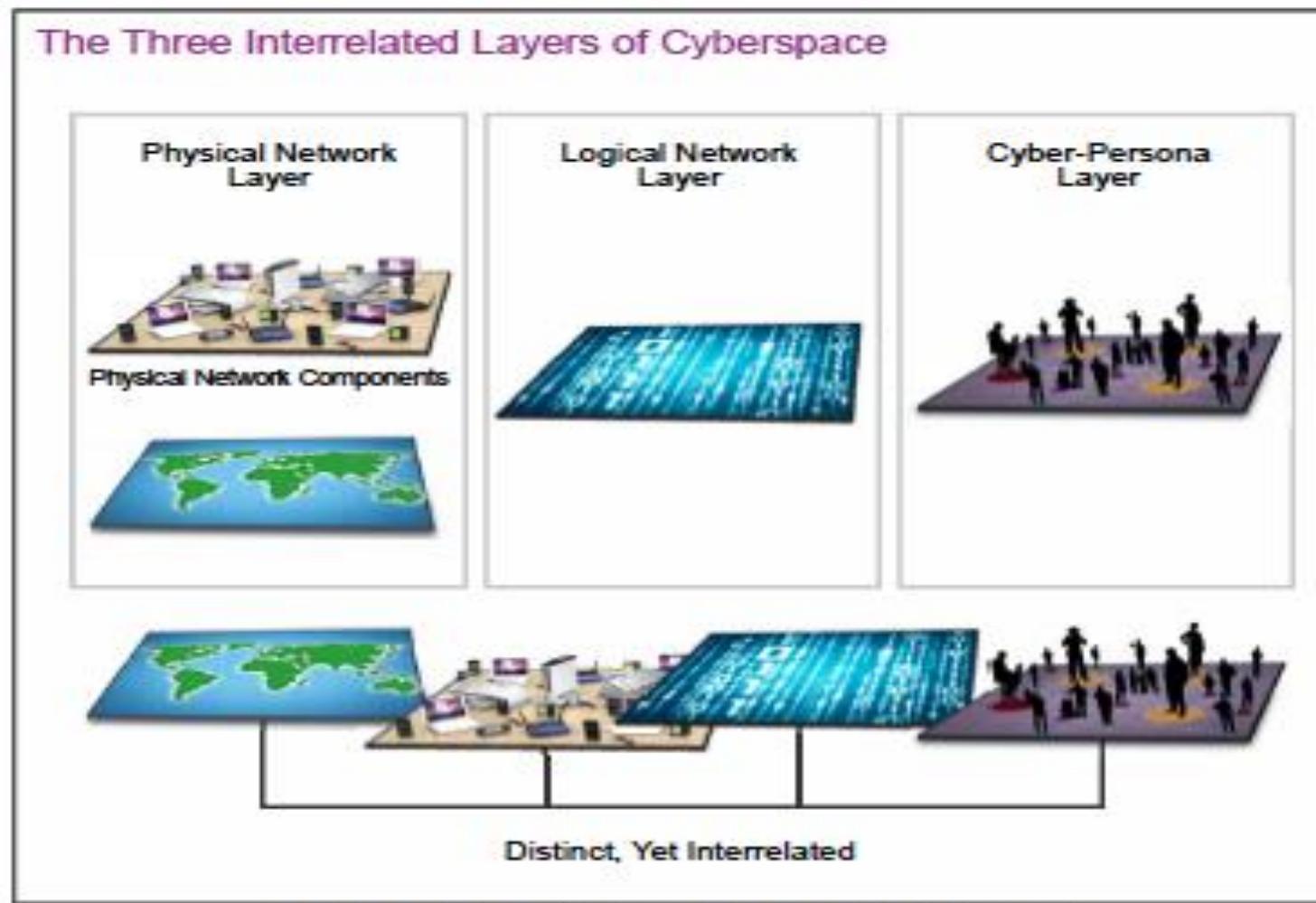


Figure I-1. The Three Interrelated Layers of Cyberspace

Source : Joint publication 3-12 – cyberspace operation

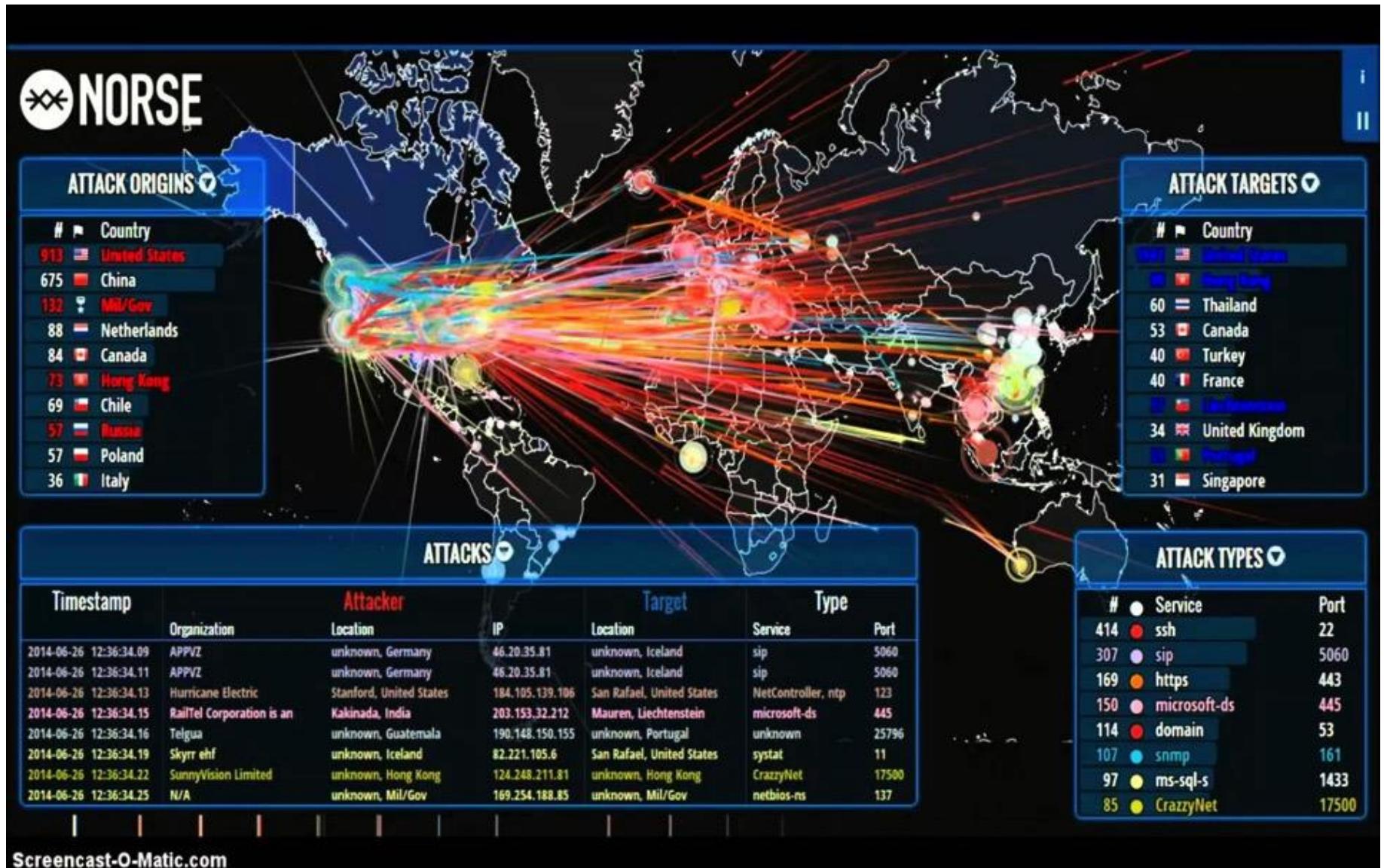
Introduction

Guillaume Poupart | FIC 2020 :

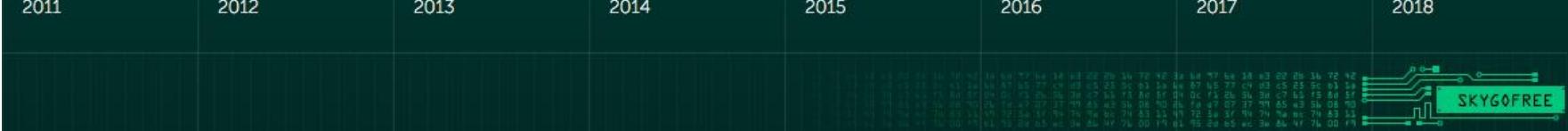
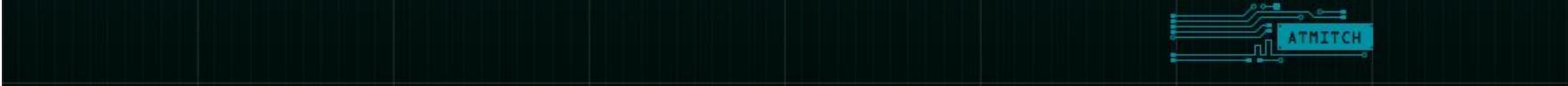
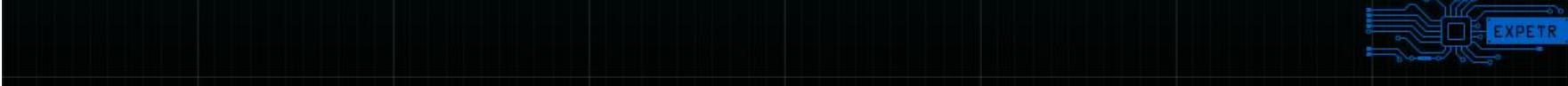
« Si vous voulez vous faire peur, dites vous que si vous prenez la somme de ce que vous trouvez en source ouverte en terme d'attaques et de victimes, vous êtes probablement à moins de 10% de la réalité. »

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

Introduction



Introduction

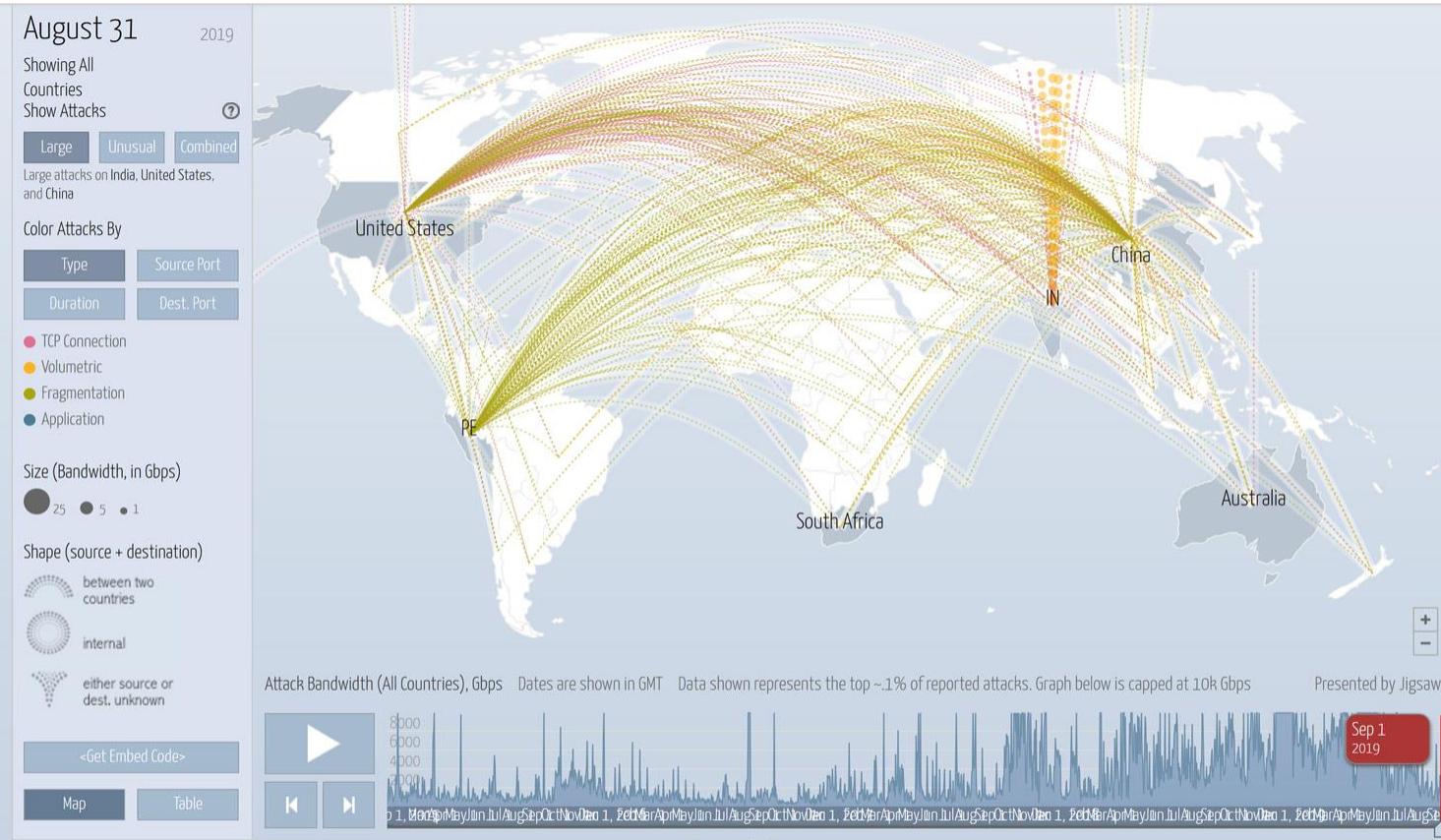
2011	2012	2013	2014	2015	2016	2017	2018		
 <p>SKYGOFREE</p> <p>This section shows a complex circuit board diagram for the SKYGOFREE threat actor. The board features numerous components like resistors, capacitors, and integrated circuits, with various connection points and labels in green and blue. A prominent blue rectangular box labeled "SKYGOFREE" is positioned on the right side of the board.</p>	 <p>BLACKOASIS</p> <p>A smaller circuit board diagram for the BLACKOASIS threat actor, showing a simplified layout with fewer components compared to SKYGOFREE. A blue box labeled "BLACKOASIS" is located on the right.</p>	 <p>WHITEBEAR</p> <p>A circuit board diagram for the WHITEBEAR threat actor, featuring a clean design with a few key components. A blue box labeled "WHITEBEAR" is on the right.</p>	 <p>SHADOWPAD</p> <p>A circuit board diagram for the SHADOWPAD threat actor, showing a simple layout with a few components. A blue box labeled "SHADOWPAD" is on the right.</p>	 <p>SATELLITE T...</p> <p>A large and detailed circuit board diagram for the SATELLITE threat actor, featuring a complex network of components and connections. A blue box labeled "SATELLITE T..." is on the right.</p>	 <p>PENGUIN TUR...</p> <p>A circuit board diagram for the PENGUIN threat actor, showing a complex layout with many components. A blue box labeled "PENGUIN T..." is on the right.</p>	 <p>ATMITCH</p> <p>A circuit board diagram for the ATMITCH threat actor, showing a simple layout with a few components. A blue box labeled "ATMITCH" is on the right.</p>	 <p>GHOUL</p> <p>A circuit board diagram for the GHOUL threat actor, showing a simple layout with a few components. A blue box labeled "GHOUL" is on the right.</p>	 <p>EXPETR</p> <p>A circuit board diagram for the EXPETR threat actor, showing a simple layout with a few components. A blue box labeled "EXPETR" is on the right.</p>	 <p>MOONLIGHT M...</p> <p>A circuit board diagram for the MOONLIGHT threat actor, showing a simple layout with a few components. A blue box labeled "MOONLIGHT M..." is on the right.</p>

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

Introduction

Digital Attack Map Top daily DDoS attacks worldwide

[Map](#) · [Gallery](#) · [Understanding DDoS](#) · [FAQ](#) · [About](#) · [g+](#) [Twitter](#) [f](#)



Plan

I

- Contexte général

II

- Cyber Threat Intelligence

III

- Perspectives

Plan

I

- Contexte général

II

- Cyber Threat Intelligence

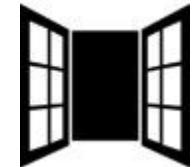
III

- 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.

