Computer Emergency Response Team
Industrie Services Tertiaire

# Prise en compte des informations de veille et d'alerte Cert-IST dans un workflow structuré

Cert-IST
Juin 2006

## Agenda

- Le workflow ?
- Quelles sont les diffusions du Cert-IST concernées
- Comment a-t-on adapté nos solutions ?
- Et après…
- Q & A - Retours d'expérience

## Le workflow ? Définition

Un workflow est un flux d'informations au sein d'une organisation, comme par exemple la transmission automatique de documents entre des personnes.

On appelle « workflow » (traduisez littéralement « flux de travail ») la modélisation et la gestion informatique de l'ensemble des tâches à accomplir et des différents acteurs impliqués dans la réalisation d'un processus métier.

Le terme de « workflow » pourrait donc être traduit en français par « gestion électronique des processus métier ».

De façon plus pratique, le workflow décrit le circuit de validation, les tâches à accomplir entre les différents acteurs d'un processus, les délais, les modes de validation, et fournit à chacun des acteurs les informations nécessaires pour la réalisation de ses tâches.

Exemple : Pour un processus de publication en ligne par exemple, il s'agit de la modélisation des tâches de l'ensemble de la chaîne éditoriale.

Industrie Services Tertiaire

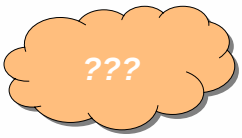


## Problématique (1/5)

- Les vulnérabilités et ensuite ?

Menaces et Failles

Incidents




RSSI et décideurs

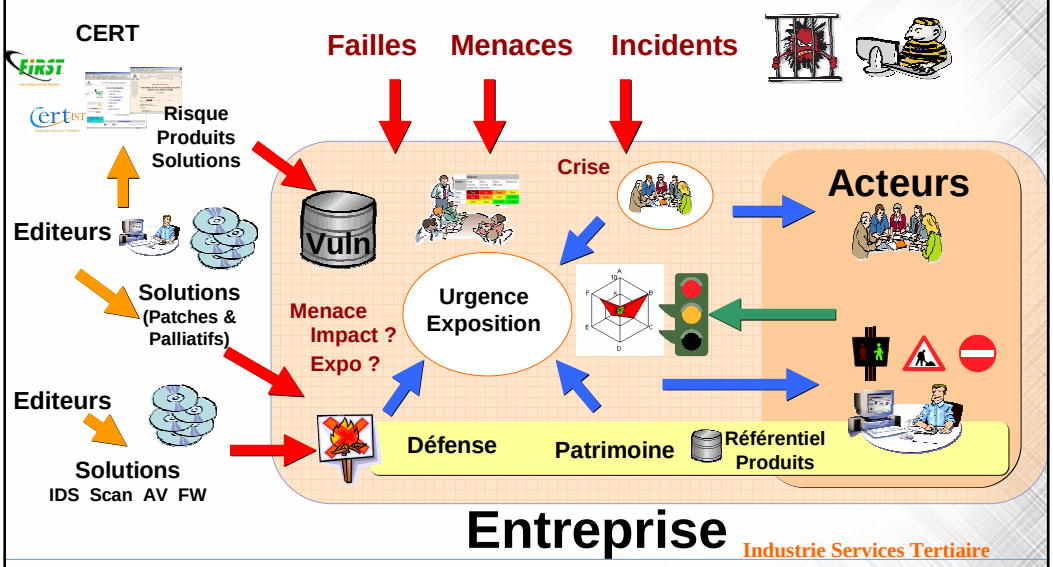
Utilisateurs

Administrateurs systèmes et réseaux

**Entreprise**

Industrie Services Tertiaire

## Problématique (1/3)




Industrie Services Tertiaire



## Problématique (2/3)

- Prendre la bonne décision

  **Industrialiser un « produit » : 1 info engendre 1 décision**

**Réponse : Mise en place d'un workflow**

- **Mais :**
  - Evaluer votre risque
  - Filtrer, valider, corréler et enrichir l'information
  - La distribuer dans le SI
  - Assurer un suivi - Tableau de bord
  - Améliorer le processus

Industrie Services Tertiaire

## Problématique (3/3)

- Evaluer votre risque
  - Votre Politique SSI : Protection de votre patrimoine
  - Identification et inventaire : projets, infrastructures, utilisateurs
  - Analyse d'impact - Evolution du Risque
- Filtrer, valider, corréler et enrichir l'information
  - Nouveau risque ou impact
  - Nouvelle Priorité de traitement
- Distribuer l'information
  - Mise en place d'une organisation adaptée
  - Outil de workflow : manuel, semi-automatique ou automatique ?
- Suivi – Tableau de bord
- Améliorer le processus

