

# Le service de Cyber Threat Intelligence du Cert-IST



Olivier BERT  
Philippe BOURGEOIS  
Laurent ZANDONA

Forum Cert-IST  
23 novembre 2016

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

# Computer Emergency Response Team

## Industrie Services Tertiaire

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

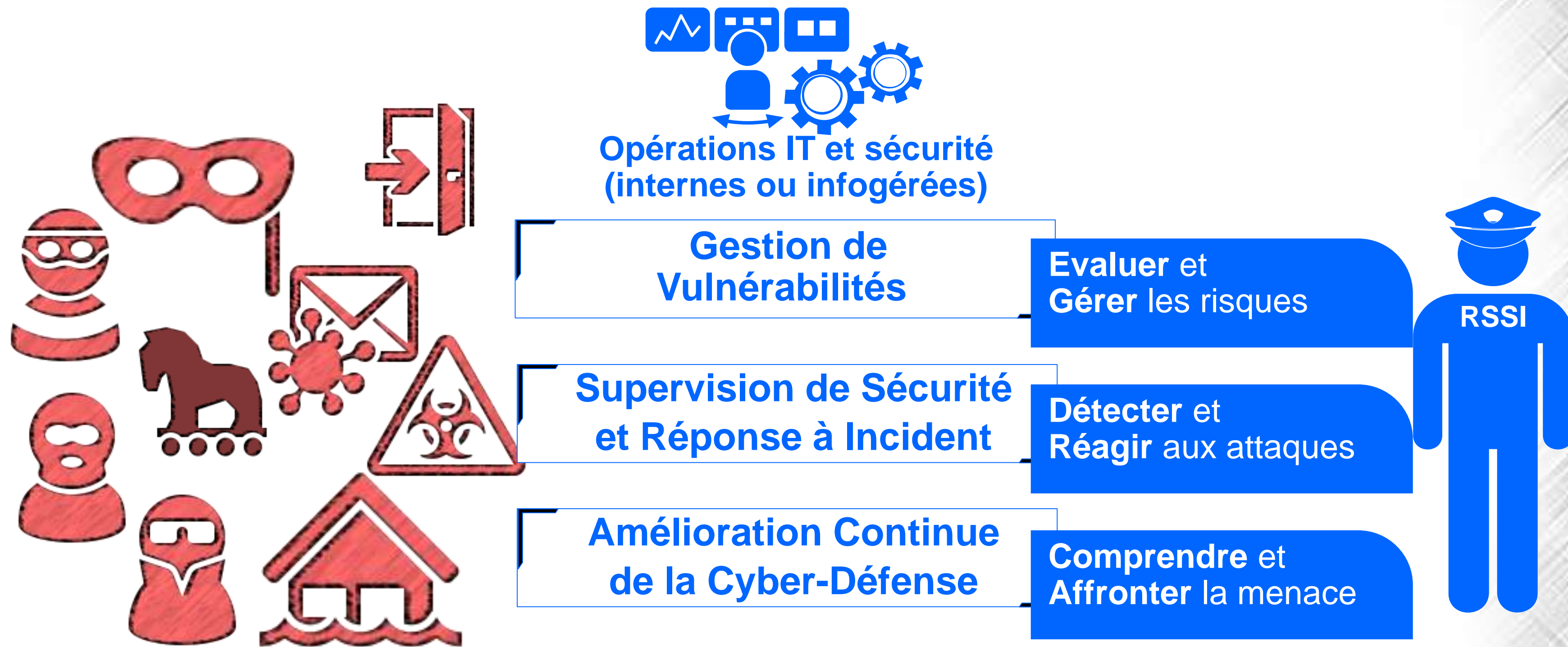


# 1. La Cyber Threat Intelligence (CTI)

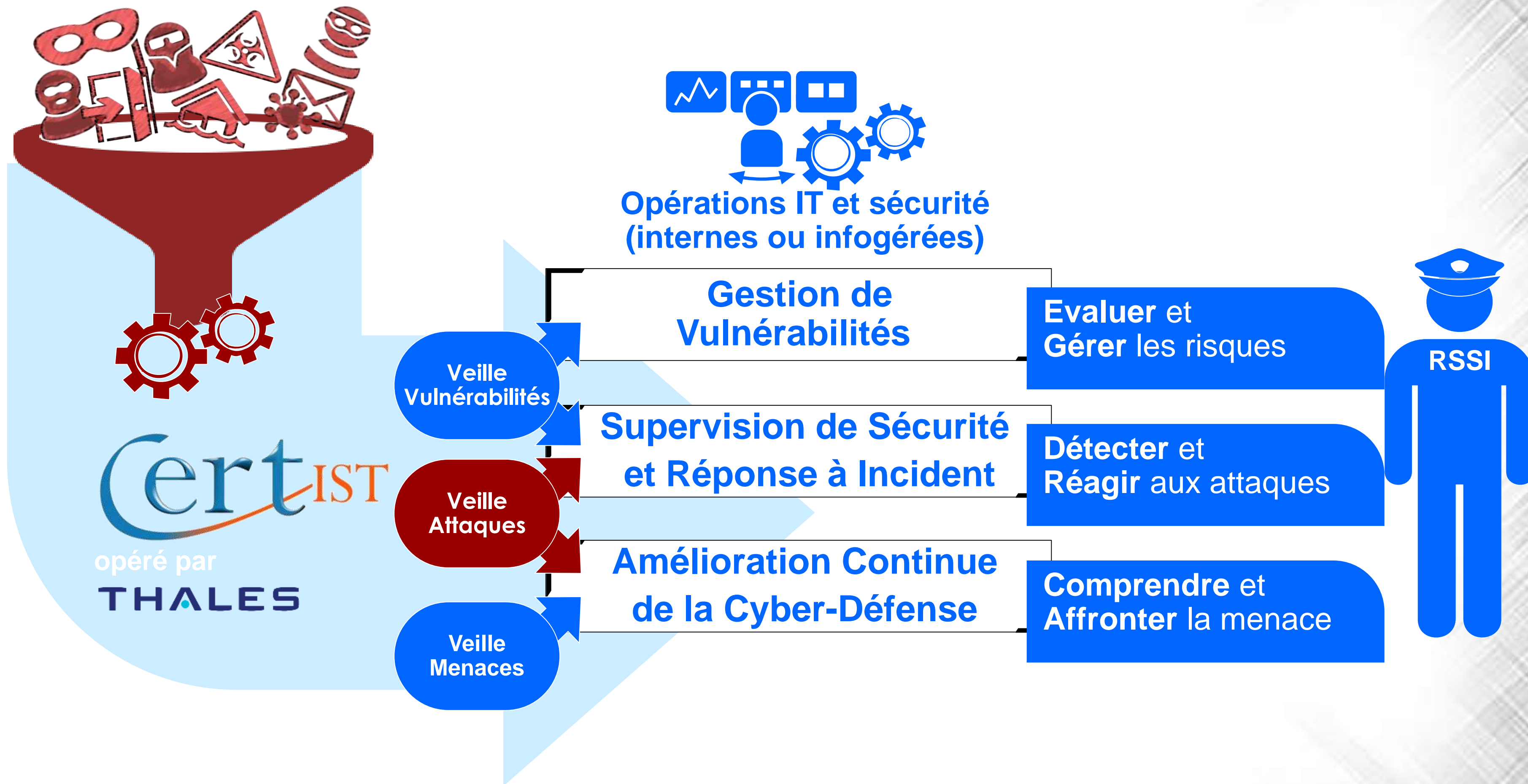


Suis-je informé ?  
Suis-je à jour ?  
Que dois-je faire ?

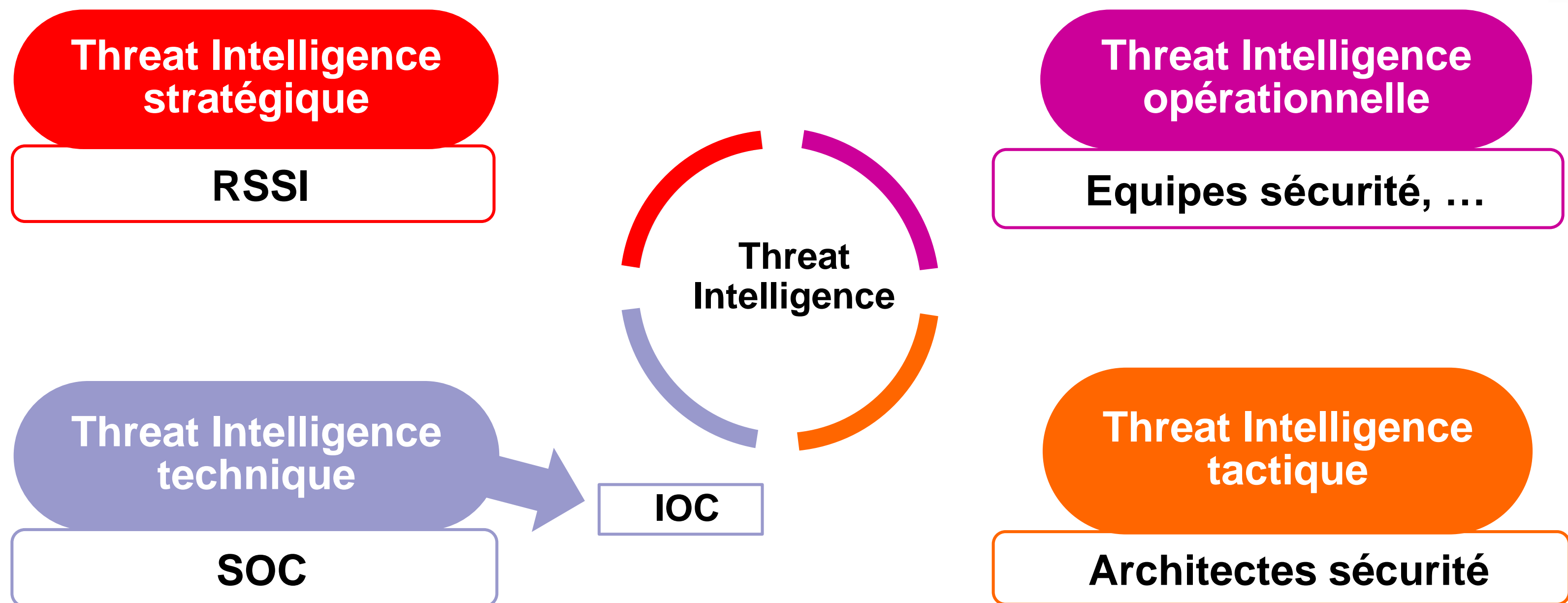
# La Cyber Threat Intelligence (CTI)



# La Cyber Threat Intelligence (CTI)



# Threat Intelligence pour qui ?



**La Threat Intelligence n'est pas uniquement pour les SOC !**

## IOC : Indicateurs de compromission

20 What's an indicator?

- File MD5 checksum is 88195c3b0b349c4edbe2aa725d3cf6ff
- File name is ripsvc32.dll
- File path contains \system32\mtxes.dll
- File PE header compile time is 2008-04-04T18:14:25
- Registry key text contains ripsvc32.dll
- Registry path contains \SYSTEM\CurrentControlSet\Services\Iprip\Parameters\ServiceDll
- Service DLL is ripsvc32.dll
- Process has a handle named RipSvc32.dll
- File path contains \system32\msasn.dll
- File path contains \system32\msxml15.dll
- File size is between 500000 and 900000
- File name is SPBBCSvc.exe
- File name is hinv32.exe
- File name is vprosvc.exe
- File name is wuser32.exe
- Service name is IPRip
- Service DLL is not iprip.dll

