Le service de Cyber Threat Intelligence du Cert-IST

Olivier BERT
Philippe BOURGEOIS
Laurent ZANDONA

Forum Cert-IST
23 novembre 2016

Sommaire

1. La Cyber Threat Intelligence (CTI)

2. Le Service Cyber Threat Intelligence du Cert-IST

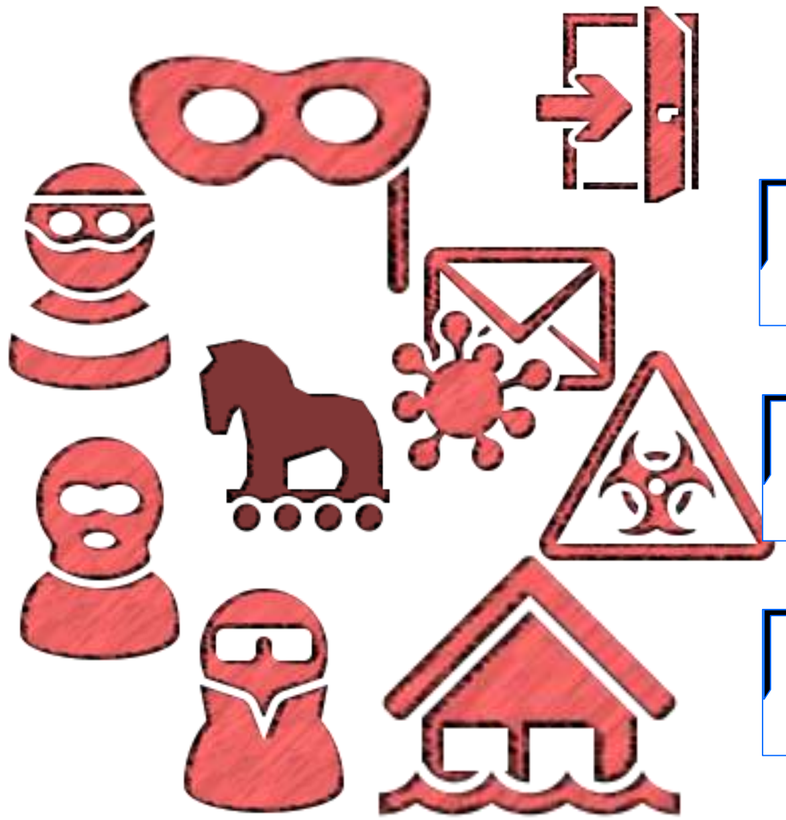
3. Démonstration

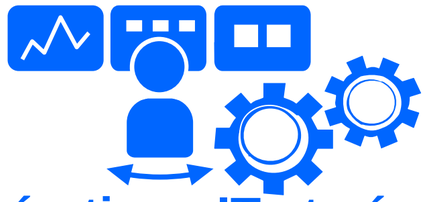
4. Questions / Réponses

1. La Cyber Threat Intelligence (CTI)
2. Le Service Cyber Threat Intelligence du Cert-IST
3. Démonstration
4. Questions / Réponses

1. La Cyber Threat Intelligence (CTI)

La Cyber Threat Intelligence (CTI)





Opérations IT et sécurité (internes ou infogérées)

Gestion de Vulnérabilités

Supervision de Sécurité et Réponse à Incident

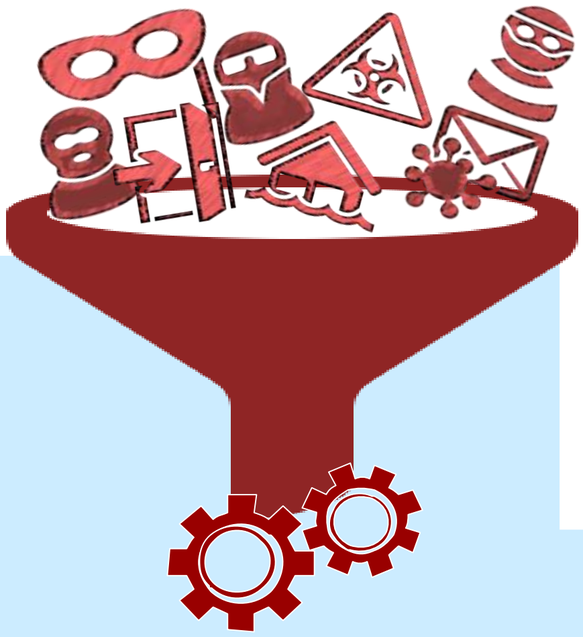
Amélioration Continue de la Cyber-Défense

Evaluer et **Gérer** les risques

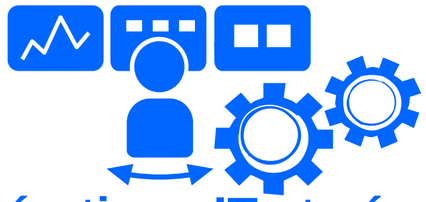
Détecter et **Réagir** aux attaques

Comprendre et **Affronter** la menace

La Cyber Threat Intelligence (CTI)



opéré par THALES



Opérations IT et sécurité (internes ou infogérées)

Veille Vulnérabilités

Veille Attaques

Veille Menaces

Gestion de Vulnérabilités

Supervision de Sécurité et Réponse à Incident

Amélioration Continue de la Cyber-Défense

Evaluer et **Gérer** les risques

Détecter et **Réagir** aux attaques

Comprendre et **Affronter** la menace

Threat Intelligence pour qui ?

