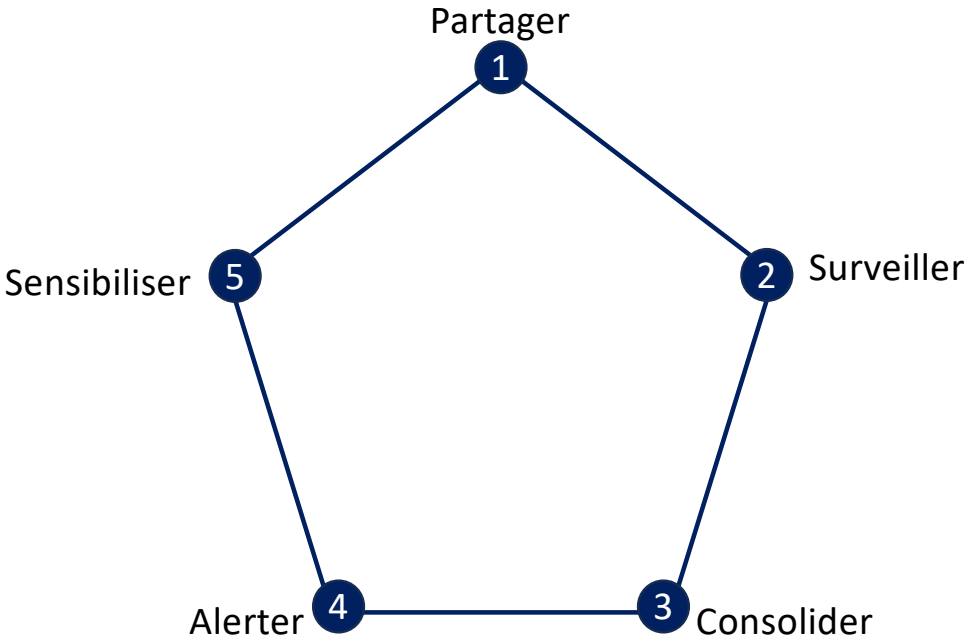
# Nouveaux services pour la SSI IN2P3

# Etat des lieux

- Une infrastructure de supervision basée sur Znets
  - NIDS historique de l'IN2P3
  - Beaucoup de faux positifs ou difficilement exploitable
    - Grand nombre de notifications par e-mail
  - Peu de corrélations avec les acteurs extérieurs (CERT-RENATER, CSIRT WLCG, …)
    - Souvent faites « à la main » après une notification
- Objectif
  - Rénover l'infrastructure afin de :
    - Faciliter la gestion des alertes
    - Automatiser l'utilisation des indices de compromission (IoC)

