22 janvier 2016

CHAMBRE FRANÇAISE
DE COMMERCE ET D'INDUSTRIE
DU MAROC

Quelles sont les tendances de la cybercriminalité pour 2016 et comment l'entreprise peut-elle y faire face ?

Frédéric GOUX

Directeur associé du cabinet Solucom

solucom
management & IT consulting

Frédéric GOUX

Parcours & Activités

- Telecom ParisTech 1996
- Rejoint Solucom en 1997
- Directeur associé en charge de la practice Risk management & Sécurité de l'information
- Conseil auprès des grandes entreprises et administrations en France et au Maroc
  Crédit Agricole, Société Générale, SNCF, SFR, TF1, Ministères, Attijariwafa Bank, RAM, Saham Assurance, Wafabail…
- Direction de grands projets de transformation d'infrastructure
  Sécurité, Télécoms, Architecture, Datacenter, Plan de Continuité d'Activité

@fredgoux ***frederic.goux@solucom.fr***

Solucom : qui sommes-nous ?

- 2ème cabinet* de conseil indépendant en France
- Présence de premier plan auprès de grands comptes Marocains
- …pour guider et réussir leurs transformations les plus structurantes

Échantillon de nos clients sur le marché marocain

- **1600 collaborateurs**
- **175 M€ de CA** *en année pleine*
- **Coté en Bourse sur Euronext Paris**

