INTRANODE
YOUR E-SECURITY PARTNER

ActiveSentry™ : le monitoring permanent de la sécurité des architectures Internet

OSSIR – 11/09/2001

Fabrice Frade – Directeur Technique

Qui est Intranode?

- Intranode est un éditeur d'une solution logicielle novatrice destinée à répondre à l'équation suivante :

Processus métier automatisés

+ Réseaux ouverts

+ Disponibilité

= Sécurité proactive + Gestion du risque en temps réel

- Métiers
  - Expertise des vulnérabilités en environnement Internet
  - Éditeur de logiciel

- La solution Intranode
  - ActiveSentry™: Surveillance du niveau de risque Internet

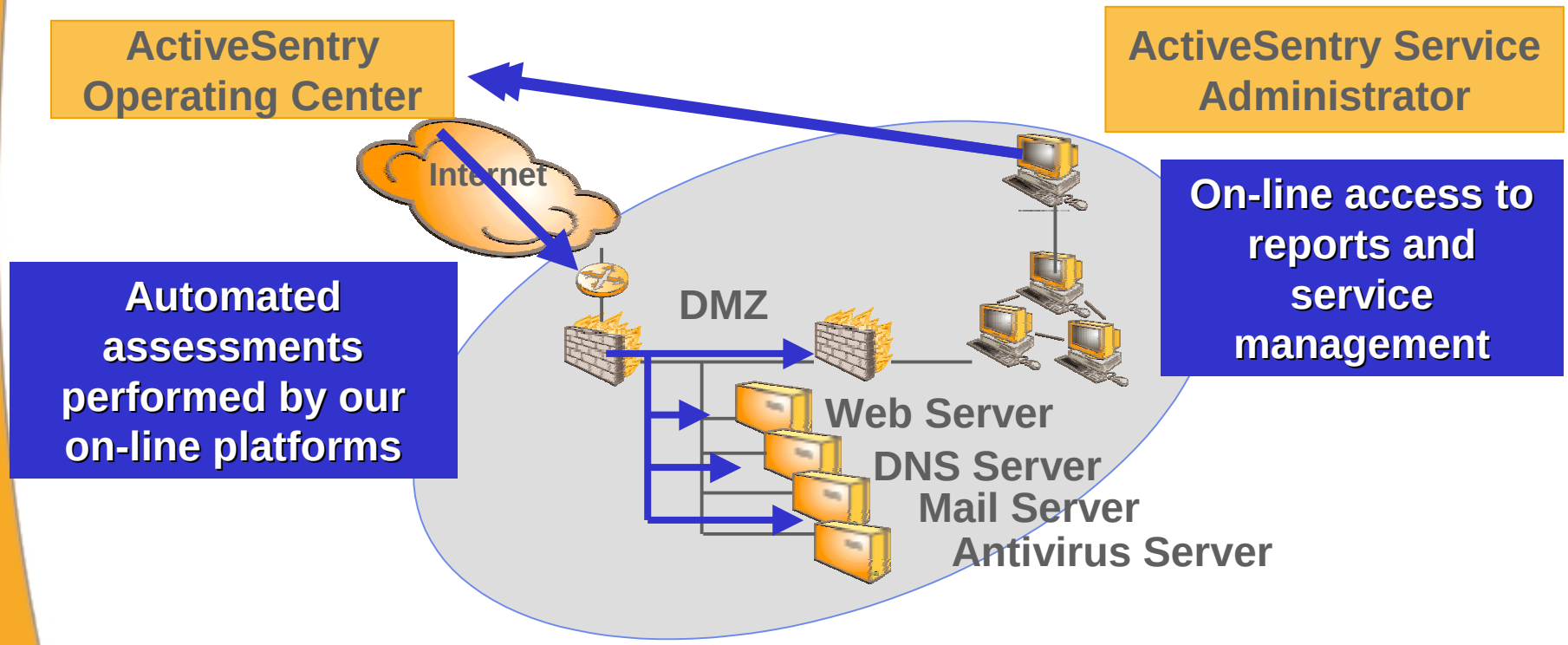
Présentation d'ActiveSentry™

- ActiveSentry™ est une solution logicielle :
  - Disponible via une interface Web sur Internet
  - Permet le lancement de tests de vulnérabilités automatiques, de façon récurrente ou à la demande
  - Fournit 2 rapports :
    - l'un technique avec les vulnérabilités détectées et les parades
    - L'autre décisionnel avec l'évolution du niveau de risque
  - Apporte la notion d'Internet Risk Factor (IRF™)
  - Licenciée sous la forme d'un abonnement annuel

L'audit récurrent en ligne pour le monitoring permanent de la sécurité

- Besoins clients
  - Avoir une visibilité sur le niveau de sécurité
  - Reproductibilité
  - Agir avant qu'il ne soit trop tard (pro-activité)
  - Disposer du savoir-faire de spécialistes à tout instant
- Démarche Intranode
  - Une approche objective s'inscrivant dans la durée
  - Automatisation / Disponibilité 24x7
  - Des outils pour l'action et l'aide à la décision
  - Mise à jour permanente et modélisation des risques