# Restructurer l’infrastructure SSI autour de 5 idées



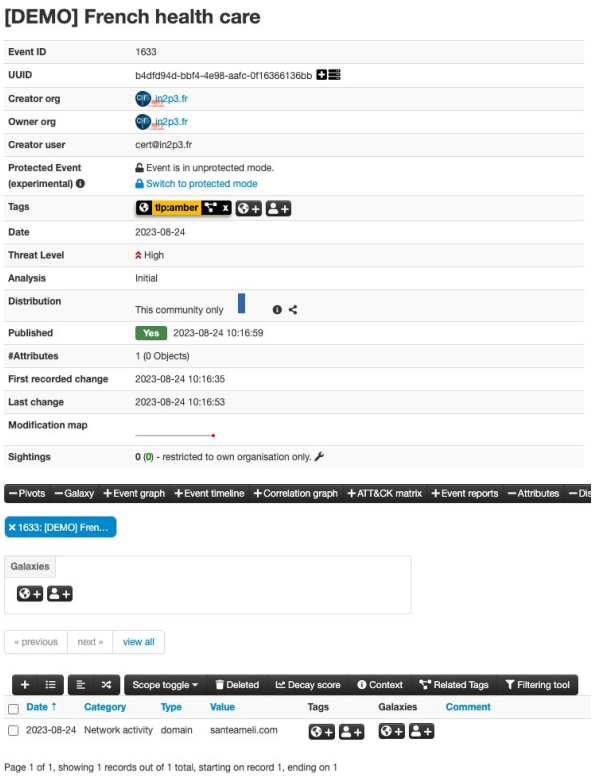
# Partager

- Avoir une base de connaissance des menaces communes dans nos communautés
  - Partager avec nos partenaires (CERN, WLCG, …) les différentes attaques et partager nos informations
  - Pouvoir utiliser ces informations pour alimenter nos outils de supervision
- MISP
  - Plateforme de partage d'IoC (indice de compromission)
    - @ IP
    - Nom de domaine
    - Checksum de fichier
    - …
  - Développé par CIRCL
    - L'ANSSI distribue un « flux » MISP
    - Utilisé par le CERN & WLCG

# Les défis du partage: la confiance

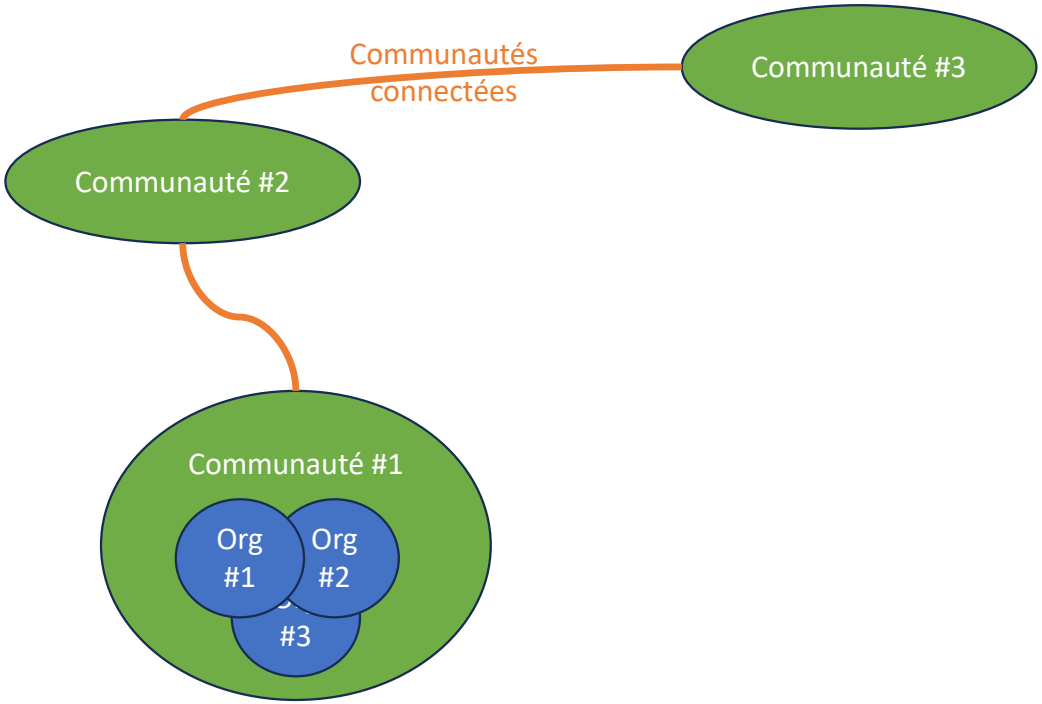
- Comment être sûr que l'information que je partage ne soit pas rendue publique ?
  - Respect des « transport light protocol » (tlp)
- Comment être sûr que l'information que je reçois est fiable ?

