Sécuriser l'informatique :

Est-ce encore suffisant ?

Paris

8 Juillet 2008

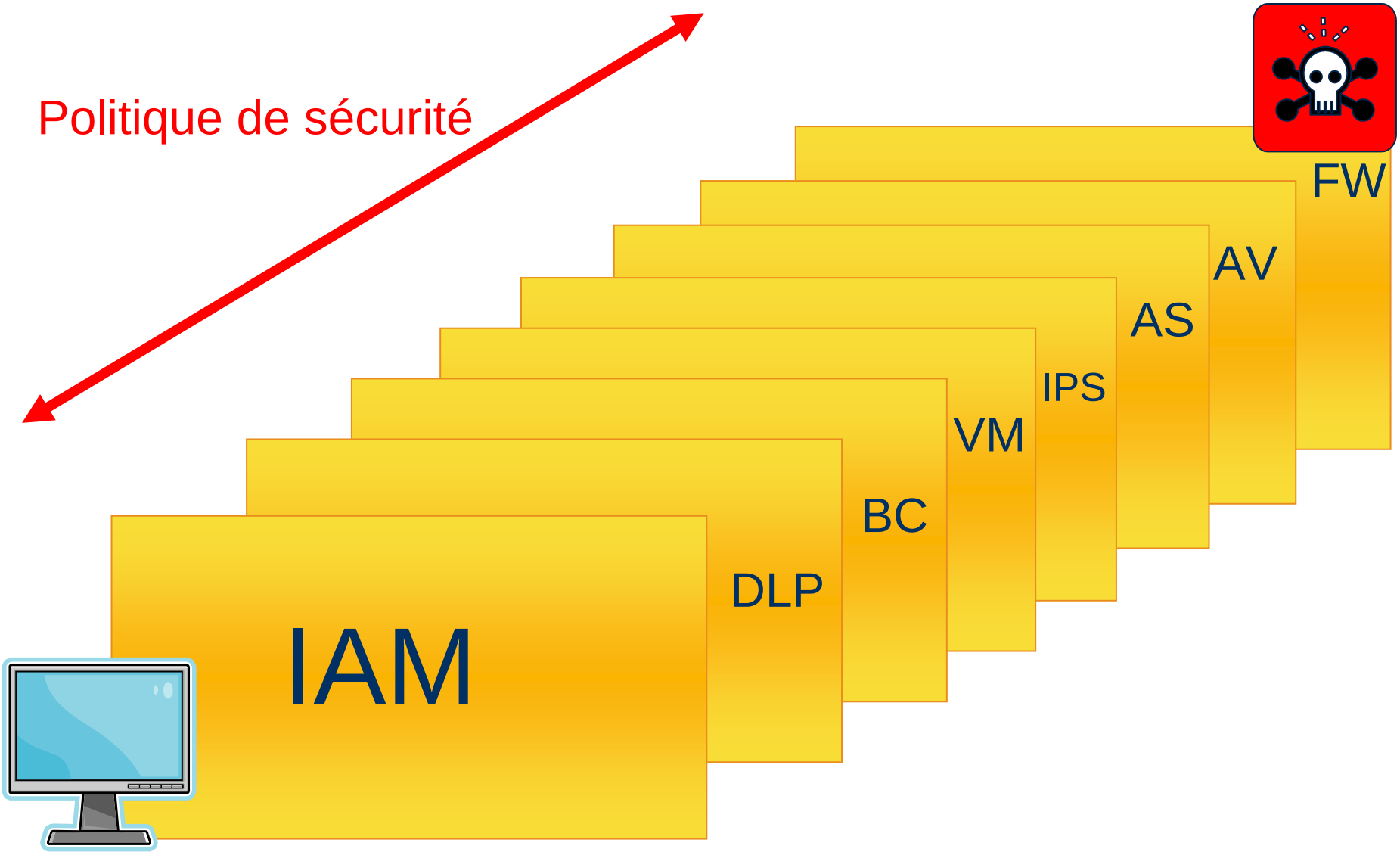
IBM Tendances Logicielles d'été 2008

L’informatique de confiance existe…

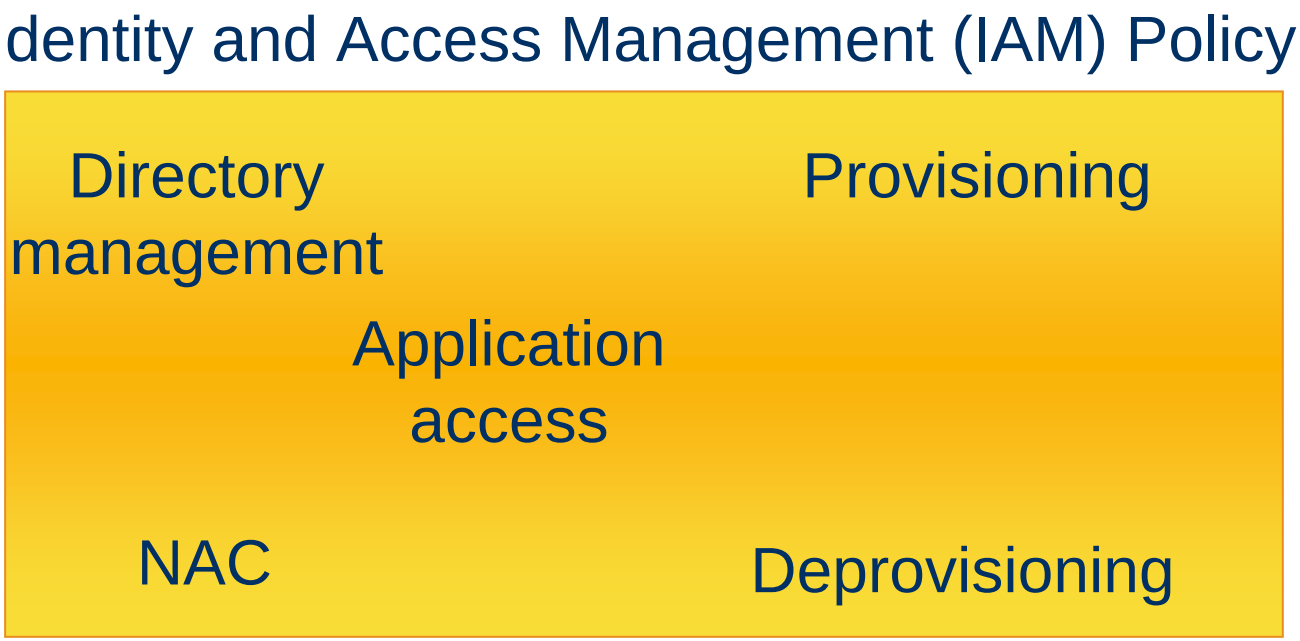
…il suffisait de le dire !