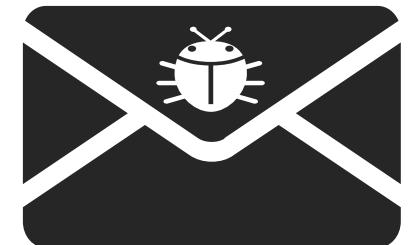


Tendance : industrialisation de la menace.

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, malwaring*),
- 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 cyberspace les systèmes d'information jugés essentiels.

Cyberdéfense (=Etatique)

Mesures techniques

Mesures non-techniques

I. Contexte général

La Cybersécurité :

Cybersécurité

SSI
(Cyberprotection)

Cyberrésilience

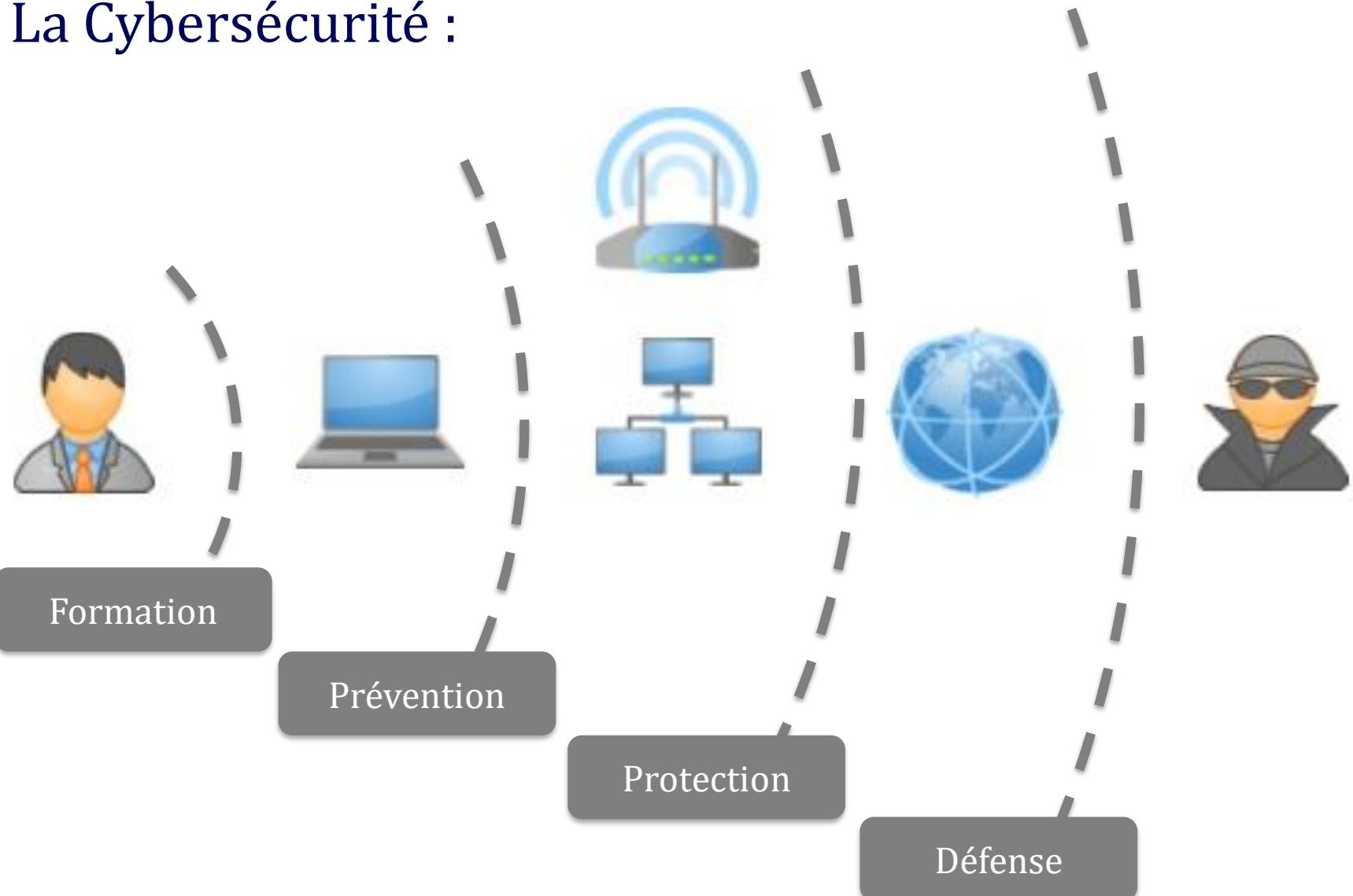
Cyberdéfense
(Lutte
informatique)

Vulnérabilités

Menaces

I. Contexte général

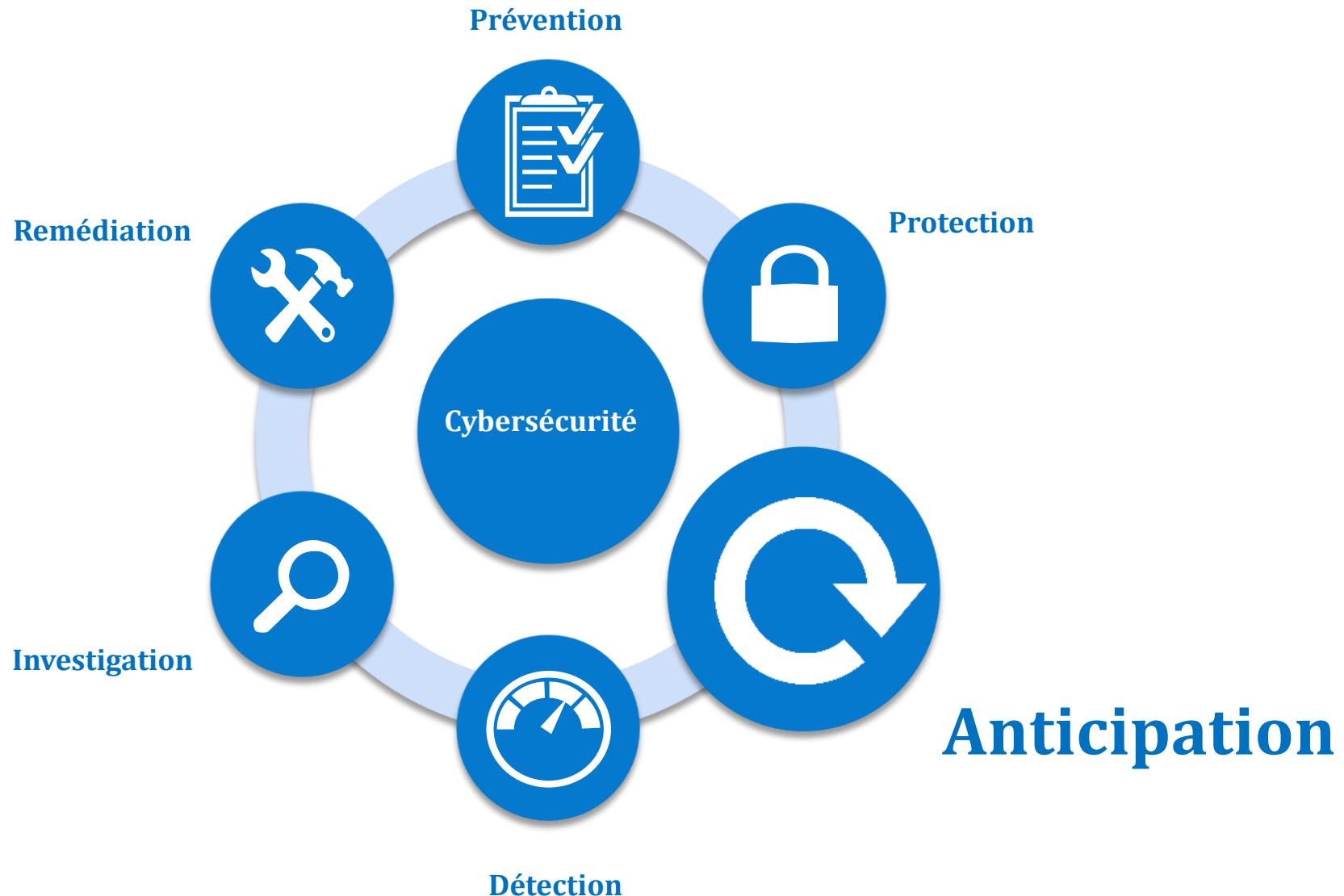
La Cybersécurité :



I. Contexte général

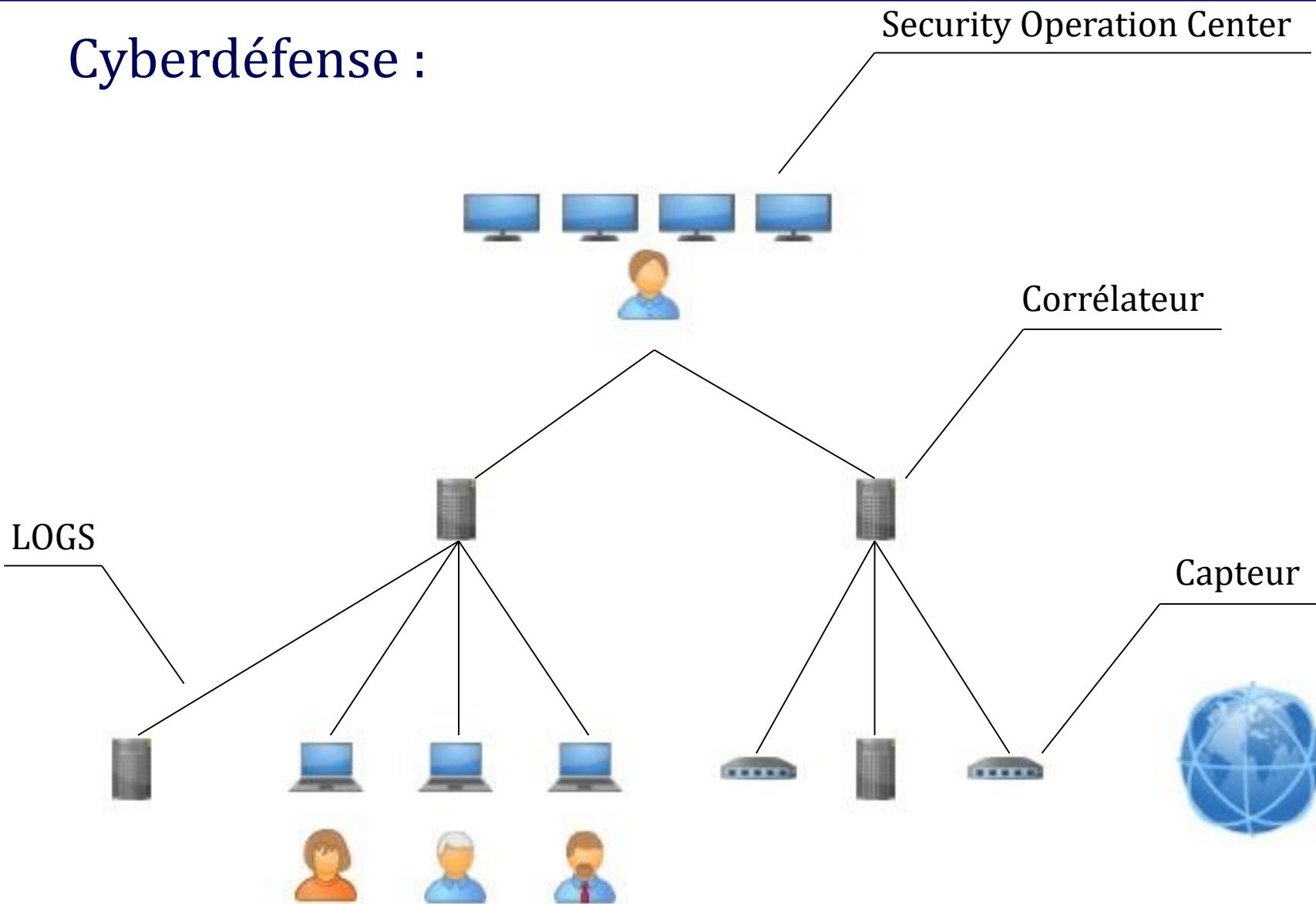


I. Contexte général



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 :