Threat Intelligence stratégique

RSSI

Threat Intelligence opérationnelle

Equipes sécurité, …

Threat Intelligence technique

SOC

IOC

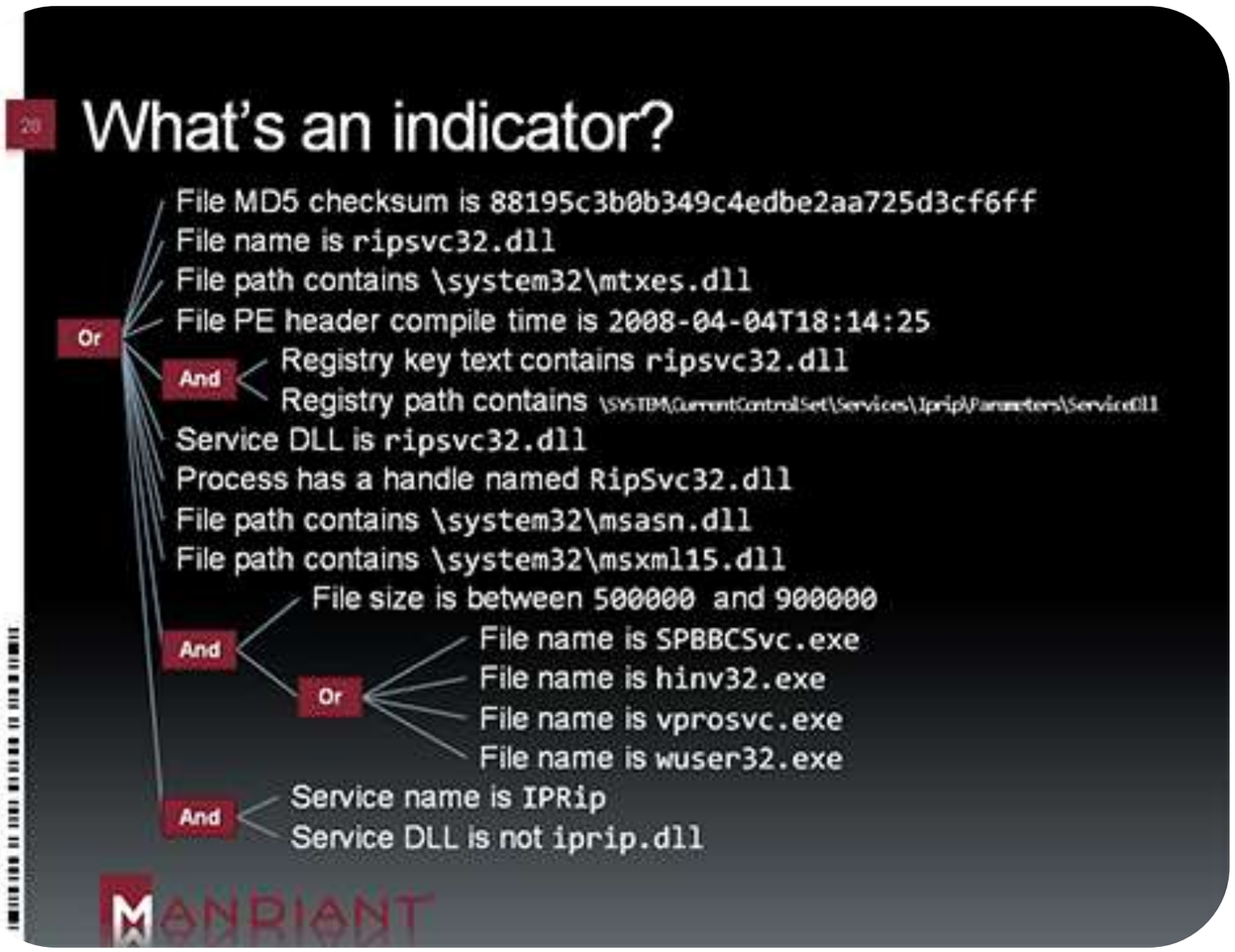
Threat Intelligence tactique

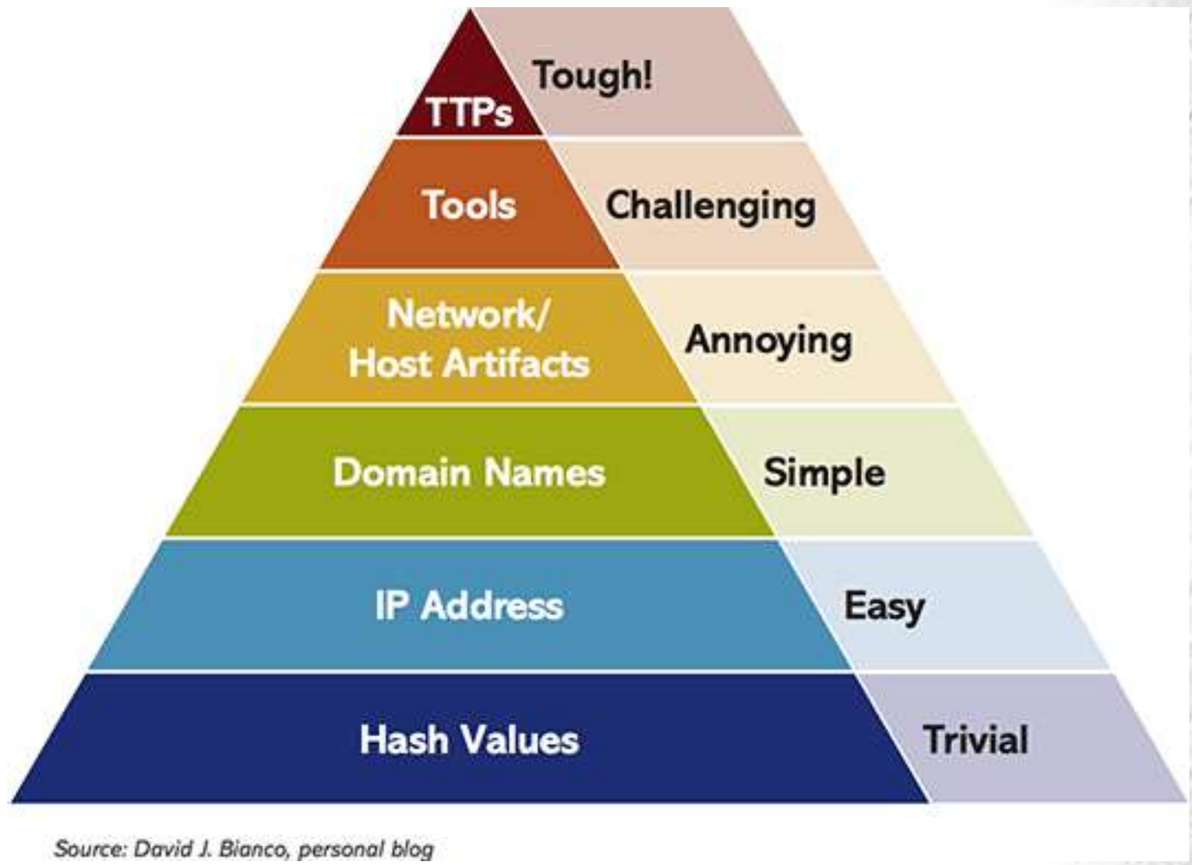
Architectes sécurité

La Threat Intelligence n’est pas uniquement pour les SOC !

IOC : Définition

I O C : Indicateurs de compromission





Les Hashs sont les IOC les plus répandus et partagés mais ils ont le moins de valeur.

1. La Cyber Threat Intelligence (CTI)
2. Le Service Cyber Threat Intelligence du Cert-IST
3. Démonstration
4. Questions / Réponses

Présentation du service 1/2

- Nouveau service qui a démarré le 1er juillet 2016
- Objectifs de ce nouveau service :
  - Répertorier les attaques connues en se focalisant sur les attaques de types APT et les attaques émergentes, mais aussi d'autres types d'attaques (Phishing, malspam,…)
  - Fournir une base d'IOC qualifiés
- Pour ce service, l'équipe Cert-IST :
  - Se concentre sur les tâches de Collecte / **Evaluation** / **Enrichissement** / Diffusion
  - Utilise diverses sources : informations publiques, signalements, …
  - Fournit des données qualifiées que les abonnés peuvent filtrer par rapport à leur environnement (exemple : secteur d'activité, zone géographique, …)