# Pourquoi MISP ?



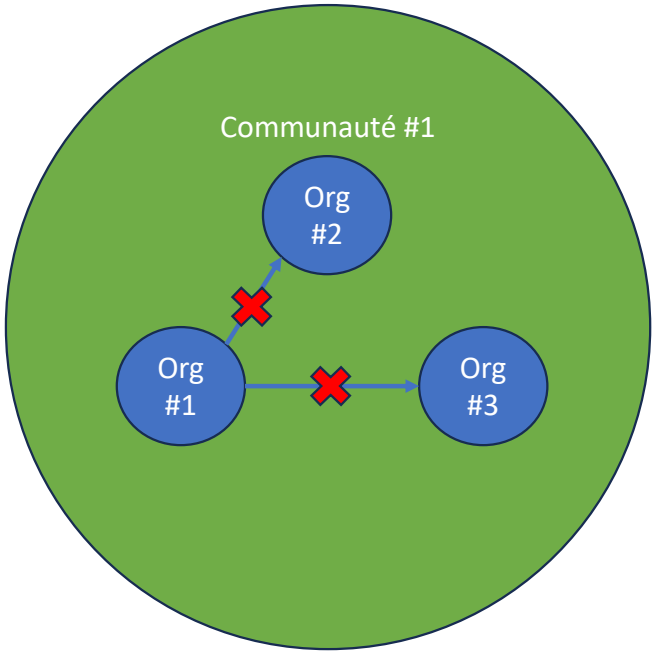

- Contextualiser (Events)
  - Les RBLs, blacklist, … ne contextualise pas les IoCs, ils ne font que fournir les listes
- Réactivité
  - Avoir accès aux IoC non publiques (tlp: green, tlp:amber)
- Exporter
  - Snort, Suricata, Yara, Zeek
  - RPZ
  - STIX[1|2]

# Comment est organisé MISP ?



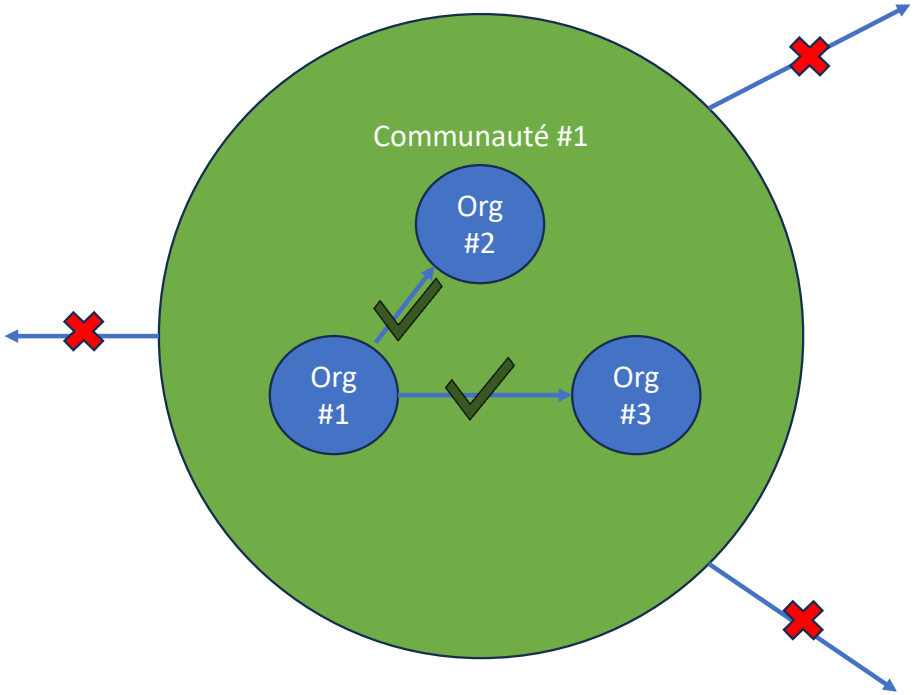

- Organisation: unité de base (laboratoire, service, …)
- Communauté: ensemble d'organisations partageant une même infrastructure MISP
- Communautés connectées: communautés partageant des IoCs
- Tous: Ensemble des communautés MISP interconnectées