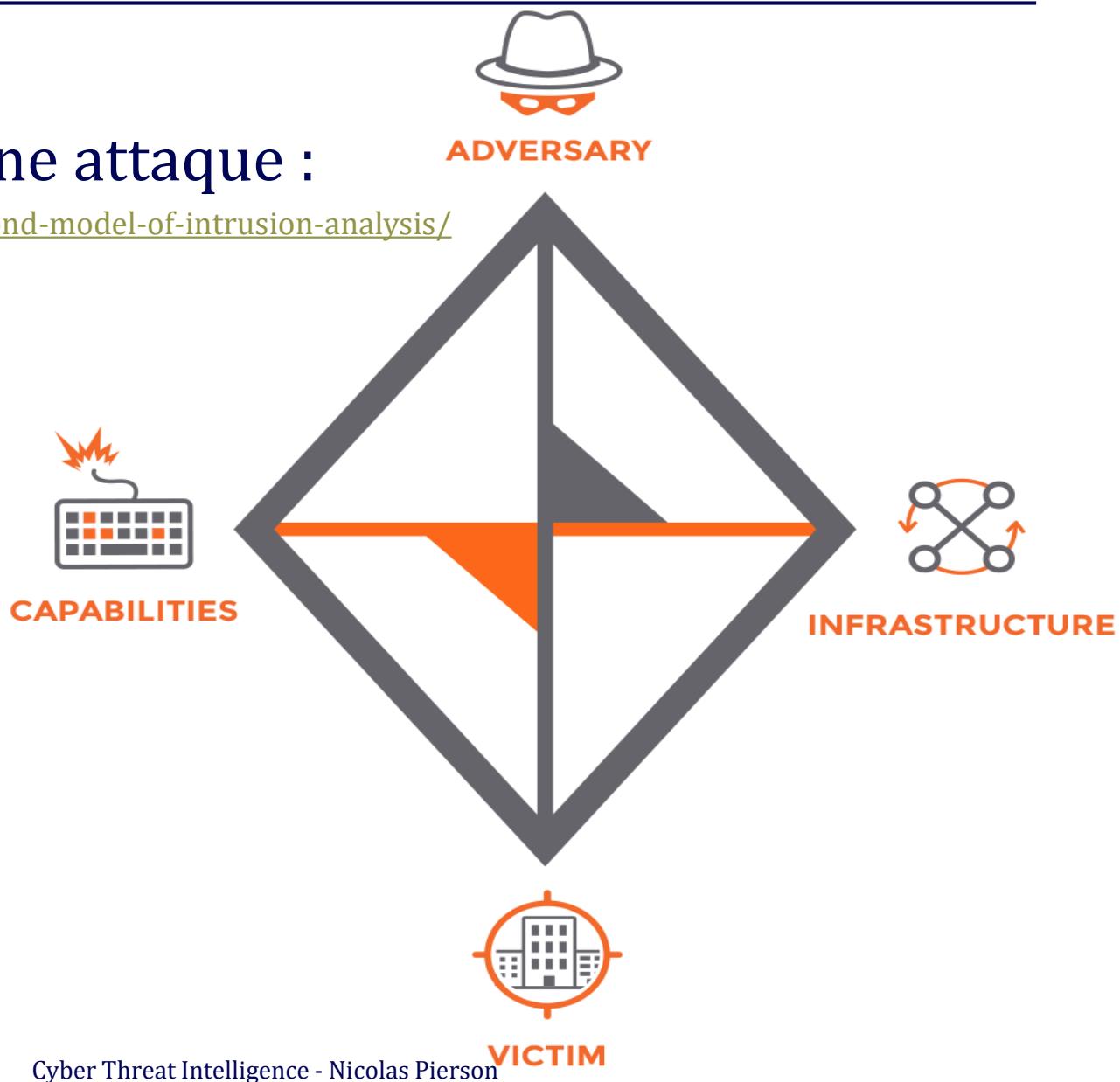
- ✓ la liste des incidents de sécurité redoutés du commanditaire ;
- ✓ **des bases de connaissances acquises auprès d'éditeurs et de sociétés spécialisées en sécurité des systèmes d'information ;**
- ✓ des bases de connaissances internes issues de l'expertise du prestataire :
 - veille et qualification 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 :

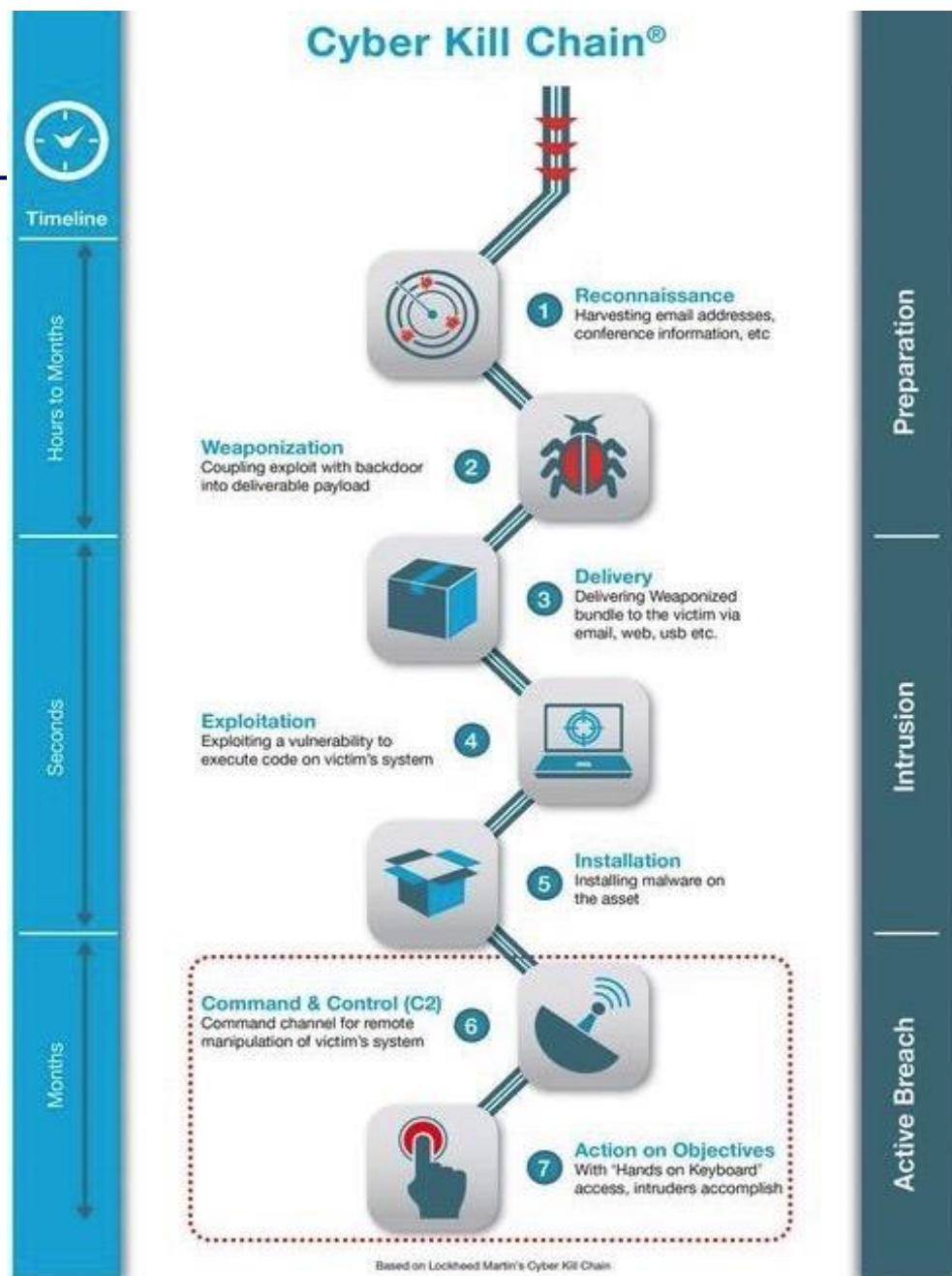
<https://threatconnect.com/tag/diamond-model-of-intrusion-analysis/>



I. Contexte général

Cyber Kill Chain :

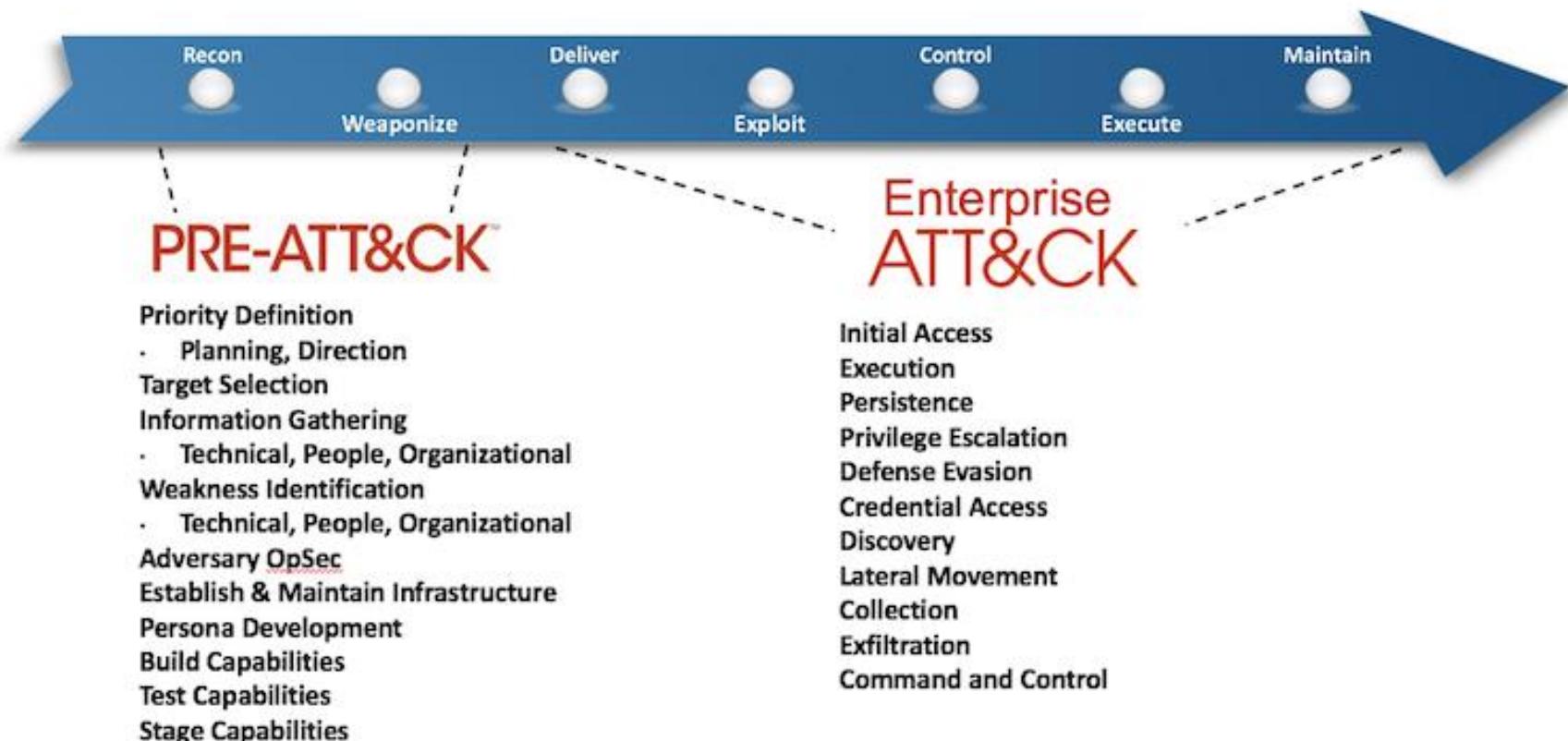
- ✓ Reconnaissance
- ✓ Préparation
- ✓ Livraison
- ✓ Exploitation
- ✓ Installation
- ✓ Contrôle
- ✓ Action



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

I. Contexte général

MITRE ATT&CK :



I. Contexte général

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Or-in Compromises	Scheduled Task			Binary Padding	Network Sniffing					Automated Collection	Data in Detection
Exploit Public-Facing Application	Launchd1		Access Token Manipulation	Account Manipulation	Account Discovery			Auto Capture	Commodity Usual Port	Data Compromised	Data Breached or Impact
External Remote Services	Local Job Scheduling		Bigass User Account Control	Batch History	Application Window Discovery			Automated Collection	Communication Through Removable Media	Data Encrypted	Data Encrypted
Hardware Additions	LSASS Driver		Extra Window Memory Injection	Brute Force	Distributed Component Object Model			Clipboard Data	Clipboard Data	Data Transfer Size Limits	Data Content Wipe
Replication Through Removable Media	Trap		Process Injection	Credentials in Files	Domain Trust Discovery			Connection Proxy	Custom Command and Control Protocol	Edit In File Over Other Network Medium	Endpoint Denial of Service
Scryptching Attachment	AppleScript		DLL Search Order Hijacking	Credentials in Registry	File and Directory Discovery			Data from Local System	Custom Cryptographic Protocol	Edit In File Over Command and Control Channel	Firmware Corruption
Scryptching Link	CIMSTP		Image File Execution Options Injection	Credentials in Registry	Logon Scripts			Data from Network Shared Drive	Data Encoding	Edit In File Over Network Protocol	File System Recovery
Scryptching via Service	Compiled HTML File		PLA Modification	Duplication for Credential Access	Network Share Discovery			Data Staged	Data Obfuscation	Resource Hijacking	Network Denial of Service
Supply Chain Compromise	Dynamic Data Exchange	AppGen DLLs	Clear Core Read/Write	Feasible Authentication	Pass the Hash			Email Collection	Device Flocking	Run-time Data Manipulation	Run-time Data Manipulation
Trusted Relationship	Execution through API	AppGen DLLs	CIM STP	Hooking	Password Policy Discovery			Remote Desktop Protocol	Input Capture	Exfiltration Over Physical Medium	Service Stop
Valid Accounts	Execution through Native API		Code Signing	Input Prompt	Peripheral Device Discovery			Remote File Copy	Domain Generation Algorithms	Scheduled Transfer	Stolen Data Manipulation
			Dll Hijacking	Input Response	Permissions Group Discovery			Remote Services	Man in the Browser		Transferred Data Manipulation
			File System Permissions Weakness	Keychain	Process Discovery			Screen Capture			
			Hooking	Query Registry	Reputation Through Removable Media			Video Capture			
Graphical User Interface	Launch Daemon		Component Firmware Hijacking	Remote Systems Discovery	Reusability			Multi-land Communication			
Install4J	New Service		Control Panel Items	Private Keys	Shared Webcam						
Mimik	Path Interception		Component Object Model Hijacking	System Information Discovery	SSH Hijacking						
PowerShell	PSofMonitor		DDoS/DoS	Secured Memory Configuration	Taint Shared Content						
Regexec/Regasm	Service Registry Permissions Weakness		Decompress/Decompile Files or Information	Two-Factor Authentication Interception	Third-party Software						
Rgexec2	SeAdd and SeGetd		Decompress/Decompile Files or Information	Windows Admin Shares	Windows Admin Shares						
Rundi32	Startup Items		Desktop Security Tools	Windows Remote Management	Windows Network Connections Discovery						
Scripting	Web Shell		DLL Side-Loading		System Controller Discovery						
Service Execution	Batch, profile and .bat/etc		Execution Guards		System Service Discovery						
Signed Library Prog. Execution	Account Manipulation		Exploration for Privilege Escalation		System Time Discovery						
Signed Script Prog. Execution	Authentication Package		ID History Injection		Virtualization and Sandbox Evasion						
Signed Script Prog. Execution	BIT5 Jobs	Studio	File Deletion								
	Stale		File Permissions Modification								
	Source		File Cache Caching								
	Space after Filenames		File System Log off Offsets								
Third-party Software	Change Default File Association		File System Log off Offsets								
Trusted Developer Utilities	Component Firmware		Group Policy Modification								
User Execution	Component Object Model Hijacking		Hidden Files and Directories								
Windows Management Infrastructure	Create Account		Indicator Removal Tools								
Windows Remote Management	External Remote Services		Indicator Removal on Host								
	Hidden Files and Directories		Inject Command Execution								
XSL Script Processing	Hybridator		Install Root Certificate								
	Kernel Modules and Extensions		Install UI								
	Launch Agent		Launchd1								
	LC_LOAD_DYLIB Addition		LC_MAIN Hijacking								
	Login Items		Memorydump								
	Login Scripts		Modify Registry								
	Modify Event Log Services		NFS Network Share Connection Renewal								
	NetInfo Helper DLL		NTFS File Attributes								
	Office Application Startup		Obliterated File or Information								
	Port Knocking		Port Knocking								
	Re-connect		Process Doppelgänging								
	Redundant Access		Process Hollowing								
	Registry Run Keys / Startup Folder		Redundant Access								
	Re-opened Applications		Regava/Regava								
	Scanner		Regava32								
	Security Support Provider		Rootkit								
	Shortcut Modification		Rundll32								
	SIP and Trust Provider Hijacking		Scripting								
	System Firmware		Signature Integrity								
	System Services		Proxy Execution								
	Time Providers		Signed Script Proxy Execution								
	Windows Management Infrastructure Event Subscription		SIP and Trust Provider Hijacking								
	Writing Helper DLL		Software Padding								
			Space after Filenames								
			Template Injection								
			Timestamp								
			Trusted Developer UI Edit								
			Virtualization Service Edition								
			Web Services								
			XSL Script Processing								

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

© 2019 The MITRE Corporation. All rights reserved. Matrix current as of May 2019.