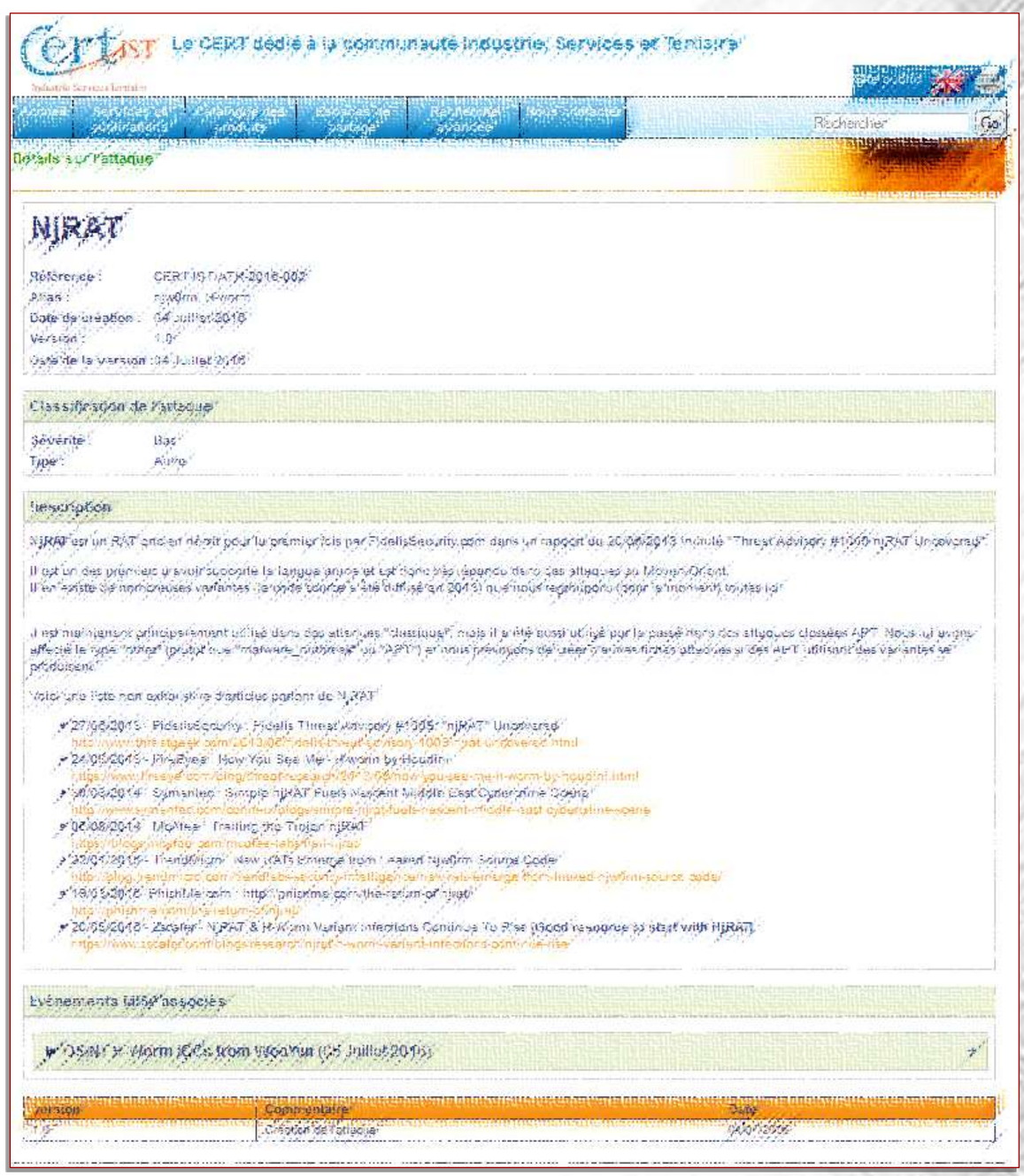
Présentation du service 2/2

- Productions associées au service :
  - Fiches attaques répertoriant et analysant les attaques connues
  - Base de données d'IOC avec des informations de contexte, et des fonctionnalités de recherche et de filtrage

    Exemple de contexte ajouté aux IOC
    - Threat-type : APT, malware outbreak, phising…
    - Domain : aerospace, banking, energy, government, …
    - Risk-level,
    - ...
