IBM Global Services

Tendances en securité

Patrick Pleinevaux, IBM

Mainframes

Protection des postes de travail

Gestion des événements

Video surveillance

Un mainframe d'ancienne génération

IBM z9 (2005)

2 frames

- CEC + E/S (droite)
- E/S (gauche)

Calcul 64 bit

Maxima:

54 processeurs

512 GB RAM

60 partitions

Qu'est ce qu'un mainframe en 2007 ?

Une machine qui:

- Tourne plusieurs OS en parallèle: zOS, Linux, etc.
- A une énorme capacité d'entrées-sorties (plus de 300 ports Fibre Channel)
- A un MTBF de plusieurs décennies
- Offre une sécurité avancée

System z9

Occupe 2.5 m^2 de surface au sol

Les capacités de communication du mainframe

Une machine à la pointe:

- Protocole IPv6, interfaces 10GE
- 640 piles TCP/IP par port pour la virtualisation
- 16 réseaux IP internes à la machine (Hipersockets)
  - Multicast, broadcast
  - Réseaux IPv4 et v6
  - IPsec en interne

Caractéristiques de sécurité du z9

Une machine conçue pour la sécurité:

- Partitionnement et virtualisation
- IPsec, SSH, SSL (accélérateur)
- Fonctions crypto sur chaque processeur
- Fonctions crypto avancées sur cartes séparées
- Services PKI
- Chiffrement de bandes magnétiques
- Très haute disponibilité

Fonctions crypto sur les z9

Chaque processeur central a une unité crypto:

- DES, 3DES, AES-128
- SHA
- Générateur de nombres aléatoires

Cartes optionnelles:

- Opérations avec clés sécurisées
- Crypto clés publiques (SSL, IPsec)
- Certification FIPS 140-2 Niveau 4

Les mainframes ont obtenu la certification pour EAL5

Basée sur les Critères Communs

EAL 7 or 6: Aucun OS

EAL 5: Conçu de façon semi-formelle et testé
z890, z990 (2005), z9 (2006) avec z/OS et LPAR

EAL4+: EAL4 augmentée
AIX 5L (2006), i5/OS V5R3 (2005)

EAL4: Conçu, testé et vérifié méthodiquement
Windows 2003

Mainframes

Protection des postes de travail

Gestion des événements

Video surveillance

IBM 5100 Portable Computer (1975)

Premier ordinateur personnel IBM

25 kg

16k – 64k mémoire

Basic et/ou APL

Bande magnétique de 200k

Les menaces sur les rares postes de travail en 1978

Pas de virus, pas de vers

Pas d'intrusions depuis Internet

Mais déjà des:

Accès non autorisés

Pertes ou vols de media

IBM 5110

Les machines ne sont pas interconnectées

Menaces sur les postes de travail en 2007

Codes malicieux

Vers, virus, troyens, etc.

Attaques 0-jour, attaques ciblées

Intrusions réseau

Depuis une autre machine infectée

Buffer overflows et autres méthodes

Usages incontrôlés

Installation de programmes piégés

Importation de fichiers infectés

Exportation de fichiers sensibles

Menaces sur les postes mobiles

Toutes les menaces des postes fixes plus:

Wireless

- Double attachement du poste
- Communications non chiffrées
- Points d'accès pirates

Pertes ou vols d'ordinateurs portables

- Trains, aéroports, hotels, voitures
- Confidentialité des données et programmes