Le discours

Les Politiques de sécurité des SI : une série d'écrans étanches



Un exemple d'écran robuste : IAM



«Tout est sous contrôle, nous avons une politique pour celà »

La Réalité

Les points d'exposition au risque se multiplient , (souvent sans contrôle)

Virtualisation

OSs

Communication

Applications Internes

Portables

PDAs, Clés USB

Mobiles

Applications Webisées

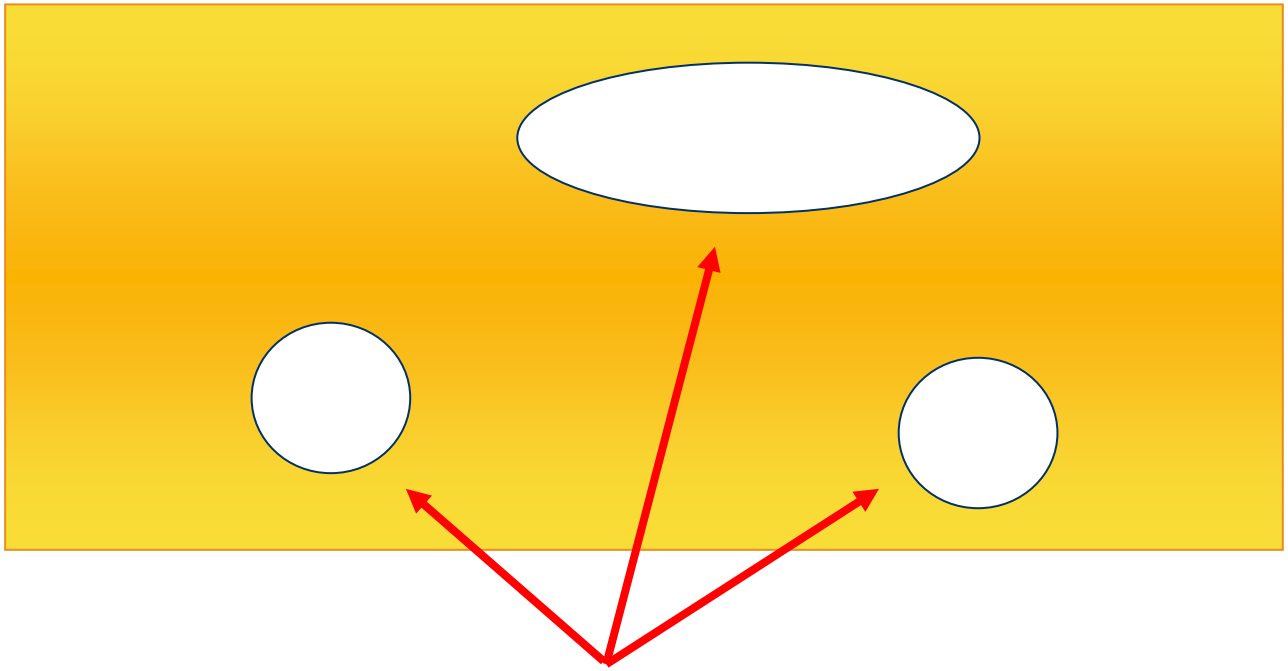
Web 2.0

VoIP

IM

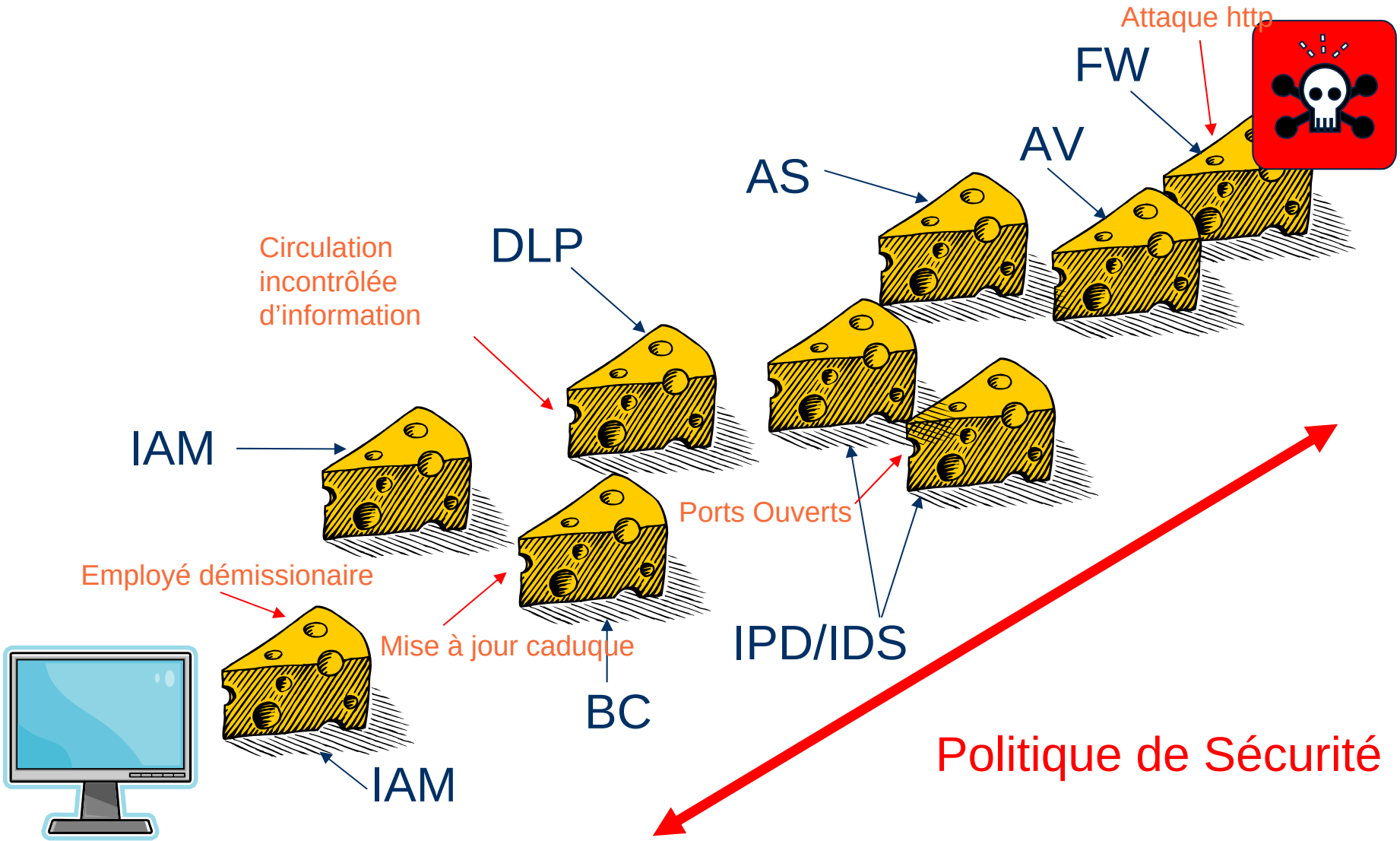
eMail

Les écrans réputés robustes sont friables….

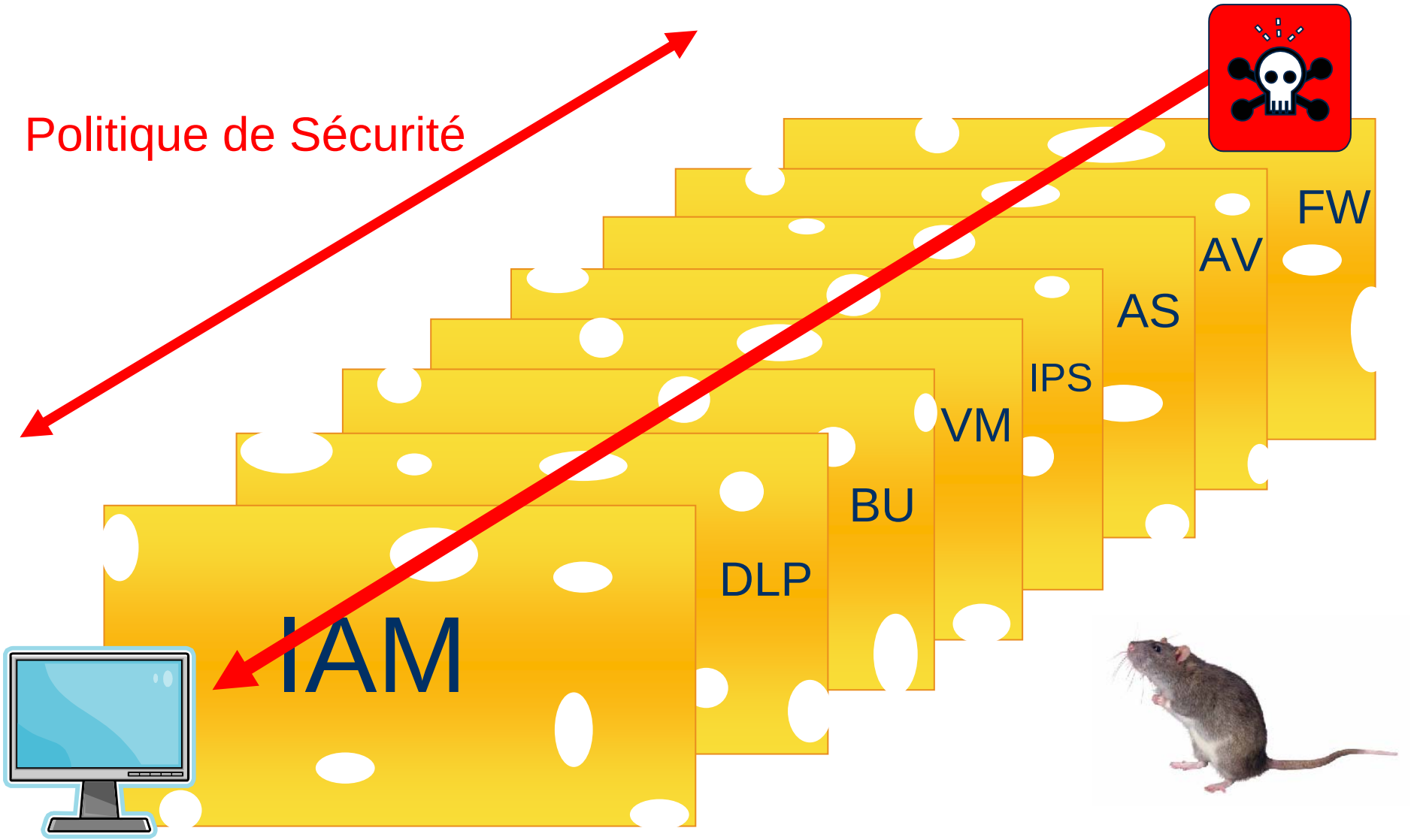


Loi de Murphy: « tout technologie faillible faillira »

La Politique de Sécurité, un gruyère ?