# Distribution de l’information



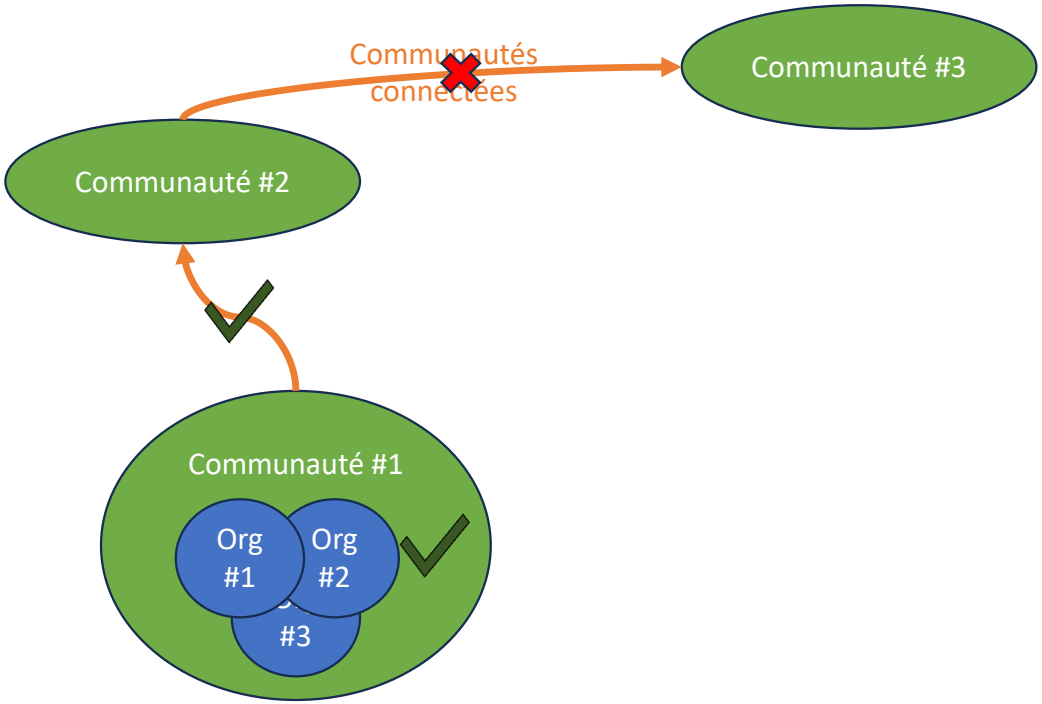

- Organisation
  - Seuls les membres de l’organisation peuvent voir l’événement

# Distribution de l'information



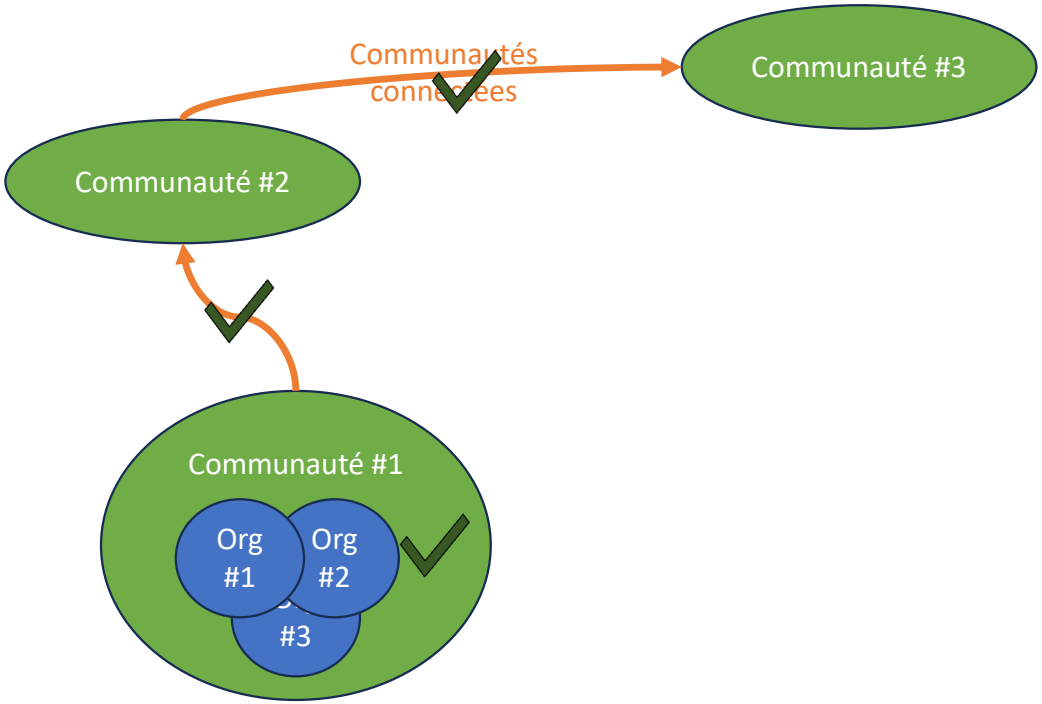

- Organisation
  - Seuls les membres de l'organisation peuvent voir l'événement
- Communauté
  - L'ensemble des organisations de la communauté peut voir l'événement
  - L'information n'est pas distribuée aux communautés connectées

