THREAT INTELLIGENCE
pour quoi faire ?

#OSSIRB #20160324

BIO

- @davidbizeul - https://fr.linkedin.com/in/bizeul
- Fondateur d'inThreat
- CSIRT Airbus Cybersecurity
- CERT Société Générale
- Publications threat intel
  - Russian Business Network
  - Pitty Tiger

REPONSE

CONCEPTS

- Avant d'investiguer, besoin de maîtriser :
  - L'accès à l'information
  - Le traitement des données
  - La structuration de l'information
  - La distribution de l'information
- Cf back to basics (cycle du renseignement)

TLP#1

CONCEPTS

RED - Personal for named recipients only

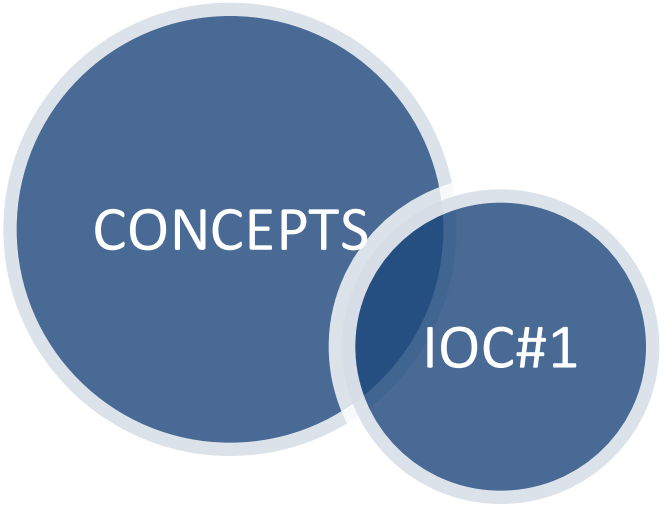
AMBER - Limited distribution

GREEN - Community wide

WHITE - Unlimited (subject to copyright)