Les bases indispensables à la protection du poste

Analyse de risques

Politique de sécurité pour les postes de travail

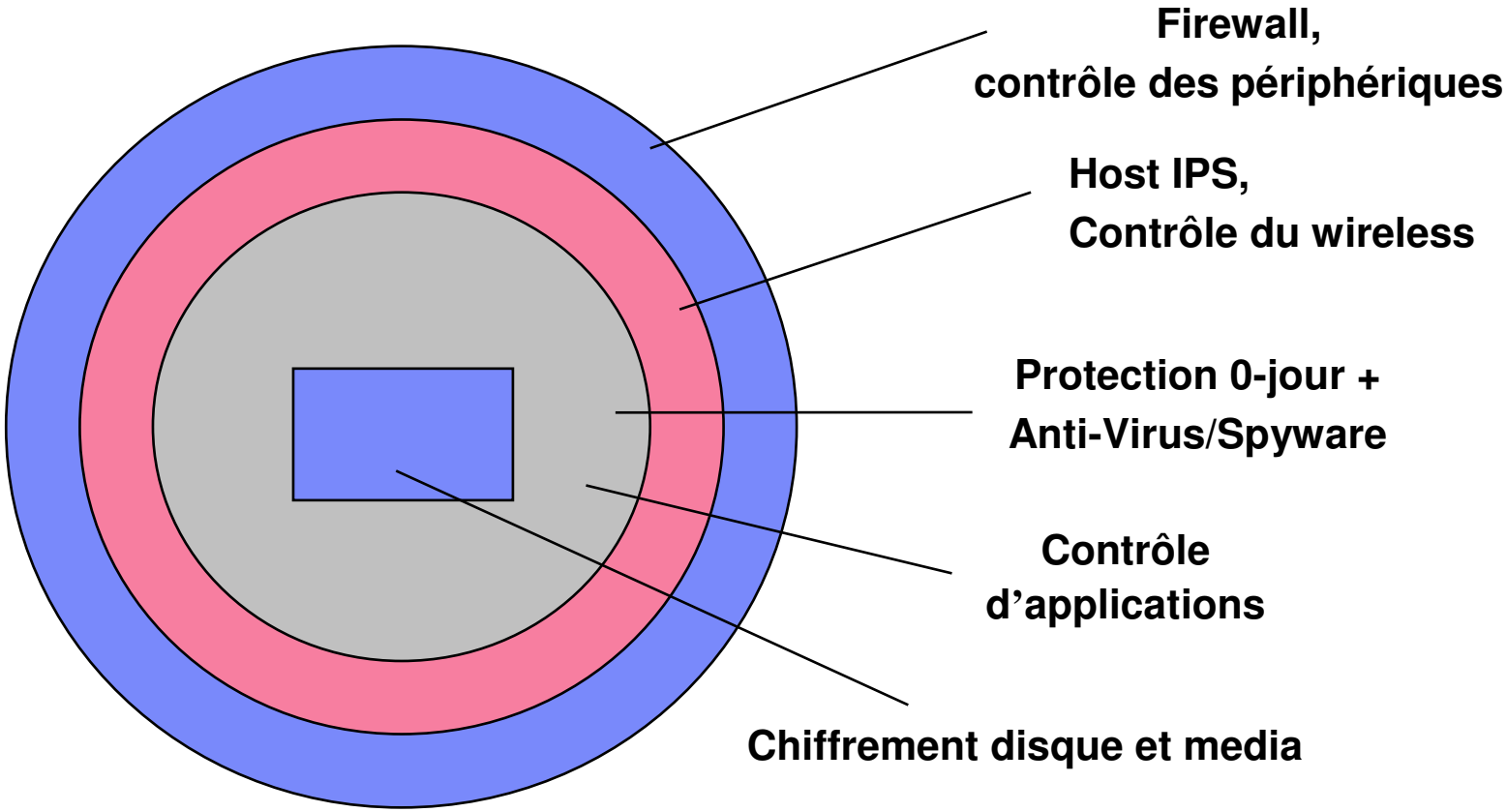
Campagne de sensibilisation des utilisateurs

Durcissement de l'OS et du browser

Application des correctifs

Eléments de la protection du poste de travail

Protection multi-niveaux contre les menaces tous azimuts



Critères de choix d'une solution

Très nombreux critères, entre autres:

Couverture des menaces

- Critère numéro 1

Transparence pour l'utilisateur

- La sécurité ne doit pas affecter le business
- Minimiser les messages à l'utilisateur

Facilité d'administration

- Sécurité dépend de la qualité de l'administration
- Console unique

Approche 1 – composants indépendants

Choisir des composants de sources différentes

Avantages – composants peuvent être adaptés aux besoins/risques identifiés et optimaux