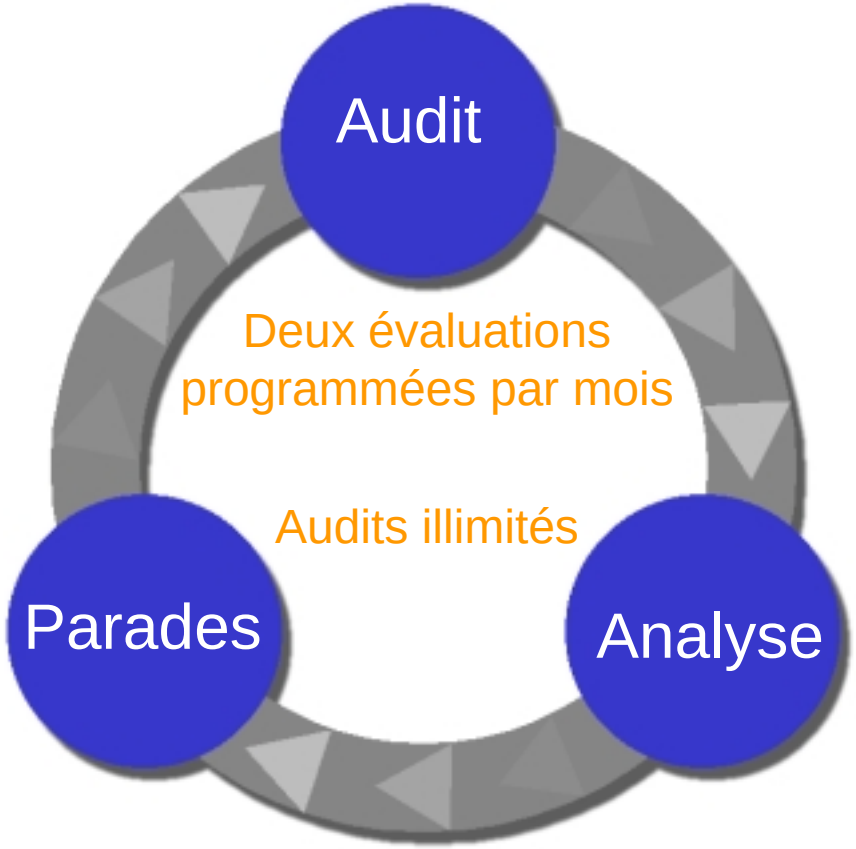
Une approche dynamique…



…pour un processus d'amélioration continu

Découverte réseau

Recensement des vulnérabilités



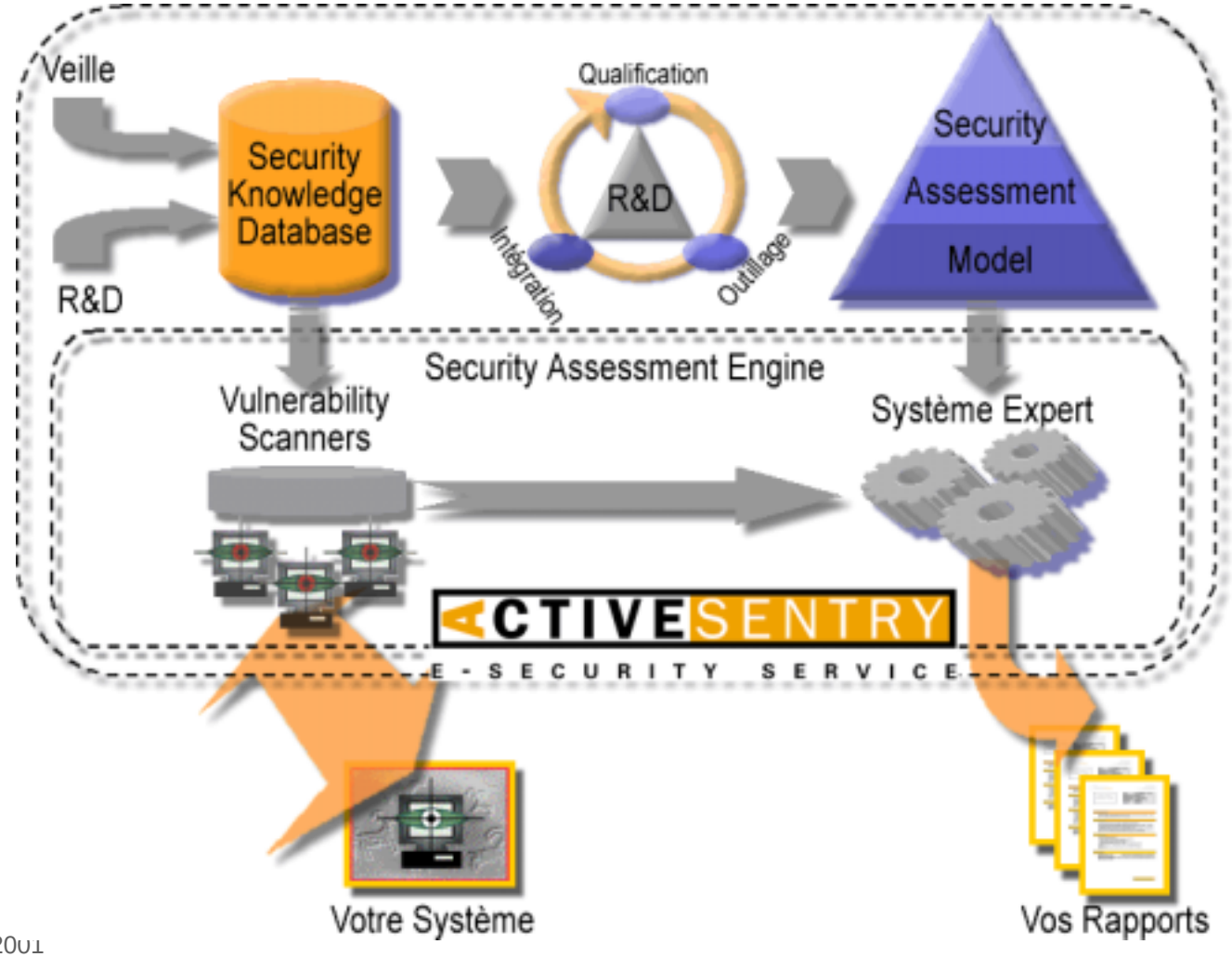
Qualification des impacts

Plan d'action opérationnel

Qualification du niveau de risque

Tableaux de bord

Couverture fonctionnelle et réactivité



Une mise à jour permanente

- Recherche des nouvelles vulnérabilités : veille sécurité journalière.
- Validation des vulnérabilités : confrontation de plusieurs sources d'informations.
- Développement et qualification (fiabilité, reproductibilité…) des vulnérabilités et des outils de détection associés.
- Analyse et intégration des vulnérabilités dans le Security Assessment Model et dans la Security Knowledge Database.
- Documentation des vulnérabilités et de l'ensemble des paramètres associés (exploits, parades).
- Mise à jour de la plate-forme de service avec les composants permettant la détection des nouvelles vulnérabilités.