  - Bulletin mensuel analysant et synthétisant l'actualité du mois en termes d'attaques

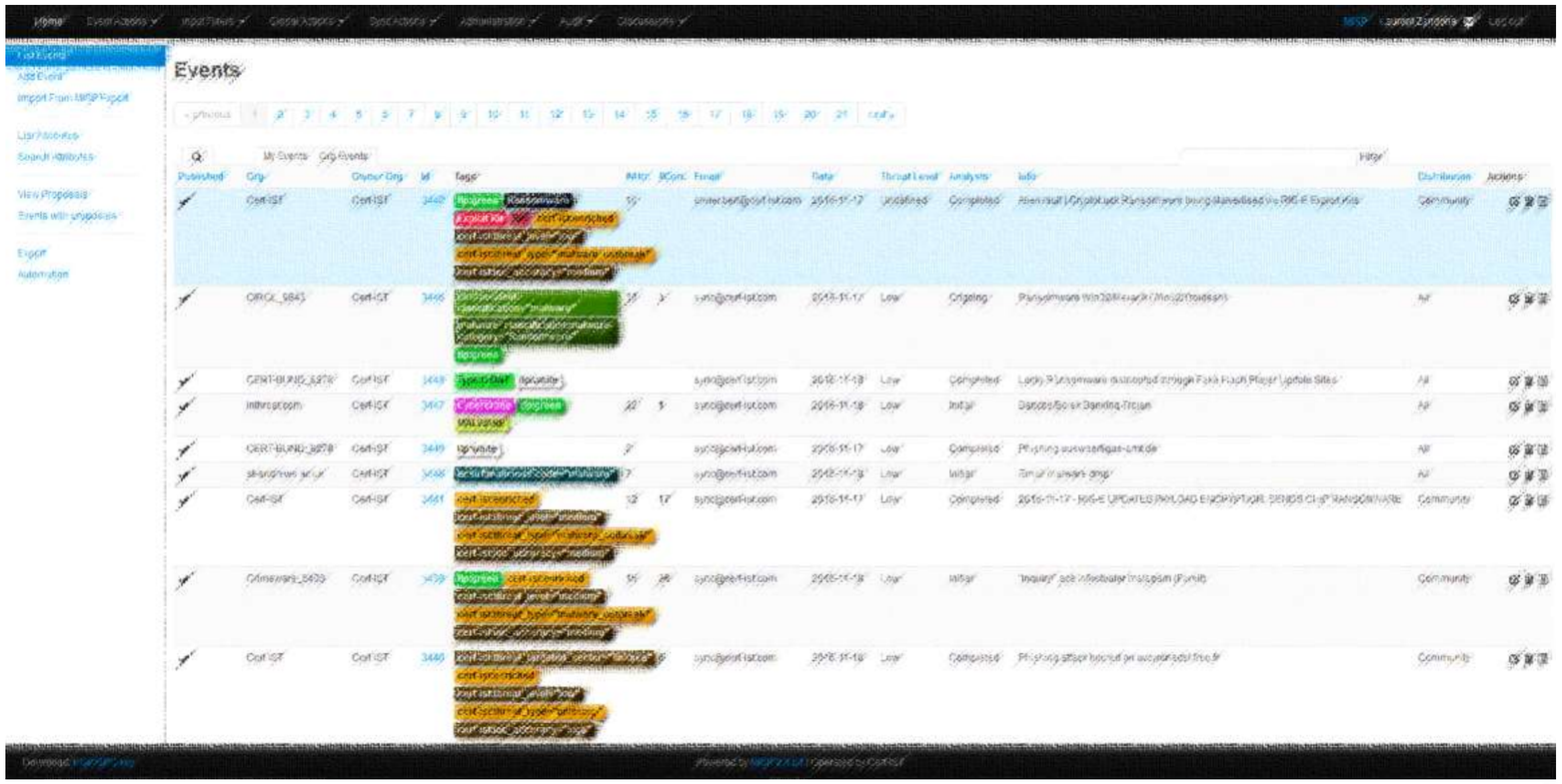
Les livrables du service Cert-IST
Fiches Attaques

- Fiches Attaques
  - Informations consolidées sur une attaque, incluant les pointeurs sur les IOC associés, et pouvant contenir des TTP, i.e. information sur les Tactiques, Techniques et Procédures utilisées par les attaquants
  - Envoyées par e-mail
  - Accessibles via la base de connaissance des attaques à travers le site web privé du Cert-IST



