Computer Emergency Response Team
Industrie Services Tertiaire

Forum Cert-IST 2008

De la vulnérabilité à la crise : optimiser sa réponse

(présentation des résultats de l'enquête)

Industrie Services Tertiaire

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

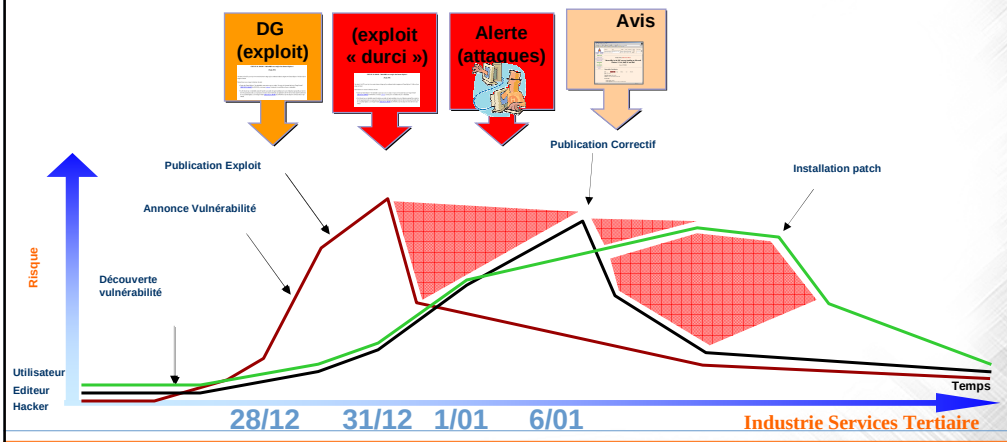
Administrateurs systèmes et réseaux

Entreprise

Industrie Services Tertiaire

Evolution du service : DG et Hub de Crise
S 'adapter à des attaques de plus en plus rapides

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



Industrie Services Tertiaire

Agenda

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

Industrie Services Tertiaire

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)

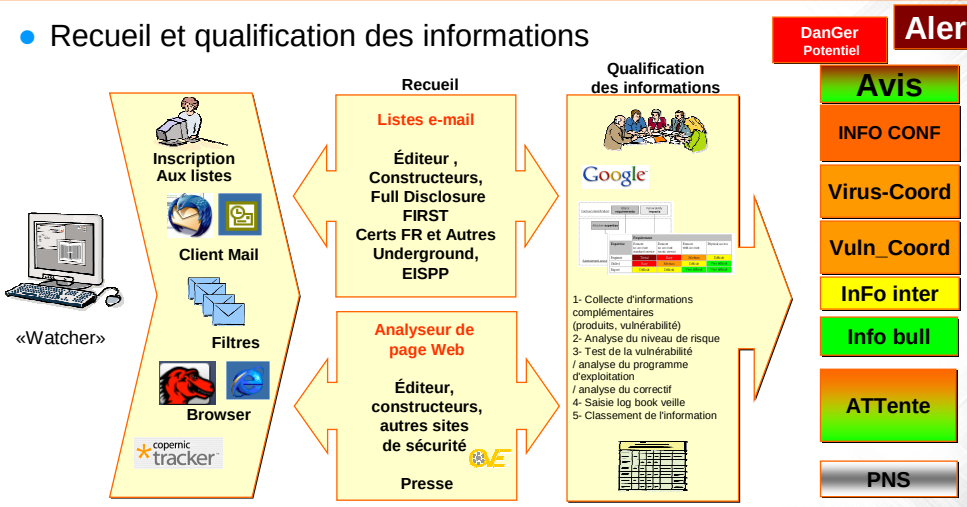
Agenda

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

Le processus de veille

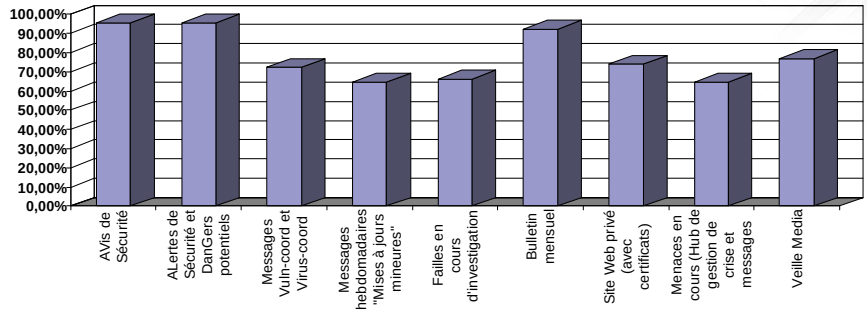
Monitoring des vulnérabilités - évènements - informations