CONCEPTS

TLP#2



IP

AS

HASH

MUTEX

CONCEPTS

TTP#1

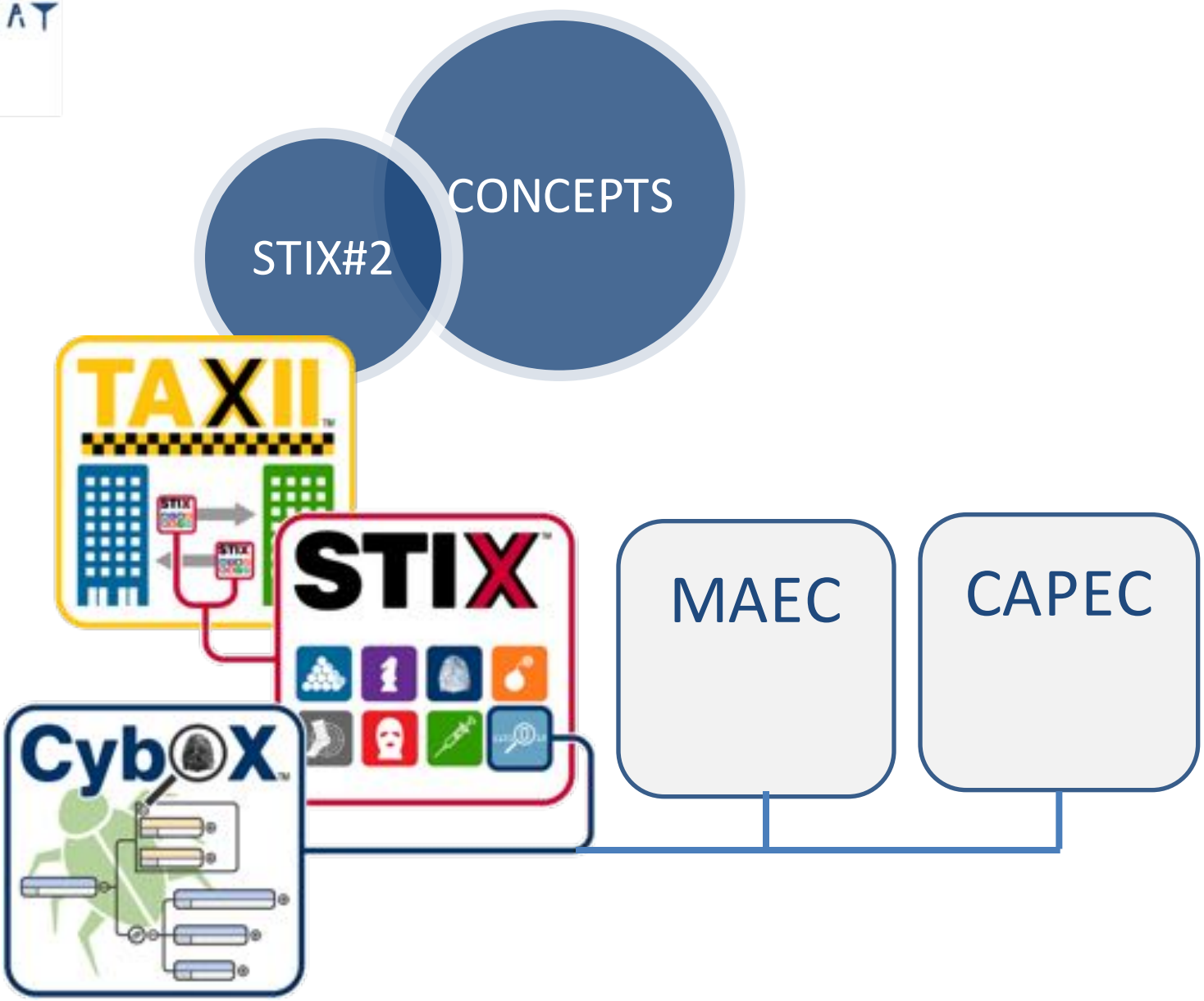
INTHREAT

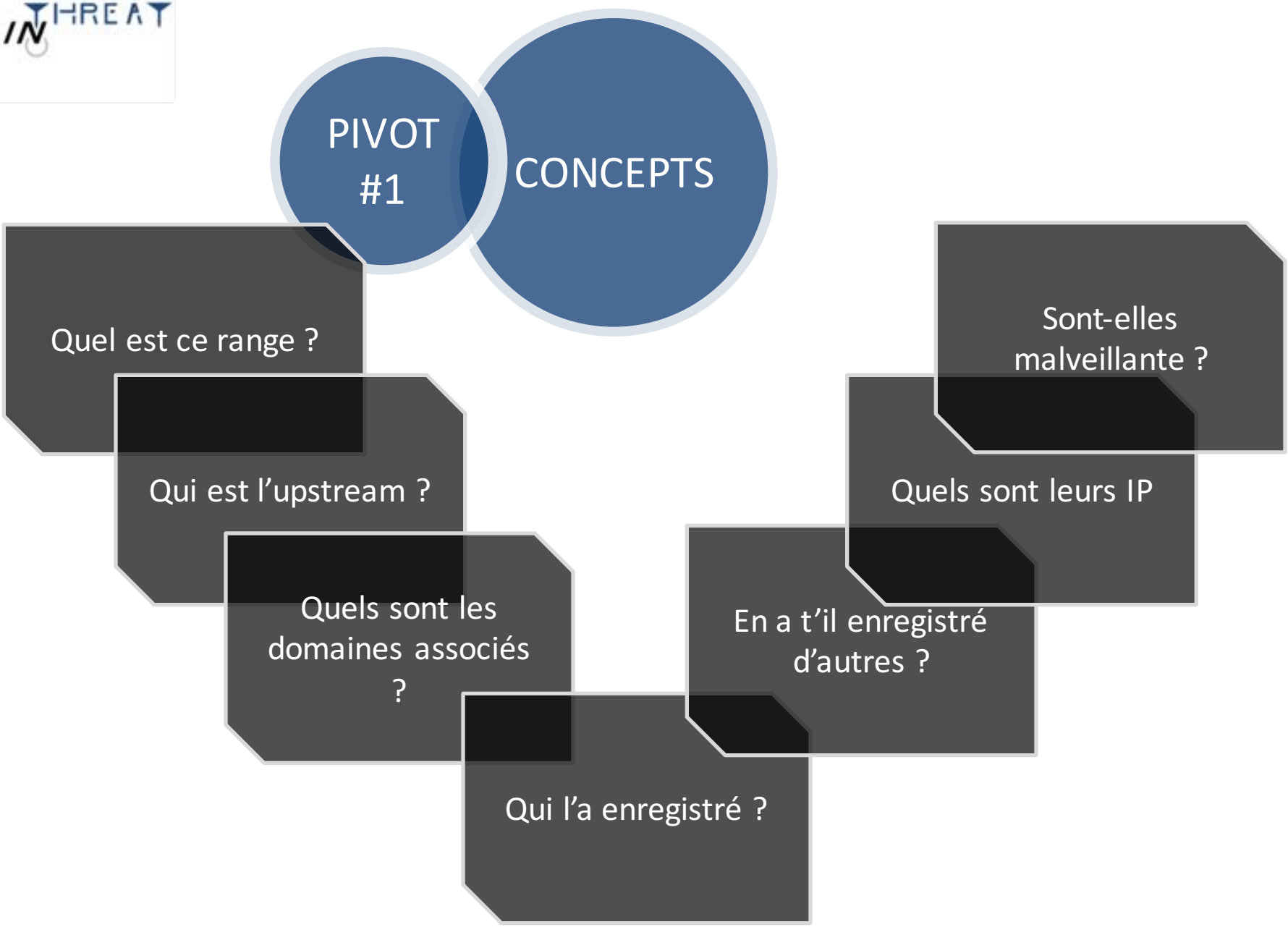
CONCEPTS

TTP#2

CONCEPTS

STIX#1


CONCEPTS
STIX#2
TAXII
STIX
CybOX
MAEC
CAPEC


PIVOT #1
CONCEPTS
Quel est ce range ?
Qui est l'upstream ?
Quels sont les domaines associés ?
Qui l'a enregistré ?
En a t'il enregistré d'autres ?
Quels sont leurs IP
Sont-elles malveillante ?

