

Traçabilité et sécurité juridique

Me Raphaël PEUCHOT, avocat, Ribeyre & Associés

1. Définition et implications de la traçabilité en droit
2. La protection des données personnelles
3. La responsabilité des prestataires techniques
4. Pédagogie des données personnelles dans l'entreprise

1. Définition et implications de la « traçabilité » en droit

- **L'absence de toute définition / les précédents légaux**
 - « traçabilité » : suivi des process industriel; vie d'un produit
 - Loi Godfrain du 5/01/1988: atteinte aux systèmes de traitement automatisé de données (art. 323-1 CP)
 - Loi sur la vidéosurveillance de 21/01/1995
 - réforme des modes de preuve (signature électronique)

- **Les implications en termes de protection**
 - art. 9 Code civil : « Chacun a droit au respect de sa vie privée »
 - protection du secret des affaires et des réseaux

- **Les implications en termes de responsabilité**
 - atteinte à l'ordre public : responsabilité pénale
 - préjudice aux tiers : responsabilité civile
 - la problématique spécifique de la collecte des preuves

2. La protection des données personnelles

- **La loi du 6 août 2004 (informatique & libertés)**
 - les aspects principaux de la réforme
 - le « correspondant à la protection des données »
 - les applications au commerce électronique (LEN)
- **Le SPAM**

3. La responsabilité des prestataires techniques Internet

- **Le régime général institué par la LEN du 21 juin 2004**
 - l'absence d'obligation générale de surveillance
 - la collaboration avec l'autorité judiciaire
- **Le régime de responsabilité des FAI**
 - construction jurisprudentielle antérieure
 - silence de la loi et droit commun de la responsabilité
- **Le régime de responsabilité des hébergeurs**
 - jurisprudence antérieure
 - le nouveau régime spécifique
- **Les autres prestataires de l'Internet**

4. Pédagogie des données personnelles dans l'entreprise

- **La finalité de la traçabilité dans l'entreprise**
 - sécurité de l'entreprise (patrimoine, réseaux, personnel)
 - surveillance dans l'entreprise

- **Le cadre légal complété par la Loi du 6 août 2004**
 - rappel des règles applicables
 - la simplification des déclarations de fichiers
 - le renforcement des contrôles

- **Les mesures adaptées**
 - l'éternelle « charte informatique »
 - le CPD
 - le volet pédagogique de la politique de sécurité

La trace informatique

Pour quelle preuve ?