- Recueil et qualification des informations



Industrie Services Tertiaire

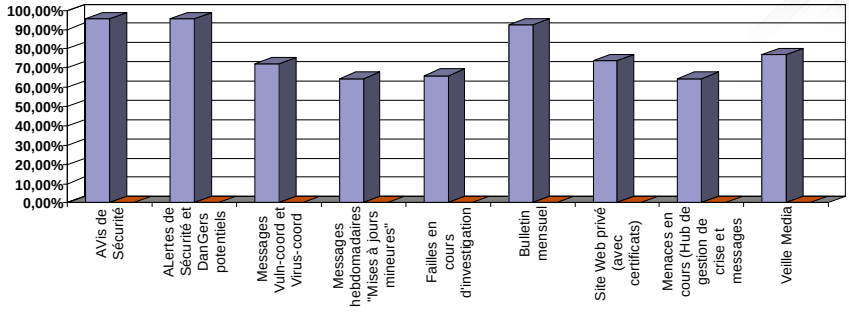
Connaissance des productions Cert-IST Analyse



- 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

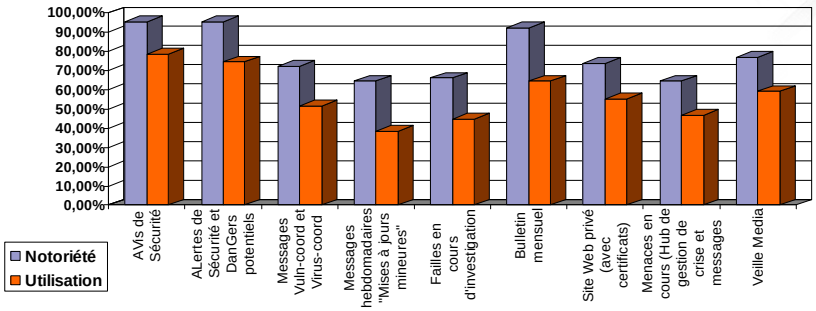
Connaissance des productions Cert-IST Analyse



- 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

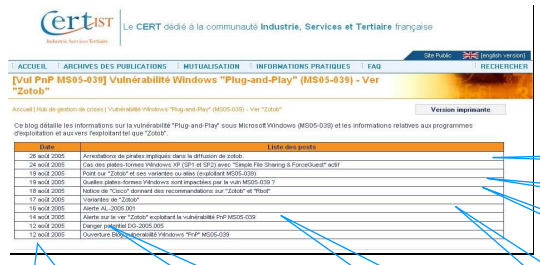


- Principaux enseignements :
  - Les productions les mieux connues sont «évidemment (?) les plus utilisées
  - Chaque produit, même les moins connus, est utilisé ou diffusé à 40/60 %.

Industrie Services Tertiaire

Le Hub de Gestion de Crise

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



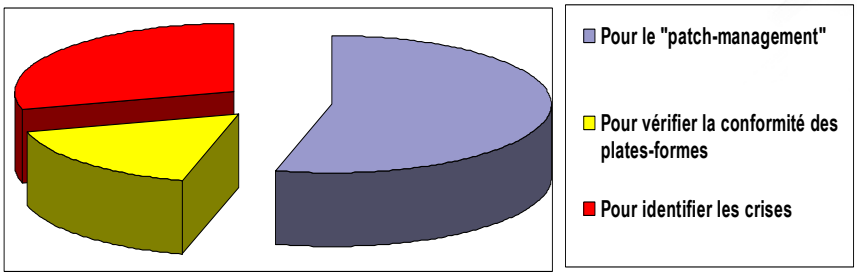
Précisions sur les plates-formes (XP SP1)

Précisions sur les alias et variantes (Esbot, Bozori)

Notice de Cisco sur zotob et Rbot

Industrie Services Tertiaire

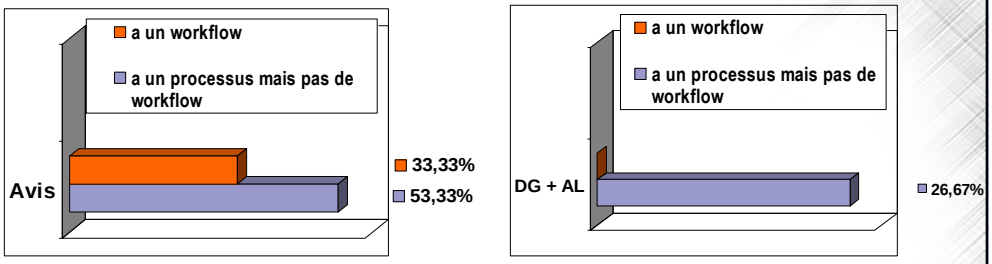
Comment utilisez-vous les avis du Cert-IST