L’alignement des failles conduit au désastre



Trois grandes démonstrations en 2007

25 millions d'identités fiscales perdues

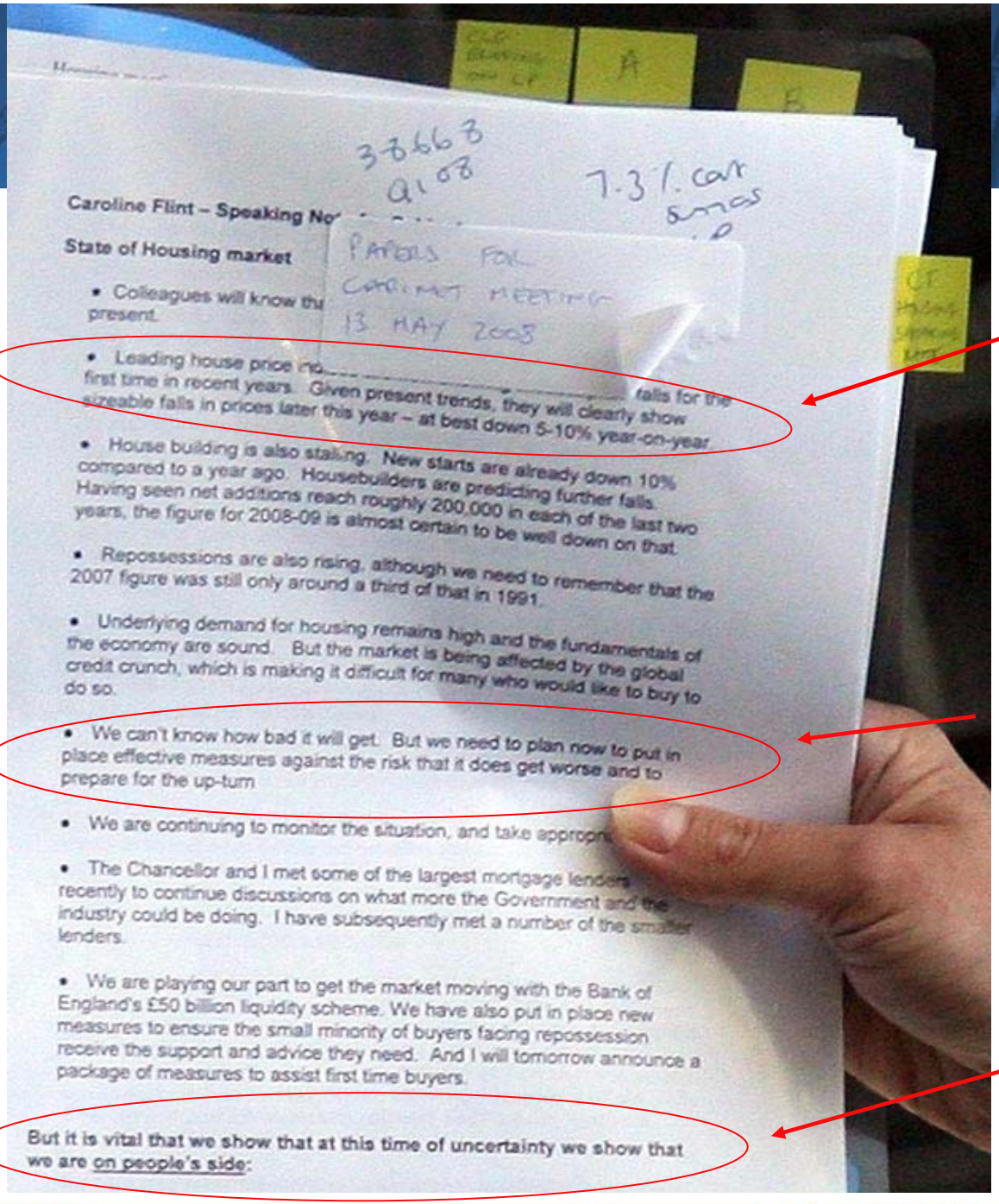
£980,000 ($2 millions) d'amende pour la perte de 11 millions de profils bancaires

Jerome Kerviel (SocGen), pour l'ensemble de son œuvre !

Attention, les candidats sont nombreux en 2008…..

- Carole Flint, Ministre UK du Logement, 13 Mai 2008, devant 10 Downing Street

Gordon Brown (10/05/08) au sujet de la crise du logement en UK : « *Pas de pessimisme exagéré. Nous ne donnerons pas de statistiques…* ».



« Les prix (du logement) ont baissé pour la première fois depuis 5 ans…on peut s'attendre à une recession de 5 à 10 % sur 12 mois glissants »

« Nous ignorons à quel point la situation va se dégrader. Il va falloir se préparer au pire et soutenir la relance… »

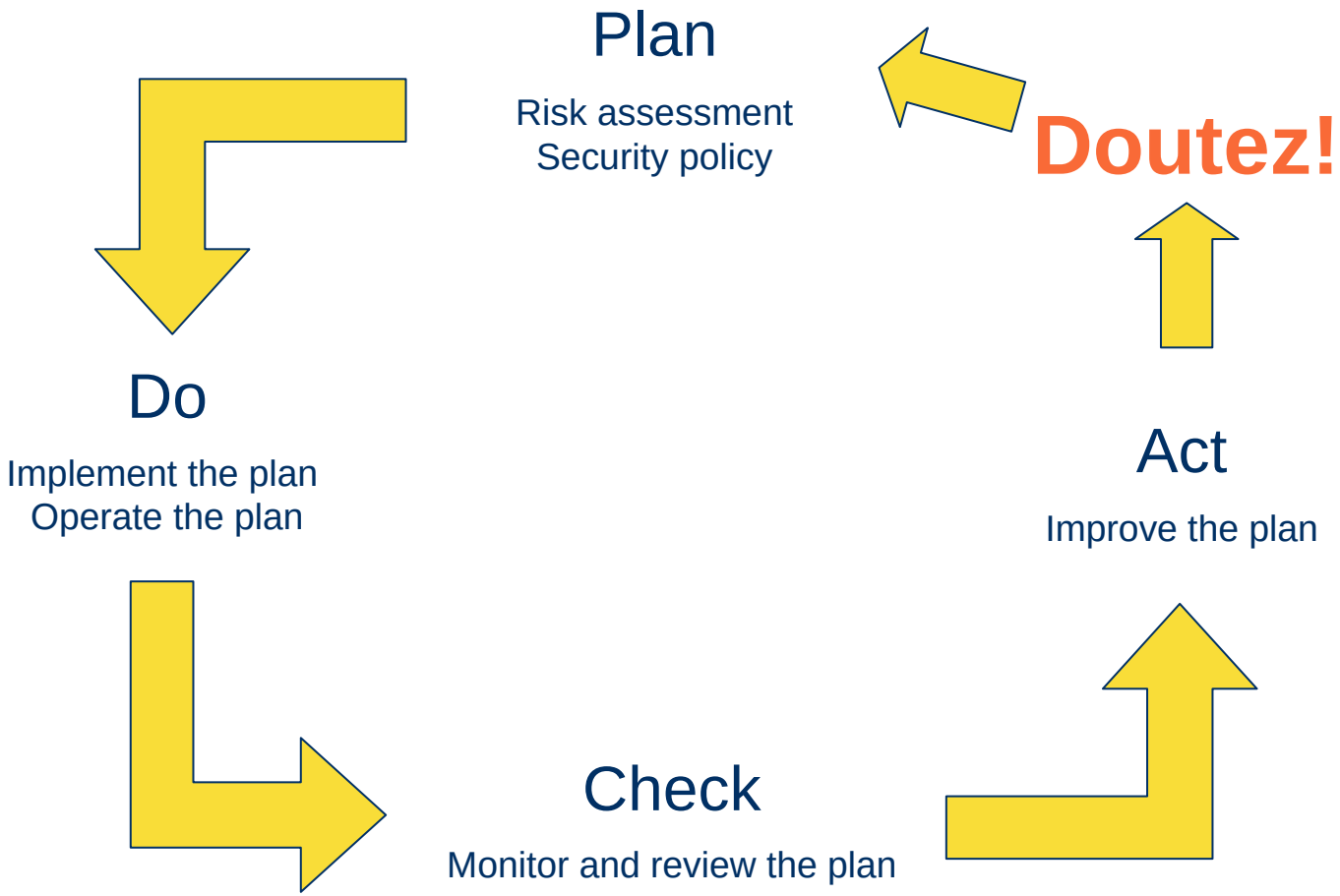
« En ces temps incertains, il est vital de montrer que nous sommes du côté des gens… »