Éric **de Bernouis**



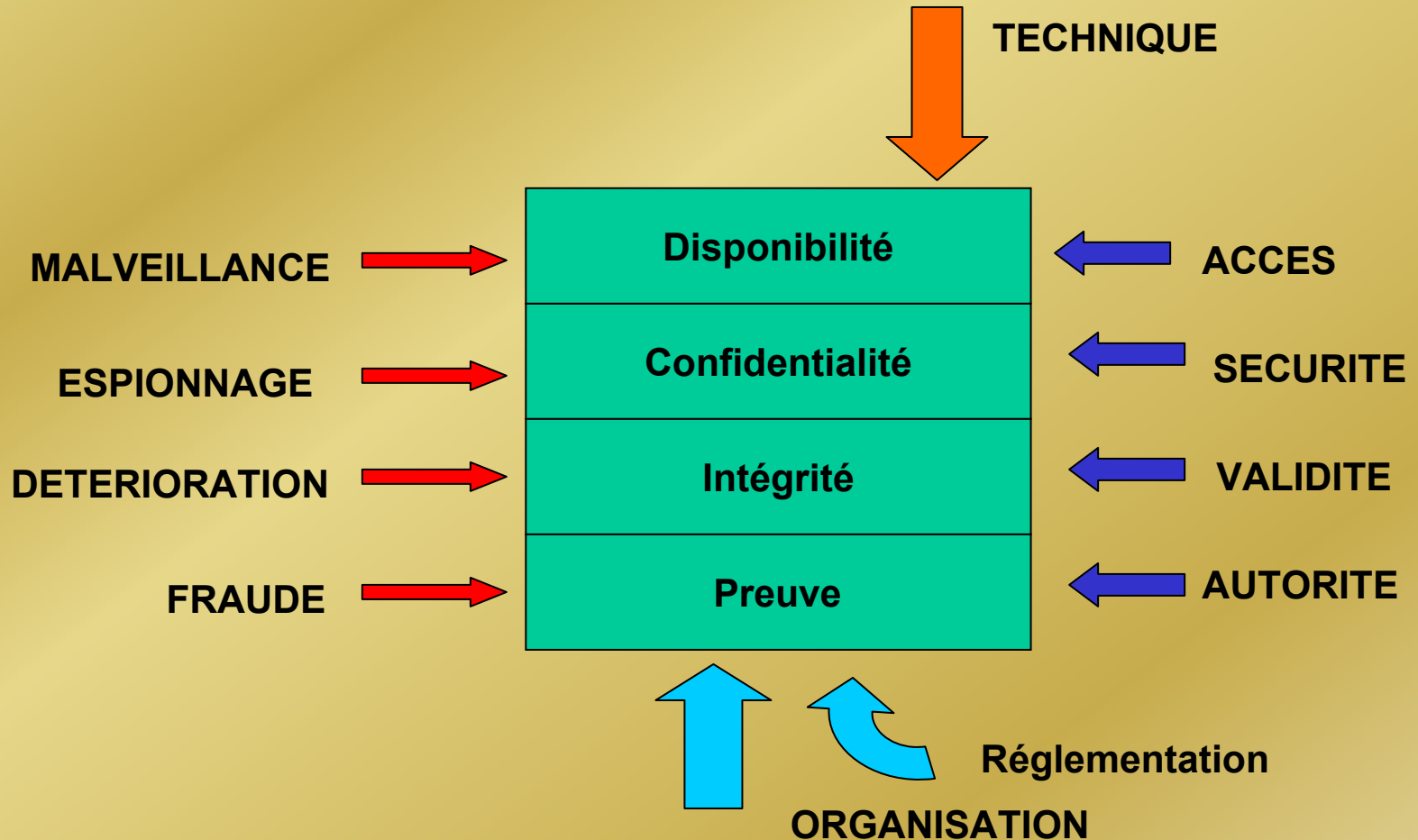
***« La révolution digitale inverse les défauts :
ce qui était autrefois difficile à copier devient facile à dupliquer,
ce qui était oublié devient mémorisé à jamais
et ce qui était privé devient public »***

Ron Rivest

- **Vol de propriété intellectuelle**
- **Périodes d'indisponibilité du système**
- **Perte de productivité**
- **Atteinte à la réputation de l'entreprise**
- **Perte de confiance des clients**
- **Pertes financières importantes dues à un manque à gagner**



La sécurité, source de traçabilité



- **Aptitude à retrouver l'historique**
- **Étapes de raffinement sur la modélisation d'un système**



*« Jadis, nous étions fichés parce que quelqu'un souhaitait nous ficher.
Aujourd'hui, nous pouvons aussi être fichés du seul fait de la technologie
qui produit des traces sans que nous en ayons toujours pleinement conscience »
20ème rapport d'activité de la CNIL pour 1999, Michel Gentot (Président)*

- **Le traçage est inhérent à l'informatique**
- **Il participe la plupart du temps d'une « démarche qualité ou sécurité »**
- **Sous l'appellation de système de « journalisation ».**

- **Anonymat (ou Pseudonymat)**
 - **Mot de passe**
 - **Authentification forte**
 - **Identité numérique**
- **Volatilité des informations**
 - **Confidentialité, intégrité, non répudiation**
 - **Enregistrement numérique**
- **Caractère international**
 - **Géographie des réseaux**
- **Réseau interne, externe**



Deux ans après la loi du 13 mars 2000 : la signature électronique sécurisée est juridiquement opérationnelle