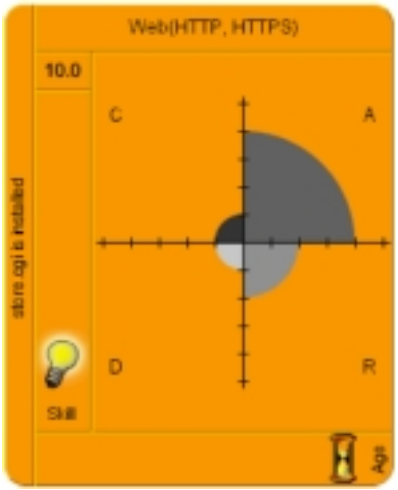
Audit intégrant les tests des nouvelles vulnérabilités

Une efficacité inégalée

- Intégration, homogénéisation et automatisation de plusieurs outils spécialisés et maîtrisés par Intranode
  - Composants propriétaires Intranode
  - Composants Open Source
- Tests non intrusifs adaptés à une évaluation distante automatisée
  - Adaptation et corrélation des tests pour limiter les « false positive »
  - Pas de tests pouvant générer un DoS
- Couverture fonctionnelle très large
  - Composants réseau (Switchs, routeurs, Firewalls…)
  - Composants systèmes (OS, services…)
  - Composants applicatifs (Mail, Web, Serveurs d'Application, Scripts…)

La modélisation de notre savoir-faire pour la qualification du niveau de sécurité

- Intranode introduit la quantification des impacts grâce à son modèle CARD
  - **C** : Corrupt Data / Modification des données
  - **A** : Access Information / Accès aux données
  - **R** : Remote Execution / Exécution illicites de programmes
  - **D** : Deny Service / Disponibilité du service
  - De nombreux paramètres enrichissent le modèle (expertise requise des attaquants potentiels, popularité et âge des vulnérabilités)



- Intranode introduit le concept IRF™ - Internet Risk Factor
  - Permet la mesure du risque Internet
  - Analyse statique : par vulnérabilité, par serveur, ou pour toute une plate-forme
  - Analyse dynamique : évolution dans le temps au cours des audits successifs

Cartographie d'une faille

Impact confidentialité

3 - *des informations supposées inaccessibles sont en fait facilement accessibles*