Depuis mai 2008…

-Note « Top Secret » sur les forces et faiblesses des troupes d'Al-Quaida et UK en Afghanistan oubliée dans le train…puis transmises à la BBC (10 Juin 2008)

-Manuscrits prises de notes reunions MI5 (14 Juin 08) oubliés dans le même train

Sécurité, le process permanent (Roue de Deming) (PDCA)



La sécurité, ce n'est pas le fait d'être en avance d'une réponse mais en avance d'une question

En 2007, nous avons appris:

- l'utilisateur est au cœur des crises IT (Déclencheur ou Amplificateur): le comportement de l'utilisateur n'est pas un (encore) un « sujet » informatique

- La sécurité est un process permanent, pas une technologie : il ne faut pas se reposer sur la révolution technologique (toujours promise, toujours frustrante) en ce domaine

- les régulateurs des années 80 – 90 (CNIL, AMF..) sont devenus adultes et autonomes…il peuvent se mêler de tout !

- Les conséquences des crises sont exponentielles (et non liénaires) : 1+1 = 3

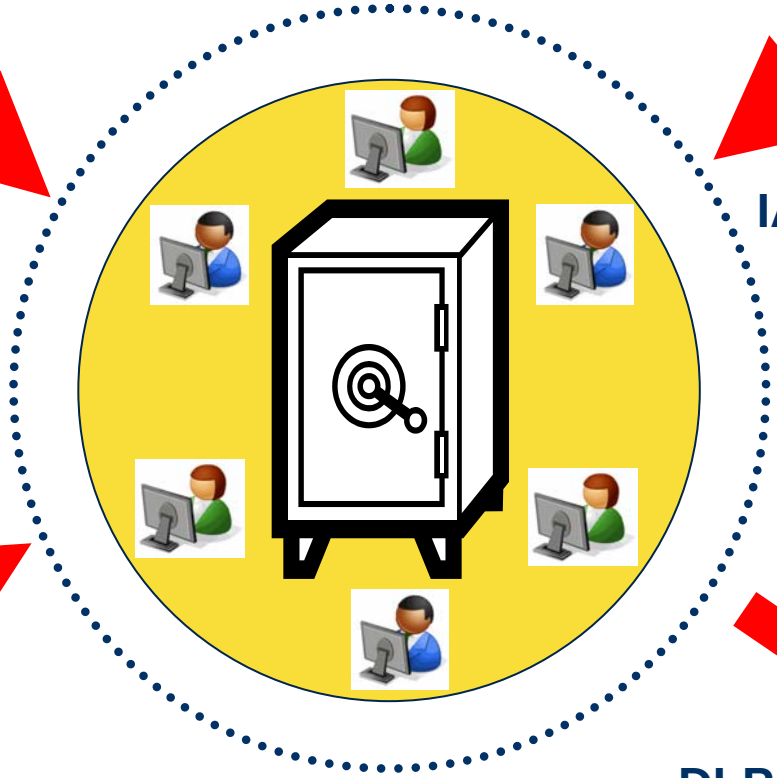
Etat des lieux France

Les projets Sécurité, outils économiques

Traitement de la menace 2007-2008

Menace Externe
Virus, Spam, Attaques ciblées

Menace Interne
Pirateries, erreurs



AV, AS, IDS, IPS….
- - -

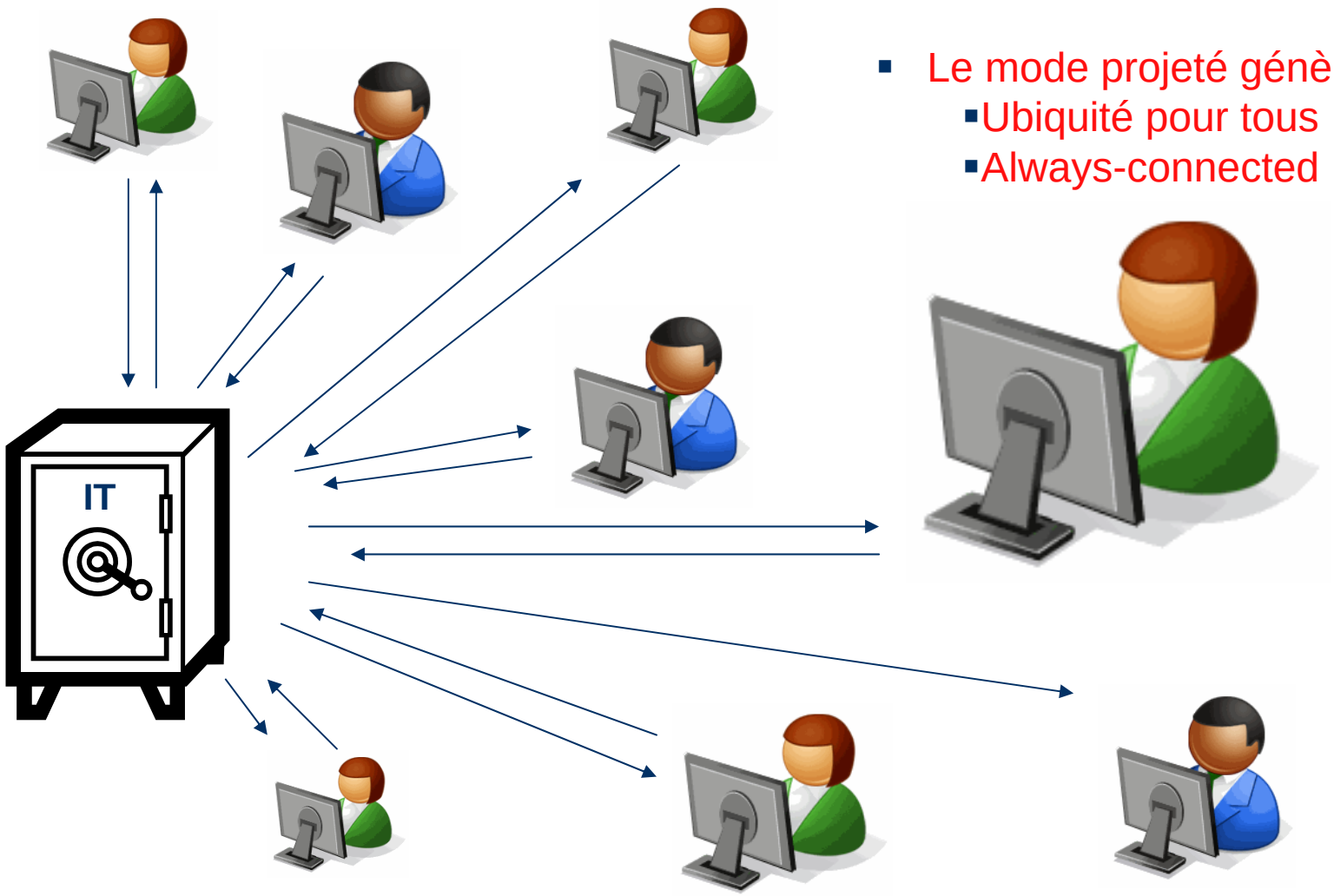
IAM, Authentification forte
+ +

Menace Réglementaire
LSF, LCEN, CNIL 2…
+ + +

Contrôle de l'information
Clés USb, Hotmail…

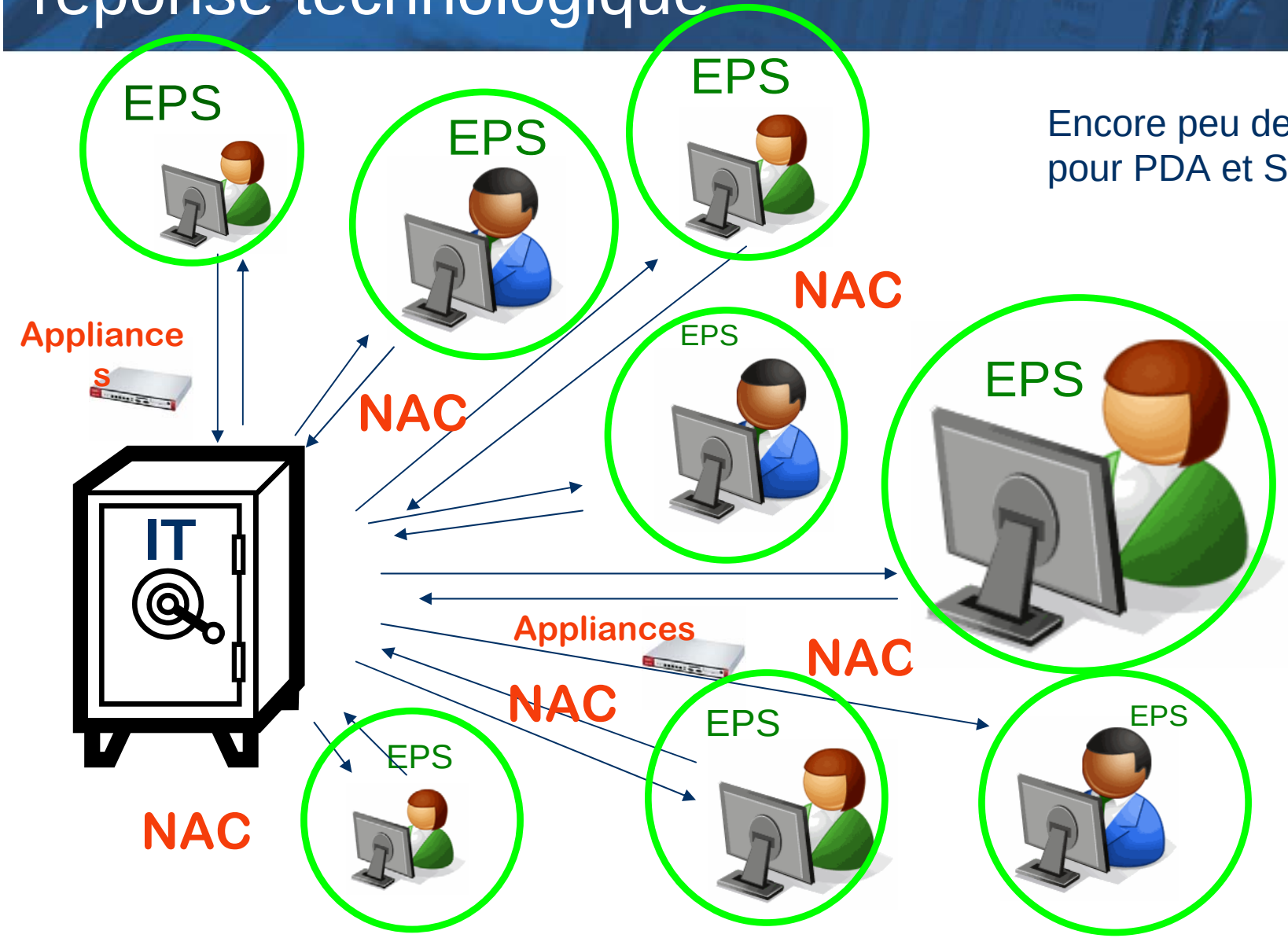
DLP ????

