

**Forum Cert-IST 2008**  
**De la vulnérabilité à la crise :**  
**optimiser sa réponse**  
**(présentation des résultats de l'enquête)**



Equipe prestataire Cert-IST –  
Juin 2008

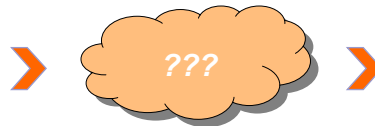


Processus de traitement des Avis Cert-IST  
Problématique

- Les vulnérabilités et ensuite ?



Menaces et Failles  
Incidents



RSSI et décideurs



Utilisateurs

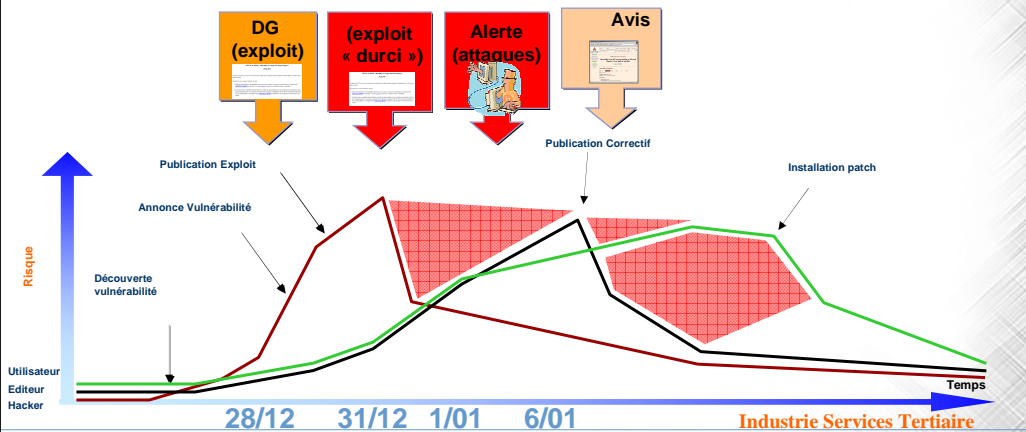


Administrateurs  
systèmes et réseaux

**Entreprise**

Industrie Services Tertiaire

- L'attaque suit de plus en plus souvent et vite l'identification d'une faille
- Quand elle ne la précède pas ... (zéro-day)



- Enquête : méthodologie
- Enquête questionnaire : résultats quantitatifs
- Enquête interview : présentation et synthèse des enseignements

## Méthodologie de l'enquête Questionnaire, complété par des interviews

- Le Cert-IST a réalisé cette année une étude auprès de ses correspondants sur la façon dont les différents services du Cert-IST sont utilisés au sein des entreprises adhérentes.
- Cette étude a plusieurs objectifs :
  - Identifier les améliorations à apporter aux services
  - Etablir des guides de bonnes pratiques pour aider chacun à mieux utiliser ces services
- La première phase de l'étude a été constituée par la réalisation et le dépouillement d'un questionnaire transmis à l'ensemble des adhérents. (taux de réponse 66%).
- Cette phase a été complétée par une interview (téléphonique) auprès d'adhérents représentatifs afin d'analyser les pratiques existantes.
  - Ont été interviewés les partenaires et membres fondateurs (parfois 2 à 3 interlocuteurs)
  - Retour des secteurs : industrie, high-tech, chimie, finance, para-public (hospitalier)