MANRIANT



Source: David J. Bianco, personal blog

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



# Computer Emergency Response Team

## Industrie Services Tertiaire

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

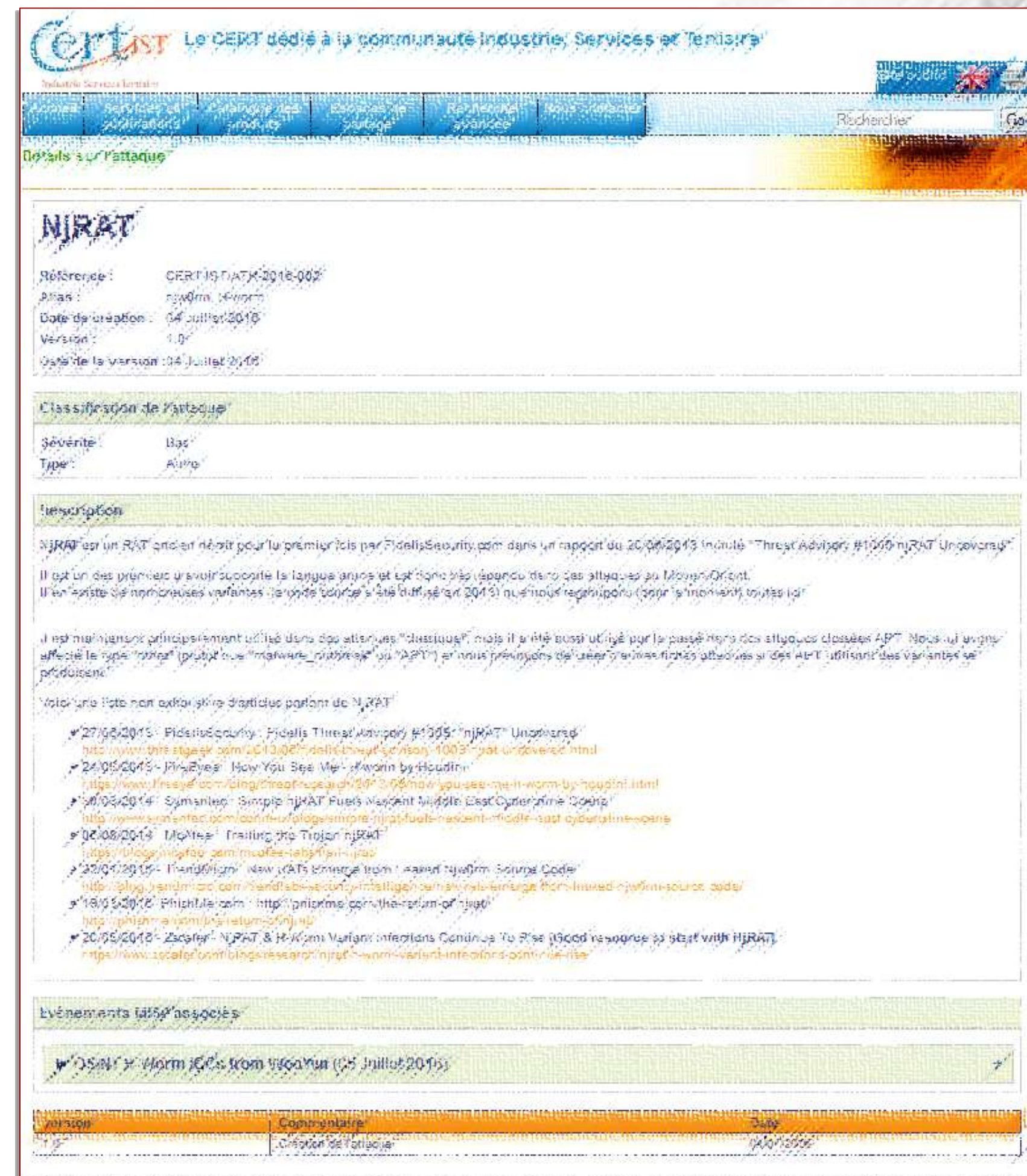


- Nouveau service qui a démarré le 1<sup>er</sup> juillet 2016
- Objectifs de ce nouveau service :
  - Répertorier les attaques connues en se focalisant sur les attaques de types APT et les attaques émergentes, mais aussi d'autres types d'attaques (Phishing, malspam,...)
  - Fournir une base d'IOC qualifiés
- 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, ...)

- 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, phishing...
      - Domain : aerospace, banking, energy, government, ...
      - Risk-level,
      - ...
  - Bulletin mensuel analysant et synthétisant l'actualité du mois en termes d'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



The screenshot displays a web page titled "NjRAT" with the following details:

- Référence:** CERT-IST-ATK-2016-003
- Alias:** njworm, Hworm
- Date de création:** 04 juillet 2016
- Version:** 1.0
- Date de la version:** 04 juillet 2016

**Classification de l'attaque**

- Sévérité:** Bas
- Type:** Autre

**Description**

NjRAT est un RAT ancien né en 2004 pour la première fois par FidelisSecurity.com dans un rapport du 20/06/2013 intitulé "Threat Advisory #1000: NjRAT Uncovered". Il est un des premiers à avoir supporté la langue arabe et est donc très répandu dans les attaques au Moyen-Orient. Il en existe de nombreuses variantes de code source qui ont été diffusées en 2013 et nous regroupons (pour le moment) toutes ici.