Inconvénients – absence d'intégration, consoles multiples

Approche 2 – agent intégrant les différents composants

Un agent combinant les différentes fonctions

Avantages – console unique, meilleure protection par intégration des composants

Inconvénients – composants peuvent être non optimaux

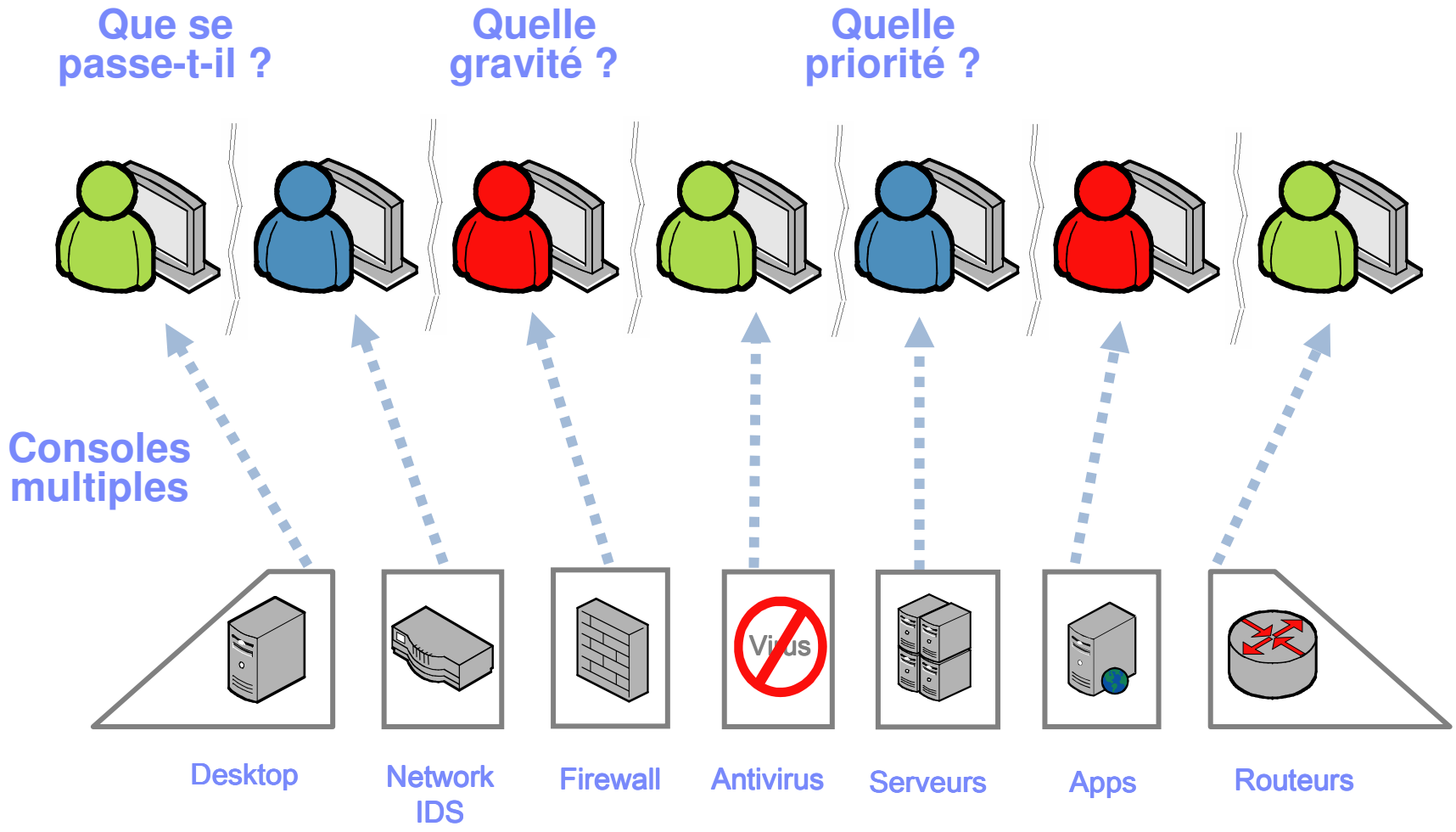
Mainframes