Décision

Procédures

Décision

Procédures

Industrie Services Tertiaire



## Réponses (1/2)

- Réactivité / fluidité dans le process
  - Réduction du temps de traitement
- Prise de décision
  - Présentation et structuration des informations et des acteurs pour la prise de décision
- Distribution
- Monitoring – Suivi
  - Traçabilité de la décision - Exemple : suivi de l'état d'avancement d'un patch
  - Actions préventives ou correctives
- Bonne vision de la sécurité de son SI
  - Tableau de bord sécurité : vision globale

Industrie Services Tertiaire

## Réponses (2/2)

- Réponse stratégique : SOX, ISO 27001, ISO 17799
  - Exigence : ***12.6.1 Control of technical vulnerabilities***

**Mise ne place d'une source de veille industrialisée**

**Une organisation adaptée pour prendre en compte ces informations**

**Un Workflow structuré pour l'implémentation concrète de cette source dans le SI**

**sont à terme**

**les seules façons de se mettre en conformité avec les standards !**

Industrie Services Tertiaire



## Retour d'expérience sur le workflow (1/2)

- Premières difficultés rencontrées
  - Outils
  - Procédures
  - Organisation - Acteurs
  - Parc de produits
    - Nommage des produits
    - Exhaustivité de la couverture produits
  - Réponse partielle : le workflow ne fait que complémenter :
    - Sécurité Perimétrique
    - Antivirus
  - Information et sensibilisation des acteurs

Industrie Services Tertiaire

## Retour d'expérience sur le workflow (2/2)

- Solutions apportées
  - Questionnaire / Pilote
  - Manuelles
    - Analyse des avis ASCII / HTML
    - Diffusion dans la structure
  - Semi-automatiques ou Automatiques
    - Orientées présentation (Intranet) et/ou redistribution (« profiling »)
    - Développements internes (10hj à 40hj)
    - « Parser » XML : XML -> BdD Interne
    - Basées sur des outils tels que Domino, lotus notes…
    - Couplées avec des solutions de patch management, scanner de vulnérabilités
    - Solutions globales : outil d'Entelience (« Esis »)

Industrie Services Tertiaire



## Agenda

- Le workflow ?
- Quelles sont les diffusions du Cert-IST concernées
- Comment a-t-on adapté nos solutions ?
- Et après…
- Q & A - Retours d'expérience

Industrie Services Tertiaire

## Quels sont les diffusions du Cert-IST concernées

- L'évaluation du risque par le Cert-IST
- Visibilité pour les membres
- Quelles diffusions pour vos acteurs

Industrie Services Tertiaire



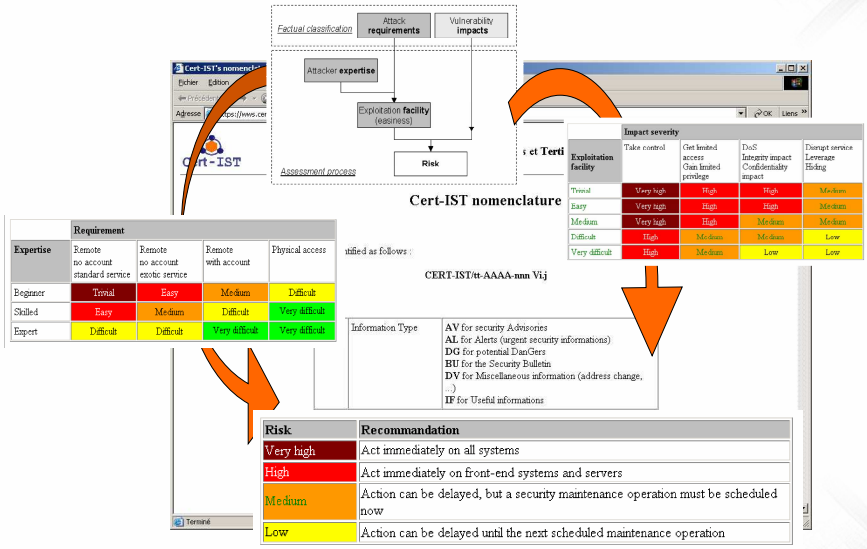
## Philosophie des informations Cert-IST

- Eléments
  - **Produit(s) impacté(s) et version(s)** : Cisco IOS 12.0
  - **Risque** :Très élevé, Elevé, Moyen, Faible, Non évalué
  - **Conséquence(s)** : Prise de contrôle, Accès non privilégié au système, Déni de service, …
  - **Moyen d'attaque** : A distance sans compte, avec un compte, …
  - **Solution(s)** : correctifs officiels, palliatifs
  - **Elément de détection, diagnostic**
  - **Lien(s) externe(s)** : CVE, CME, CVSS, Avis constructeurs, avis CERTs, …
  - **Type de problème** : Débordement de pile, Cross-Site Scripting, Traversée de répertoire, ..