Il est maintenant principalement utilisé dans des attaques "classiques", mais il a été aussi utilisé par le passé dans des attaques classées APT. Nous lui avons affecté le type "other" plutôt que "malware\_routine" ou "APT" en nous prévoyant de créer de nouvelles fiches dédiées si des APT utilisant des variantes se produisent.

Voici une liste non exhaustive d'articles parlant de NjRAT:

- 27/06/2013: FidelisSecurity.com: Fidelis Threat Advisory #1000: "NjRAT" Uncovered  
<http://www.threatsense.com/2013/06/fidelis-threat-advisory-1000-njrat-uncovered.html>
- 24/05/2013: PhishEye: How You See Me - A worm by Houdini  
<https://www.phisheye.com/blog/2013/05/24/how-you-see-me-a-worm-by-houdini.html>
- 20/03/2014: Symantec: Simple NjRAT Fuels Masses of Middle East Cybercrime 'Cobots'  
<http://www.symantec.com/connect/blog/simple-njrat-fuels-masses-of-middle-east-cybercrime-cobots>
- 02/08/2014: McAfee: Trailing the Trojan NjRAT  
<https://blogs.mcafee.com/mcafee-labs/2014/08/02/trailing-the-trojan-njrat/>
- 22/04/2015: ThreatMag: New RATs Emerge from a Mass of Trojan Source Code  
<http://blog.threatmag.com/2015/04/22/new-rats-emerge-from-a-mass-of-trojan-source-code/>
- 18/05/2016: PhishEye.com: http://phisheye.com/the-return-of-njrat/  
<http://phisheye.com/the-return-of-njrat/>
- 20/05/2016: Zscaler: NjRAT & H-Worm Variant Infections Continue To Rise (Good response to start with NjRAT)  
<https://www.zscaler.com/blog/news/njrat-h-worm-variant-infections-continue-to-rise>

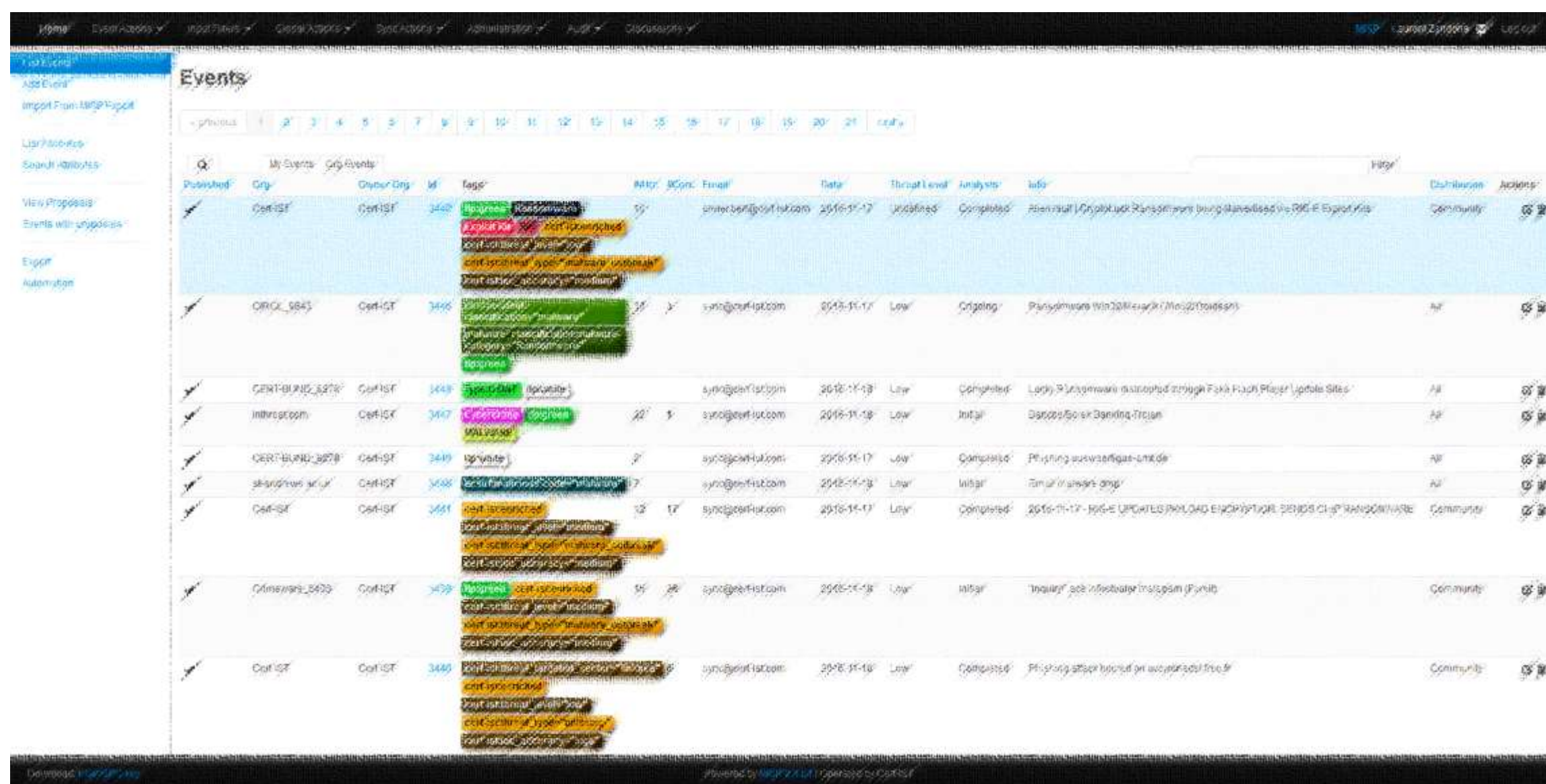
**Événements liés associés**

- OSINT - Worm I/Os from Houdini (05 juillet 2013)