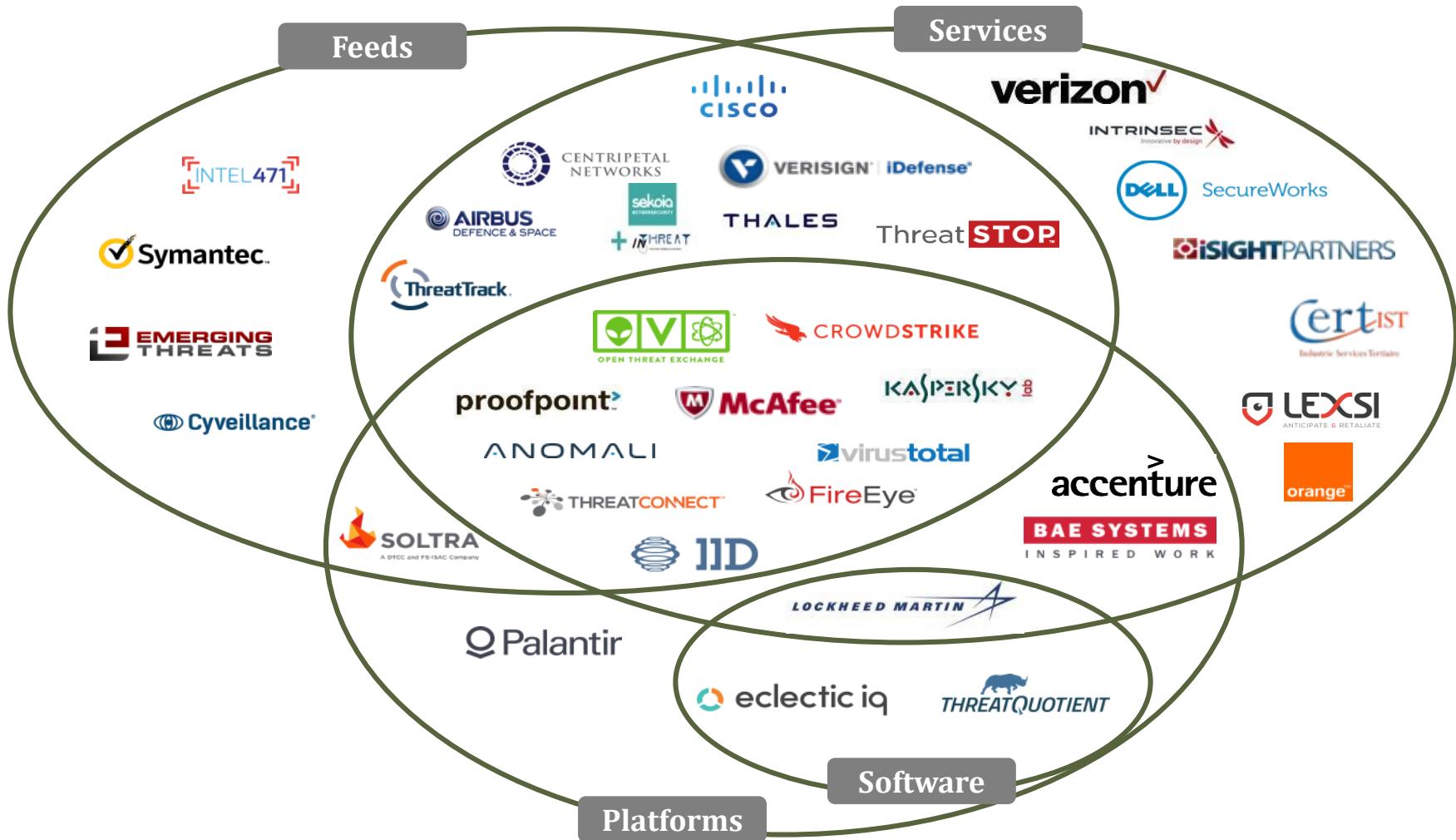
MITRE

I. Contexte général

STIX : Structured Threat Information eXpression (MITRE)

Object	Name	Description
 Attack Pattern	Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
 Campaign	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	Course of Action	An action taken to either prevent an attack or respond to an attack.
 Identity	Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
 Indicator	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
 Intrusion Set	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
 Malware	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	Observed Data	Conveys information observed on a system or network (e.g., an IP address).
 Report	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	Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
 Tool	Tool	Legitimate software that can be used by threat actors to perform attacks.
 Vulnerability	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 ?

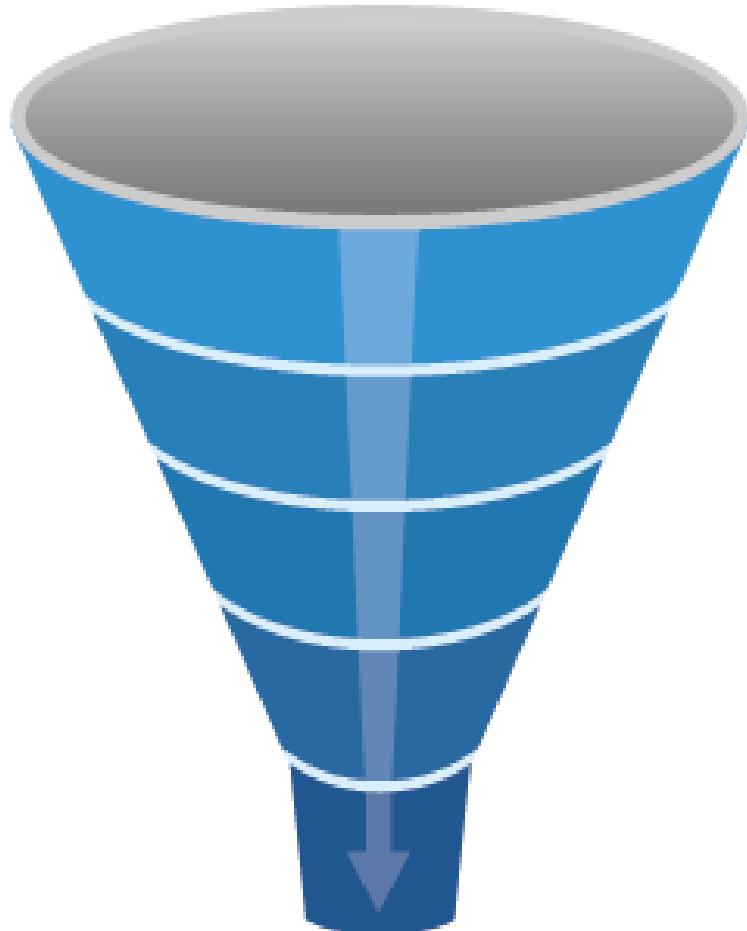
Définition de la Threat Intelligence :

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

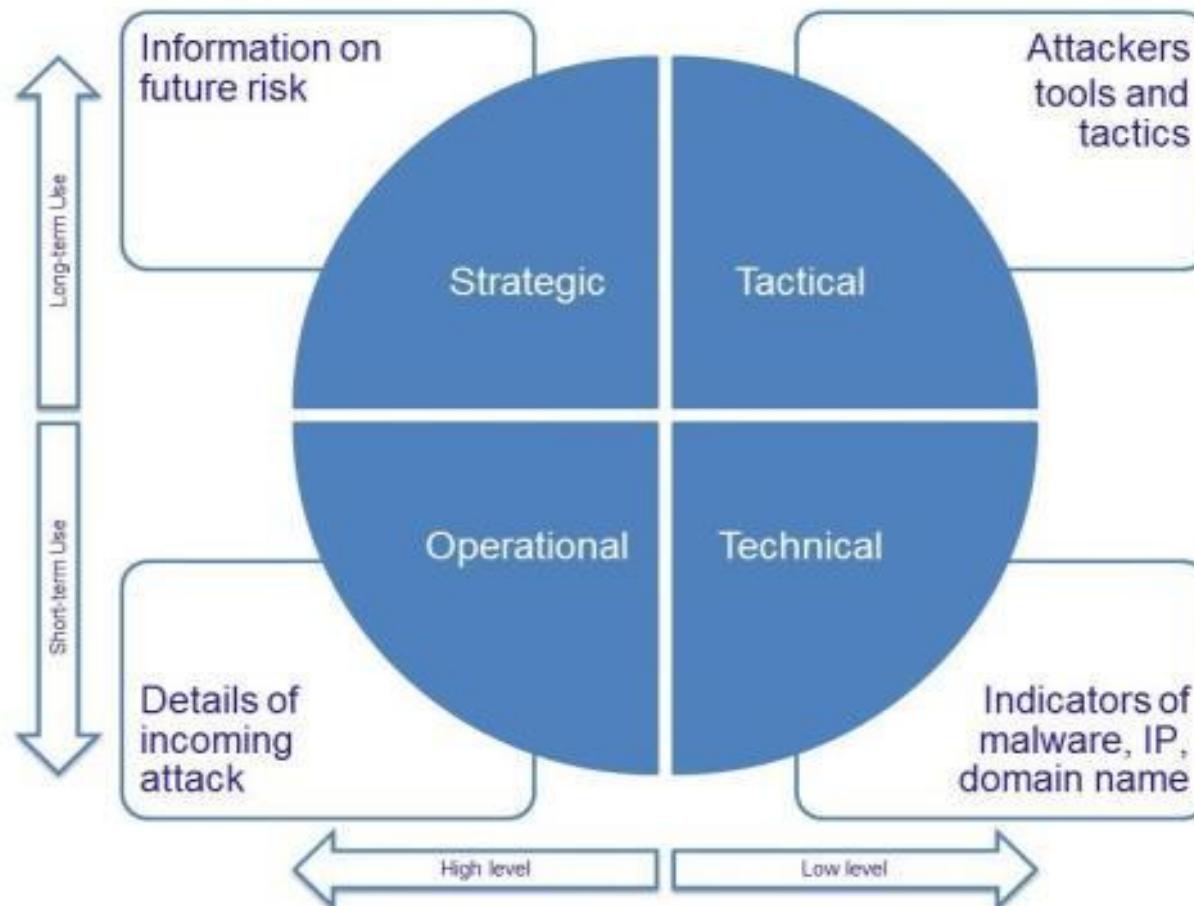
Information is data with a purpose. Once it is assigned a purpose it becomes information.

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 :