PIVOT #2

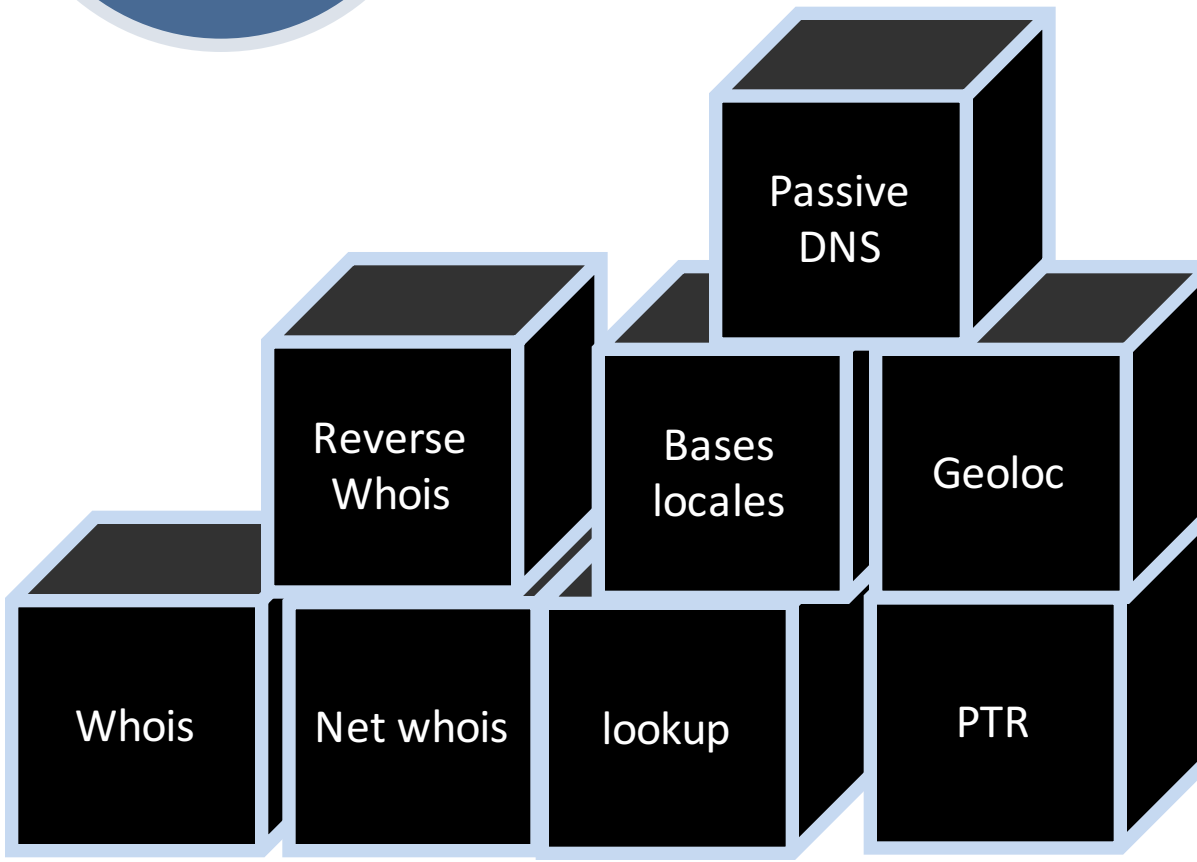
CONCEPTS

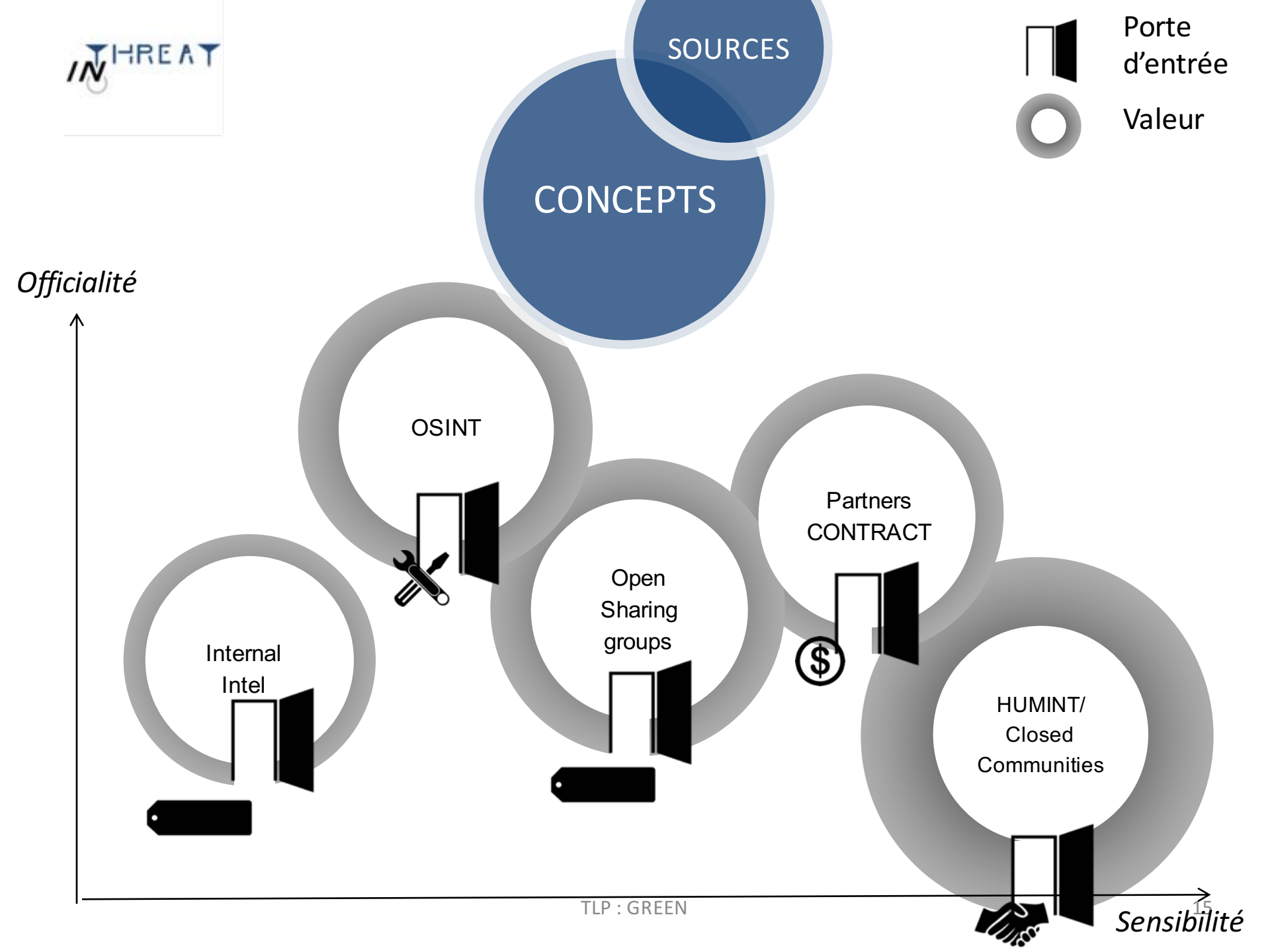
= OBJECTIF

= RISQUE

PIVOT #3

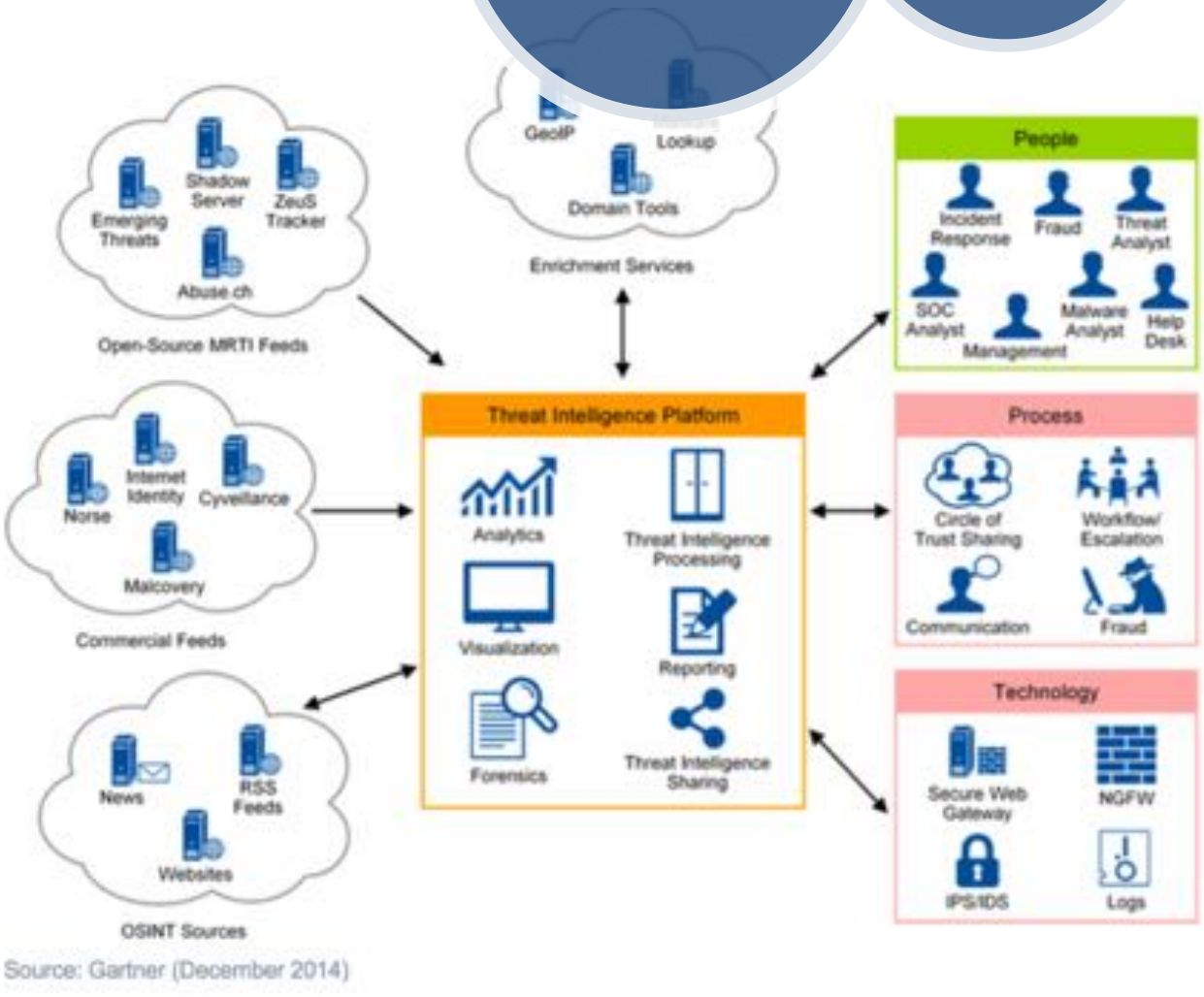
CONCEPTS




SOURCES
CONCEPTS
Porte d'entrée
Valeur
Officialité
OSINT
Internal Intel
Open Sharing groups
Partners CONTRACT
HUMINT/ Closed Communities
Sensibilité