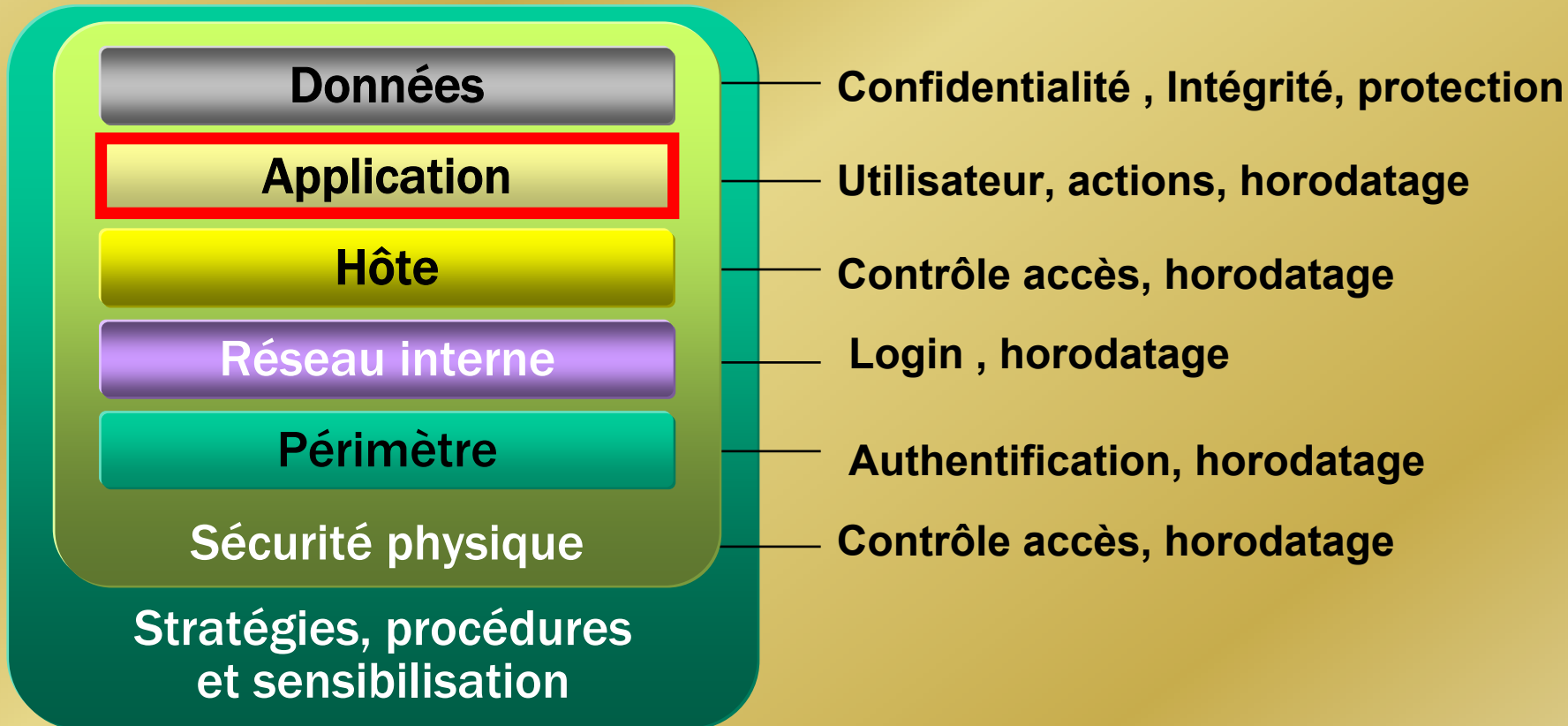
En matière numérique, il s'infère de l'article 1316-1 du Code Civil que la **notion d'original est indépendante de celle du support pour autant que l'intégrité du document soit conservée**

L'écrit numérique ne peut servir de preuve que s'il **est doté d'une signification intelligible,**