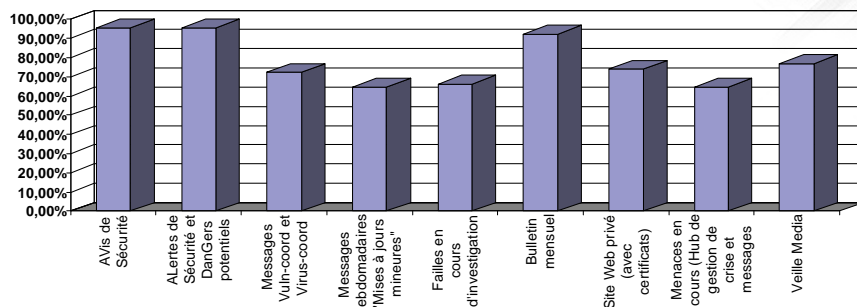
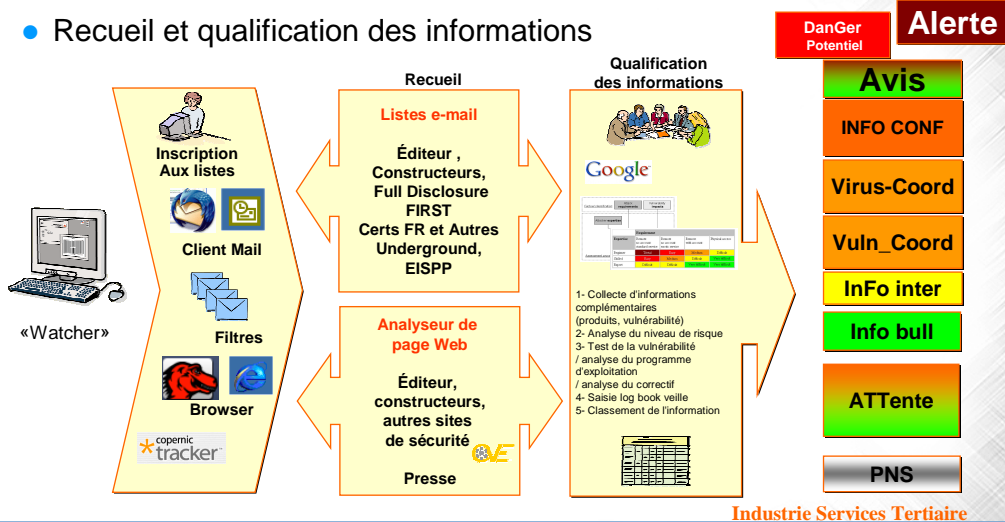
Industrie Services Tertiaire

## Agenda

- Enquête : méthodologie
- Enquête questionnaire : résultats quantitatifs
- Enquête interview : présentation et synthèse des enseignements

Industrie Services Tertiaire

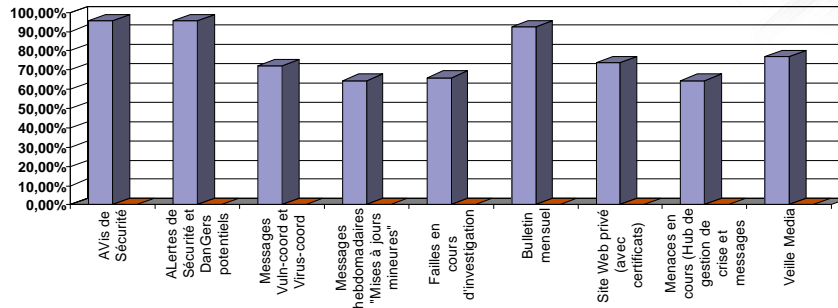
### • Recueil et qualification des informations



### • Principaux enseignements :

- Les productions de base (Avis, Alertes) forment le socle commun pour tous
- Les formes éditoriales (Site Web, Bulletin, et même la très récente Veille media) ont une bonne notoriété.
- Même les productions les plus pointues sont connues à plus de 60%.

## Connaissance des productions Cert-IST Analyse

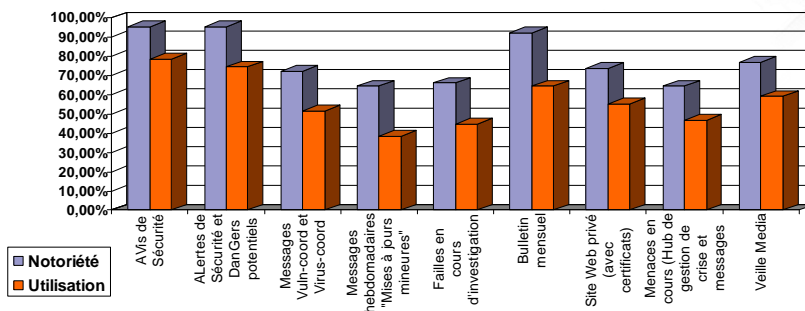


● Principaux enseignements :

- Les productions de base (Avis, Alertes) forment le socle commun pour tous
- Les formes éditoriales (Site Web, Bulletin, et même la très récente Veille media) ont une bonne notoriété.
- Même les productions les plus pointues sont connues à plus de 60%.