France
Royaume-Uni
Suisse
Belgique
Maroc
Singapour*
Dubaï*

** Partenariat stratégique*

Cybercriminalité : Les tendances pour 2016

Le retour de la menace diffuse

Le retour de la menace diffuse

Savoir reconnaître les différents types de menaces

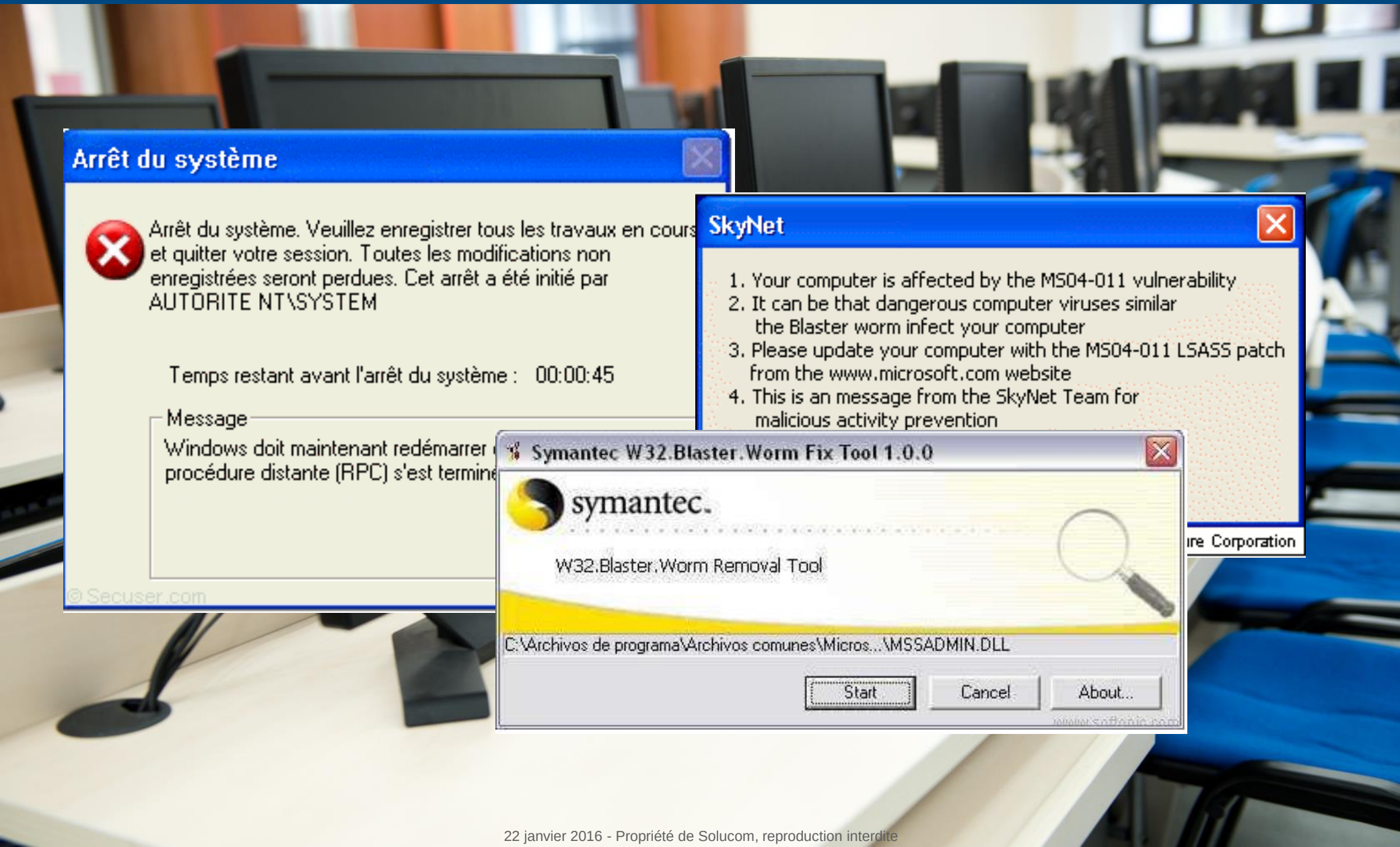
CIBLEE

OPPORTUNISTE

DIFFUSE

Le retour de la menace diffuse

Souvenez-vous en 2003, les vers réseau nous envahissent



Le retour de la menace diffuse

En 2015, au tour des ransomwares et autres cryptolockers !