- 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

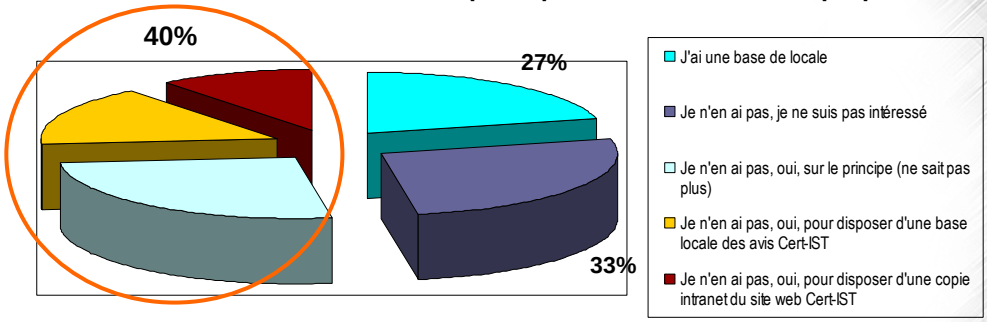


- Une majorité des adhérents ont mis en place un processus formalisé de traitement des avis du Cert-IST
- Un tiers d'entre eux ont automatisé ce processus à l'aide d'un workflow
- Pour les DG et les Alertes, le traitement est généralement au cas par cas
  - (Pas de workflow car traitement par une petite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

Industrie Services Tertiaire

Avez-vous une base de donnée locale ?

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

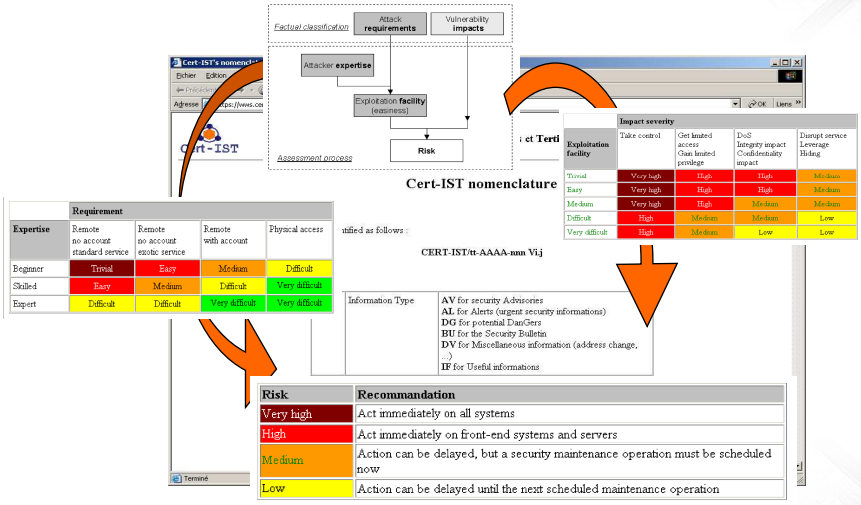


27% ont déjà en interne une base dédiée au suivi des avis
40% sont intéressés pour mettre en place une base locale
33% se contentent de la base hébergée par le Cert-IST

Industrie Services Tertiaire

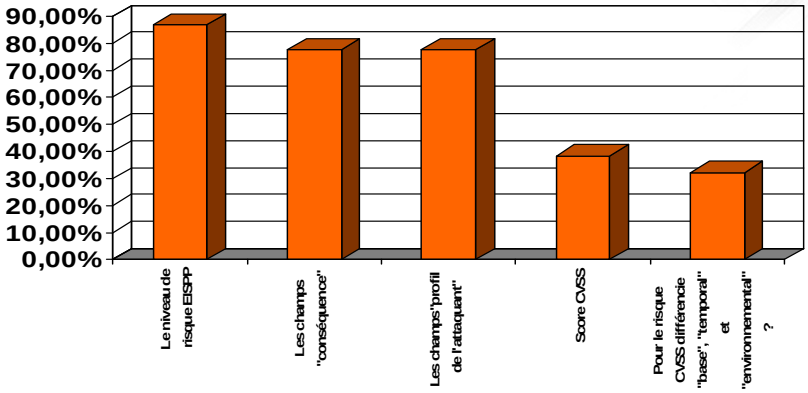
Évaluation du niveau de risque

La métrique EISPP



Risk	Recommandation
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

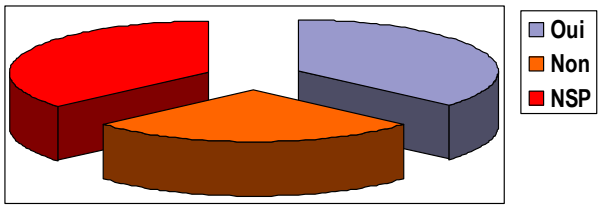
Niveau de risque et caractéristiques de la vulnérabilité (1) : intérêt des champs …