Navigation: [Retour](#) | [Commentaire](#) | [Ajouter un commentaire](#) | [Ajouter un commentaire](#)

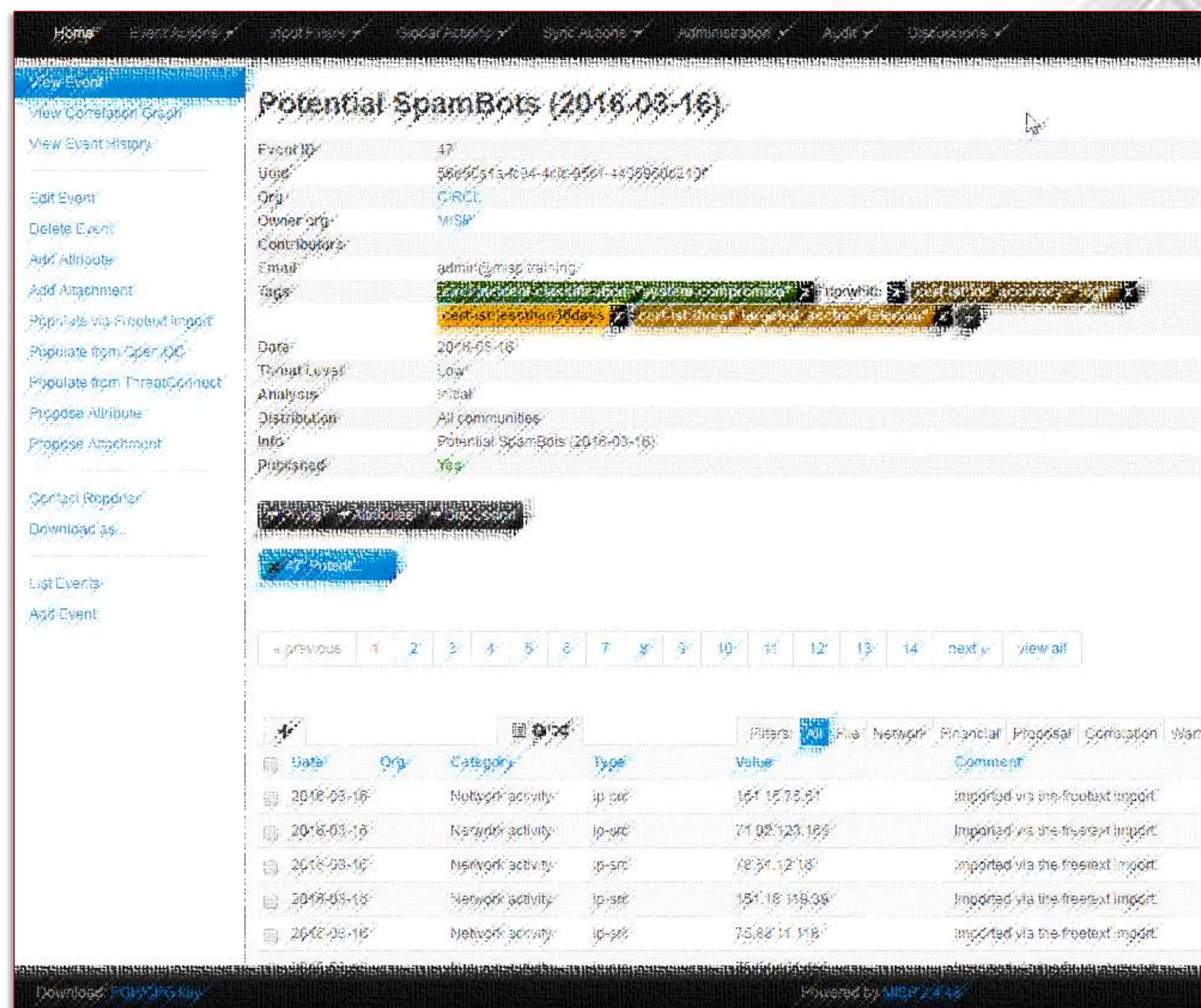
- Malware Information Sharing Platform

- 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, ...

Published	Org	Owner Org	ID	Tags	MITR	BCIC	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	Cert-IST	Cert-IST	3442	Malware, Rootkits, ...	55		syn@cert-ist.com	2016-11-17	Undefined	Completed	Abnormal Cryptolux Ransomware being distributed via POC E-Export file	Community	🔍 📄 🗑️
✓	CIRCL_5645	Cert-IST	3446	Malware, ...	21	21	syn@cert-ist.com	2016-11-17	Low	Ongoing	Phishing emails (Win2011) (Malicious)	All	🔍 📄 🗑️
✓	CERT-BUND_3278	Cert-IST	3448	Malware, ...			syn@cert-ist.com	2016-11-18	Low	Completed	Logic Ransomware distributed through Foxit Flash Player Update Sites	All	🔍 📄 🗑️
✓	Intelligence	Cert-IST	3447	Malware, ...	22	3	syn@cert-ist.com	2016-11-18	Low	Initial	Darknet/Spam Bouncing Trojan	All	🔍 📄 🗑️
✓	CERT-BUND_3278	Cert-IST	3449	Malware, ...	2		syn@cert-ist.com	2016-11-17	Low	Completed	Phishing emails (Win2011) (Malicious)	All	🔍 📄 🗑️
✓	shard/rev/air/	Cert-IST	3448	Malware, ...	17		syn@cert-ist.com	2016-11-17	Low	Initial	Remote access (RDP)	All	🔍 📄 🗑️
✓	Cert-IST	Cert-IST	3451	Malware, ...	12	17	syn@cert-ist.com	2016-11-17	Low	Completed	2016-11-17 - 195-E UPDATES (WIN2011) (Malicious)	Community	🔍 📄 🗑️
✓	Coinbase_5433	Cert-IST	3453	Malware, ...	55	26	syn@cert-ist.com	2016-11-18	Low	Initial	Initial access (RDP) (Malicious)	Community	🔍 📄 🗑️
✓	Cert-IST	Cert-IST	3446	Malware, ...			syn@cert-ist.com	2016-11-18	Low	Completed	Phishing emails (Win2011) (Malicious)	Community	🔍 📄 🗑️

- 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, ...