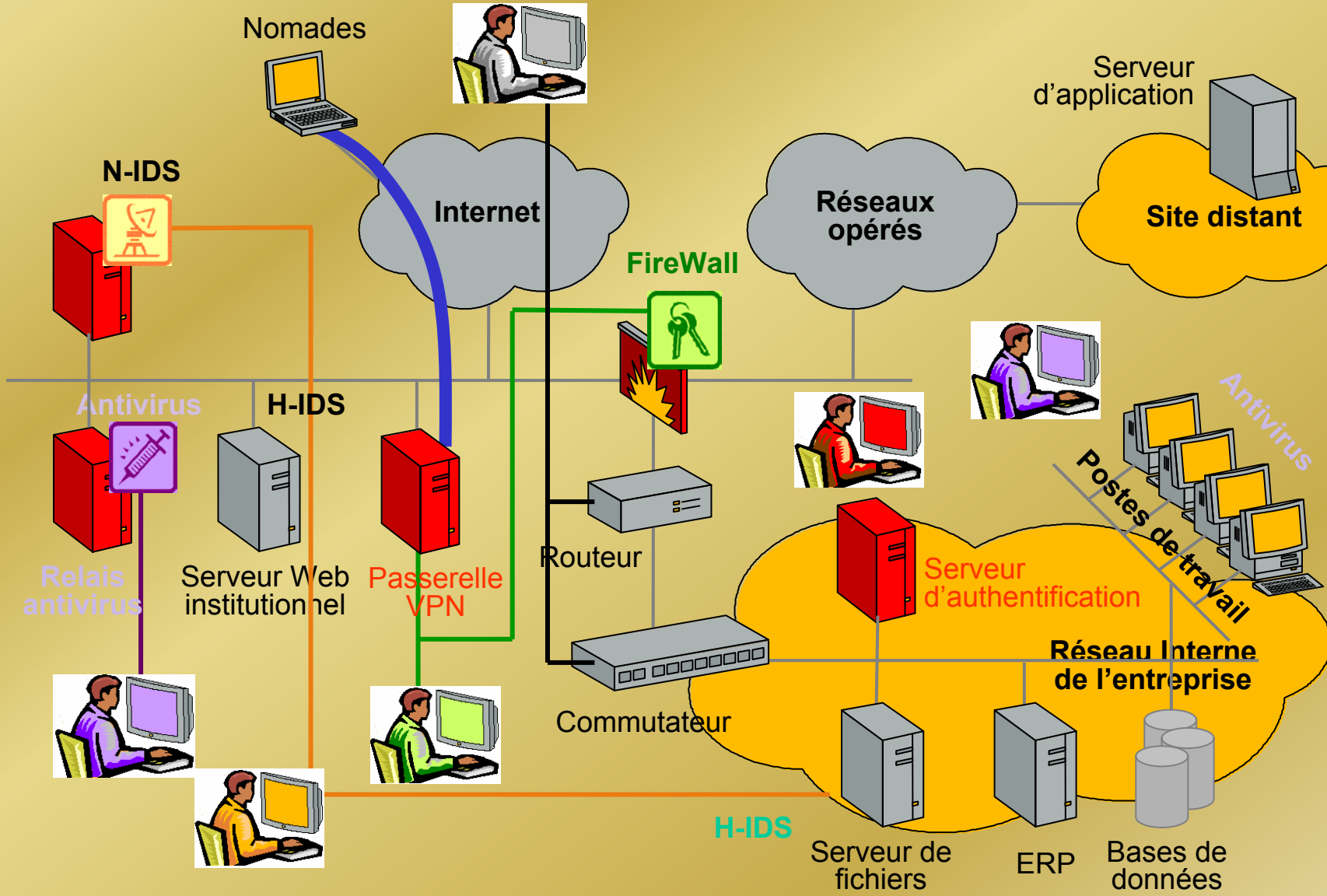
- **Est-il indispensable de conserver l'ensemble de l'environnement informatique ayant procédé à la création du document numérique signé si...**
 - a) on est capable de garantir l'intégrité de ce document au moment de sa création, par l'utilisation du service d'un " tiers de confiance ", par exemple,
 - et si
 - b) la traçabilité du document " en clair " est assurée depuis sa création, dans des conditions de sécurité technique et juridique garanties ?