Protection des postes de travail

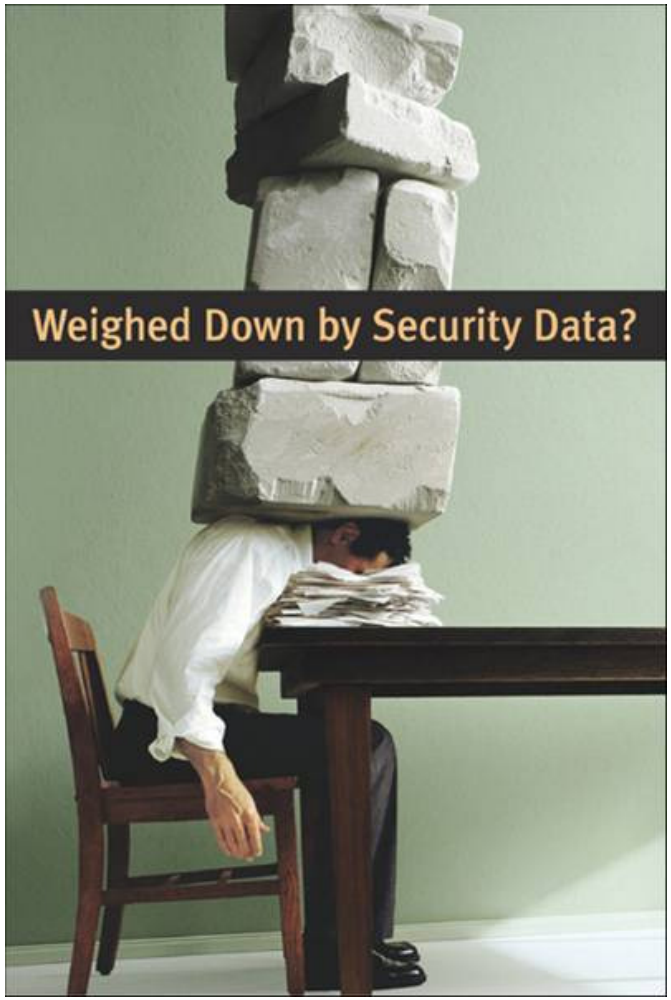
Gestion des événements

Video surveillance

Defi 1 – Avoir une vision globale en temps réel



Defi 2 – le nombre colossal d'événements à examiner

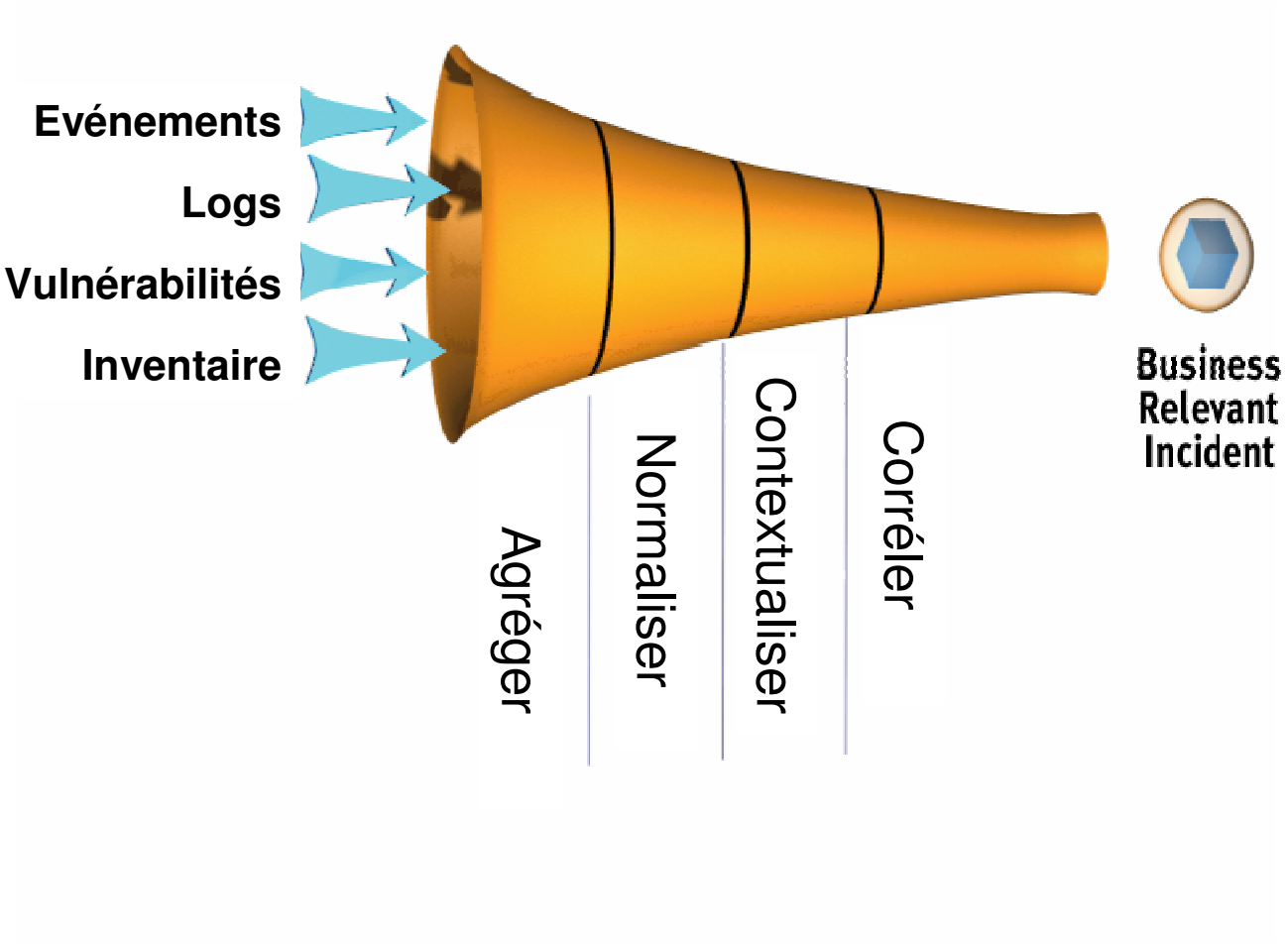


Des millions d'événements chaque jour

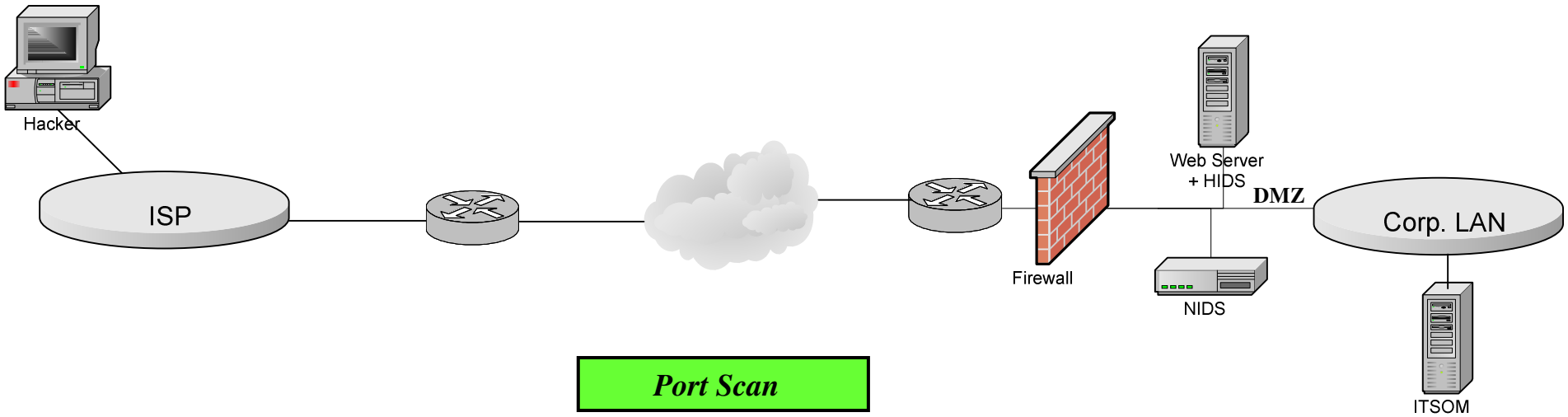
Solutions:

- Filtrage
- Corrélation
  - Source
  - Destination
  - Temporelle
  - Vulnerabilités

Un système de gestion des événements de sécurité permet d'obtenir une telle vue globale

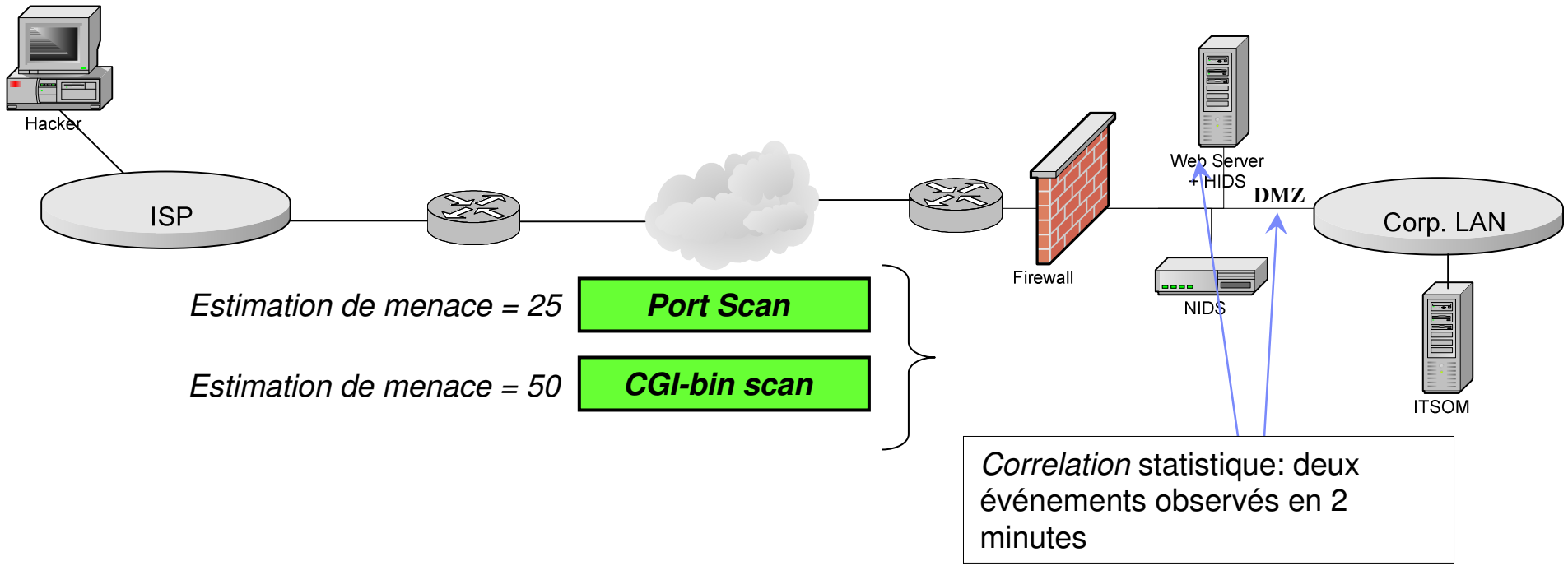


Exemple – Correlation d'impact sur une attaque



Première attaque – Port Scan – Le système analyse et effectue une *Correlation d'Impact.*
Cette analyse produit une estimation de menace que la plateforme mémorise