Traitement du péril : la mobilité- ubiquité



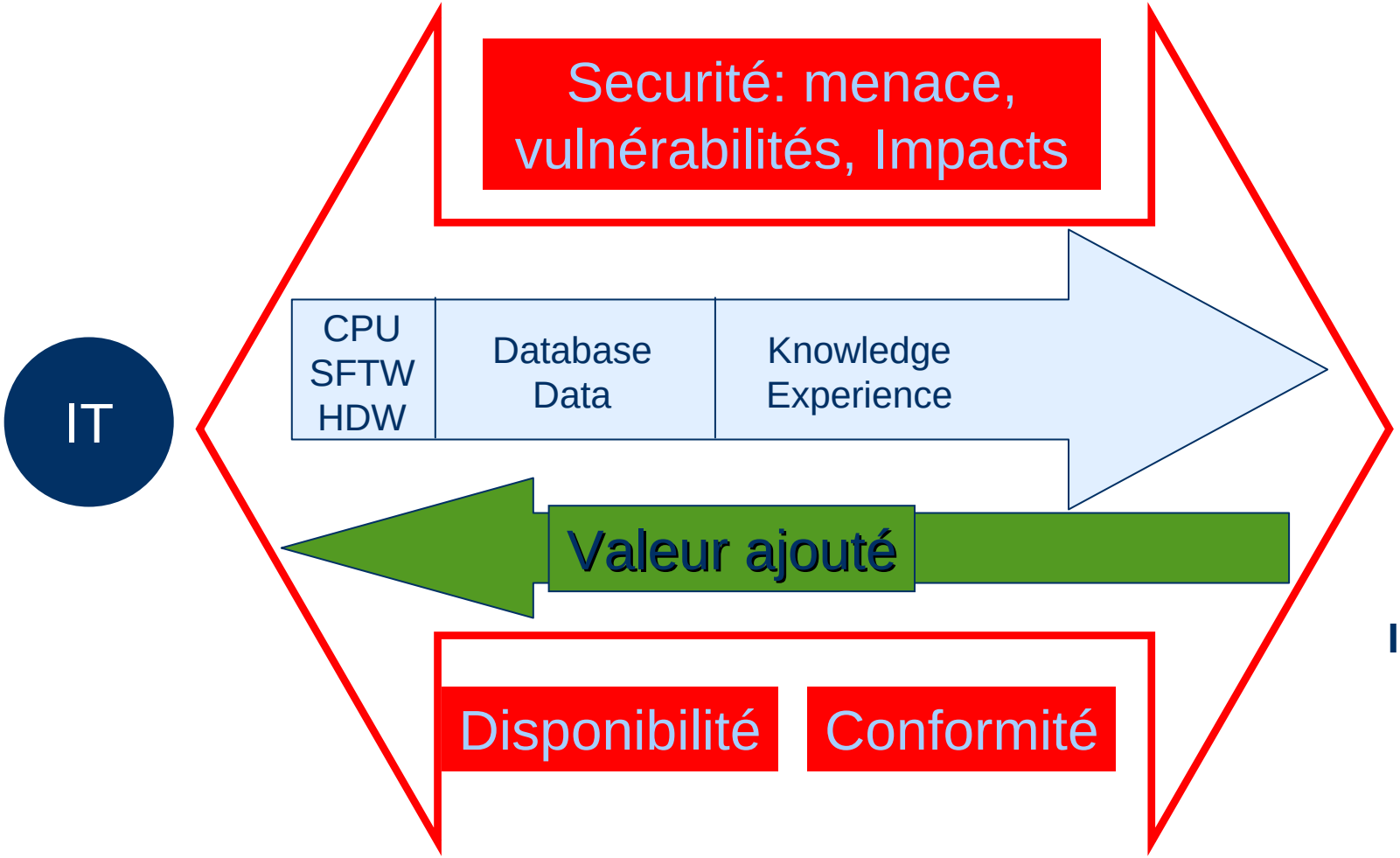
- Le mode projeté génère
  - Ubiquité pour tous
  - Always-connected