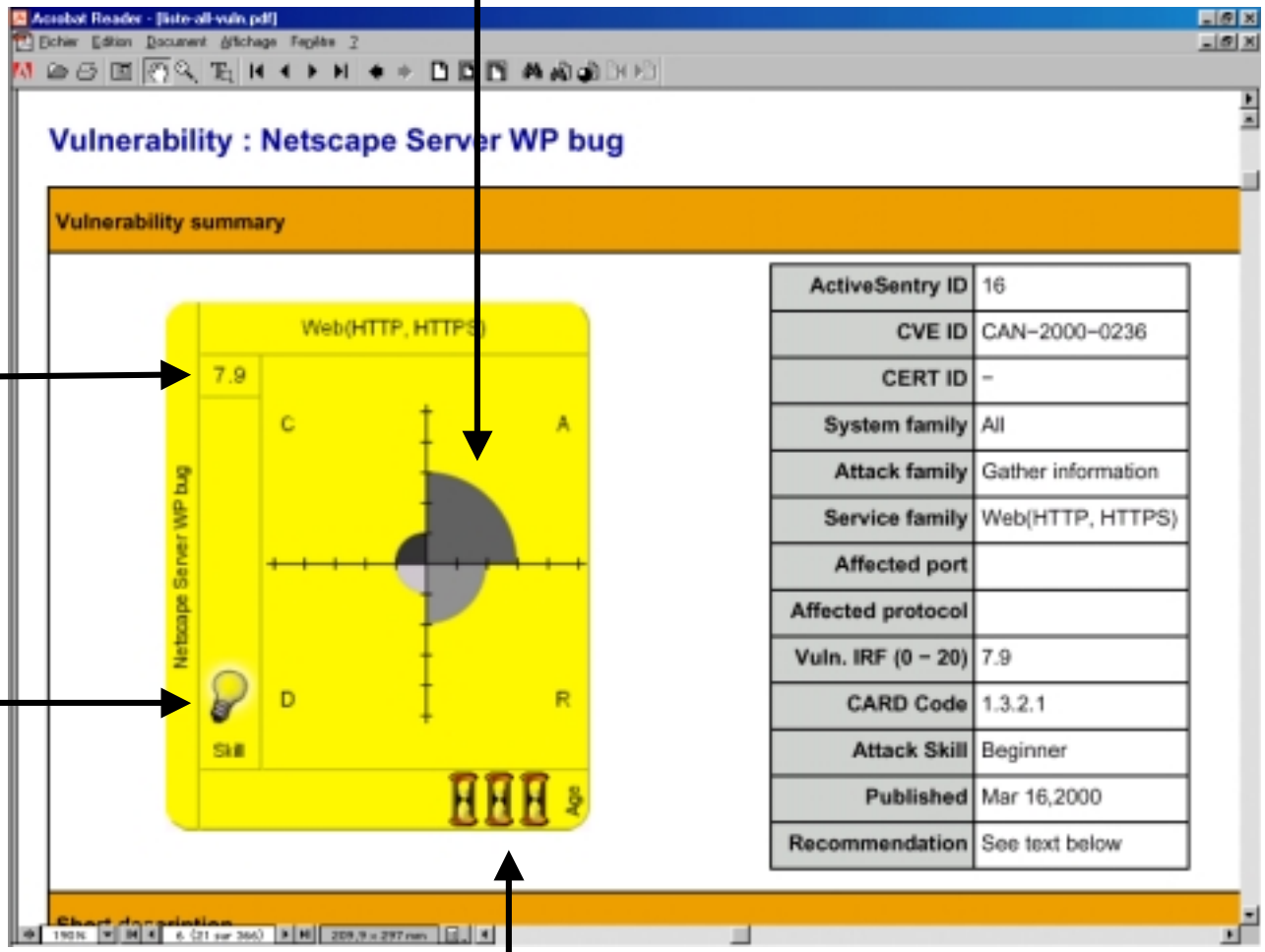
IRF™

7.9 (sur 20)