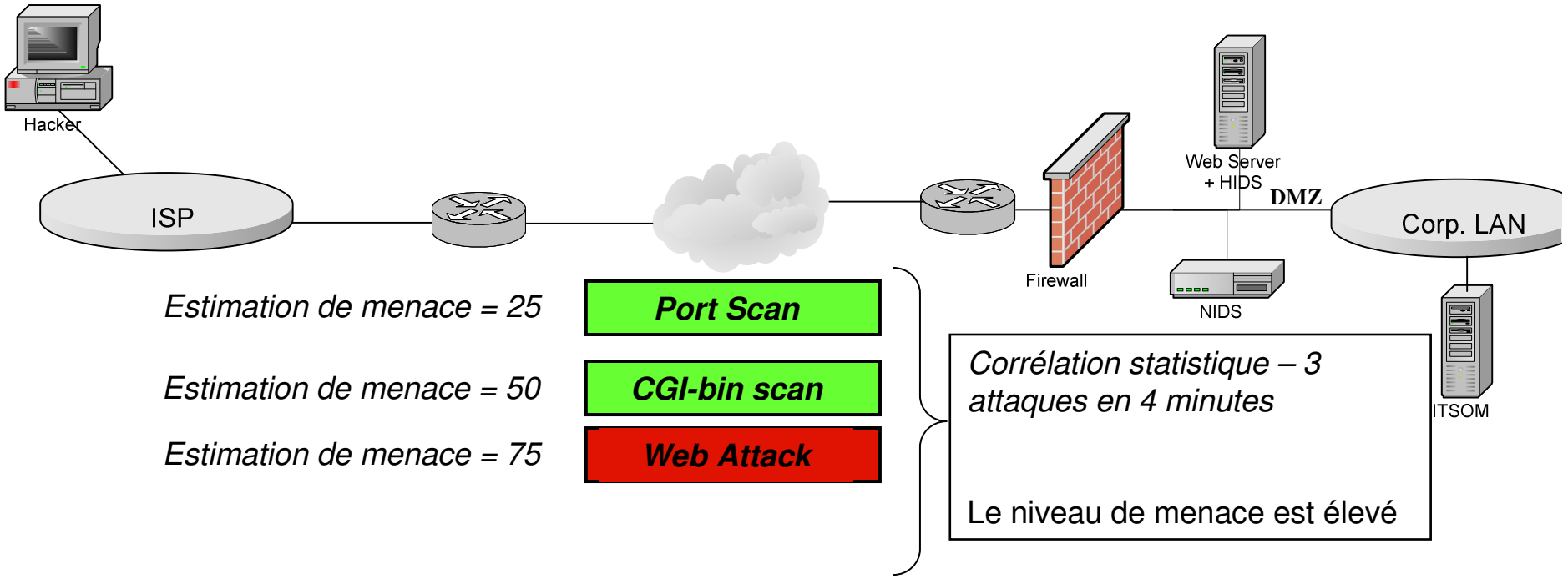
Exemple – Correlation statistique



Seconde attaque – Le hacker voit que le port 80 est ouvert. Il lance un ensemble de sondes pour chercher des vulnérabilités dans le serveur Web (i.e. CGI Bin scan)

Une fois encore une corrélation d'impact est effectuée. Mais il s'agit du 2e événement venant de cette machine, donc il est maintenant détecté par la **Correlation statistique**.

Troisième attaque – corrélation statistique



Intérêt d'un système de gestion des événements de sécurité

Vue globale des menaces – prise en compte de nombreuses sources

Vue en temps réel

Prise en compte de l'importance business des cibles potentielles

Prise en compte des vulnérabilités des cibles

Définition des priorités de traitement

Mainframes

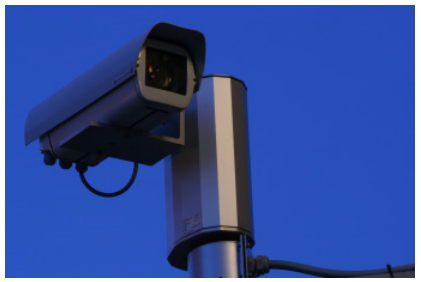
Protection des postes de travail

Gestion des événements

Video surveillance

Les applications de la video surveillance

Sécurité physique: surveillance de sites, bâtiments, centres de calcul



Transports: routes, autoroutes, métros, etc.

Lutte contre la fraude: grandes surfaces, casinos, banques

Optimisation, étude de comportement: grandes surfaces

Historique de la vidéo surveillance en Grande Bretagne

1961: caméras dans la gare de Londres

1967: début du déploiement dans les stations à essence

1974: surveillance des principales artères de Londres

198x: déploiements dans les centres-villes

1994: début de surveillance des bancomats

1997: reconnaissance des numéros de plaques de voiture (Londres)

Historique de la vidéo surveillance en Grande Bretagne

1998: début de reconnaissance faciale

2002: Nombre de caméras en UK: 4’200’000 (estimation)

2005: Attentats de Londres

2006: Couplage avec des microphones

2007: Organe de contrôle signale de grandes violations de la protection de la sphère privée

Défi 1: des études montrent qu'après 20 minutes, le taux de reconnaissance d'un agent tombe en dessous de 5%

Taux de reconnaisance des événements

- Moniteurs: deux ou plus
- Après 12 minutes: 45%
- Après 22 minutes: 5%

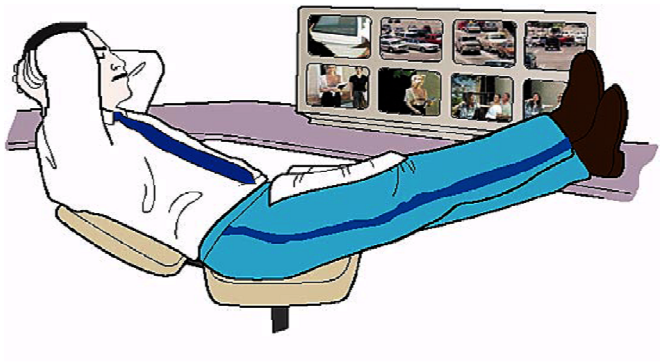


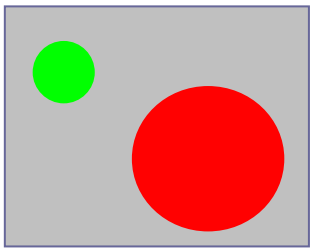
Exhibit 2.5. Monitoring video output is a boring task and usually nonproductive in most security applications, even for the motivated employee.