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

Niveau de risque et caractéristiques de la vulnérabilité (2) : EISPP vs 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)

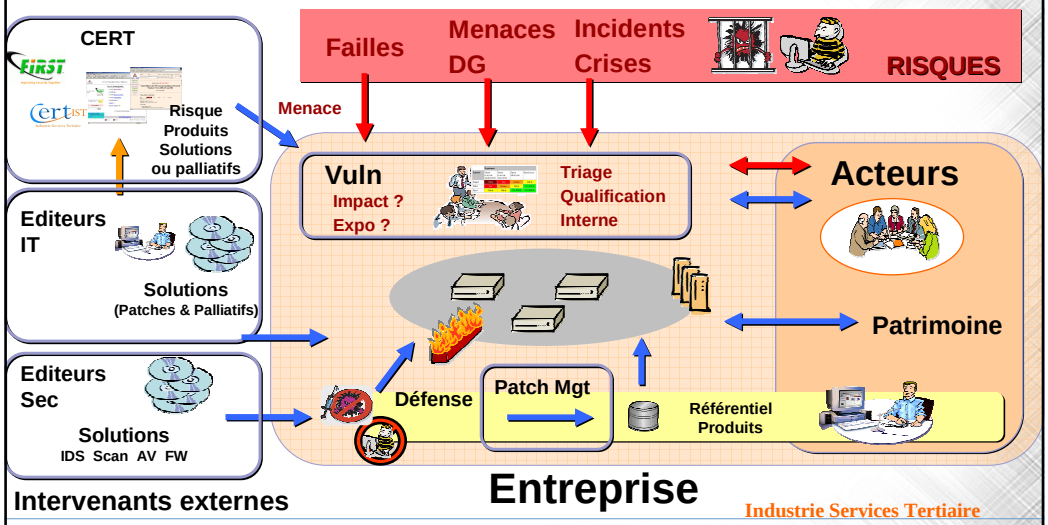
Industrie Services Tertiaire

Agenda

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

Industrie Services Tertiaire

Processus de traitement des Avis Cert-IST
Problématique 2/2



Industrie Services Tertiaire

Enseignements des interviews
Traitement des avis

- 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 patchs.

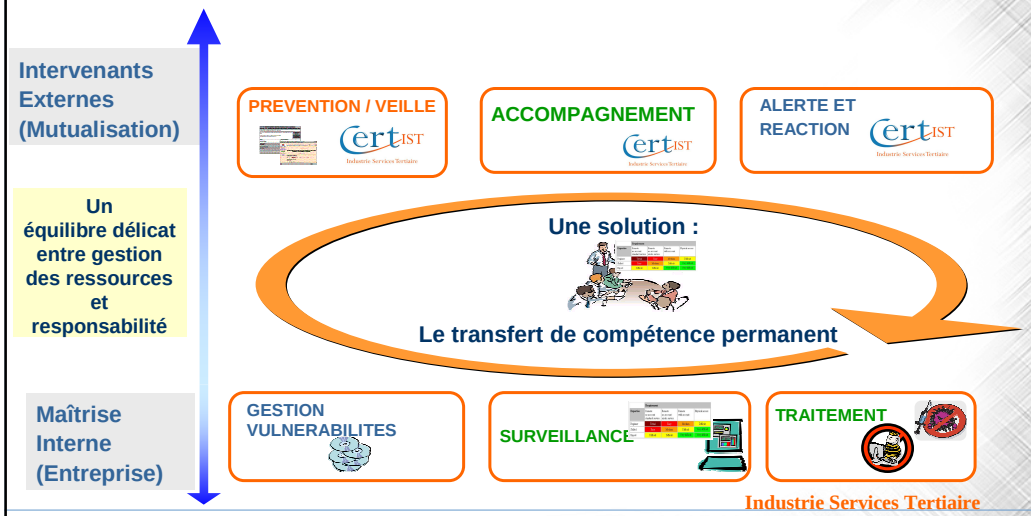
Industrie Services Tertiaire

Enseignements des interviews
Utilisation des Dangers et Alertes

- 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 policies (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.

Industrie Services Tertiaire

Le succès de l'utilisation des avis du cert-IST dépend de son appropriation par tous les intervenants



Industrie Services Tertiaire