The screenshot displays the 'View Event' page for 'Potential SpamBots (2016-03-16)'. The interface includes a navigation menu on the left with options like 'View Correlation Graph', 'View Event History', 'Edit Event', and 'Delete Event'. The main content area shows event details:

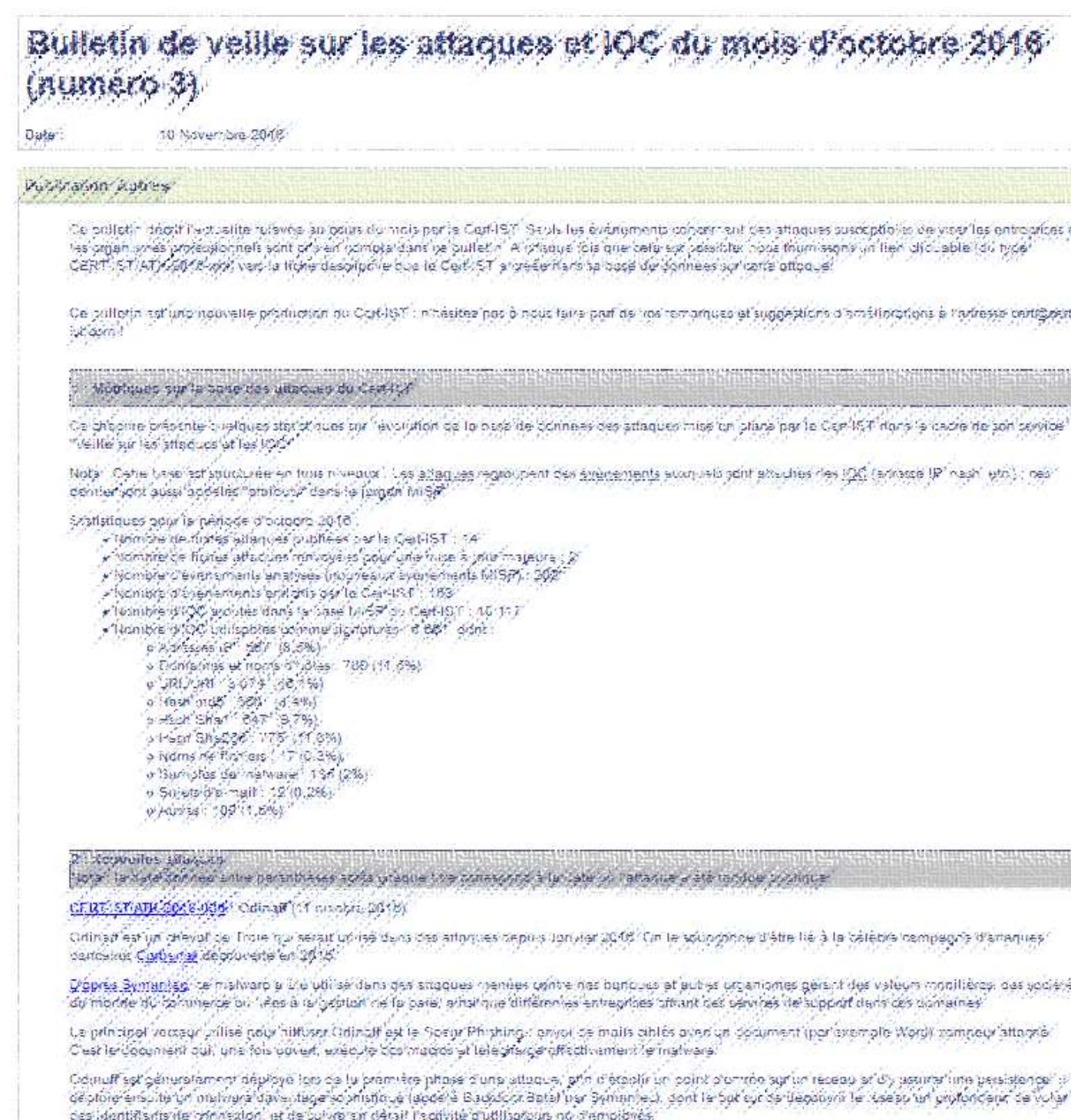
- Event ID: 47
- Urg: 5665f5f3-4024-402e-9561-447695002104
- Org: CERT
- Owner org: MISP
- Contributors: admin@misp.training
- Email: admin@misp.training
- Tags: Cert-ist, es, other, add, ...
- Date: 2016-03-16
- Threat Level: Low
- Analysis: Initial
- Distribution: All communities
- Info: Potential SpamBots (2016-03-16)
- Published: Yes

Below the details is a table of related events:

Date	Org	Category	Type	Value	Comment
2016-03-16		Network activity	ip-cc	151.15.75.51	Imported via the freetext import.
2016-03-16		Network activity	ip-wc	71.02.123.189	Imported via the freetext import.
2016-03-16		Network activity	ip-sr	1834.12.18	Imported via the freetext import.
2016-03-16		Network activity	ip-sec	151.18.118.35	Imported via the freetext import.
2016-03-16		Network activity	ip-sec	75.82.11.118	Imported via the freetext import.