# Distribution de l'information



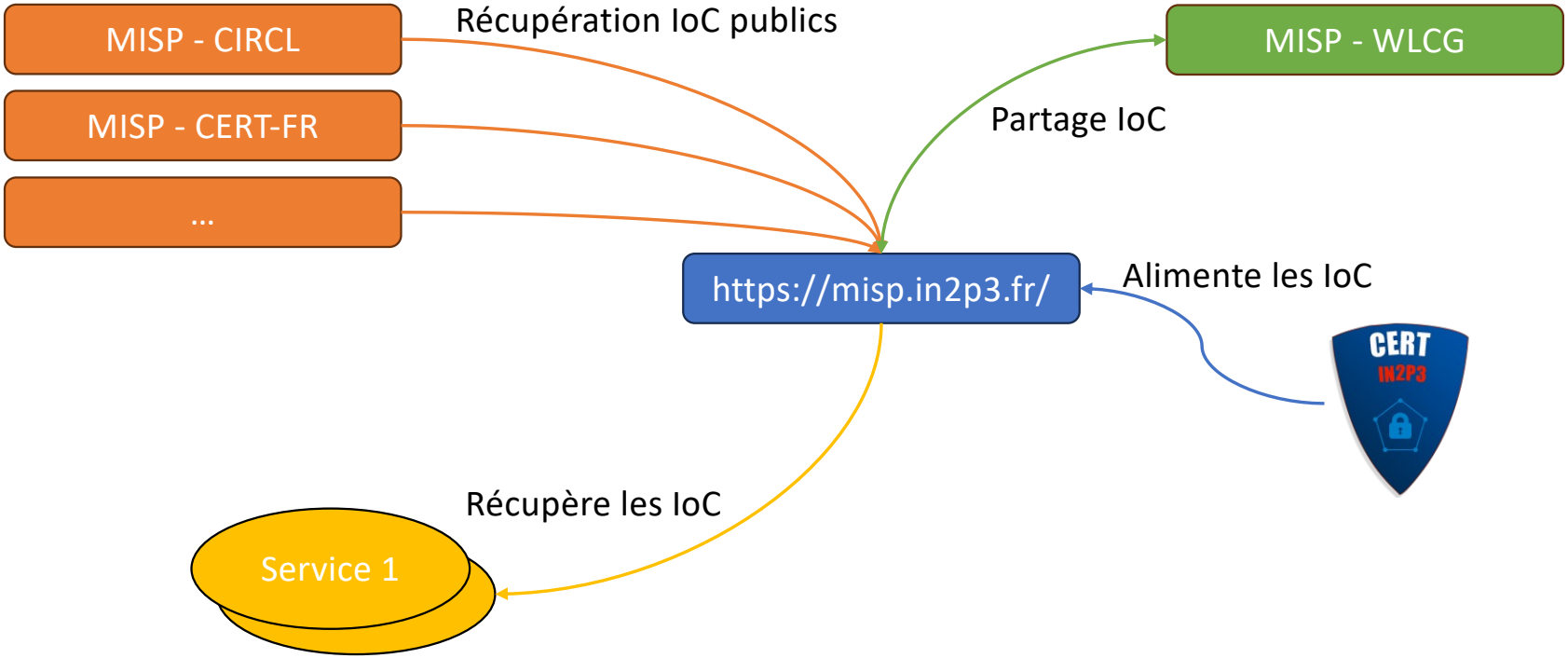

- Organisation
  - Seuls les membres de l'organisation peuvent voir l'événement
- Communauté
  - L'ensemble des organisations de la communauté peut voir l'événement
  - L'information n'est pas distribuée aux communautés connectées
- Communauté connectée
  - Seules les communautés directement connectées à notre communauté peuvent voir l'événement, il ne sera pas distribué au delà