Traitement du péril en mode projeté, la réponse technologique



Encore peu de réponses pour PDA et Smartphones

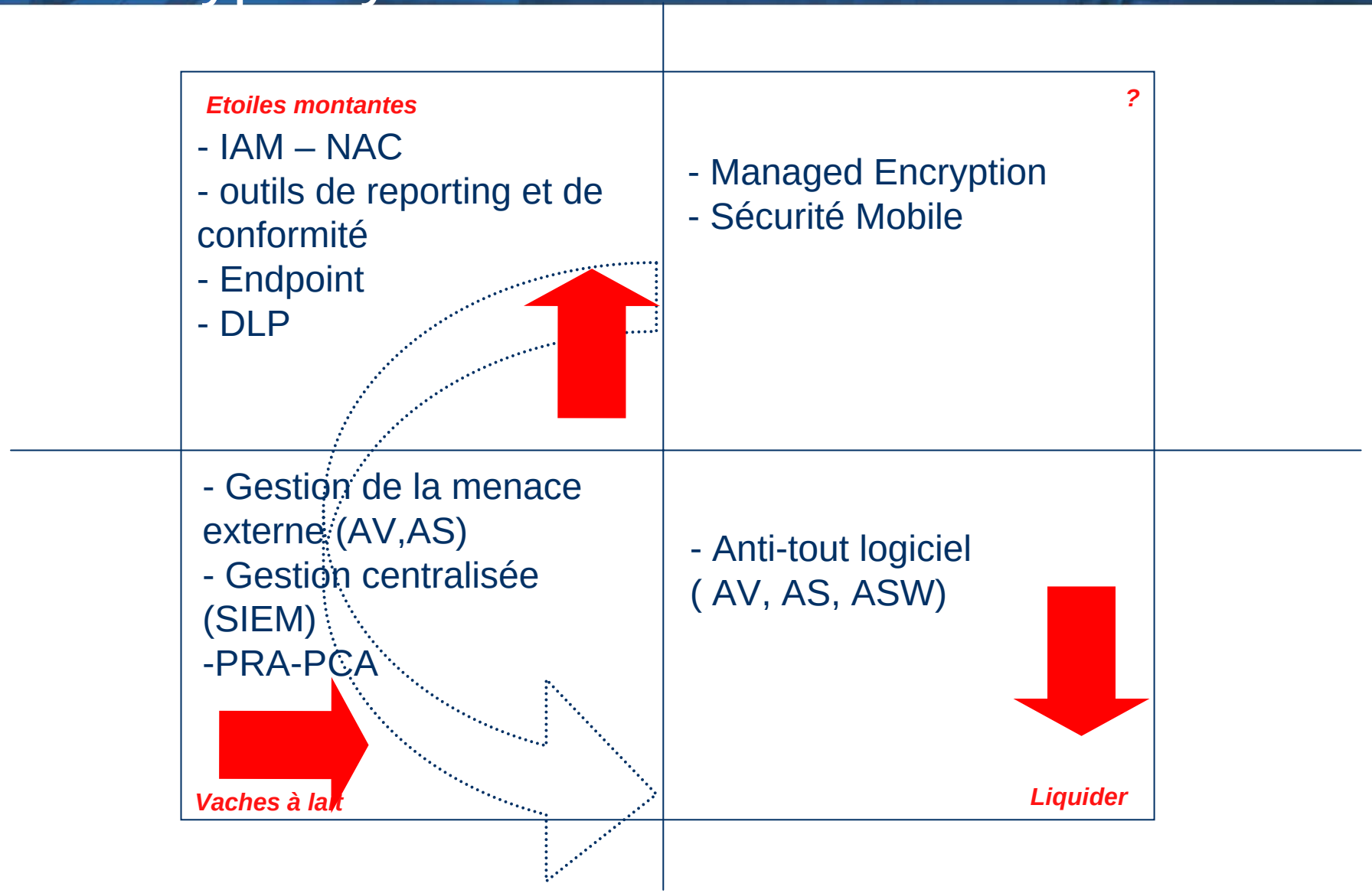
Le challenge sécuritaire du mode projeté



IAM-NAC 5W's

Who?
What?
Where?
When?
Why?

Evolution des dépenses de Sécurité Tech. hype by IDC



Les arbitrages 2007- 2008

Productivité :
Laisser travailler
Sponsoriser l'ubiquité
Favoriser l'utilisateur

Sécurité :
Interdire,
Processer
Mesurer

Éducation
Expliquer
Faire confiance
Répeter

Répression:
Règles d'usages
Collecte de preuve
Punition

Les arbitrages de projets 2007- 2008

Logiciel :
Licence en interne
Remise éditeur
Management maîtrisé

Saas :
Délocalisation complexité
Prix prévisible
Best of breed

Valeur ajoutée
Coût par utilisateur
Churn aisé
Scalabilité

Valeur ajoutée
Partage de la complexité
Partage des tâches
++ avec autant
Tout compris

Les solutions à envisager (1)…

1- **Solutions d'escorte de l'utilisateur – périmètre étendu (E et GC)**

- (EndPoint Solutions, NAC-UTM, Continuité Locale, Cryptograhie Locale, Solution de mobilité sécurisée)
  - KFS :
    - Solutions centralisées, projetées et discrètes (EPS et BC et crypto)
    - Solutions embarquées dans le réseau (NAC, UTM)

2- **Solutions de Gestion des accès et de conformité – le retard à combler**

- (IAM, Conformité projetée)
  - KFS :
    - Multiplateformes
    - Fonctions avancées (RM, RBAC)
    - Rôle de l'intégrateur – Outsourcing des tâches

Les solutions a envisager…(2)

3 - Sécurité et application

- Firewall applicatif, Revue de Code, test et audit externes, Cycle de vie applicatif

4 - Gestion des évènements et des politiques

- Consoles de gestion et de management (SIEM et Hypervision), pré-Audit et contrôles de conformitéFirewall applicatif, Revue de Code, test et audit externes, Cycle de vie applicatif

5 - Sécurité outsourcée

- (Hébergée ou managée)
  - KFS :
    - GC: délocalisation des tâches a faible VA, ROI
    - PME : Réduction de la complexité, Partage de l'expertise, aligenement besoin de l'entreprise

Les bonnes questions

Où est la valeur ajoutée ?

- Gestion de la menace (AV, AS, Am, Anti-tout…)

- Les anti-tout sont tous les mêmes. Désolé.
- Les prix des anti-tout baissent, les meilleurs acteurs sont gratuits. Forte concurrence venue de l'Europe de l'Est. Bientôt la Chine.
- Les anti-tout se transforment en service à forte concurrence

- Le Firewall "basique"

-Contrôle à la frontière, encore éfficace ?

-La Webisation extrême déplace le sujet sur Http. Quelle est la valeur ajoutée du FW en Port 80 ?

-Concurrence FW- IDS/IPS (Appliances, PCI)

Les marchés en début de cycle

- **DLP (Data Leakage Prevention)**
  - Pas d'innovation technologique (Crypto, contrôle de port, Authentification)
  - Marketing poussif et peu localisé
  - Valeur ajoutée peu ou mal expliquée (Propriété Intellectuelle…)
- **Sécurité et mobilité**
  - Où placer les solutions ? Portable, téléphone, Réseau ?
  - Qui gère, administre et assume ?

2008, Une nouvelle ère de la Sécurité informatique

La sécurité n'est plus un problème technique, c'est un problème d'entreprise (Survie, Continuité, Performance, Confiance, conformité)

- Les Projets de Sécurité contribuent à la bonne marche de l'entreprise : la technologie sert le projet d'entreprise.

→ Donner du sens aux projets, aux investissments,aux missions

La Sécurité 2008 est pro-active. Le mode défensif-périmétrique n'est plus suffisant.

- La sécurité, ce n'est plus être en avance d'une réponse mais en avance d'une question.

→ La planification, la méthode, l'expérience partagée éduquent les choix. Pas les slideshows !

Merci de votre attention

Eric Domage

Research Manager,
European Security Products
and Strategies

IDC EMEA Software Group

124 Bureaux de la Colline

92213 Saint-Cloud Cx

+33155396107

+33607030776

edomage@idc.com

www.idc.com