Industrie Services Tertiaire

## Utilisation des productions Cert-IST Analyse



● Principaux enseignements :

- Les productions les mieux connues sont «évidemment (?)» les plus utilisées
- Chaque produit, même les moins connus, est utilisé ou diffusé à 40/60 %.

Industrie Services Tertiaire

- Anticipation et gestion des risques (prévention)
- Accompagnement jusqu'à la clôture des crises



Le CERT dédié à la communauté Industrie, Services et Tertiaire française

ACCUEIL | ARCHIVES DES PUBLICATIONS | MUTUALISATION | INFORMATIONS PRATIQUES | FAQ | RECHERCHER

**[Vul PnP MS05-039] Vulnérabilité Windows "Plug-and-Play" (MS05-039) - Ver "Zotob"**

Accueil | Vue de gestion de crises | Vulnérabilité Windows "Plug-and-Play" (MS05-039) - Ver "Zotob" | Version imprimable

Ce blog détaille les informations sur la vulnérabilité "Plug and Play" sous Microsoft Windows (MS05-039) et les informations relatives aux programmes d'installation et aux vers exploitant les que "Zotob".

Date	Liens des posts
26 août 2005	Annulations de patchs effectués dans la diffusion de zotob
26 août 2005	Critique des patchs Windows XP SP1 et SP2 avec "Remote File Sharing & FileCaching" actif
19 août 2005	Point sur "Zotob" et les variantes ou alias (exploitant MS05-039)
18 août 2005	Quelques plates-formes Windows sont impactées par le vuln MS05-039 ?
18 août 2005	Notes de "Cisco" devant des recommandations sur "Zotob" et "Rbot"
17 août 2005	Variante de "Zotob"
16 août 2005	Alerte AL 2005-001
14 août 2005	Alerte sur le ver "Zotob" exploitant la vulnérabilité PnP MS05-039
12 août 2005	Change d'alias de MS05-039
12 août 2005	Ouverture d'exploitabilité Windows "PnP" MS05-039

Précisions sur les plates-formes (XP SP1)

Précisions sur les alias et variantes (Esbot, Bozori)

Notice de Cisco sur zotob et Rbot

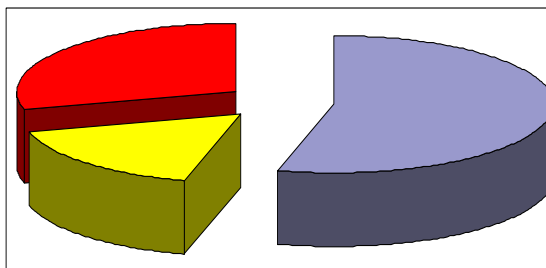
**Avis AV -294**

**DG 05**

**Alerte Veille 24/7 & SMS**

**Alerte Virus 04**

Industrie Services Tertiaire



- Pour le "patch-management"
- Pour vérifier la conformité des plates-formes
- Pour identifier les crises

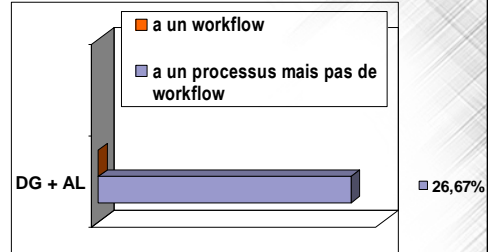
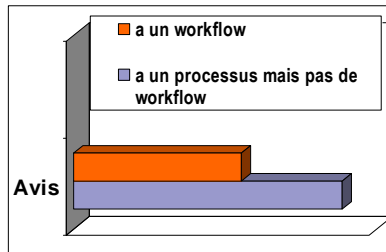
- Réponses Non (0) Oui (1), multiples possibles

- Pour la majorité de nos interlocuteurs, les avis du Cert-IST sont le principal déclencheur du processus de patch management.
- Pour plus d'un quart ils servent à identifier les crises.