Industrie Services Tertiaire

# Évaluation du niveau de risque

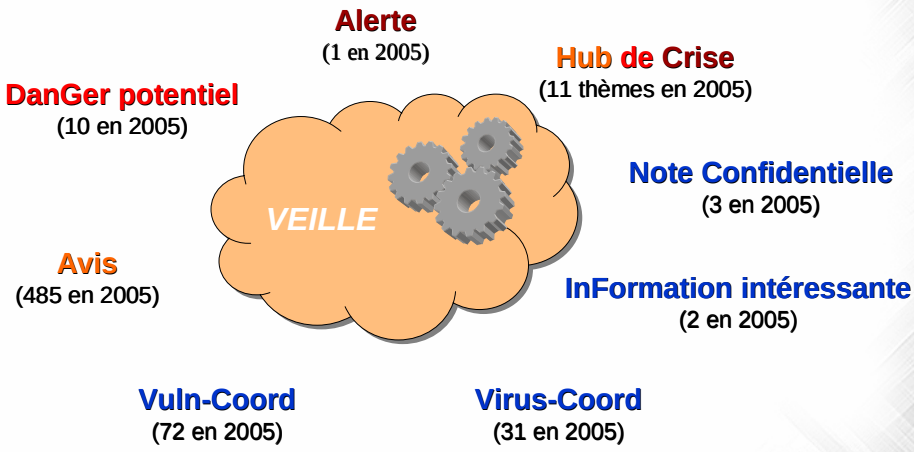
*La métrique EISPP*






# Les informations produites par le Cert-IST

## Visibilité des membres du Cert-IST



## Quelles diffusions pour vos acteurs

- Les diffusions par acteurs du SI
  - Décideurs : Alertes et tableaux de bords (internes)
  - RSSI : Alertes / Dangers / Hub de Crise / édito bulletin…
  - Administrateurs systèmes et réseau : Avis / Alertes / Dangers / Hub / xxx-coord
  - Utilisateurs : Alertes / notes internes
  - Externes : Alertes / notes internes
- Les formats par acteurs du SI
  - Décideurs : HTML
  - RSSI : HTML / TXT / XML / RSS
  - Administrateurs systèmes et réseau : XML / RSS / HTML / TXT
  - Utilisateurs : HTML / RSS
  - Externes : HTML / RSS

Industrie Services Tertiaire



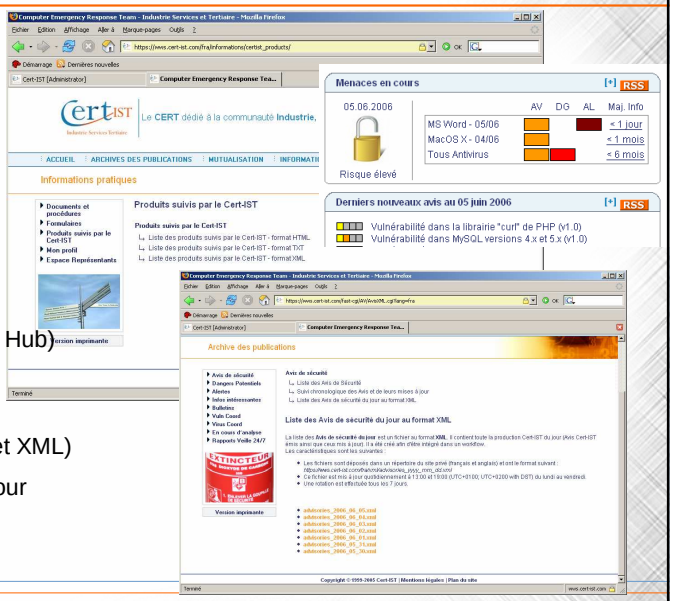
## Agenda

- Le workflow ?
- Quelles sont les diffusions du Cert-IST concernées
- Comment a-t-on adapté nos solutions ?
- Et après…
- Q & A - Retours d'expérience