# Distribution de l'information




- Organisation
  - Seuls les membres de l'organisation peuvent voir l'événement
- Communauté
  - L'ensemble des organisations de la communauté peut voir l'événement
  - L'information n'est pas distribuée aux communautés connectées
- Connectée
  - Seules les communautés directement connectées à notre communauté peuvent voir l'événement, il ne sera pas distribué au delà
- Tous
  - Toutes les communautés recevront l'événement

# MISP


MISP - CIRCL
MISP - CERT-FR
...
Récupération IoC publics
MISP - WLCG
Partage IoC
https://misp.in2p3.fr/
Alimente les IoC
CERT IN2P3
Récupère les IoC
Service 1

# Surveiller

- Znets
  - NIDS historique
  - Basé sur une liste d'adresses à surveiller + analyse comportementale
  - Beaucoup d'alertes « faux-positifs » ou difficilement exploitables (ie brute force extérieur, scan extérieur, …)
- pDNSSOC
  - Développé par le CERN
  - Analyse les logs DNS
    - À partir des IoC MISP
  - Alerte lors de la détection d'un IoC
    - Risque de « faux positif » (tinyurl.com, bit.ly, …)

# Pourquoi pDNSSOC ?

| pDNSSOC client | First Occurrence | IoCs detected | MISP event | Total # of IoCs | Publication | Organisation | Comment | Tags |
|---|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] | 88 | 2023-07-16 | [redacted] | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 88 | 2023-07-16 | | Malware hosting / lure page | |
| | | | | 80 | 2017-07-13 | | social network lure | |
| | | | | 575 | 2018-03-15 | | | |
| | | | | 575 | 2018-03-15 | | | |
| | | | | 19 | 2020-01-25 | | Trickbot connected to this domain | |

- Avec l'émergence du cloud, l'analyse purement IP ne fonctionne plus
  - Beaucoup de pirates utilisent des services cloud
  - Faiblesse face à l'IP hopping
- Le DNS, comme le routeur, est un point de passage obligatoire
  - Possibilité de superviser de façon passive
- Une solution imparfaite
  - Faiblesse face à DGA (Domain Generation Algorithm)
    - Mais une initiative passive DNS commence à émerger

# C’est quoi le passive DNS ?

- Mettre en commun l’ensemble des résolutions DNS pour tracer les différents changements de nom de domaine
  - Si le nom de domaine evil.com est résolu par l’IP 1.1.1.1 et que daemon.com est maintenant résolu par 1.1.1.1 alors il y a eu un DGA
- De façon internationale
  - Partager l’information pour être plus réactif
  - De façon anonyme (l’IP cliente n’est pas transmise)

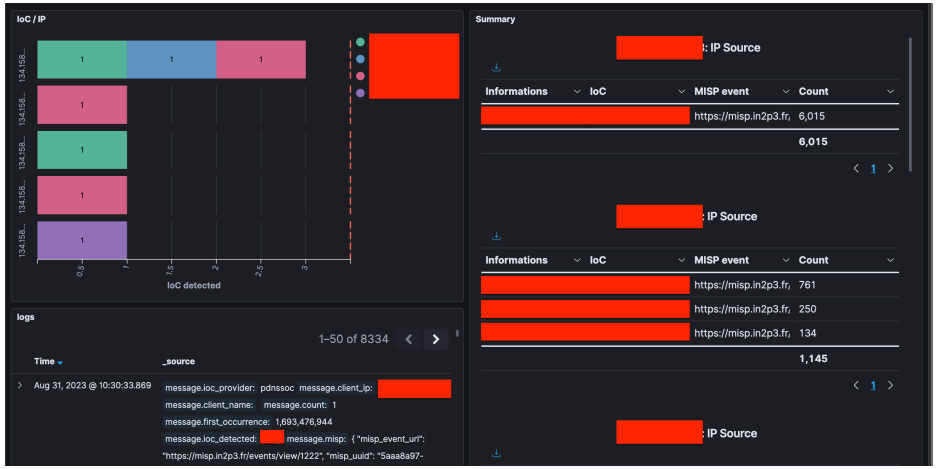
# pDNSSOC


https://misp.in2p3.fr/
Récupération des IoC
(domaine + @IP)
DNS 1
Envoi des logs DNS
https://pdnssoc.in2p3.fr/
Publie les alertes