II. Cyber Threat Intelligence

Technique



Malware



Indicator



Observed Data

Tactique



Attack Pattern



Intrusion Set



Tool

Opérationnelle



Campaign



Vulnerability



Course of Action

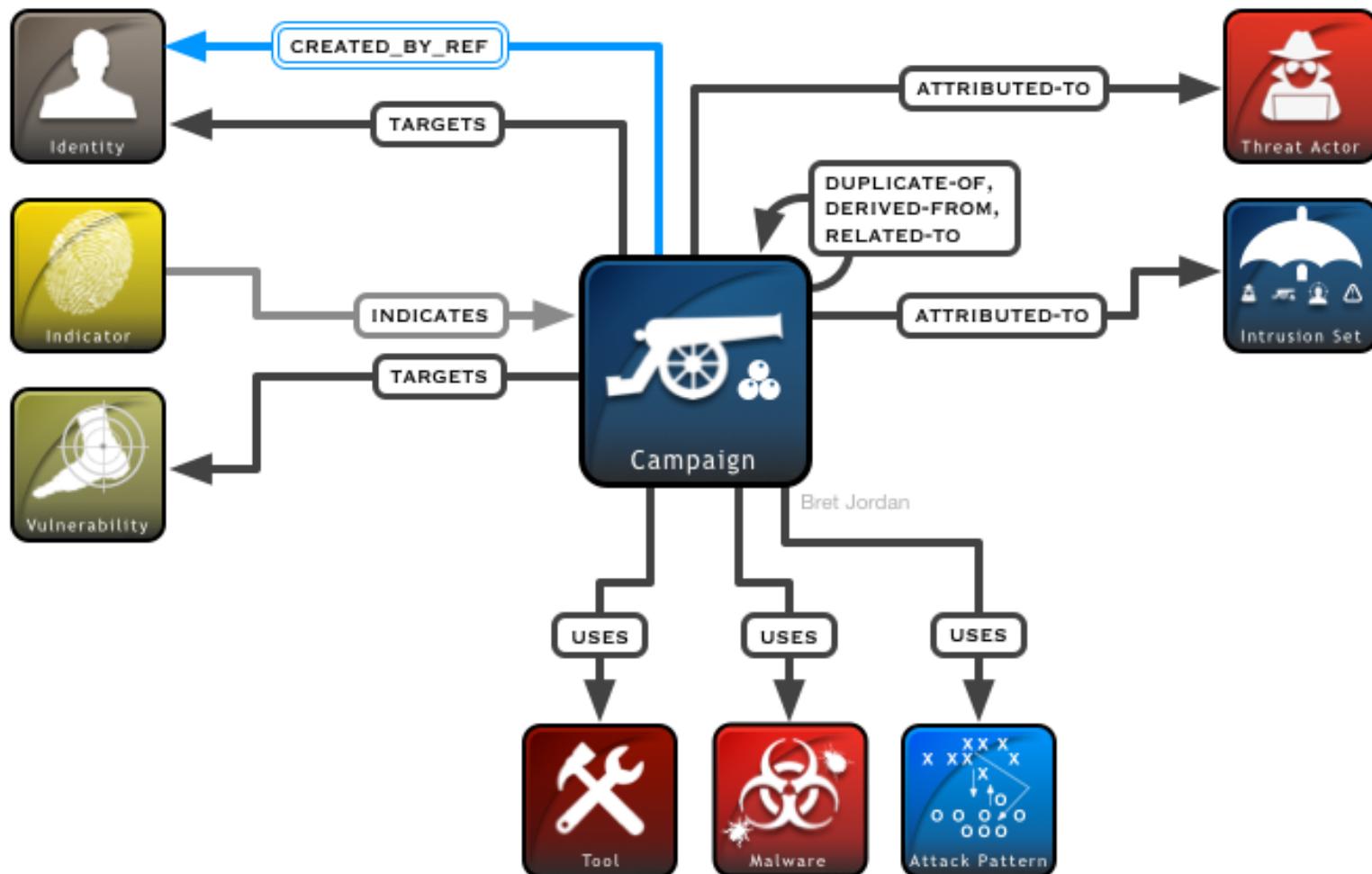
Stratégique



Threat Actor

II. Cyber Threat Intelligence

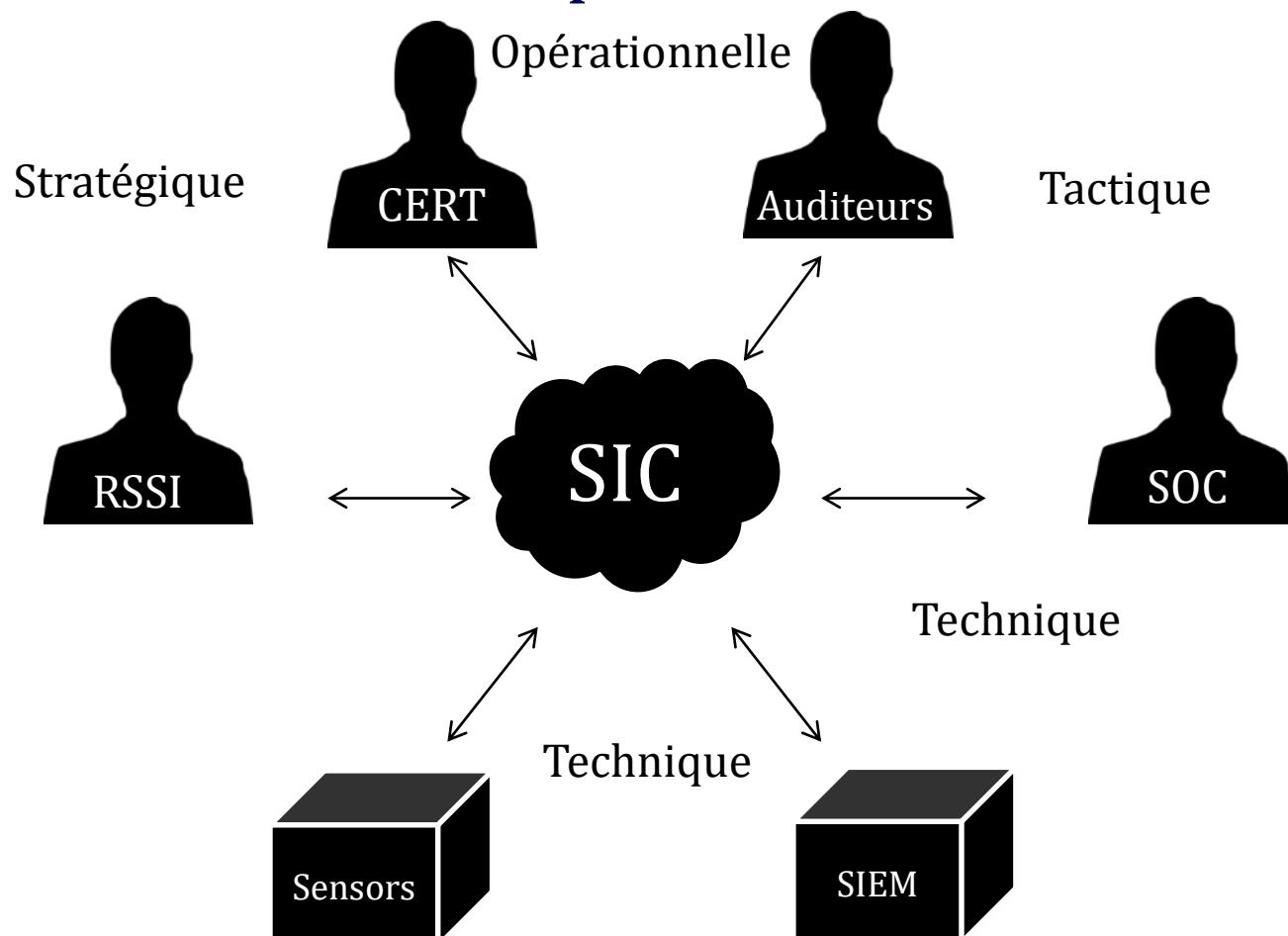
Campaign Relationships STIX 2.0



II. Cyber Threat Intelligence

Pour qui ?

Des destinataires multiples :



SIC: Security
Intelligence
Center

II. Cyber Threat Intelligence

Un écosystème :



II. Cyber Threat Intelligence

Pourquoi ?

Utilisation de la CTI Technique :

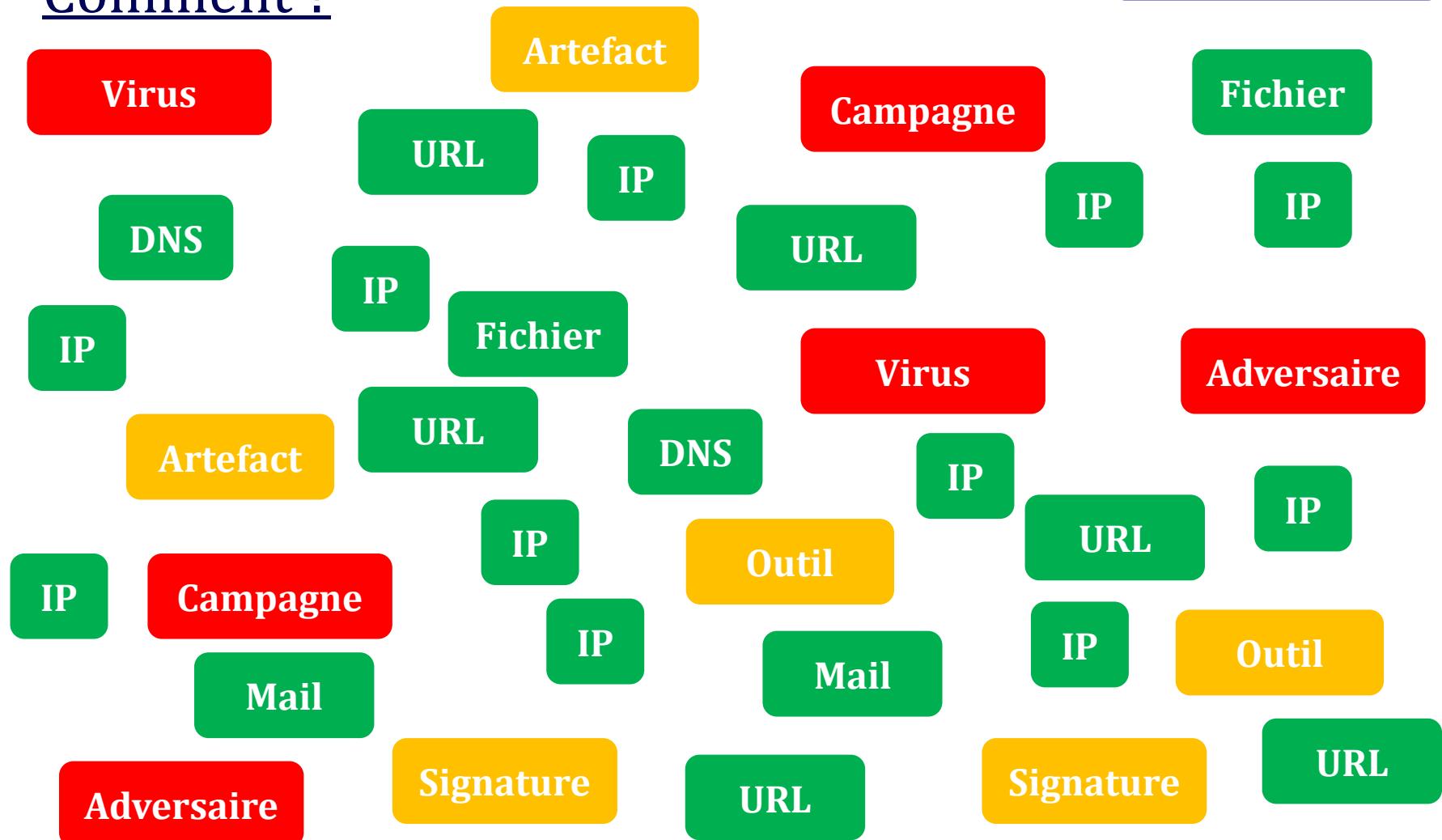
- ✓ Blocage en temps réel (*Firewall, IPS*)
- ✓ Détection (*IDS, Sonde, SOC*)
- ✓ Recherche *a posteriori* (*« Hunting »*)



II. Cyber Threat Intelligence

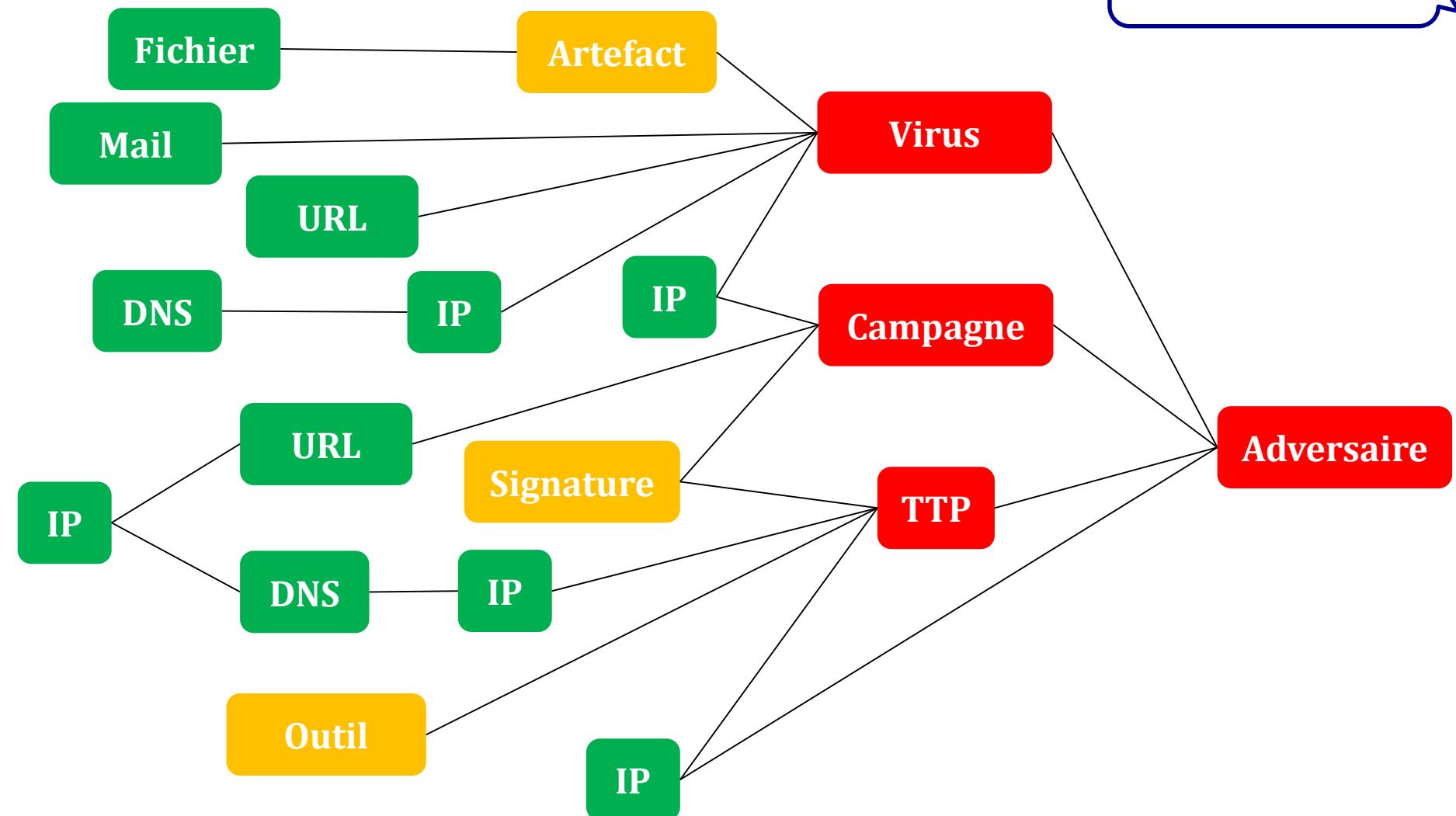
Comment ?