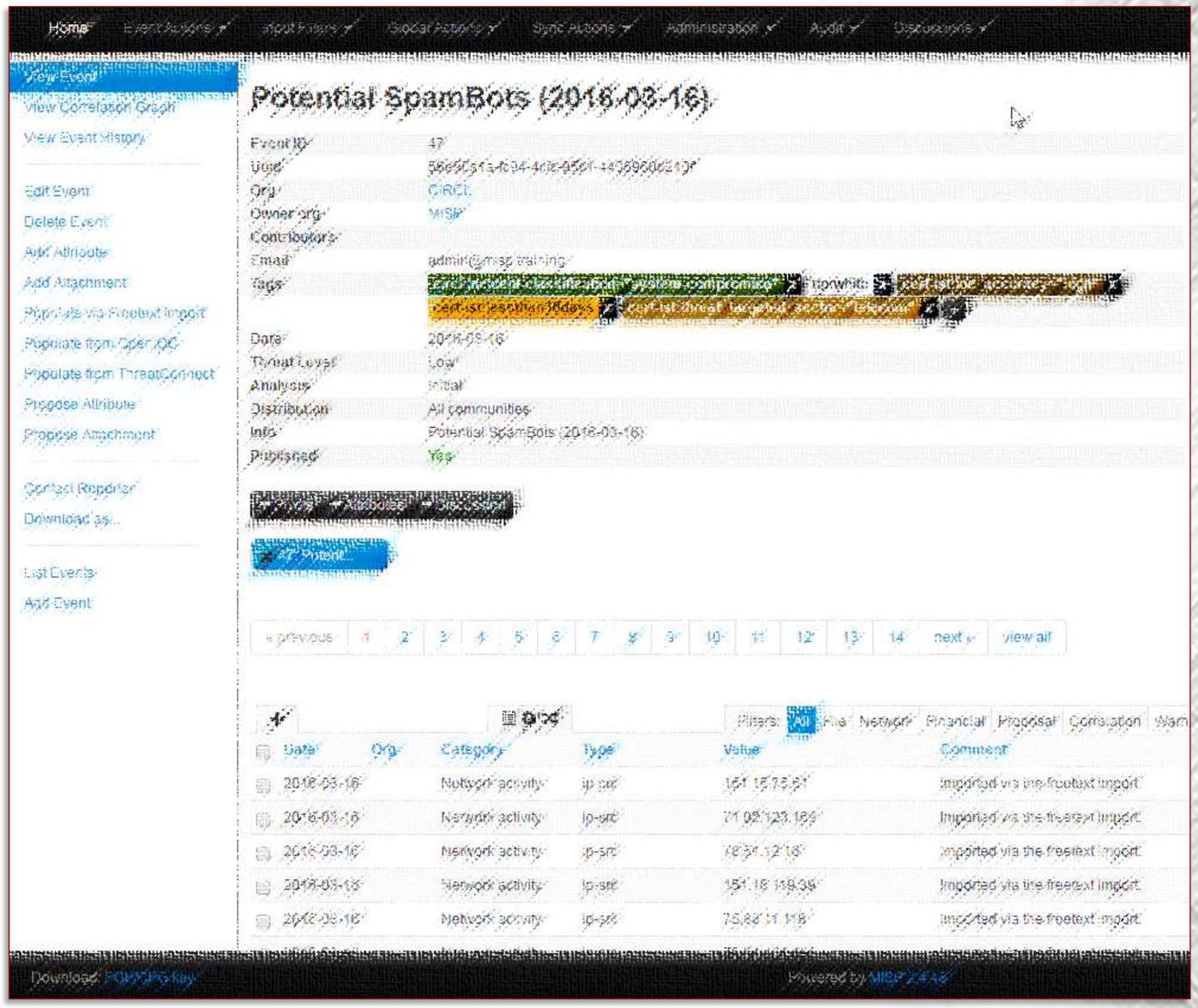
Les livrables du service Cert-IST
Plate-forme d'échange d'IOC 1/2

- Malware Information Sharing Platform
  - Plate-forme pour partager des IOC sur les menaces en cours
    - Interface Web + API (REST, Python,)
  - Solution open-source qui rencontre un grand succès en Europe
    - Utilisé par NATO, Belgian Defence, CERT-EU, CIRCL.lu, …