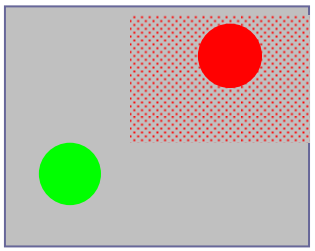
Défis: durée et nombre de caméras

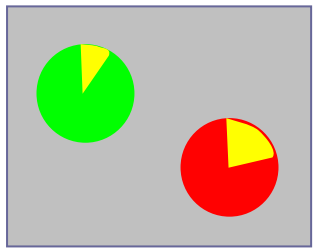
Solution: automatisation

L'analyse automatique détecte des conditions définies par l'utilisateur

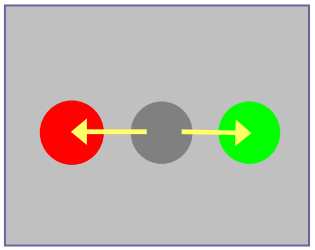
- Taille
- Position
- Temps

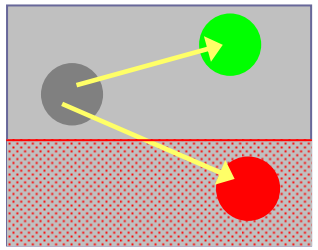


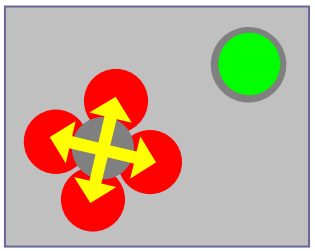


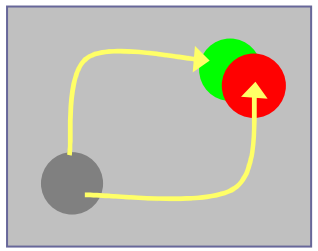


- Direction
- Passage de frontières
- Mouvement ou immobilité
- Files

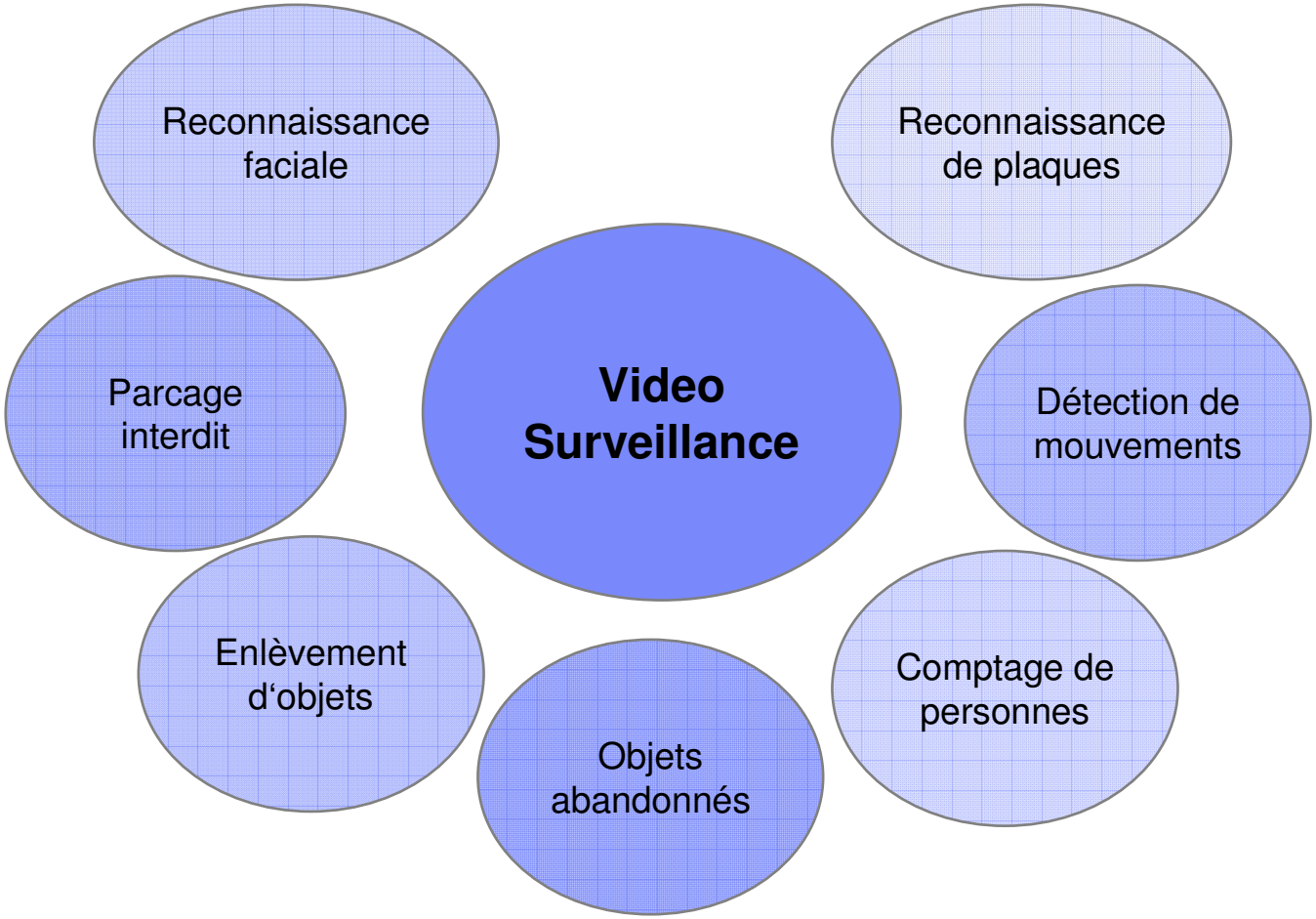




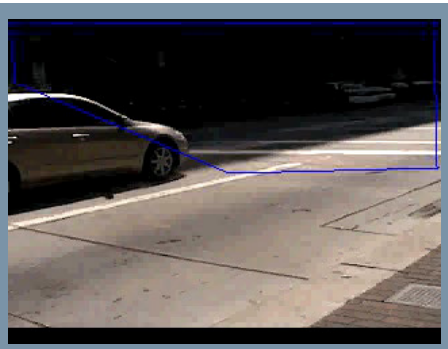




Applications élémentaires



La detection d'événements



Motion Detection

Triggers on movement of object within a zone

Sensitive Detection

Tripwire function with high-motion sensitivity – triggers on the cat crossing the road

Directional Motion

Triggers on right-turns, when the cars move in the direction of the arrow

Tripwire

Triggers based on the direction of wire crossing, one for North Traffic and another for South Traffic

Object Removal

Triggers when object outlined in blue is removed from its position

Abandoned Object

Triggers when object is abandoned within the blue zone outlined in the image. Left—original video, Right – output result