risque acceptable pour un système non critique

Niveau d'expertise

1 *- débutant*



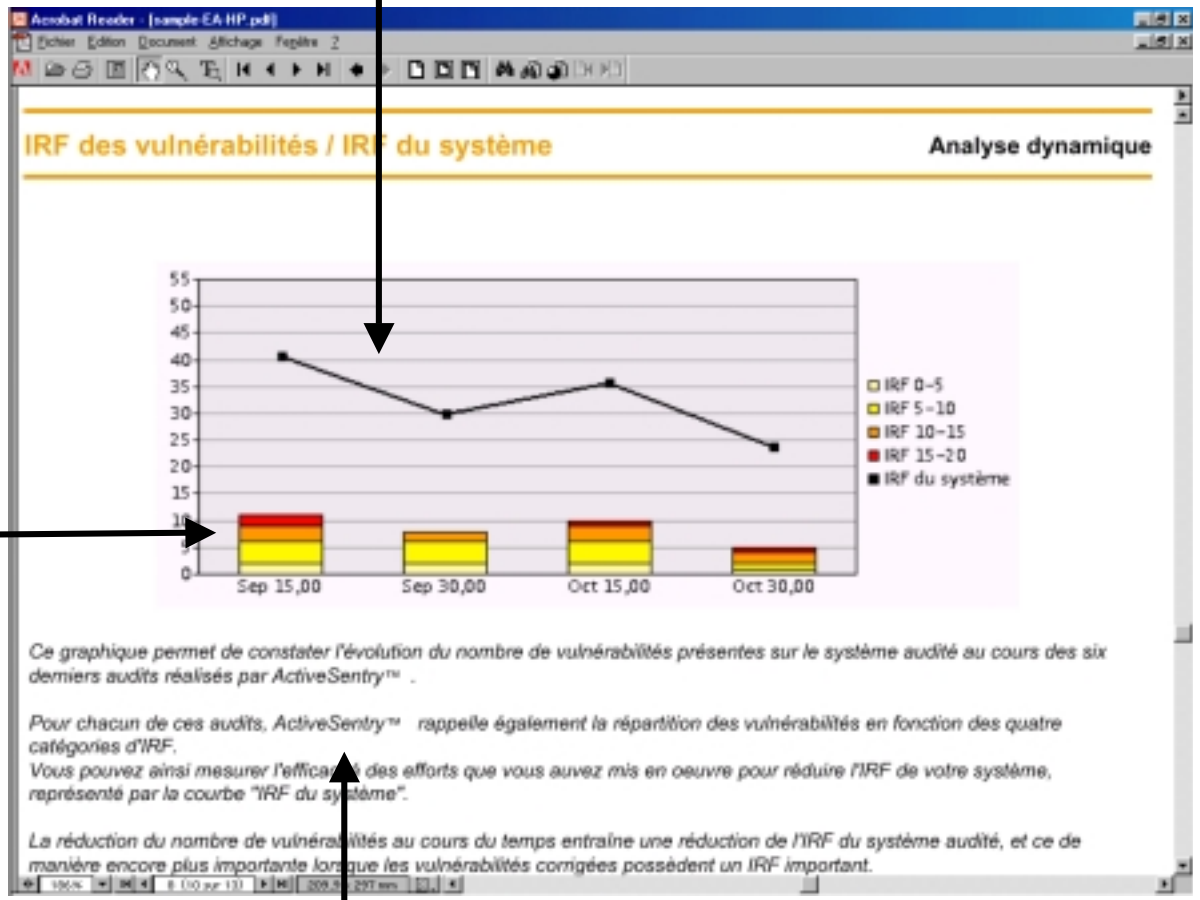
Age de la vulnérabilité

9 mois

Mesure du risque

Évolution du niveau de risque (IRF™) dans le temps

Évolution du nombre de vulnérabilités réparties par niveau d'IRF™

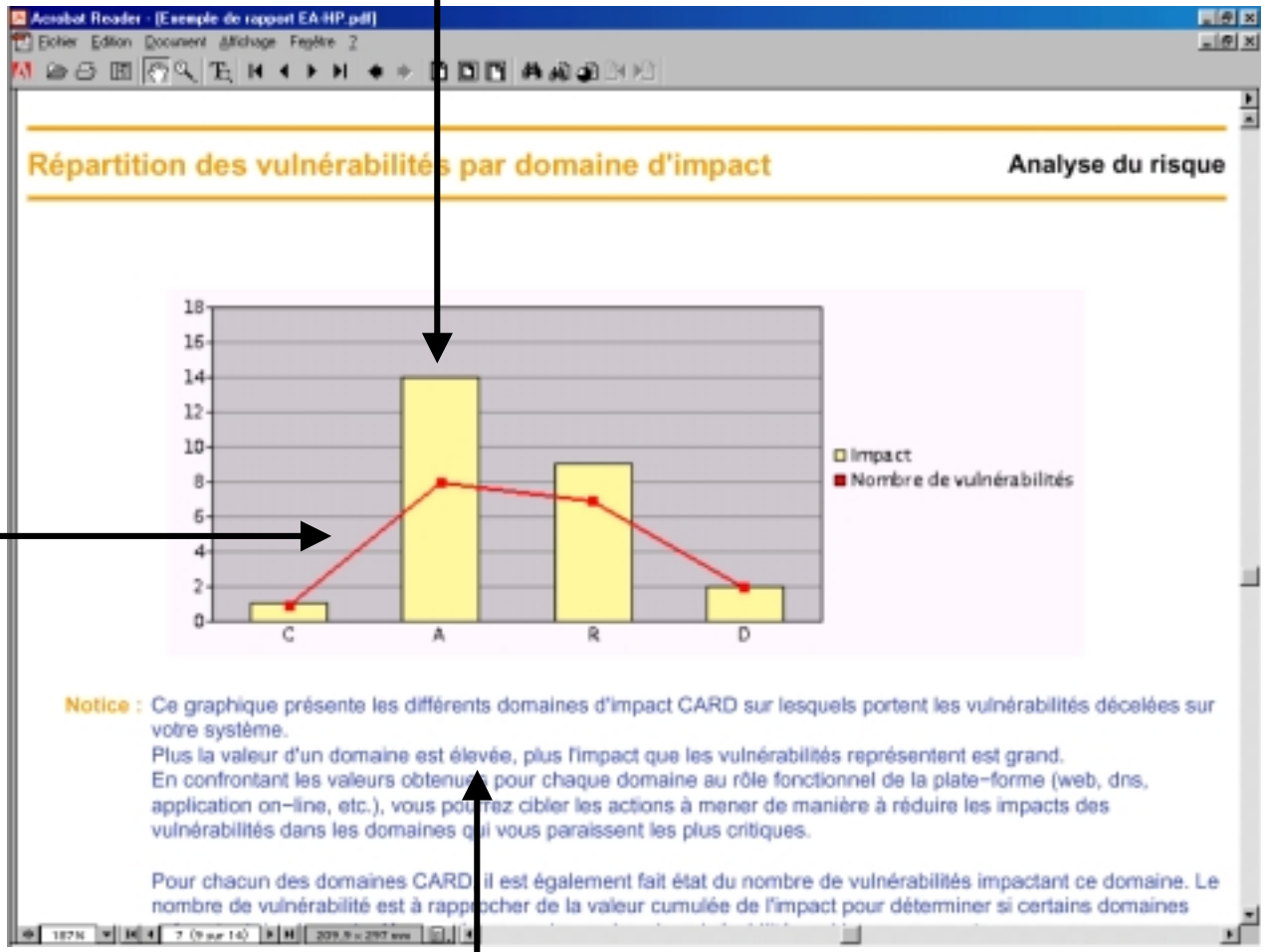


Guide de lecture du graphique

Profil des risques

Impact global des vulnérabilités sur le critère de confidentialité

Nombre de vulnérabilités pour chaque domaine d'impact



Guide de lecture du graphique

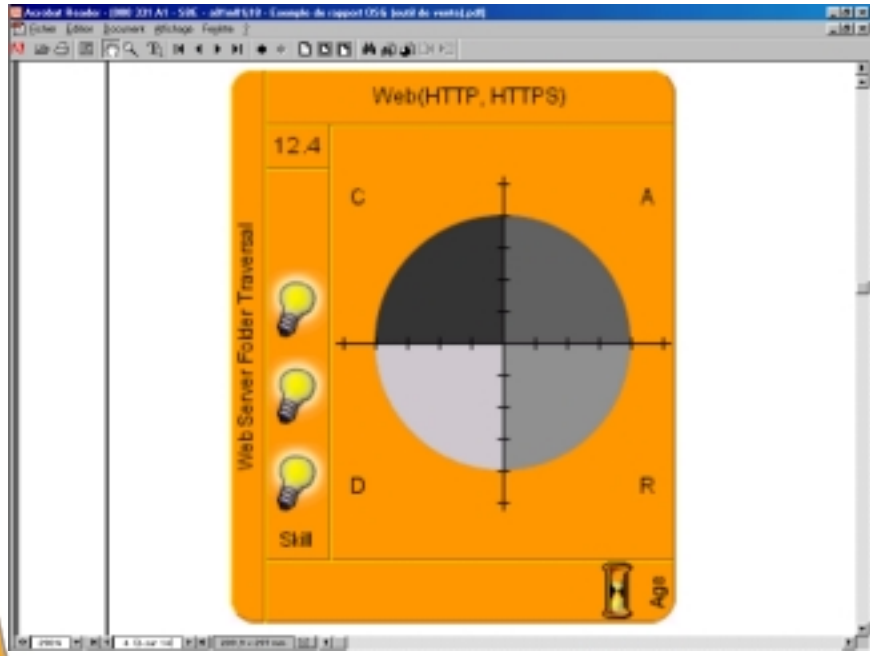