CONCEPTS

PLATEFORMES
#Théorie



CONCEPTS

PLATEFORMES
#Choix

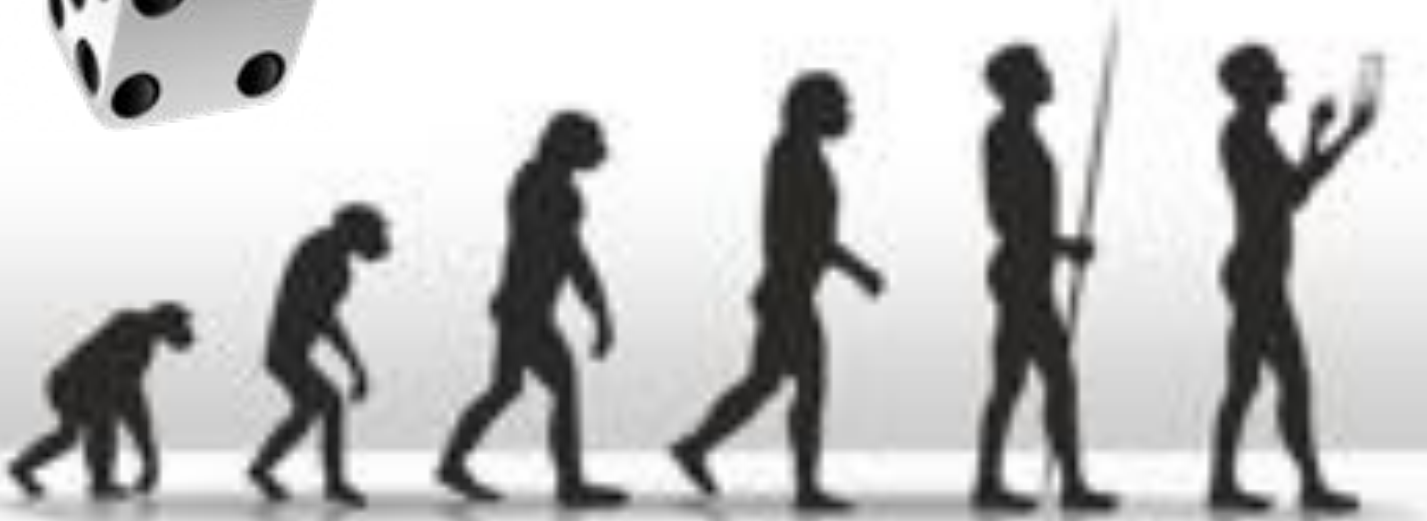
CONCEPTS

PLATEFORMES
#Marché

PLATEFORMES
#Bonne
Approche

CONCEPTS

Hasard vs Courbe de maturité



Rien

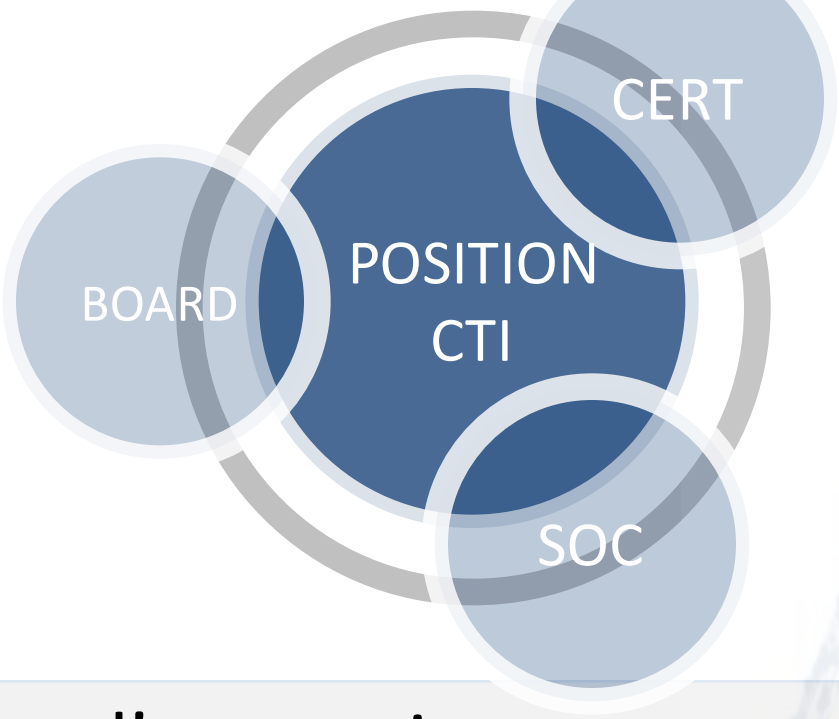
Infra sécu

SOC

IR

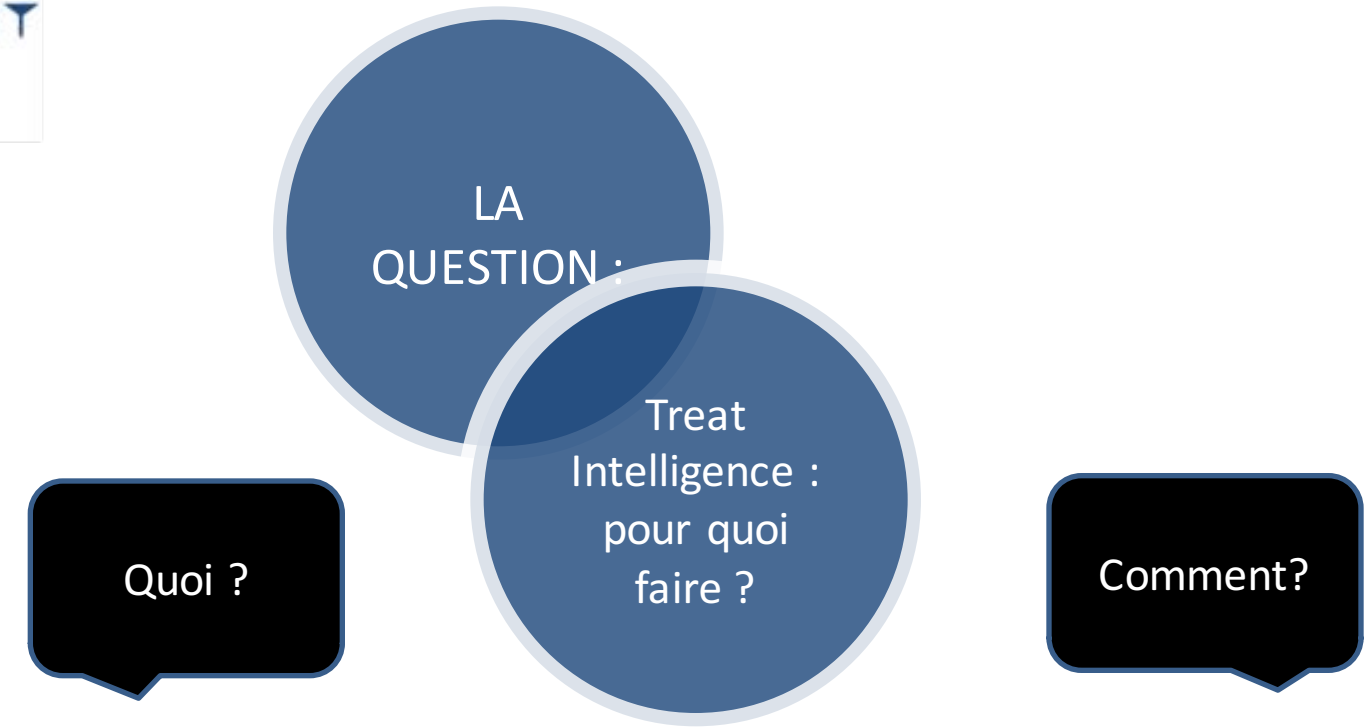
CTI basique

CTI stratégique



Place dans l'entreprise

- Rôle essentiel dans la protection et la détection
- Accélérateur et facilitateur sur incident
- Guide pour le management



REPONSE : TENTER DE LA DONNER

Pourquoi ?

Quand ?

Qui ?

VOS
QUESTIONS

david@inthreat.com @davidbizeul 06.64.45.84.29