- 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



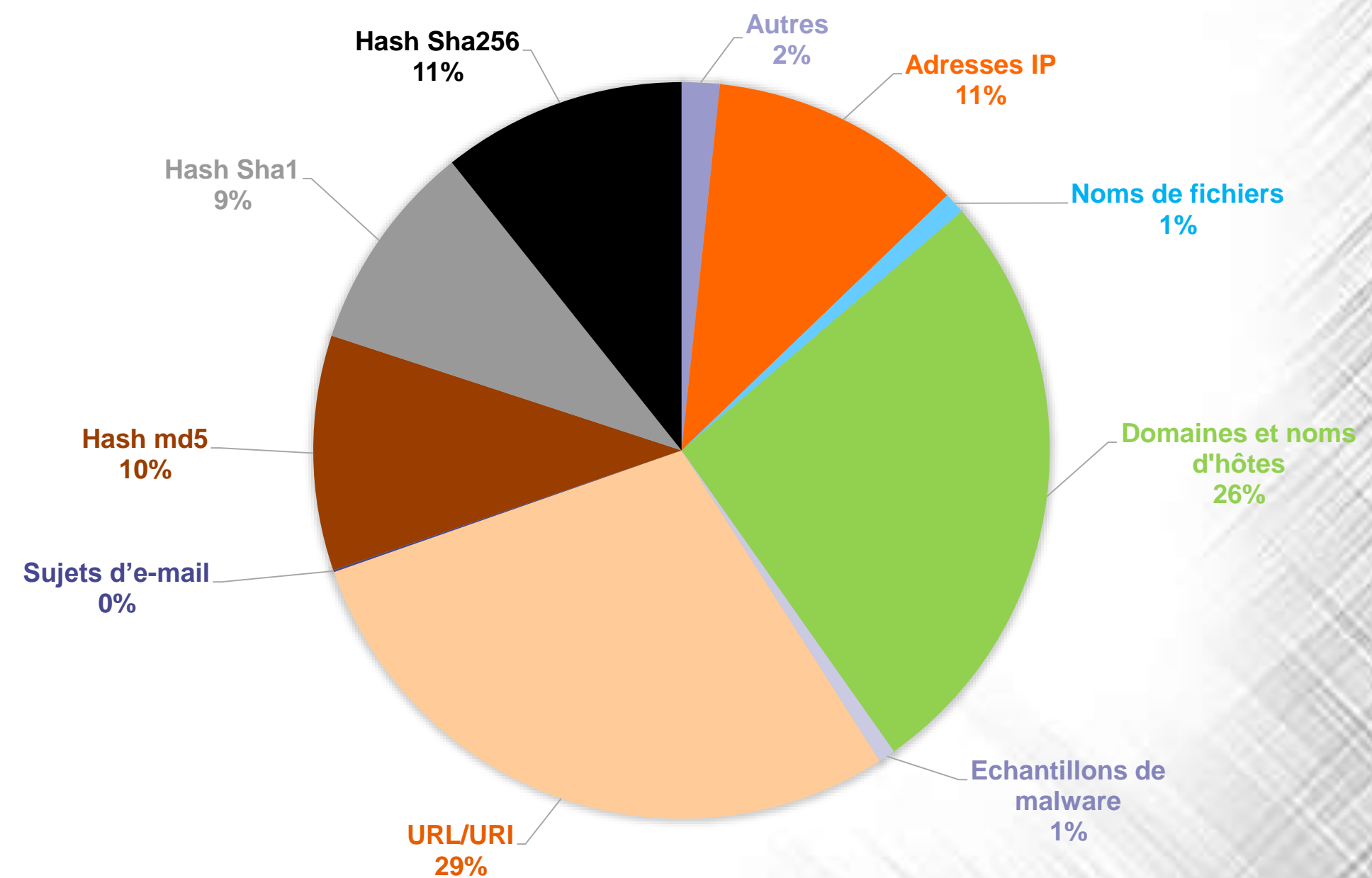
- Pour la période de juillet à octobre 2016 :