Industrie Services Tertiaire



## Comment utilisez-vous les avis du Cert-IST

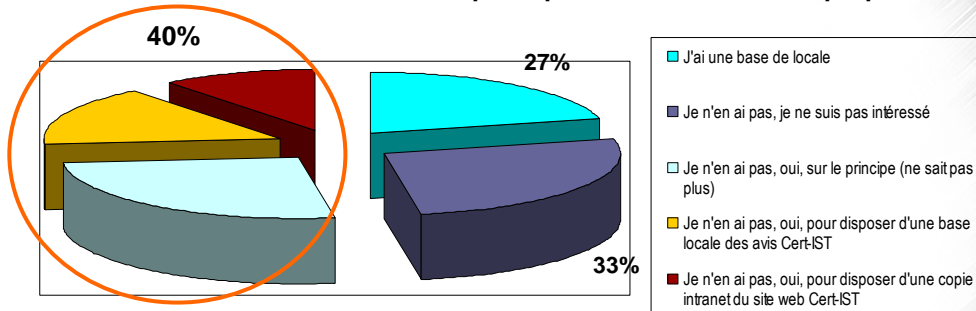


- Une majorité des adhérents ont mis en place un processus formalisé de traitement des avis du Cert-IST
- Un tiers d'entre eux ont automatisé ce processus à l'aide d'un workflow
- Pour les DG et les Alertes, le traitement est généralement au cas par cas
  - (Pas de workflow car traitement par une petite cellule)

Industrie Services Tertiaire

## Avez-vous une base de donnée locale ?

... ou seriez-vous intéressé pour que le Cert-IST vous en propose une ?



27% ont déjà en interne une base dédiée au suivi des avis  
40% sont intéressés pour mettre en place une base locale  
33% se contentent de la base hébergée par le Cert-IST

Industrie Services Tertiaire

**Cert-IST nomenclature**

Expertise	Requirement	Remote no account standard service	Remote no account exotic service	Remote with account	Physical access
Beginner	Trivial	Easy	Medium	Difficult	Very difficult
Skilled	Easy	Medium	Difficult	Very difficult	Very difficult
Expert	Difficult	Difficult	Very difficult	Very difficult	Very difficult

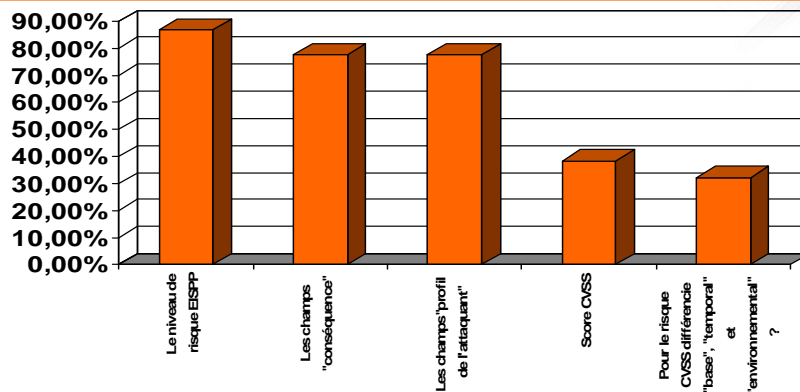
Information Type

- AV for security Advisories
- AI for Alerts (urgent security informations)
- DG for potential DataGens
- BI for the Security Bulletin
- DV for Miscellaneous information (address change, ...)
- IF for Useful informations

Risk	Recommendation
Very high	Act immediately on all systems
High	Act immediately on front-end systems and servers
Medium	Action can be delayed, but a security maintenance operation must be scheduled now
Low	Action can be delayed until the next scheduled maintenance operation

**Impact severity**

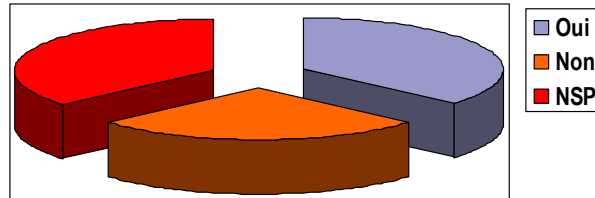
Exploitation facility	Take control	Get limited access	Disrupt service	Get limited privilege	Disrupt service Leverage
Trivial	Very high	High	High	High	Medium
Easy	Very high	High	High	High	Medium
Medium	Very high	High	Medium	Medium	Medium
Difficult	High	Medium	Medium	Low	Low
Very difficult	High	Medium	Low	Low	Low



- Les champs technique issus de la métrique « EISPP » sont très utilisés.
- L'adhésion est pour l'instant beaucoup moins marquée pour le score CVSS.