# Consolider

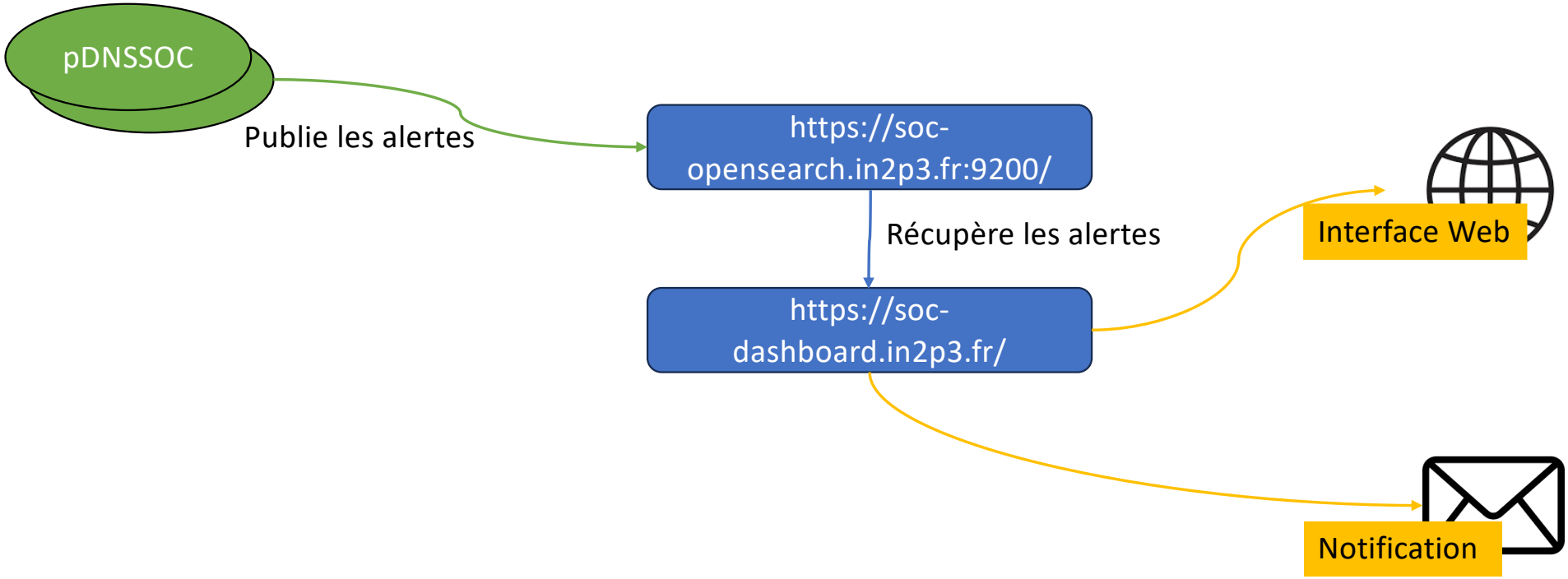
- Comment limiter les alertes non-exploitables ou les faux-positifs ?
  - Les IoC n'ont qu'un rôle indicatif
    - Alerter à chaque détection est contre-productif
  - Limiter des alertes à plusieurs IoC sur la même cible ou le même IoC sur plusieurs cibles
- Centraliser les alertes
  - Basé sur opensearch (fork de elasticsearch)
  - Ne stocke que les alertes liées à des IoC
  - Tableau de bord web
  - Vue par laboratoire (CSSI) ou pour tout l'institut (CERT-IN2P3)