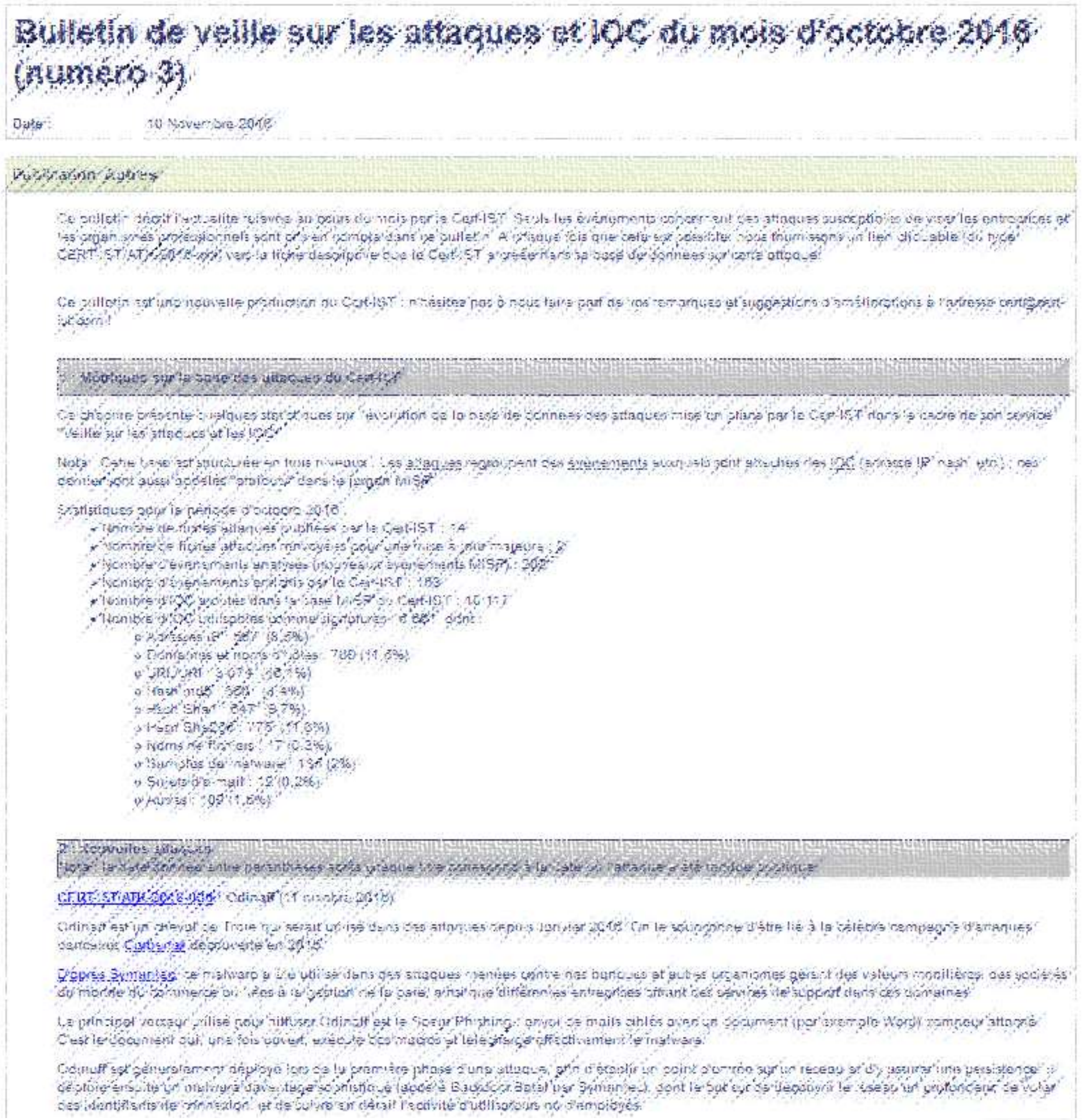
Les livrables du service Cert-IST
Plate-forme d'échange d'IOC 2/2

- Marqueurs techniques permettant d'identifier une attaque ou un attaquant
  - e.g. IP @, nom de domaine, URL, MD5 ou Sha-1 hash, clé de registre, fichier
- Qualifiés et enrichis avec des tags permettant la contextualisation client
  - e.g. niveau de confiance et de menace, type d'attaque, secteurs d'activité ou zones géographiques visées, ancienneté, …



- Bulletin mensuel Veille sur les attaques et IOC

  - Synthèse des informations sur les attaques et IOC
  - Statistiques sur les IOC publiés dans la base MISP
  - Synthèse des informations sur les nouvelles attaques et l'évolution des attaques existantes