Défi 2 – Recherche de séquences d'images

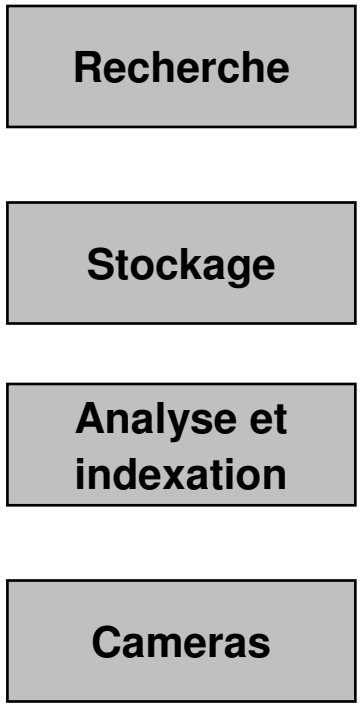
Analyse d'incidents *a posteriori*

Comment retrouver une séquence dans des milliers d'heures d'enregistrement ?

Solution: Analyse automatique et en temps-réel des flux vidéo, indexation des images

Stockage des méta-données dans une base SQL

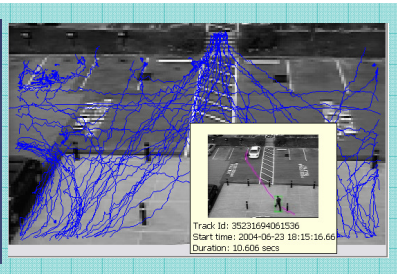
Recherche de séquences sur base de mots clés

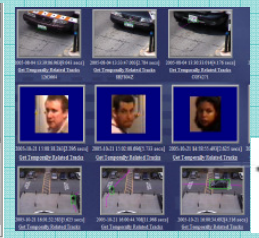


Evolution de la video surveillance

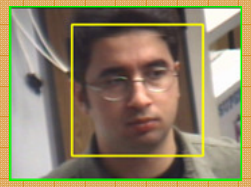
Large Truck parked near both train station

Data Mining & Pattern Discovery Layer
Delivery Truck –2nd Delivery, Unusual
Pattern Discovery, Planning etc
Pre-emptive Use





Meta-data Management Layer:
Extensible Indexing, Search & Correlation
Find Red Cars & correlate to ID #'s
Behavior Discovery, Configurable Alerts
Proactive Use / Cross leverage



Data Analytics Layer
Predefined behavior detection
Crossing Tripwire
Security Applications –defined response
Real-time intervention

Capture Layer
Automated Data Capture
Exploitation – users
Reactive Use

IBM Global Services

Merci pour votre attention