- 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





- **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**

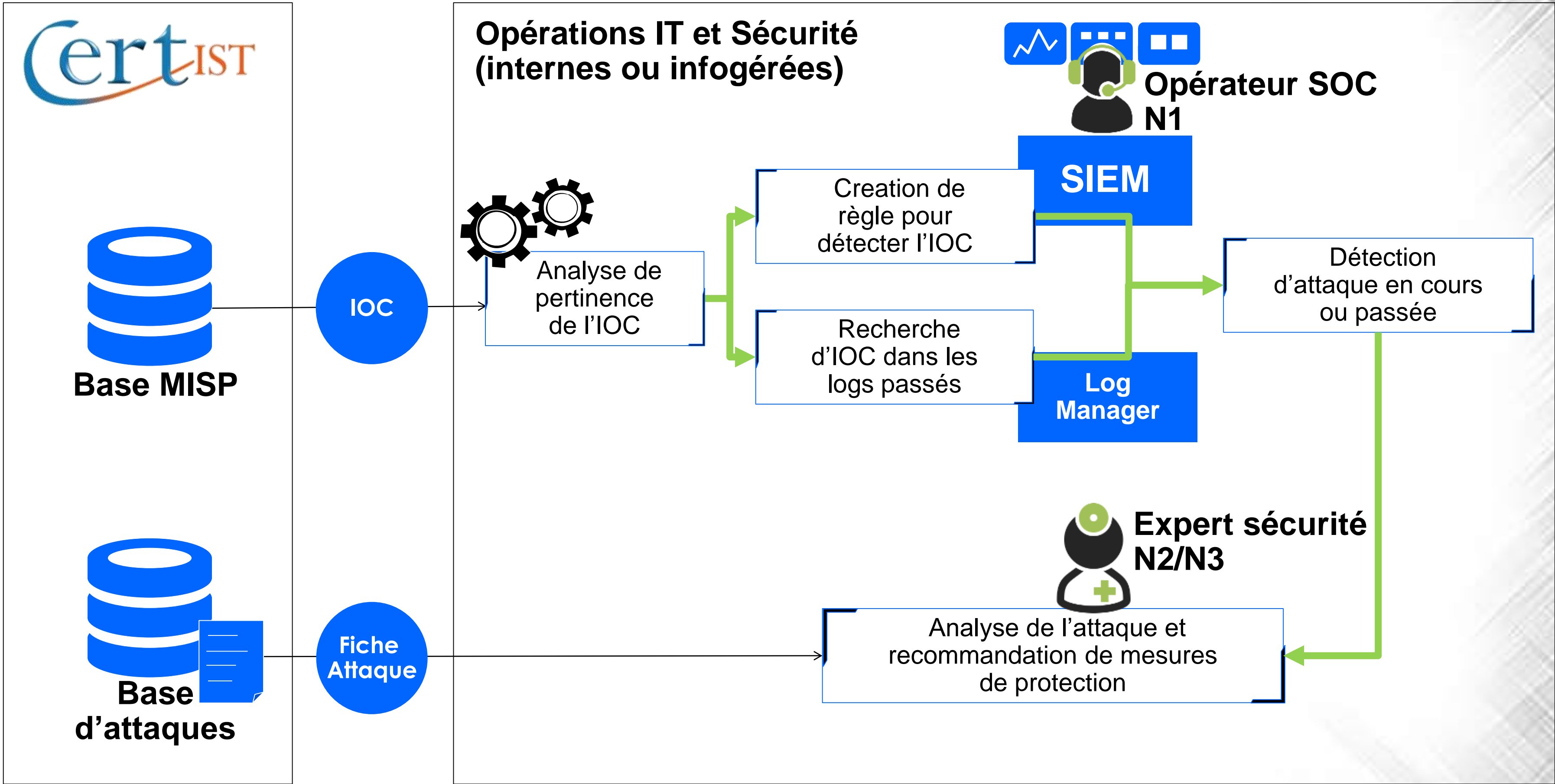
- Utilisation par le SOC ou l'IR (Incident Response team) de la base d'IOC pour savoir si un élément suspect correspond à un incident connu et obtenir la fiche attaque correspondante

- **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

- **Informers**

- Sensibilisation de l'ensemble des acteurs concernés (attaques, cibles, TTP, ...)



# Computer Emergency Response Team

## Industrie Services Tertiaire

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



# Démonstration du service

The screenshot shows the CertIST website interface. At the top, the logo and tagline "Le CERT dédié à la communauté industrielle, Services et Tertiaire" are visible. The navigation menu includes "Services et publications", "Espaces de partage", and "Espace Adhérents". A sidebar on the left lists various services like "Suivi des vulnérabilités" and "Suivi des menaces". The main content area features a "Liste des attaques" section with a table of recent incidents.

Date	Motif de l'attaque	Vulnérabilité	Evénement
2018-11-15	Cryptolock	1, 0	18 novembre 2018
2018-11-17	Manoia	1, 0	17 novembre 2018

The screenshot displays the "Events" dashboard in the CertIST system. It shows a table of security incidents with columns for "Published", "Org", "Owner/Corp", "Risk", "Date", "Threat Level", "Analysis", and "Info". Several incidents are listed, including "Crimesware\_2493" and "CRQL\_2843".

Published	Org	Owner/Corp	Risk	Date	Threat Level	Analysis	Info
✓	Crimesware_2493	CertIST	3489	2018-11-21	Low	Initial	Logon 2018-11-21 - 105...
✓	Crimesware_2493	CertIST	3489	2018-11-21	Low	Initial	Driveby attack on...
✓	Crimesware_2493	CertIST	3487	2018-11-21	Low	Initial	Logon 2018-11-21 - 105...
✓	CRQL_2843	CertIST	3499	2018-11-21	Low	Completed	CRQL - demopage.gov...
✓	IT-CASA	CertIST	3500	2018-11-21	Medium	Completed	New address banking...
✓	CRICERT	CertIST	3492	2018-11-17	Medium	Completed	IT's Parliament - 105...
✓	Crimesware_2493	CertIST	3482	2018-11-20	Low	Initial	Problems with sym...
✓	CertIST	CertIST	3487	2018-11-17	Undefined	Completed	Manoia - Cryptolock...

The screenshot shows a detailed view of a security event titled "Driveby citylink.co.nz (Rig per Punch++)". It includes fields for "Event ID", "Date", "Threat Level", "Analysis", and "Info". A "Related Events" section lists other incidents that are linked to this event.

Date	Org	Category	Type	Value	Comment	Related Events	RIS	Dist/Status	Actions
2018-11-21	External analysis	external	Driveby First Discussed Date	2018-11-21	CertIST First Discussed Date	3491-3495-3496-3499	100	Initial	🔍 🗑️ 🔄
2018-11-21	External analysis	external	CertIST First Discussed Date	2018-11-21	CertIST First Discussed Date	3496-3497-3498-3499	100	Initial	🔍 🗑️ 🔄
2018-11-21	External analysis	hack	https://news.cert-ist.com/insights/clear_data/external-manual-driveby-attack-on-citylink.co.nz	https://news.cert-ist.com/insights/clear_data/external-manual-driveby-attack-on-citylink.co.nz	CertIST External link	3491-3495-3496-3499	100	Initial	🔍 🗑️ 🔄
2018-11-21	External analysis	hack	Driveby 2018-11	Driveby 2018-11	CertIST Attack Name	3491-3495-3496-3499	100	Initial	🔍 🗑️ 🔄

# Computer Emergency Response Team

## Industrie Services Tertiaire

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