Le retour de la menace diffuse

Les impacts des ransomwares aujourd'hui

Une activité **extrêmement lucrative…**

ROI 1 425%

Source : Trustwave

…touchant de plus en plus les **entreprises**

1/3 des DSI touchées

Source : webroot

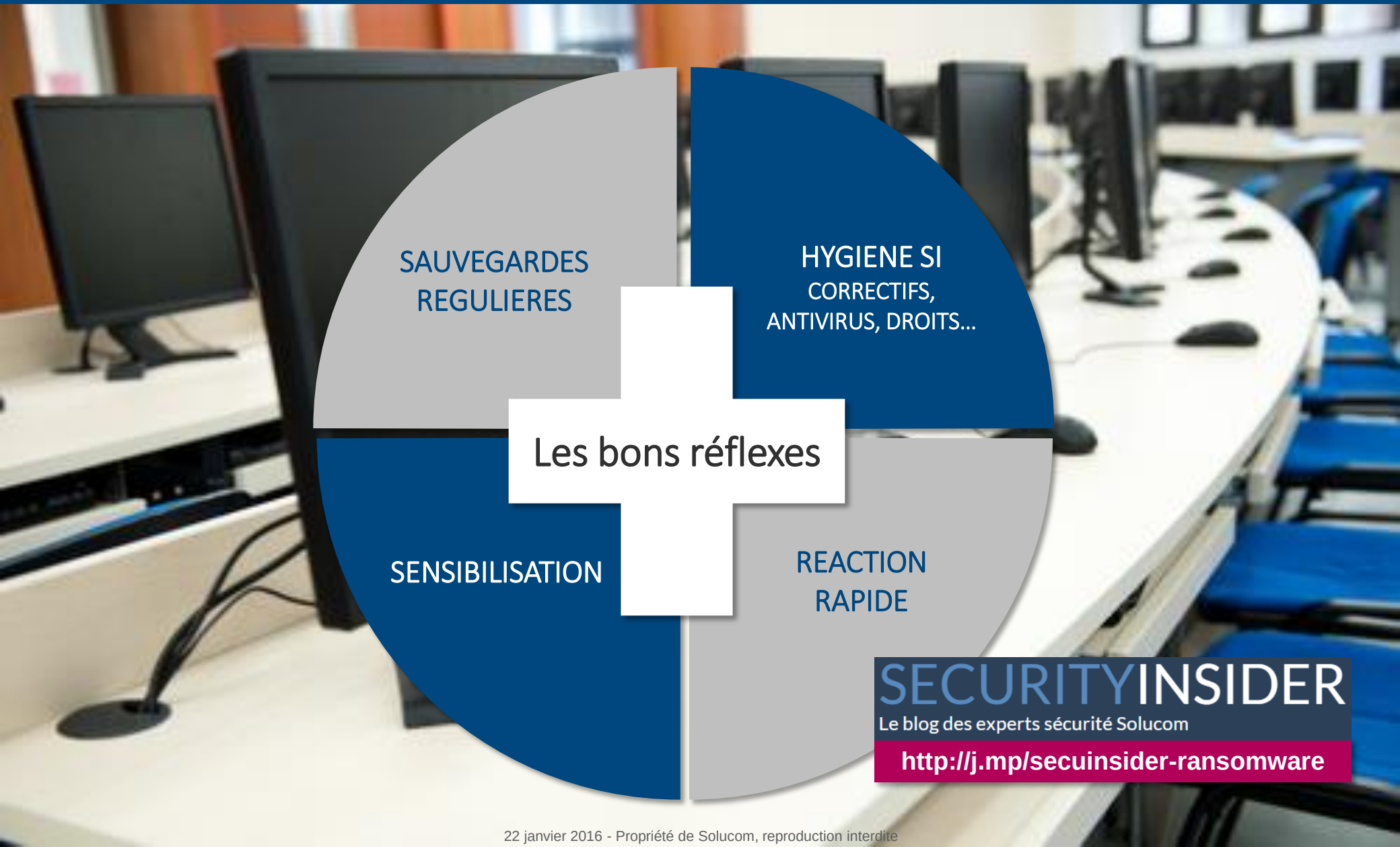
Des impacts immédiats

- Perte d'accès aux fichiers
- Désorganisation

Plusieurs jours de crise

Le retour de la menace diffuse

Face aux ransomwares…



SECURITYINSIDER

Le blog des experts sécurité Solucom

http://j.mp/secuinsider-ransomware

Destruction, oui mais encore ?

L'incroyable attaque de Sony Pictures

Chez Sony Pictures, le 24 novembre 2014

L'incroyable attaque de Sony Pictures

Les éléments déclencheurs


From: Frank David <sfrank1973.david@gmail.com>
Subject: **Notice to Sony Pictures Entertainment Inc.**
To: michael_lynton@spe.sony.com, amy_pascal@spe.sony.com, doug_belgrad@spe.sony.co

We've got great damage by Sony Pictures.

The compensation for it, monetary compensation we want.

Pay the damage, or Sony Pictures will be bombarded as a whole.

You know us very well. We never wait long.

You'd better behave wisely.

From God'sApstls

~ Septembre 2014 :

Intrusion initiale dans le SI par un moyen encore inconnu (0day ?) et extraction de près de 100 To de données

21/11/2014

Demande de **rançon** par email

22-23/11/14

Déploiement d'un **outil d'attaque destructeur** (Wiper Destover)

24/11 – Lancement de l'attaque

Effacement de **plusieurs dizaines de millier de postes de travail Windows et de 75% des serveurs**

Destruction, oui mais encore ?

L'incroyable attaque de Sony Pictures

- Révélation des salaires et polémique
- Messages acerbes

Dirigeants

- Mise en ligne de 5 films inédits :19% de perte/film
- Coûts liés à la résolution de l'incident (45 M$)

Perte financière

- Révélation d'informations personnelles de 47000 employés
- Class-action en cours

Employés

- Divulgation d'informations stratégiques
- Contrats et négociations en cours sur la place publique

Concurrence

SI de Sony

- Révélation des contentieux et des dossiers en cours

Juridique

- Perte de contrôle des comptes Twitter et Facebook

Réseaux sociaux

- Révélations d'informations personnelles et sensibles sur des acteurs employés par le studio

Ecosystème

- Plus de 8 semaines d'interruption
- Révélation d'informations techniques détaillées

SI de Sony

Destruction, oui mais encore ?

L'incroyable attaque de Sony Pictures

Une prise d'otage numérique qui s'aggrave de jour en jour

08/12/2014: Révélation des emails d'Amy Pascal, vice présidente & Steven Mosko, président

10/12/2014: Menace sur tous les employés et demande de l'abandon du film « The interview »

12/12/2014: Au tour de Leah Weil, general counsel (département juridique)

16/12/2014: Puis Michael Lynton, PDG

Et le basculement…

Le 16/12/2014 : les pirates menacent d'attentat les salles qui diffuseront le film « The Interview » utilisant une analogie avec le 11 septembre 2001…
… et effraient les chaînes de cinémas !

Et pendant ce temps, Sony tente de museler les médias / réseaux sociaux et de limiter les téléchargements des données…

Destruction, oui mais encore ?