Industrie Services Tertiaire

# Solutions - Historique

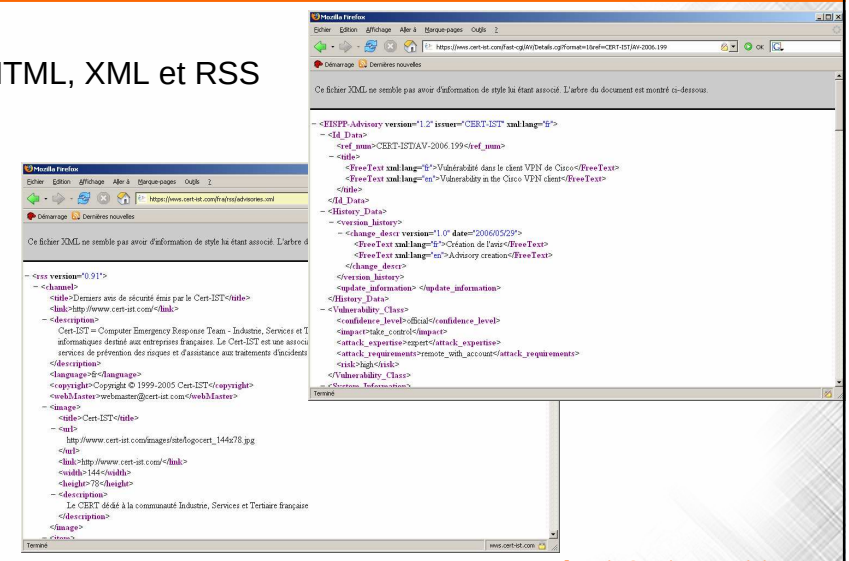
- 1999
  - « Profiling »
- 2003 : Push
  - EISPP et le XML
- 2005 : Pull
  - Flux RSS (Avis, News, Hub)
- 2006 : Pull
  - Produits (TXT, HTML et XML)
  - Fichier production du jour
  - Alertes et DG en XML






# Solutions - Les différents formats

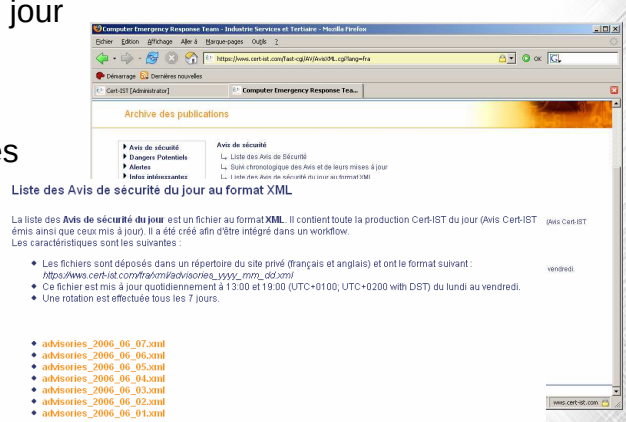
- TXT, HTML, XML et RSS
- LANG



Industrie Services Tertiaire

# Solution - La production du jour

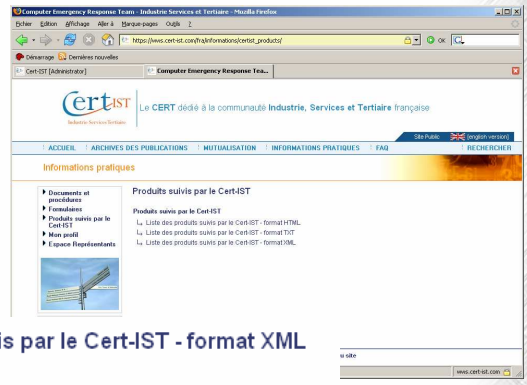
- Envoi des Avis et leurs mises à jour au fil de l'eau
- Fichier production du jour
  - Mis à jour quotidiennement
- Avis, Dangers, Alertes






# Solution - Les produits suivis (1/2)

- Liste des produits / versions
  - WEB : Format TXT, HTML, XML
  - Liste mise à jour quotidiennement
  - Mail personnalisé