Le risque EISSP devrait-il à terme disparaître au profit de la notation CVSS

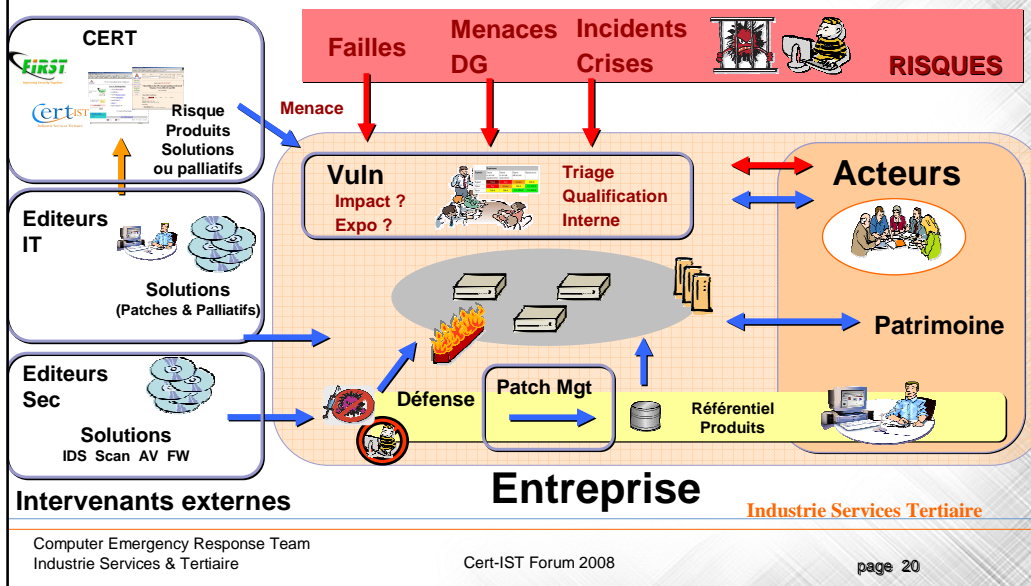


- Les adhérents sont partagés sur ce point.
  - Rappel: les adhérents répondent que EISPP est aujourd'hui la notation la plus pertinente et la plus utilisée. (cf slide et question précédents)
  - Mais 30% nous demandent de migrer vers le standard international CVSS à terme
    - (en prévoyant une phase de transition)

Industrie Services Tertiaire

- Enquête : méthodologie
- Enquête questionnaire : résultats quantitatifs
- Enquête interview : présentation et synthèse des enseignements

Industrie Services Tertiaire



- La plupart des adhérents effectuent une évaluation interne complémentaire à réception des avis pour prise en compte
  - Confirmation présence cible dans le parc
  - Exposition réelle cible (mesures de protection/défense ?)
  - Impact attaque
- Cette qualification aboutit à une classification valant recommandation
  - Correction « immédiate » (de l'ordre de 4 à 5 jours)
  - Déploiement ou non de palliatifs, mise aux plannings du patch.
- Ces avis « internes » parviennent aux équipes en charge des déploiements des patches.

- Le processus est moins formalisé car traité au sein d'une cellule ad hoc.
- Il nécessite une analyse et une qualification interne plus poussée par la cellule SSI.
  - Confirmation présence cible dans le parc
  - Exposition réelle cible (mesures de protection/défense ?)
  - Impact attaque
- Cette analyse aboutit à la définition d'un processus « à façon ».
  - Comparaison aux polices (les flux, l'application, nécessaires à l'attaque, sont-ils autorisés ?)
  - Blocage de sites, ou de ports
- DG et Alertes ne sont pas des déclencheurs automatiques de cellules de crise.