**EXIGENCE : Origine de la preuve électronique doit être sécurisée
et sa non falsification garantie**



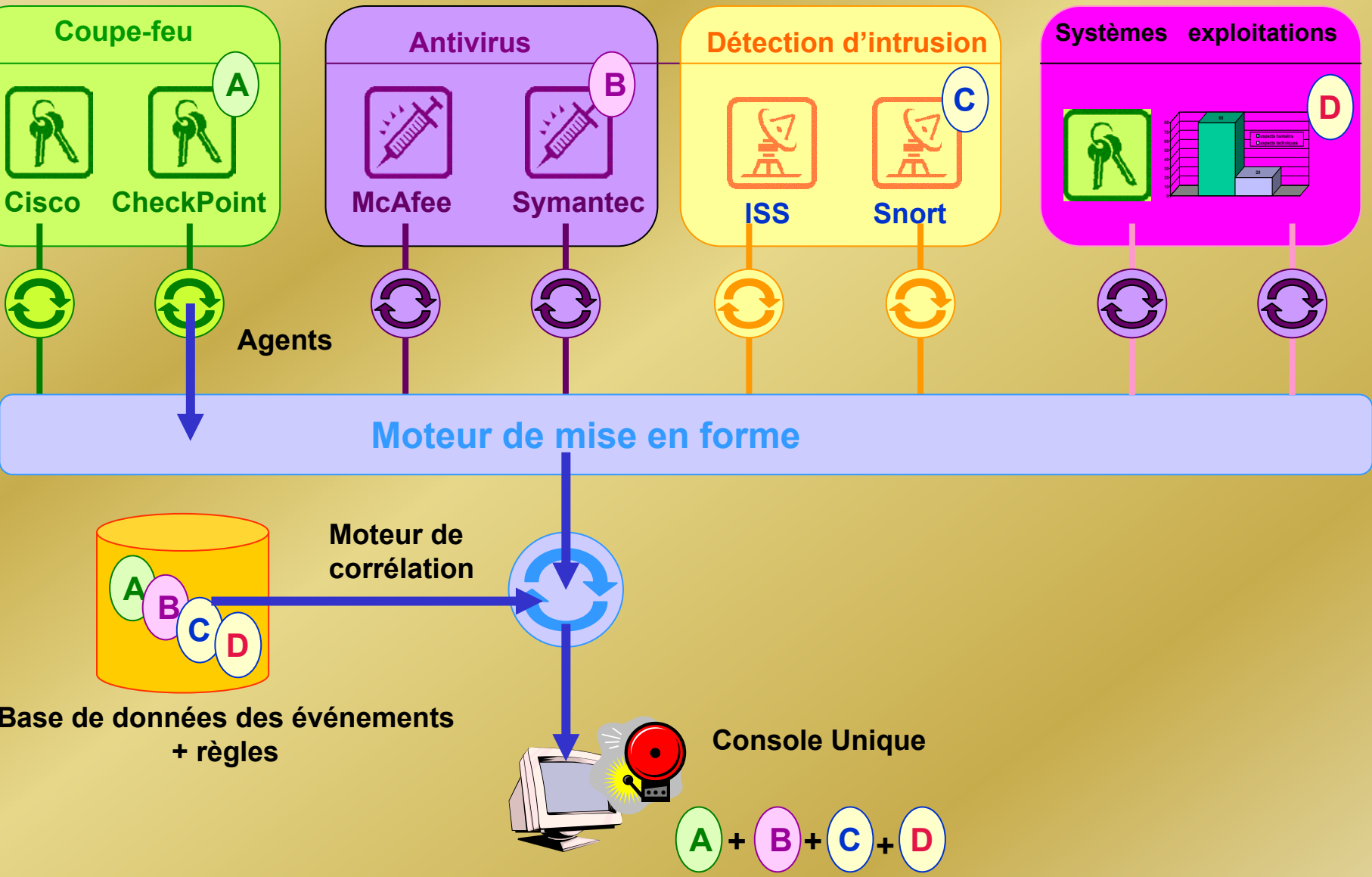
Sources



- **La centralisation des fonctions de supervision de la sécurité est aujourd'hui quasiment acquise.**
 - Les outils de consolidation des logs et alarmes apportent une aide non négligeable.
- **Mais la standardisation des fonctions d'administration relève encore du rêve : les équipements et les logiciels contribuant à la sécurité frappent par leur hétérogénéité.**
 - Les éditeurs gardent la main sur leurs outils.
 - Absence de standards, formats, protocoles, ...

- **Sources issues du Management du SI**
 - Administration
 - Politique de sécurité
 - Respects des lois sur les données nominatives
- **Traçabilité = $\Sigma [(\text{LOGS}(T-\Delta) , \dots, \text{LOGS}(T+\Delta))]$**
 - Antériorité, et postérité des données
 - Conservation des données (temps de la justice ...)
- **Vraisemblance de la preuve \Leftrightarrow Corrélation**
 - Scénarii possibles \rightarrow Chronologies de Faits + Traces

Le SIM



- Une preuve pour quoi faire ?
 - Données nominatives
 - Données fonctionnelles
- Une preuve reconnue par toutes les parties ?
 - Reconnaissance du collecteur
 - Privé
 - Public (organismes assermentés)