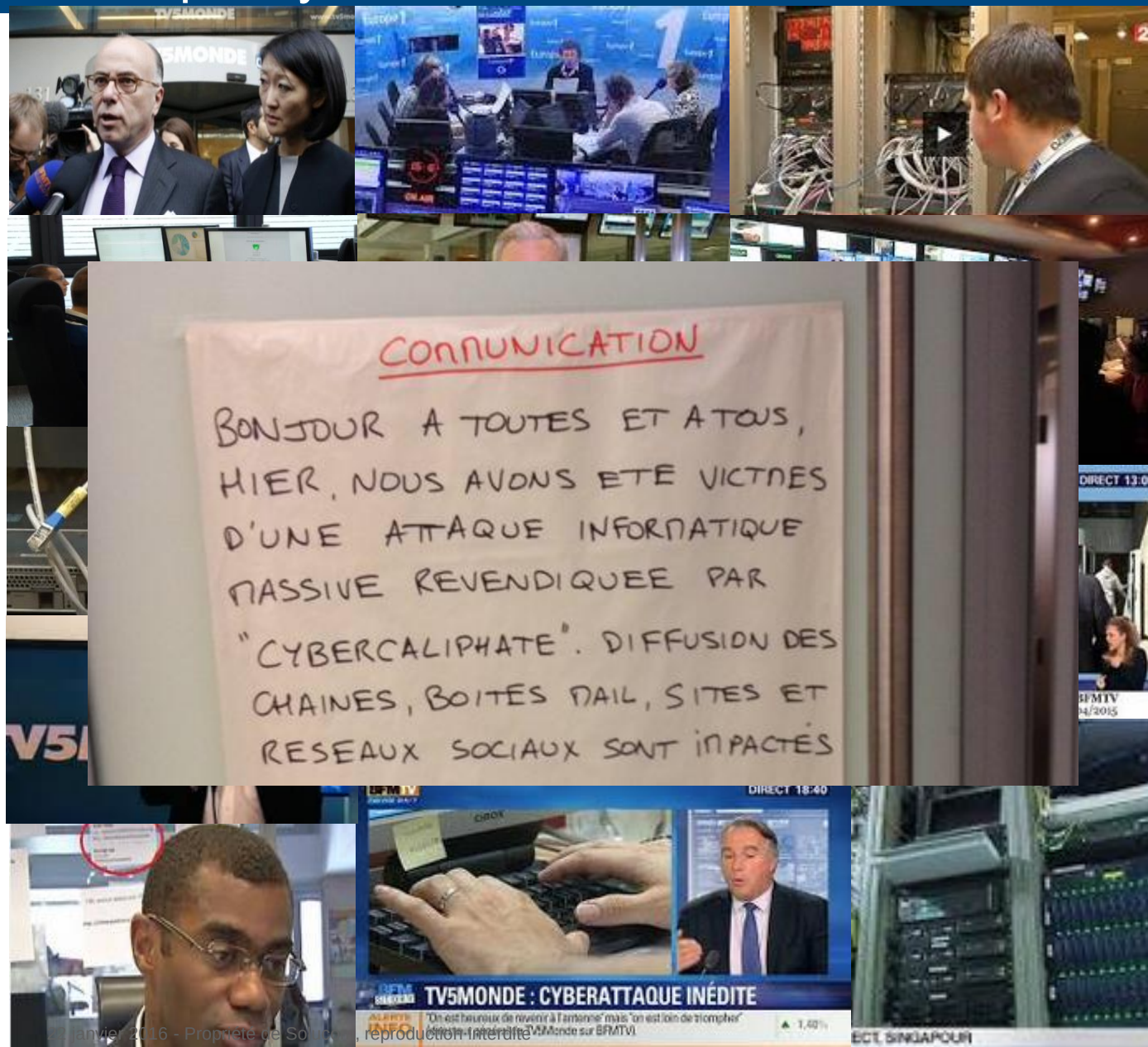
L’incroyable attaque de Sony Pictures… Barack Obama s’en mêle !

**Le 25 décembre, « The Interview » sort en salle et en ligne, il rapporte plus de 40 M$** (pour un budget de 44 M$+10 de marketing)

Destruction, oui mais encore ?

L’attaque de TV5 Monde : une paralysie totale de la chaîne

Dans la nuit du 08/04/2015 : paralysie pendant plusieurs heures de la diffusion des chaînes, du site Web et des réseaux sociaux de TV5



Destruction, oui mais encore ?

L'attaque de TV5 Monde : une paralysie totale de la chaîne

Dans la nuit du 08/04/2015 : paralysie pendant plusieurs heures de la diffusion des chaînes, du site Web et des réseaux sociaux de TV5

Une mobilisation au plus haut niveau

Un appui de l'ANSSI et une coordination sectorielle

Des mesures d'isolation radicale

Une communication de crise réactive et immédiate

Une maladresse de taille

Que retenir de ces attaques ?