Pourquoi la mesure des risques

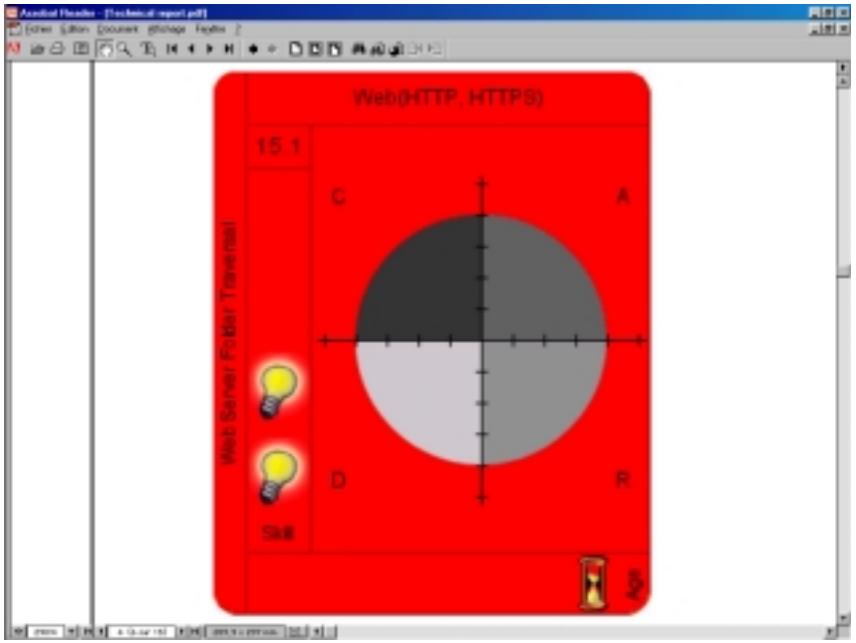
- Intégrer la sécurité logique dans une démarche de « risk management » :
  - Il existe toujours un risque résiduel qu'il faut connaître pour savoir comment le traiter :
    - le diminuer en agissant dessus (investissement),
    - l'accepter (et éventuellement l'assurer)
  - Dans une démarche qualité, il faut pouvoir comparer les niveaux de sécurité de différentes architectures au sein d'une même entreprise

- Disposer d'un outil de pilotage continu de la sécurité
  - Visualisation immédiate en cas d'évolution de l'environnement :
    - nouveau serveur ou nouvelle configuration,
    - nouvelle faille ou évolution d'une faille ancienne
  - Priorisation des actions à mener en fonction de leur impact,
  - Reporting auprès de la Direction Générale ou des MOA.

Un exemple de dynamisme: la faille Unicode

- Découverte en Octobre avec un niveau d'expertise requis élevé -> IRF = 12,4
- Mise à jour en Décembre suite a l'apparition d'un « exploit » automatique -> IRF = 15,1





INTRANODE
YOUR E-SECURITY PARTNER

Questions - Réponses

Fabrice.Frade@intranode.com