Sans CTI

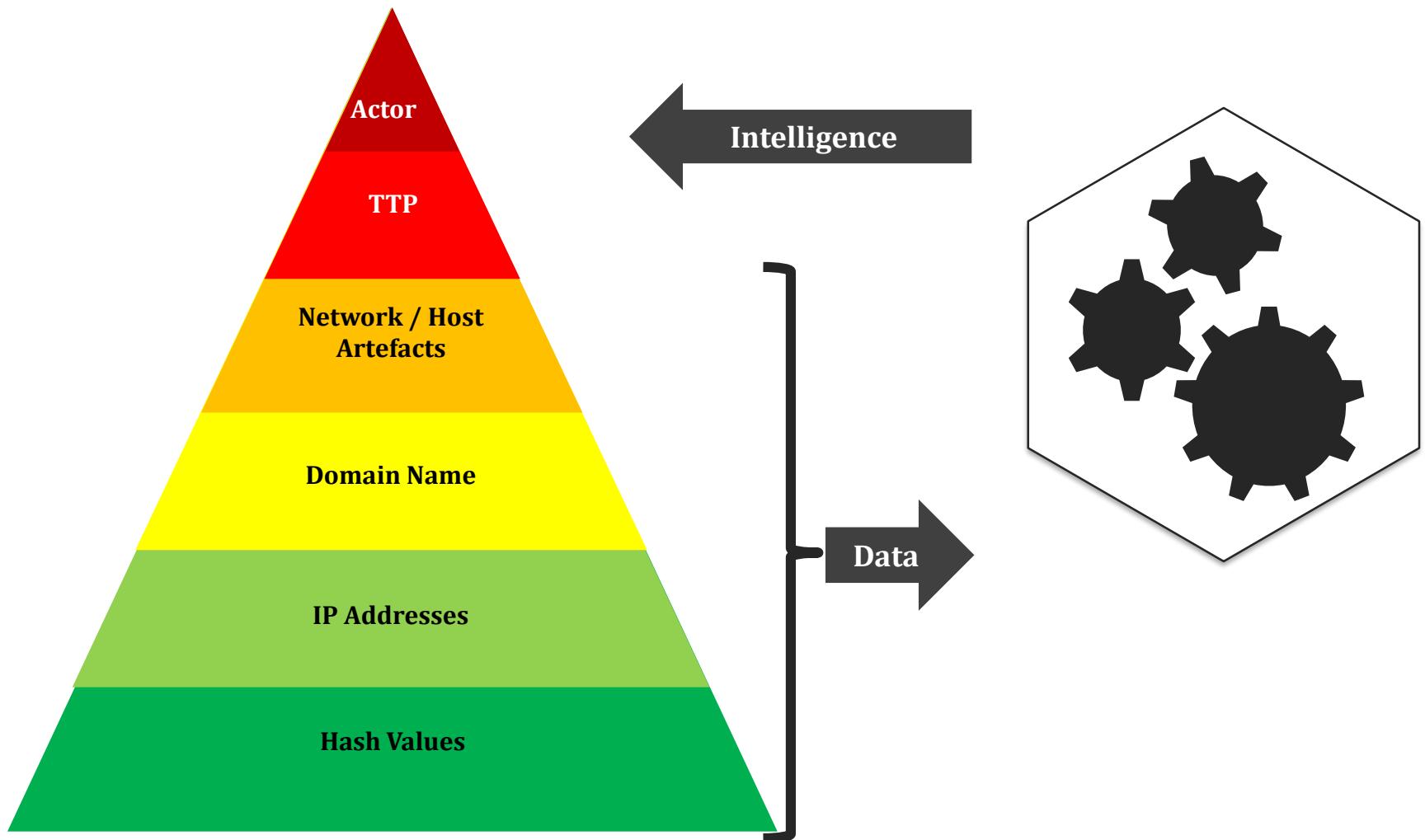


II. Cyber Threat Intelligence

Avec CTI

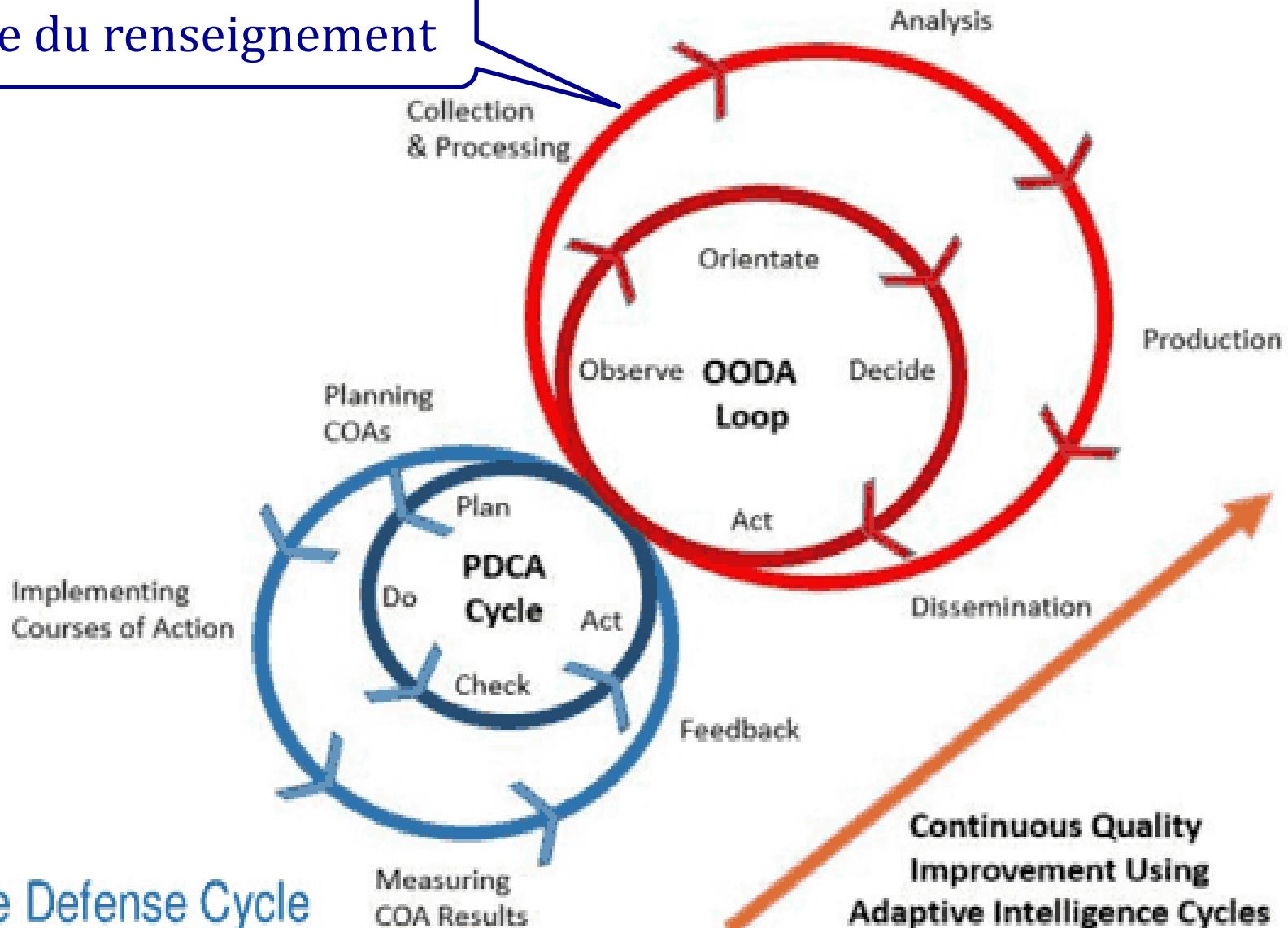


II. Cyber Threat Intelligence



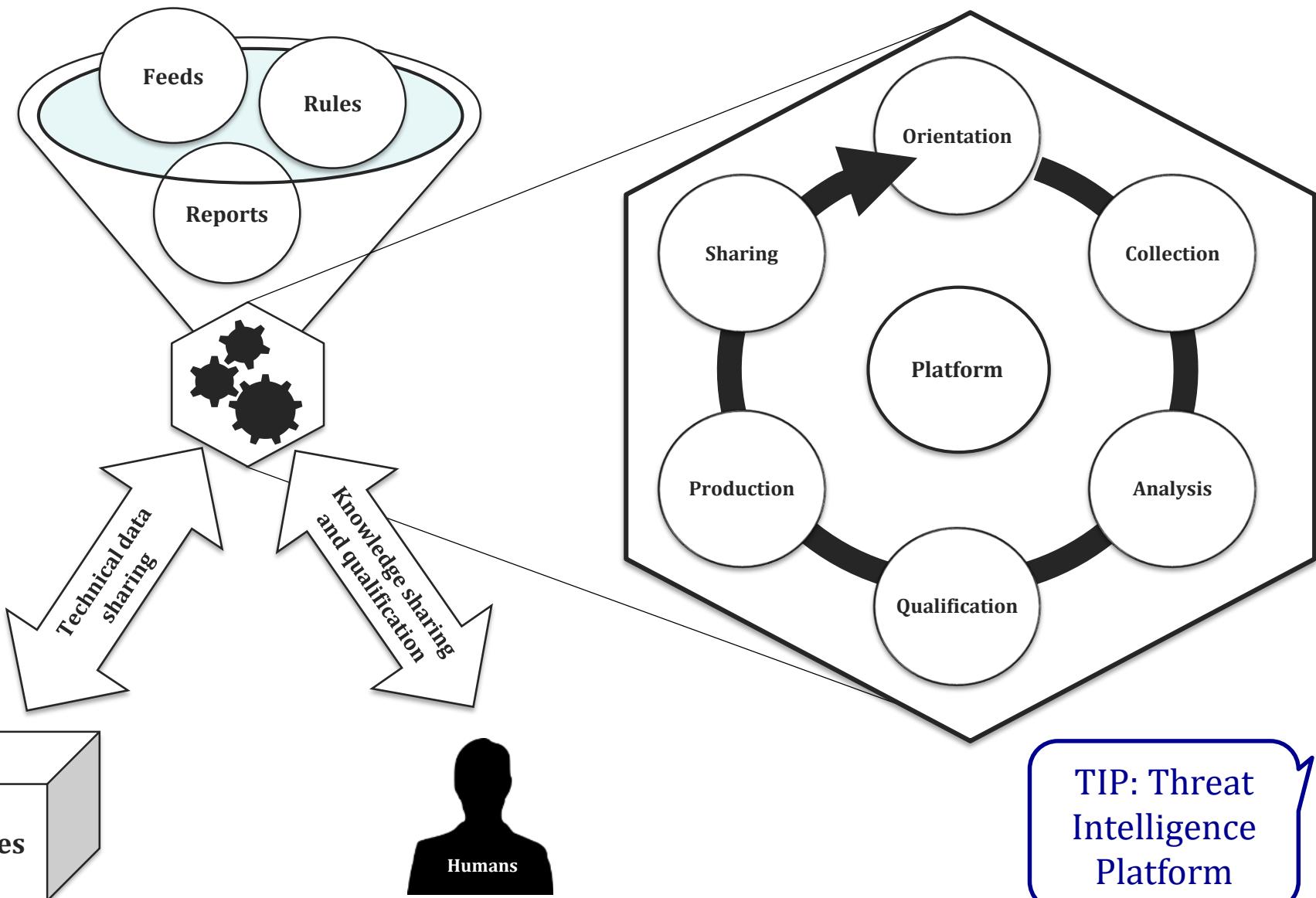
II. Cyber Threat Intelligence

Cycle du renseignement



Active Defense Cycle

II. Cyber Threat Intelligence



Machines



II. Cyber Threat Intelligence

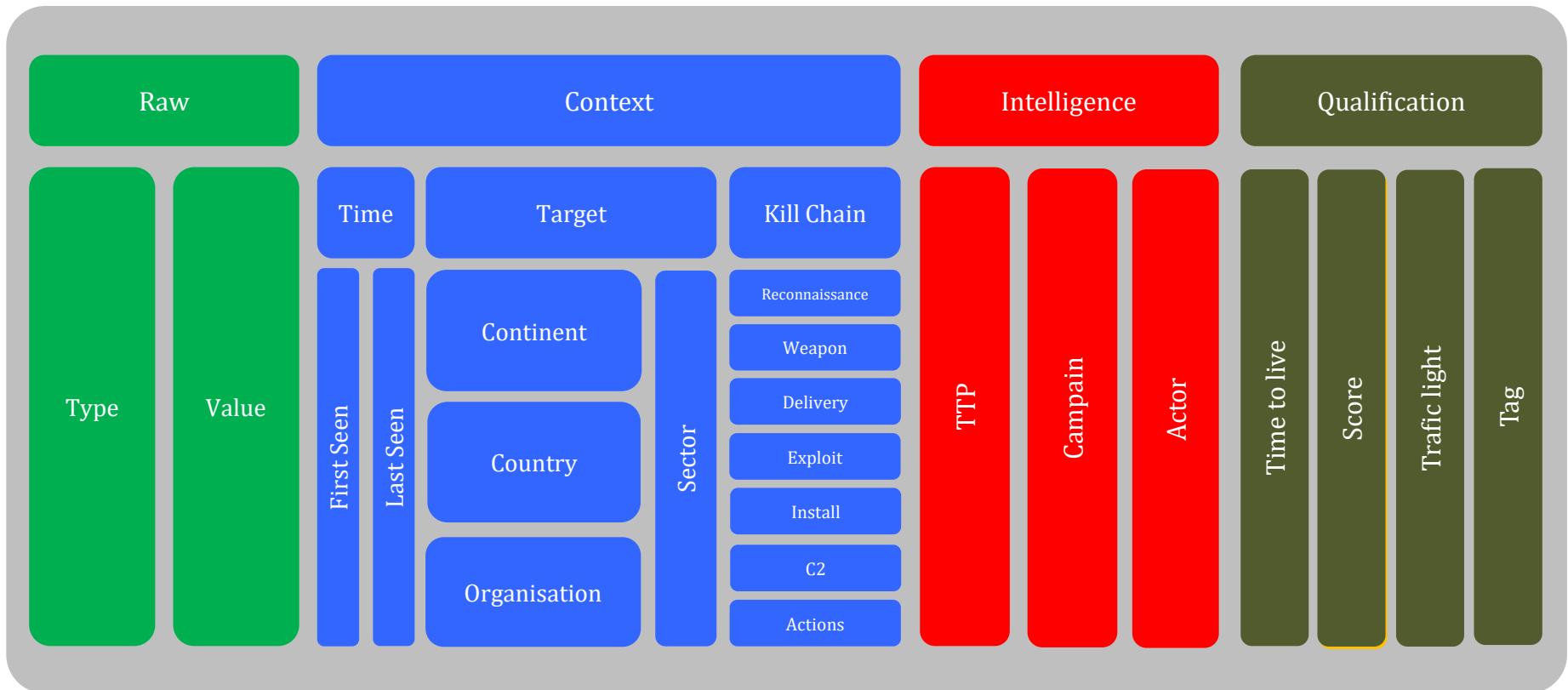


Fonctions d'une plateforme de Threat Intelligence :

- ✓ 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 :



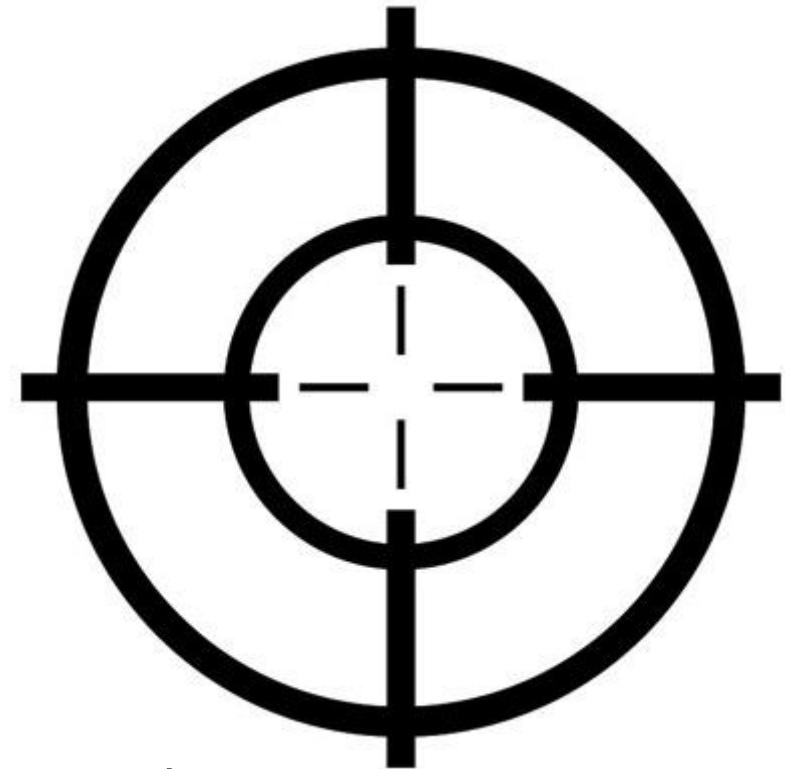
Base de travail

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

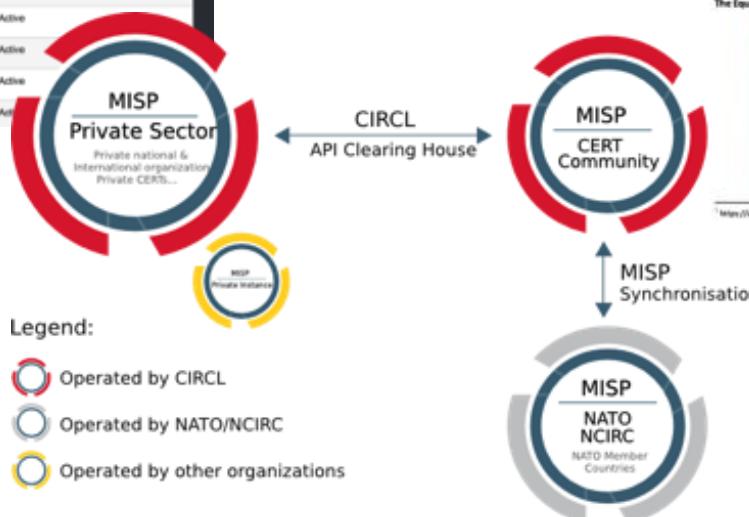
Automatique
(Feeds, rapports, connecteurs)

Collecte

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

The screenshot shows the ThreatQ web application. At the top, there are tabs for Indicators, Events, Adversaries, and Files. A search bar and a 'Create New' button are also at the top. A context menu is open over a table listing 46 OSINT Feeds. The menu options include My Account, ThreatQ Configuration, Incoming Feeds, Whaling Indicators, Exports, Tools, OAuth Management, System Configurations, and Log Out.