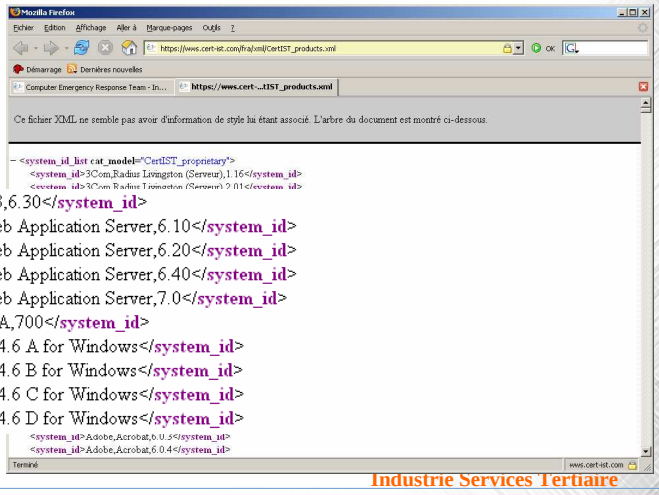



Liste des produits suivis par le Cert-IST - format XML

Télécharger la liste des produits suivis par le Cert-IST en cliquant ici

## Solution - Les produits suivis (2/2)

- Vendeur, Produit, Version



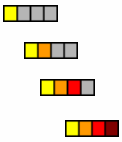
```
<system_id>SAP,SAP R/3,6.30</system_id>
<system_id>SAP,SAP Web Application Server,6.10</system_id>
<system_id>SAP,SAP Web Application Server,6.20</system_id>
<system_id>SAP,SAP Web Application Server,6.40</system_id>
<system_id>SAP,SAP Web Application Server,7.0</system_id>
<system_id>SAP,SAPDBA,700</system_id>
<system_id>SAP,SAPgui,4.6 A for Windows</system_id>
<system_id>SAP,SAPgui,4.6 B for Windows</system_id>
<system_id>SAP,SAPgui,4.6 C for Windows</system_id>
<system_id>SAP,SAPgui,4.6 D for Windows</system_id>
```

Industrie Services Tertiaire



## Solutions - Autres informations à prendre en compte (1/2)

- Risque



```
- <Vulnerability_Class>
    <confidence_level>official</confidence_level>
    <impact>gain_privilege</impact>
    <impact>take_control</impact>
    <impact>confidentiality</impact>
    <attack_expertise>skilled</attack_expertise>
    <attack_requirements>remote_no_account_exotic_service</attack_requirements>
    <risk>very-high</risk>
  </Vulnerability_Class>
```

- Références

```
<ref_num>CERT-IST/AV-2006.155</ref_num>
```

- Versions

```
- <change_descr version="1.12" date="2006/04/24">
  - <FreeText xml:lang="fr">
      Avis de sécurité de SCO UnixWare SCOSA-2006.22 (solution 10)
    </FreeText>
  - <FreeText xml:lang="en">
      SCO UnixWare security advisory SCOSA-2006.22 (solution 10)
```

Industrie Services Tertiaire

## Solutions - Autres informations à prendre en compte (2/2)

- CVE / CME
- Score CVSS
- Références Externes
- Solutions

```
− <Vulnerability_ID>
  − <reference ref_type="vuln_id" issuer="CVE" ref_num="CVE-2006-2753">
    − <uri xml:lang="fr">
        http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2753
      </uri>
```

```
− <li>
    CVE-2006-2753 - Base score : 7.0 (AV:R/AC:L/Au:NR/C:P/I:P/A:P/B:N) - Source : NVD
```

```
− <Additional_Resources>
  − <reference ref_type="vendor_advisory" issuer="MySQL" ref_num="MySQL_4.1.20">
    − <ref_title>
      − <FreeText xml:lang="fr">
          Annonce de MySQL concernant MySQL 4.1.20 du 31 mai 2006
```

```
− <Solution>
  − <sol_section sol_type="software_upgrade">
    − <sol_title>
        <FreeText xml:lang="fr">01 - Mettre à jour MySQL</FreeText>
        <FreeText xml:lang="en">01 - Update MySQL</FreeText>
```

Industrie Services Tertiaire



## Agenda

- Le workflow ?
- Quelles sont les diffusions du Cert-IST concernées
- Comment a-t-on adapté nos solutions ?
- Et après…
- Q & A - Retours d'expérience

Industrie Services Tertiaire

## Et après …

**Standards communs : CVE CME CVSS - Formats - Produits**

**Le positionnement des outils va évoluer**
- **IDS signalement & neutralisation**
- **Patch management**
- **FW Antivirus**
- **Desktop**
- **Services**

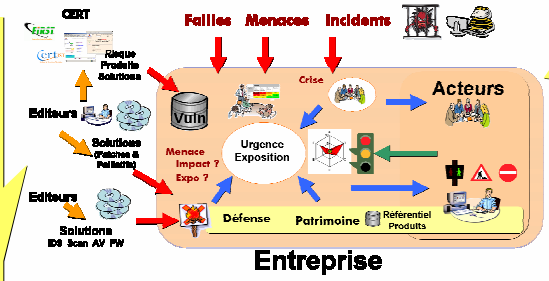



**Tableau de bord de l'exposition et de la couverture des risques de mon patrimoine**

**Modélisation impact et faiblesse sur mon infrastructure SIC**

Industrie Services Tertiaire



## Q & A - Retours d'expérience ?

Fin de la présentation

Industrie Services Tertiaire