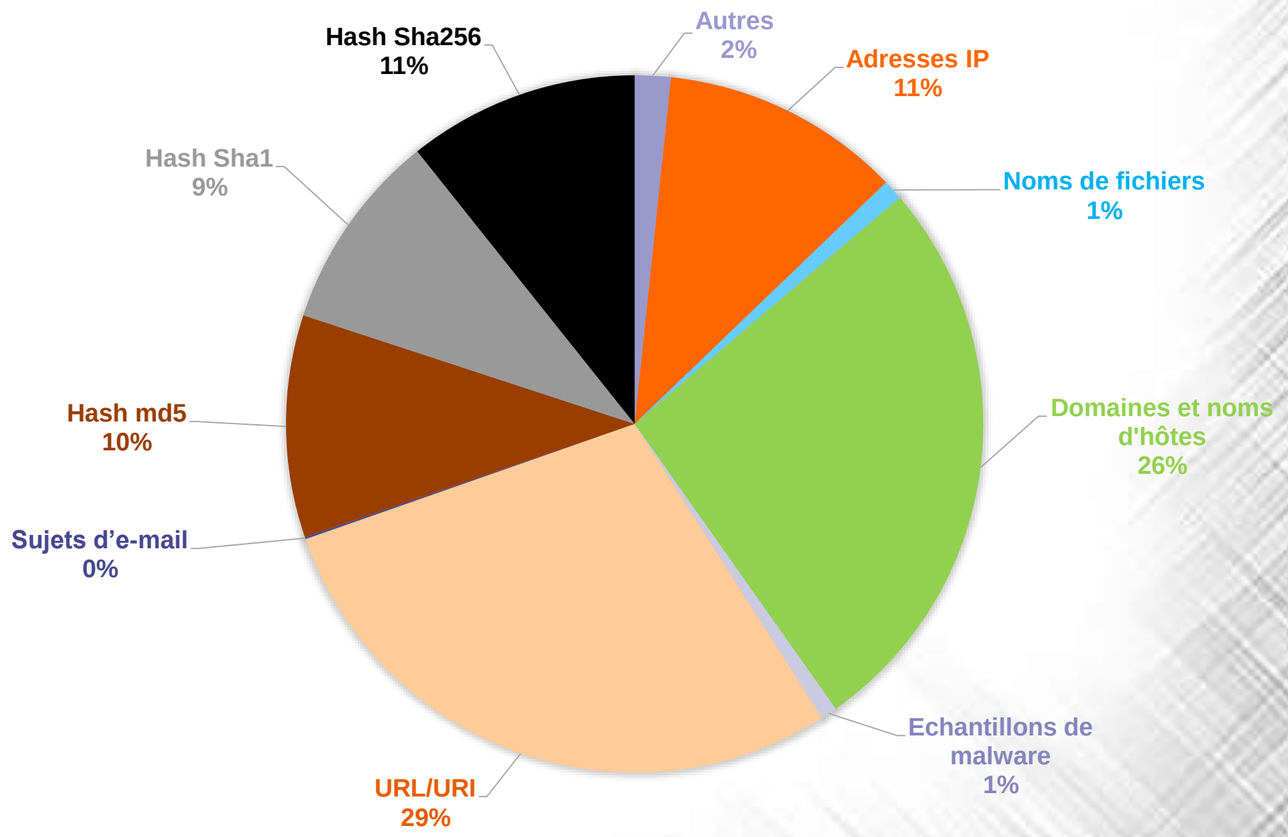


Bulletin de veille sur les attaques et IOC du mois d'octobre 2016 (numéro 3)

Date : 10 Novembre 2016

Statistiques sur le service

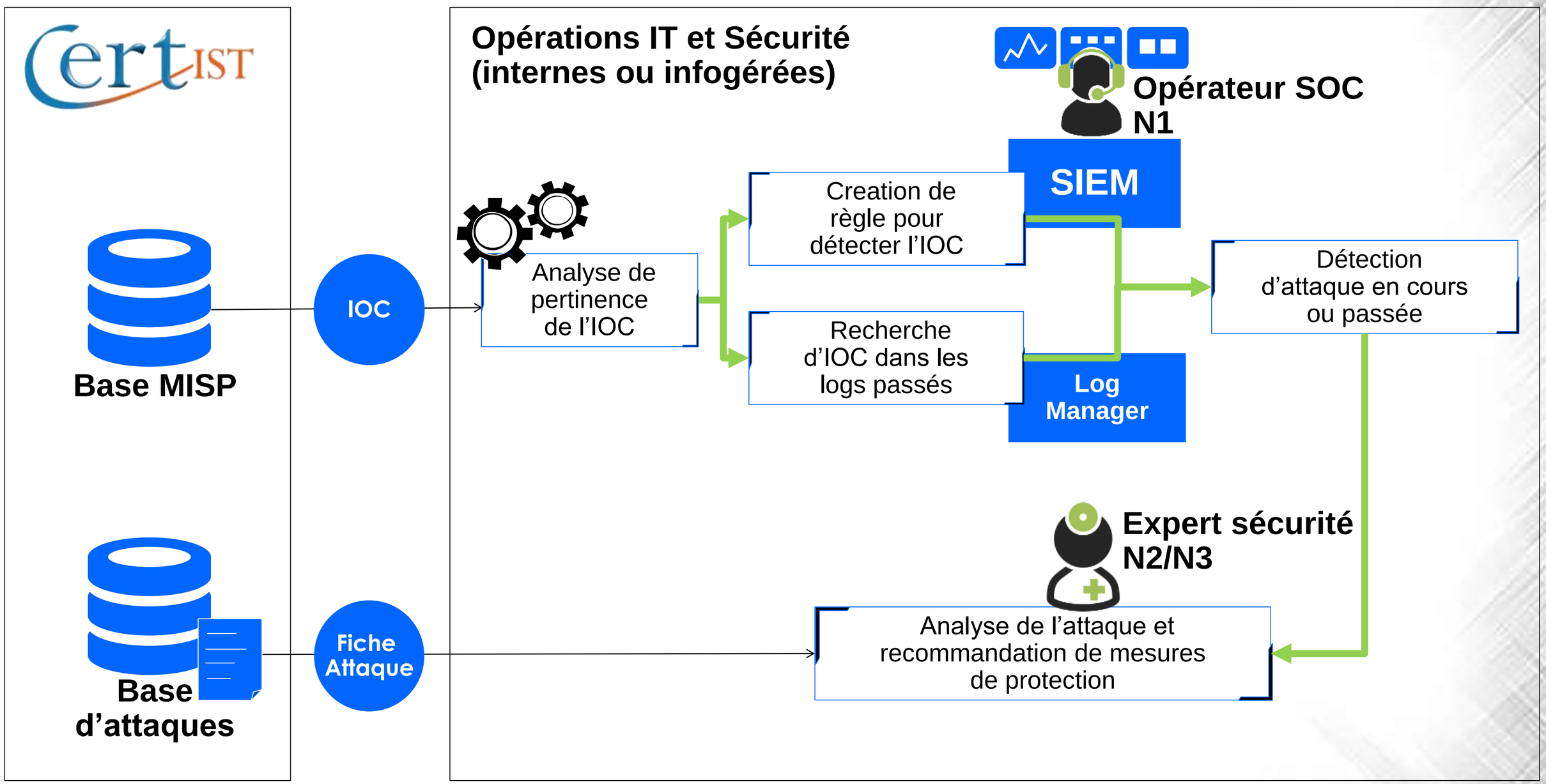
- Pour la période de juillet à octobre 2016 :
  - Nombre de fiches attaques publiées par le Cert-IST : 41
    Nombre d'événements analysés (nouveaux événements MISP) : 695
  - Nombre d'événements enrichis par le Cert-IST : 616
    Nombre d'IOC ajoutés dans la base MISP du Cert-IST : 38 890
  - Nombre d'IOC utilisables comme signatures : 30 055, dont :
    - Adresses IP : 3 354
    - Domaines et noms d'hôtes : 7 953
    - URL/URI : 8 620
    - Hash md5 : 3 100
    - Hash Sha1 : 2 777
    - Hash Sha256 : 3 221
    - Noms de fichiers : 281
    - Echantillons de malware : 223
    - Sujets d'e-mail : 26
    - Autres : 500