ORIGIN	Feed Name	Action	Status
abuse.ch	abuse.ch Feodo Bad IP Blocklist	edit settings	Active
abuse.ch	abuse.ch Feodo Domain Blocklist	edit settings	Active
abuse.ch	abuse.ch Feodo IP Blocklist	edit settings	Active
abuse.ch	abuse.ch Pateno Domain Blocklist	edit settings	Active
abuse.ch	abuse.ch Pateno IP Blocklist	edit settings	Active
abuse.ch	abuse.ch SSLBL (Extended)	edit settings	Active
abuse.ch	abuse.ch SSLBL IP Blocklist	edit settings	Active
abuse.ch	abuse.ch SSLBL SSL Blocklist	edit settings	Active
abuse.ch	abuse.ch ZeuS Block Bad FQDNs	edit settings	Active
abuse.ch	abuse.ch ZeuS Block Bad IPs	edit settings	Active



II. Cyber Threat Intelligence

THREATQ

Indicators ▾ Events Adversaries Files Create New ▾ Search ▾

RESURRECTION OF THE EVIL MINER edit

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

+ Add Details Delete

RELATED INDICATORS

% Link Indicator

RELATED EVENTS

% Link Event

RELATED ADVERSARIES

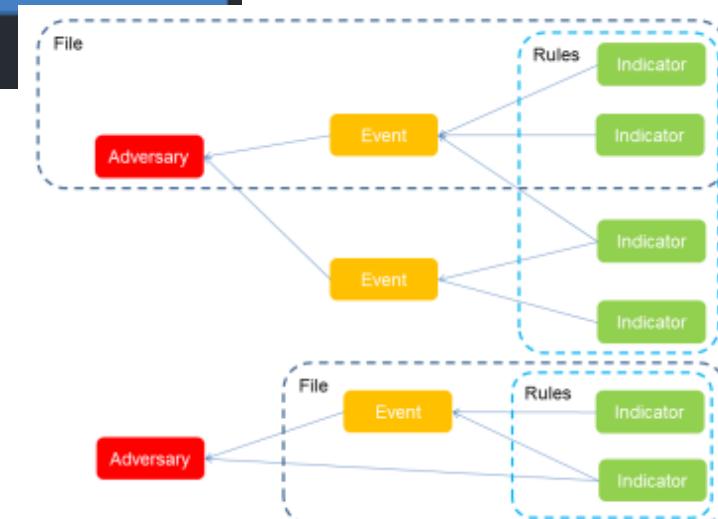
% Link Adversary

RELATED FILES

% Link File

COMMENTS

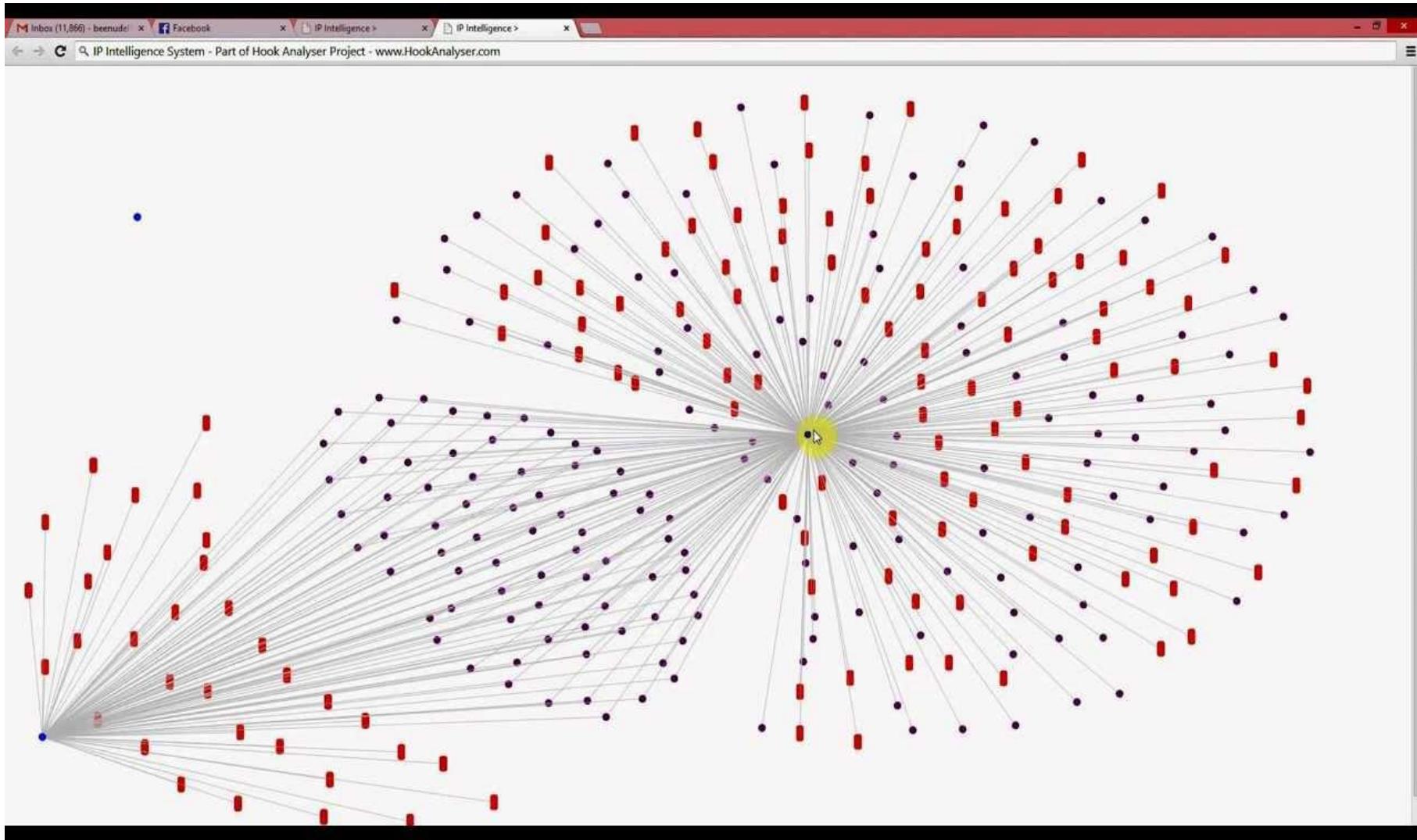
AUDIT LOG



Analyse

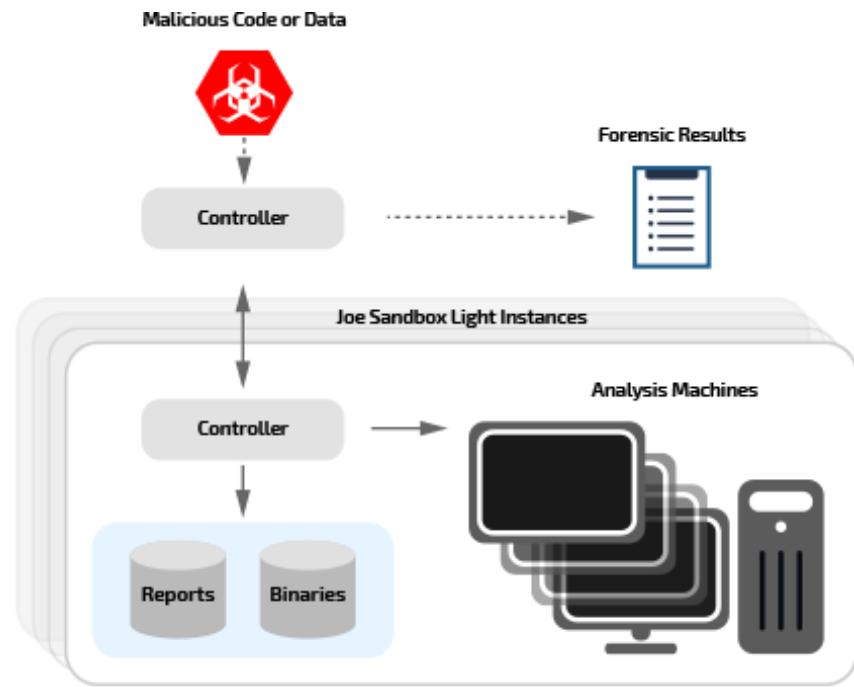
II. Cyber Threat Intelligence

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, a sidebar lists various entities: IP Address (208.71.106.48), Indicator Summary, Related Adversaries (0), Related Events (4), Related Files (0), Related Indicators (0), Comments (0), and Data Enrichment. The main area shows two detailed views of indicators.

Indicator Summary View: Shows an IP address (208.71.106.48) with a status of "Active".

Indicator Detail View 1: Shows an indicator for "Malspam 2016-08-26 (.wsf in .zip) - campaign: "Voice Message from Outside Caller" (0x5f323664)". It includes a summary table with columns for Attribute Key (Comment, IQRisk Score, IQRisk Category) and Attribute Value (download location (W), 123, 35). A note indicates the event was created on 06/27/16 at 06:04pm.

Indicator Detail View 2: Shows another indicator with a status of "Active". It includes a summary table with columns for Attribute Key (Status, Campaign_type) and Attribute Value (Active, Malspam). A note indicates the event was created on 06/29/16 at 03:18am.

Score (highlighted in red) is positioned below the first detail view, and **Statut : actif/inactif** (highlighted in red) is positioned below the second detail view.

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 it is a search bar and a 'Create New' dropdown. A modal window titled 'OUTPUT FORMAT' is open, asking 'Which type of information would you like to export?'. The 'Indicators' option is selected. Under 'Output type:', 'text/plain' is chosen. In the 'Special Parameters (optional)' section, there's a note about providing a URL to refine the export. Below the modal, there's an 'Output Format Template' section with some code and an 'Insert' button. At the bottom of the modal are 'Save Settings' and 'Cancel' buttons.

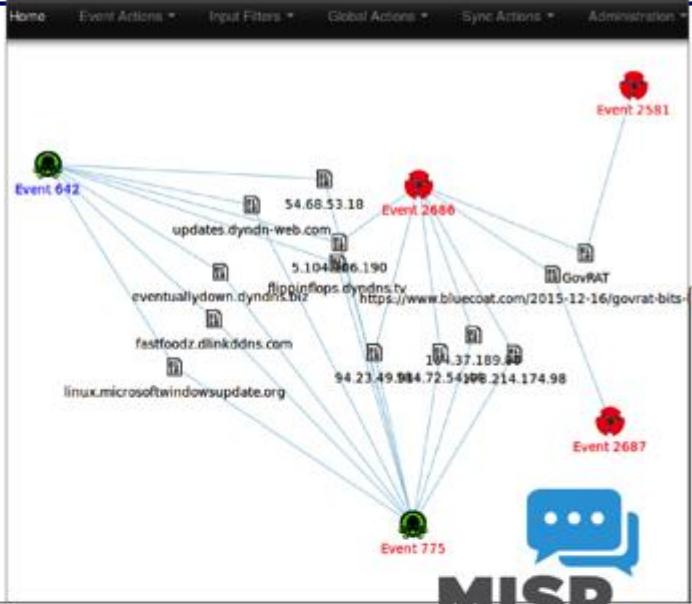
```
#fields($stab$)indicator($stab$)indicator_type($stab$)meta.source($stab$)meta  
(foreach $data as $indicator)  
(assign $var=$parts value$);  
($explode $indicator.value$)  
alert udp any any->any 53 (msg:"ThreatQ: DNS Query - (foreach $pa  
$sp){$sp$count_characters}{$sp}($foreach{j=0 00 01 00 01}; nocase;  
classtype:ThreatQ; sid:($indicator.id+8400000); rev:1)  
($foreach)
```

Save Settings or 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	
222.21.160.15	
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

TLP Taxonomy Library

ID	Name	Taxonomy	Tagged Events
6	APT	tp	31
7	Actionable: NO	tp	5
3	TLP:AMBER	tp	131
8	TLP:EX:CHR	tp	11
5	TLP:GREEN	tp	550
4	TLP:RED	tp	3
2	TLP:WHITE	tp	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

Tag Expanded

Tag	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="radio"/>
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="radio"/>
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="radio"/>
tip:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	<input type="radio"/>
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="radio"/>



Partage

Cyber Threat Intelligence - Nicolas Pierson

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

- Perspectives

III. Perspectives

Apport de la « science des données » :

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

Threat Intelligence

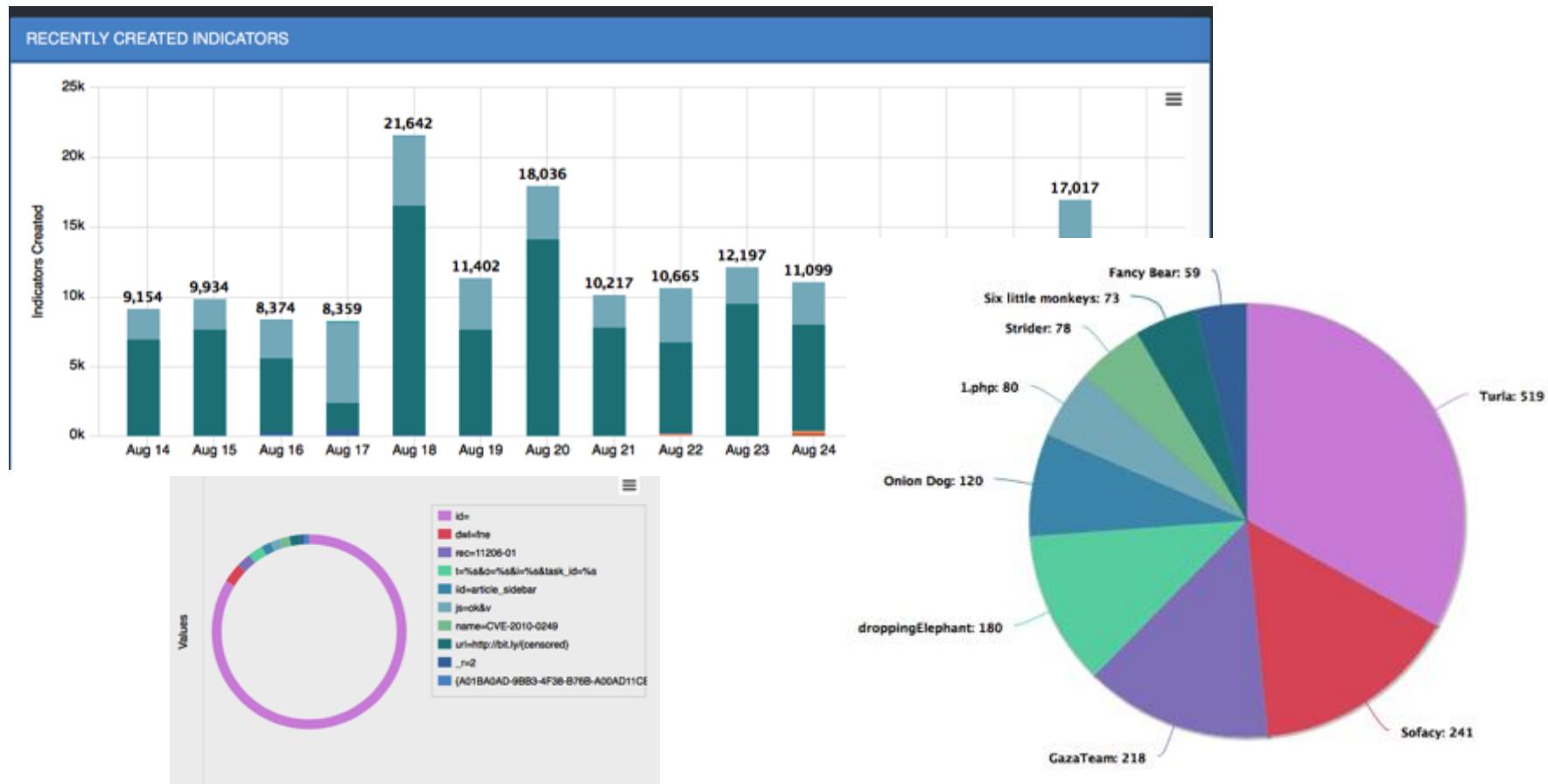
Mais aussi :