# Pourquoi consolider ?




- Avoir une vue synthétique des potentielles attaques
  - Un évènement MISP est-il surreprésenté ?
  - Plusieurs clients sont-ils impliqués dans un même IoC
- Alerter au plus juste
  - Eviter le syndrome du SPAM d'alerte

# Consolider


pDNSSOC
Publie les alertes
https://soc-opensearch.in2p3.fr:9200/
Récupère les alertes
https://soc-dashboard.in2p3.fr/
Interface Web
Notification

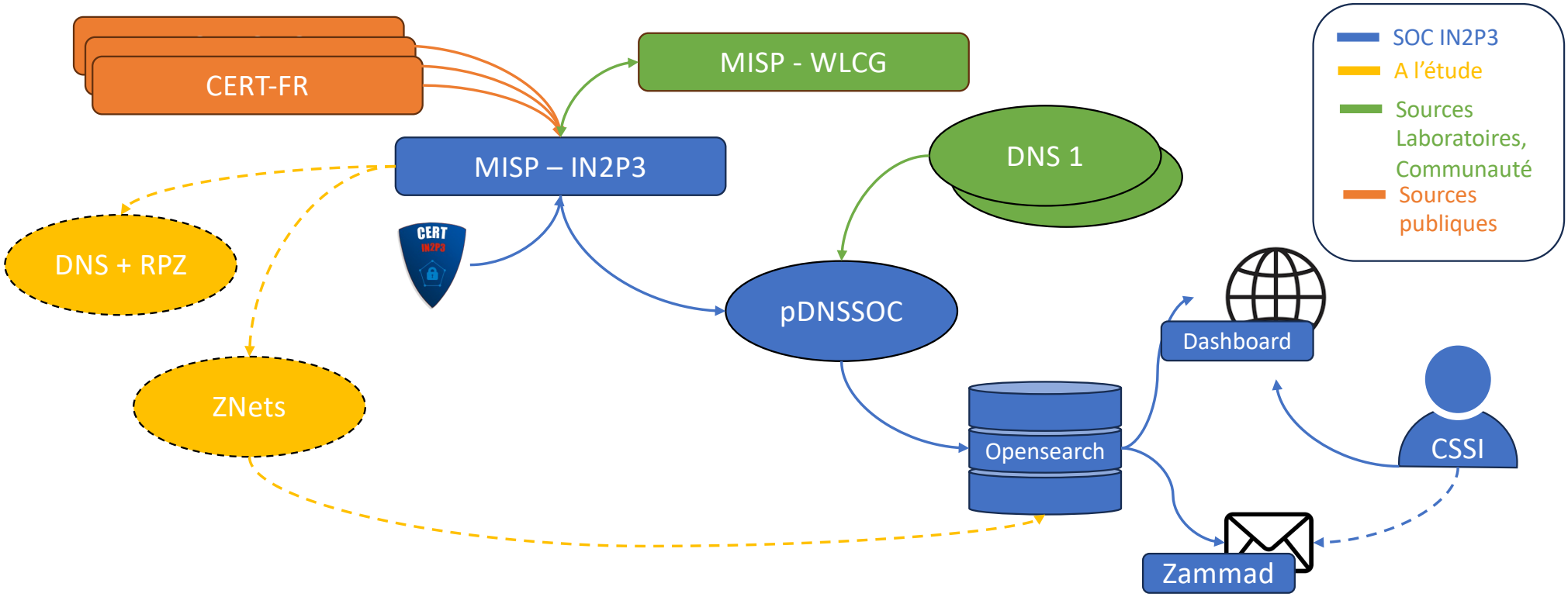
# Alerter

- Etre réactif face aux menaces
  - Ne pas être noyé dans les notifications
  - Etre capable de faire un suivi des alertes
- Basé sur zammad
  - En lien avec opensearch qui publie les alertes dans Zammad
  - Permet de collecter les mails dans une boite aux lettres
  - Permet de conserver l'interface mail pour la communication avec les laboratoires
    - Ouvrir aux CSSI des laboratoires ?

# Pourquoi Zammad ?


- Interface simple et claire
  - Mais avec beaucoup de fonctionnalité
- API REST
  - Qui permet de créer des tickets via opensearch

# Le workflow complet



# Merci