Usages types du service IOC du Cert-IST 1/2

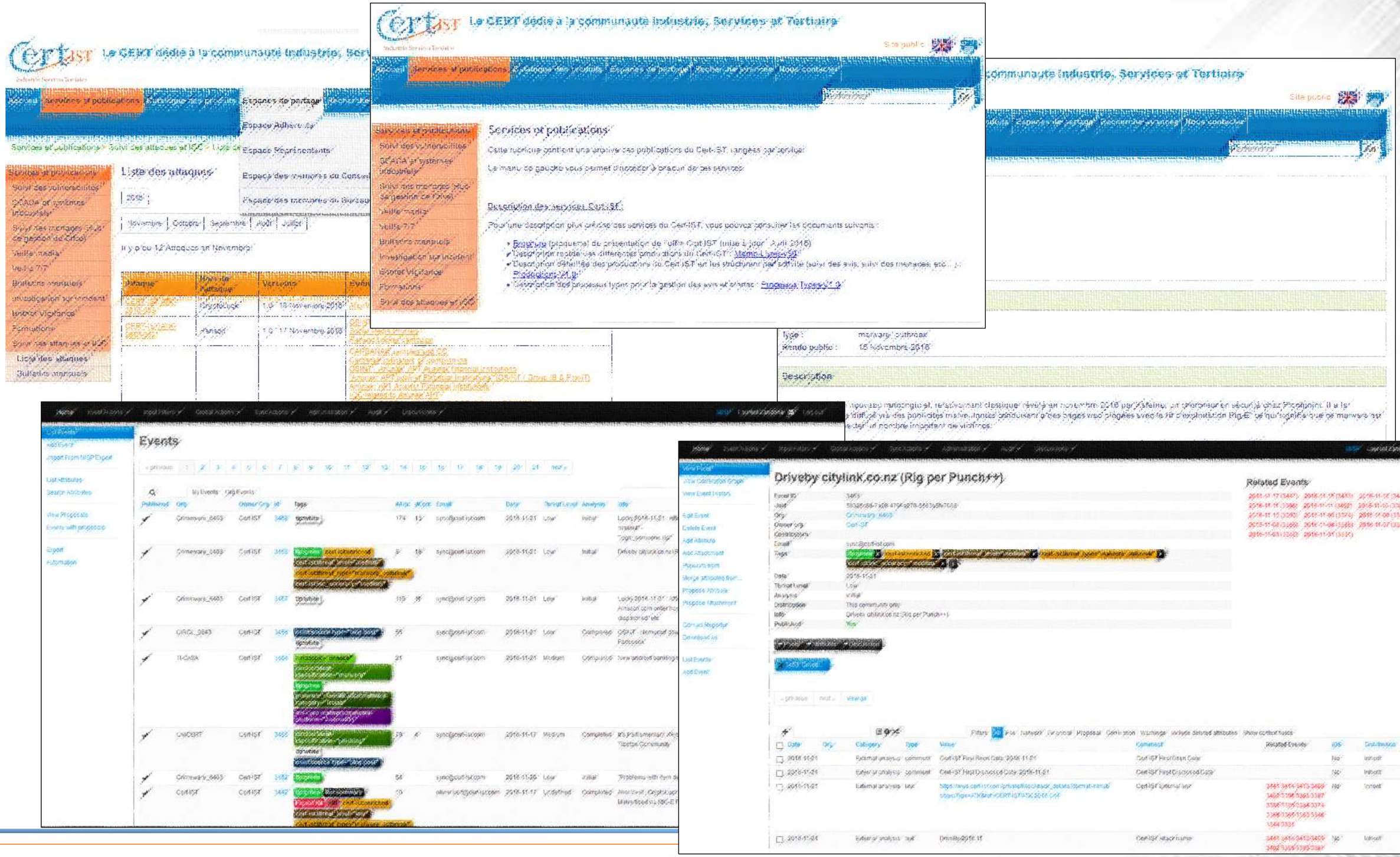
- Prévenir les tentatives d'attaque
  - Mise à jour des outils de prévention temps réel (IPS réseaux ou solutions « End-point Protection », …)
- Détecter les incidents
  - Recherche de traces : le SOC s'appuie sur une base IOC pour détecter que l'organisation a ou non été touchée par une attaque (et si besoin déclencher des actions de « remediation »)
  - Détection en temps réel via des règles au niveau des SIEMs
- Qualifier un incident
  - Utilisation par le SOC ou l'IR (Incident Response team) de la base d'IOC pour savoir si un élément suspect correspond à un incident connu et obtenir la fiche attaque correspondante
- Circonscrire un incident
  - Construction par l'IR des listes d'IOC lors de l'analyse d'un poste victime pour rechercher ensuite tous les postes ayant les mêmes symptômes
- Informer
  - Sensibilisation de l'ensemble des acteurs concernés (attaques, cibles, TTP, …)

Usages types du service IOC du Cert-IST dans un SOC 2/2



1. La Cyber Threat Intelligence (CTI)
2. Le Service Cyber Threat Intelligence du Cert-IST
3. Démonstration
4. Questions / Réponses

Démonstration du service



1. La Cyber Threat Intelligence (CTI)
2. Le Service Cyber Threat Intelligence du Cert-IST
3. Démonstration
4. Questions / Réponses