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

Cyberdéfense

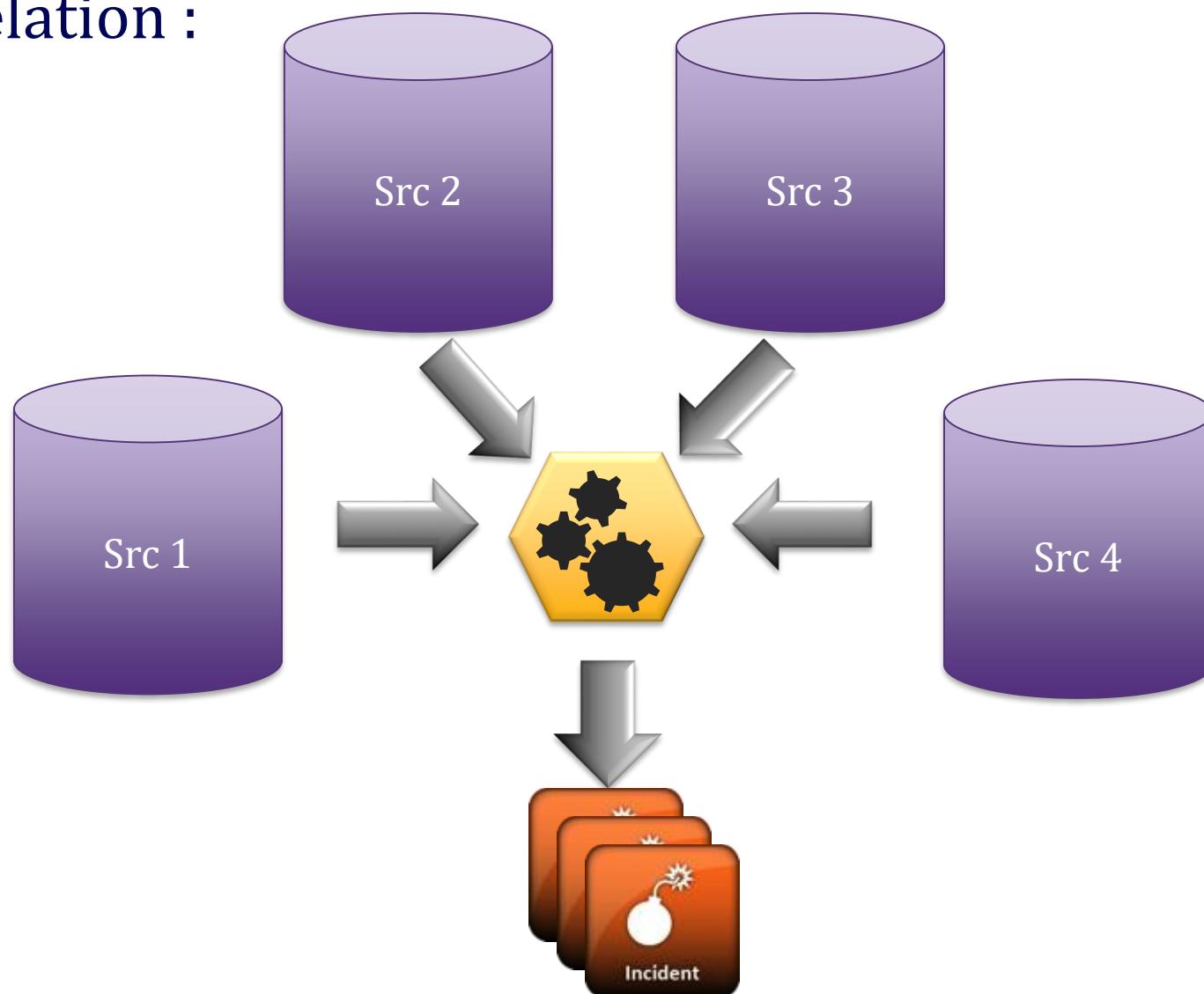
III. Perspectives

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



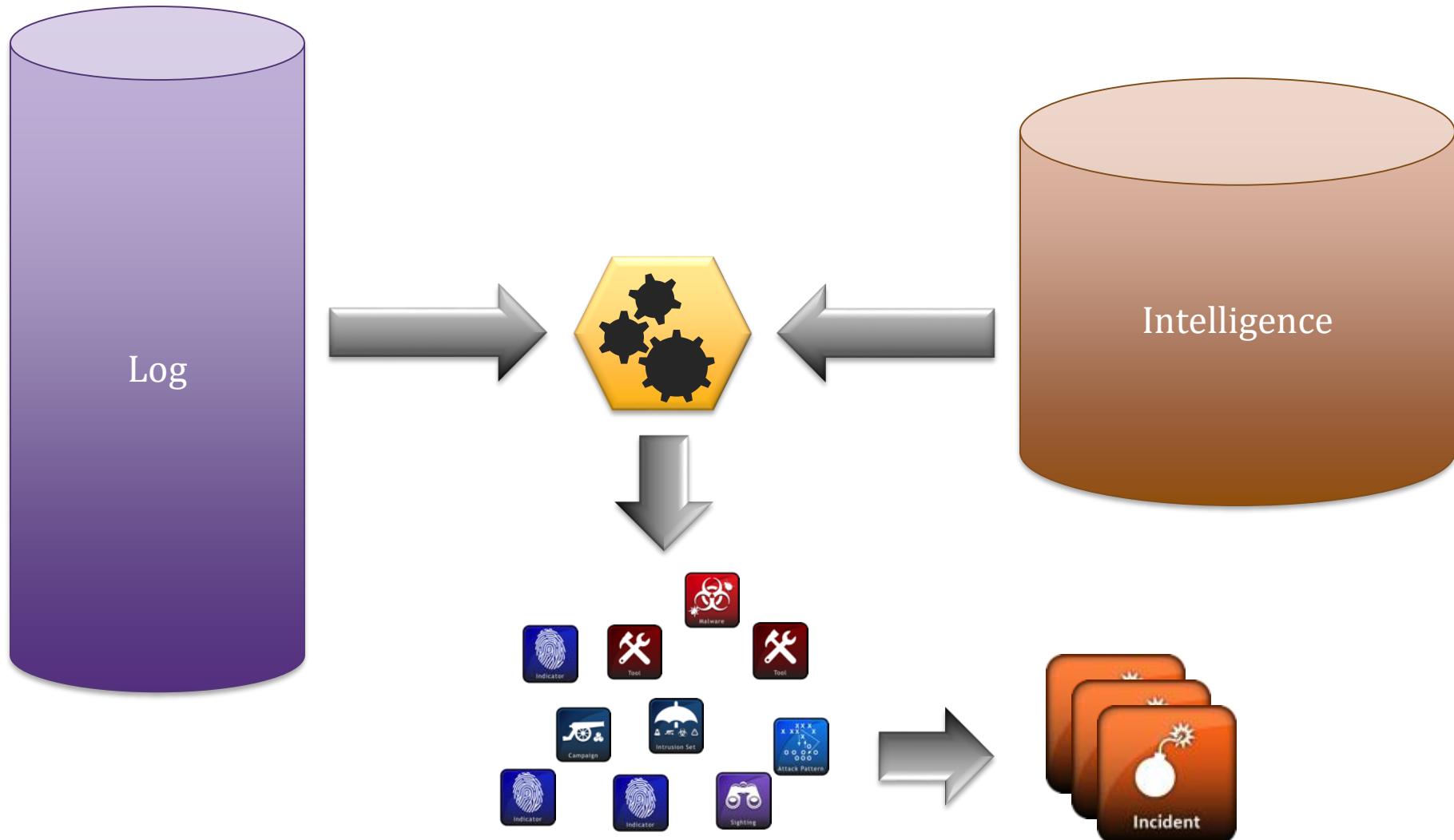
III. Perspectives

Corrélation :



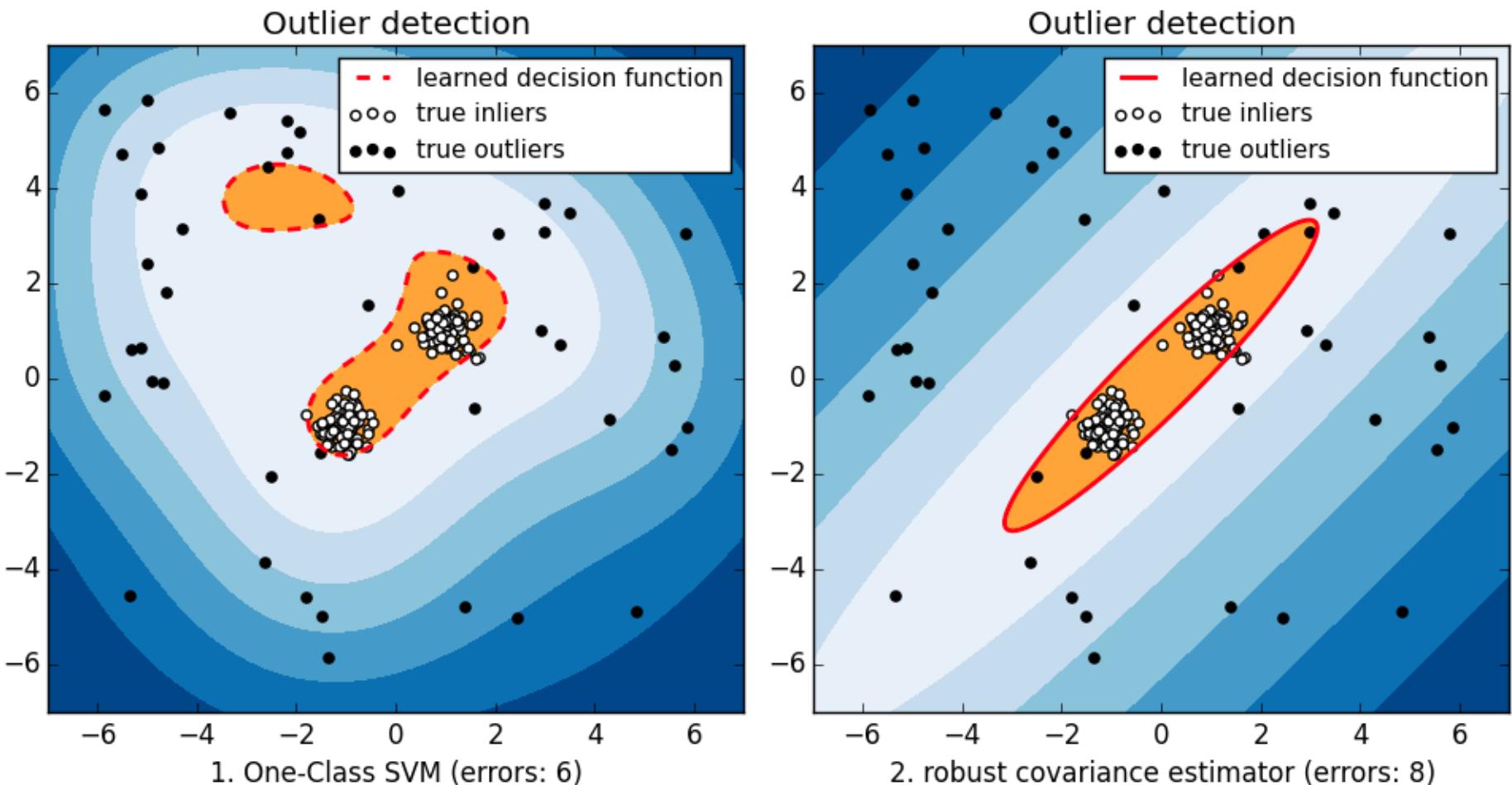
III. Perspectives

Recherche/hunting :



III. Perspectives

Analyse comportementale :



III. Perspectives

Recherche de signaux faibles :

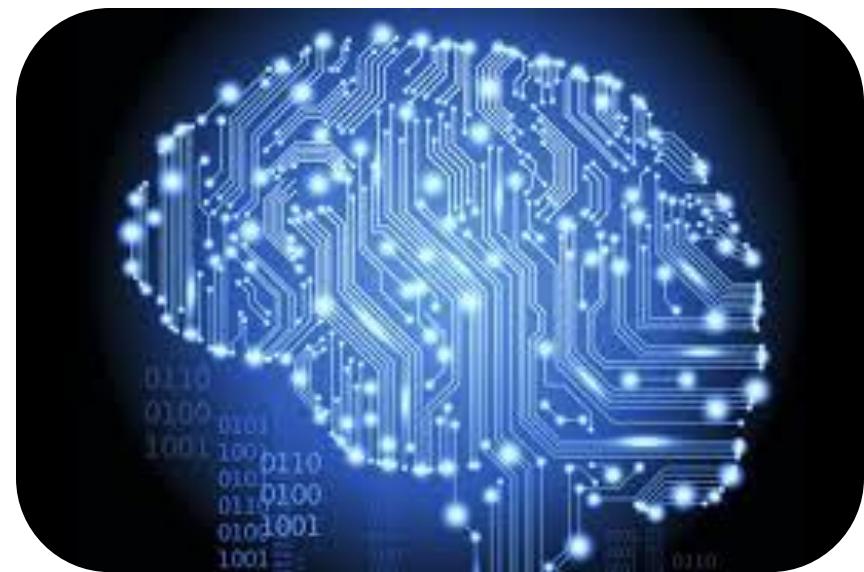
```
12/30 01:42:32 23.75.345.200 example.com /index.php?2346354=-349087 WordPress/3.7.2
12/30 01:42:31 23.75.345.200 example.com /index.php?7231344=4454226 WordPress/3.3.1
12/30 01:42:25 23.75.345.200 example.com /index.php?1243847=9161112 WordPress/3.7.2
12/30 01:42:23 23.75.345.200 example.com /index.php?8809549=4423410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

✓ **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