Retour sur investissement de la SSI

Une question essentielle,
des réponses (trop ?) multiples

Denis **Pélanchon**

Le contexte : maîtriser les coûts

- La question des coûts est une question de performance :
 - Ce n'est pas ... diminuer les coûts
 - C'est ... accroître l'efficacité et l'efficience

 - Efficacité :
 - Délivrance du service attendu
 - Respect des délais
 - Satisfaction des clients

 - Efficience :
 - Optimisation des infrastructures (mutualisation des moyens)
 - Diminution des charges de travail (gestion des projets)
 - Diminution des coûts du travail (offshore)

Outils de mesure : TCO et ROI

- TCO : total cost of ownership
 - Estimation d'un coût moyen par poste de travail (études, matériels, logiciels, services, fournitures)
 - Objectif : le réduire (limiter les dépenses ou allonger les durées d'amortissements)

- ROI : return on investment
 - $(\text{Résultat d'exploitation} + \text{Produits financiers}) / (\text{Capitaux propres} + \text{Dettes})$
 - Objectif : maximiser le résultat économique, tout en minimisant les investissements

La DSI « consomme » des capitaux et des dettes
 mais la DSI ne génère pas de résultat économique => ROI = 0 !!?

- En théorie le calcul du ROI revient donc à estimer un résultat économique pour la DSI :
 - Évaluer les revenus que les « clients » seraient prêts à consentir à la DSI au regard du service rendu et en déduire les charges et achats liés à l'exploitation du SI
 - Éventuellement, intégrer des produits financiers
- Les contraintes à prendre en compte :
 - Lois et règlements
 - Bonnes pratiques, normes et standards
 - Stratégie de l'entreprise
 - Place de la DSI dans l'entreprise
- Dans la pratique :
 - Optimisation des processus
 - Diminution des coûts de fonctionnement
 - Gains de qualité de service (vue métiers)

ROSI : return on security investment

- Définitions¹

- **ROSI = (bénéfices-coûts) / coûts**
- Temps nécessaire pour récupérer la mise de fonds initiale d'un investissement
- Déterminer a priori la solution de sécurité optimale d'un projet ou d'un système

- Coûts :

- Ponctuels : investissements, déploiement, incidents
- Récurrents : exploitation, administration, maintenance, supervision
- Tangibles : perte de productivité, perte de revenus, coûts d'assurance, ...
- Intangibles : perte de réputation, perte de part de marché, non conformité à la réglementation, ...

- Bénéfices :

- Technologiques : coûts d'infrastructure (VPN), réduction des incidents (anti-virus), qualité de service
- Maîtrise des risques
- Conformité réglementaires ou normative
- Réputation sur le marché

1 : source CLUSIF « ROSI : Quelques clés pour argumenter »

Les modèles de ROSI¹

- Amélioration de la performance
 - Mettre en place une métrique permettant de mesurer les gains réalisés au travers d'une solution de sécurité (temps de réponse, traitement d'incidents, appels utilisateurs, etc.)
- Prévention des incidents
 - Comparer les pertes prévues liées à une solution sans sécurité, les pertes potentielles liées à une solution sécurisée et les coûts de la solution sécurisée
- Analyse de risque
 - Couvrir les pertes potentielles liées à un risque de sécurité, par une solution de coût moindre
- Enjeux métiers
 - Garantir la fourniture d'un service sécurisé, permettant de prendre un avantage sur la concurrence ou de limiter un risque métier ou juridique
- Normes et standards
 - Justifier un investissement en sécurité par rapport à une mise en conformité aux standards proposés par le marché
- Benchmarking
 - Mettre en œuvre les bonnes pratiques, ayant fait la preuve de leur efficacité afin de s'aligner sur le marché

1 : source CLUSIF « ROSI : Quelques clés pour argumenter »

Le coût de la SSI est une question nécessaire et sans doute vitale, mais ...

- Le calcul du retour sur investissement en SSI, emprunte à de multiples méthodes et outils, les comparaisons semblent difficiles et les interprétations discutables
- Il semble avant tout être lié à un consensus, parfois subjectif, entre la DSI, une DAF et une DG
- La SSI reste :
 - une composante de la stratégie de l'entreprise,
 - qui doit faire face à des risques technologiques, environnementaux, contextuels (concurrence) et humains,
 - dans un cadre économique,
 - mais aussi légal et éthique,
 - décidée par le plus haut niveau hiérarchique.