Des contextes géopolitiques particuliers
➔ Tension avec la Corée du Nord, Daesh, au Moyen-Orient, Ukraine…

La limite des PCA classiques : de nouvelles méthodes pour limiter les conséquences des cyberattaques
➔ **Des sujets à traiter : exercice de crise & cyberrésilience**

Des attaques précédées de **phases d'apprentissage du SI** par les pirates

Si, si, les pirates savent apprendre !

Une capacité d'apprentissage souvent sous-estimée

Mais comment voulez-vous qu'un pirate comprenne ce processus, c'est trop spécifique !

Si, si, les pirates savent apprendre !

La capacité d'apprentissage des pirates : une réalité

Rappel des attaques de Sony Pictures et TV5 Monde :

1. Une première étape **d'intrusion dans le SI**
2. Une phase d'apprentissage de plusieurs semaines pour **identifier les infrastructures critiques et leurs fonctionnements**
3. Le **lancement de l'attaque** mettant à profit les connaissances spécifiques des pirates

Focus sur un exemple concret : l'attaque Anunak / Carbanak

Si, si, les pirates savent apprendre !

Anunak/Carbanak : un cyber-casse bien préparé

Cible	Des **banques et institutions** financières
Mode opératoire	**Infiltration du réseau** de la banque par le malware Anunak/Carbanak, **recherche des systèmes métiers** utilisés pour gérer les distributeurs de billets et les transactions financières
Quand	Premiers « **cyber casse** » enregistrés début 2013, activité majoritaire à l'été 2014
Impacts	**Vol de plusieurs millions de dollars** à des **dizaines de banques** et **institutions financières** (perte entre 2,5 et 10 millions US$ par institution)

Une enquête internationale toujours en cours pour suivre les traces du groupe Anunak/Carbanak

Anunak/Carbanak : un cyber-casse bien préparé

Reconnaissance

- **Ingénierie sociale** pour cibler les employés
- **Espionnage des conversations** afin de créer des messages personnalisés

Intrusion du malware

- **Spear phishing :** envoi de mails apparaissant comme provenant de collègues et contenant le malware **via des pièces jointes « Office »**
- **Utilisation de botnets** ayant déjà infectés la cible

Propagation et gain en privilège

- Exploitation de vulnérabilités et installation de **backdoor**
- Reconnaissance manuelle des réseaux des victimes
- Modification des configurations de **filtrage réseaux**

Accès aux données convoitées

- Utilisation de différents outils **(lateral movement tools)** pour accéder au système critique
- Installation de logiciels (dont d'administration)

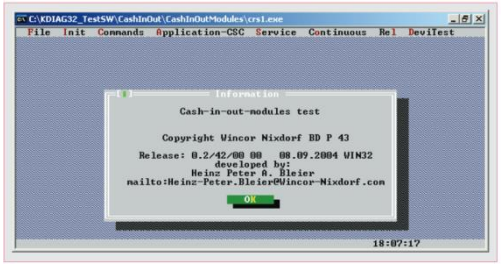
Collecte des informations

- **Enregistrement vidéo** des activités des employés de banques
- **Apprentissage des processus internes pour imiter le personnel** (enregistrement de toutes les étapes nécessaires et les codes d'accès des employés pour accéder aux fonctions de virements bancaires)

Actions frauduleuses

- **Vol via les distributeurs de monnaie (52 compromis) à des heures précises avec des complices sur place**
- **Modifications directes des bases de données (**soldes, plafonds…)
- **Transferts de fonds** vers des comptes bancaires variées et/ou étrangers en utilisant par exemple SWIFT

```
REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\
Wincor Nixdorf\ProTopas\CurrentVersion\LYNX-
PAR\CASH_DISPENSER" /v VALUE_4 /t REG_SZ
/d "5000" /f
```



Mais comment font-ils ?

En capturant puis **analysant les documents** présents sur les serveurs de fichiers ou encore sur l'intranet

Ils apprennent comme tout le monde…

En déployant des malwares sur les postes pour enregistrer des **captures d'écran** voir des films

Concrétiser ce risque et ne pas accuser à tort les équipes internes !

Et si pendant une gestion de crise, on vous dit…

“Il connait les processus métiers, c’est forcément quelqu’un de chez nous qui attaque !”

N’hésitez pas à répondre…

“En combien de temps les collaborateurs sont-ils formés ? Et depuis combien de temps dure l’attaque ?”

Et pour le futur…

Pourquoi la cybercriminalité est-elle en forte croissance ?

04 CIBLES DE + EN + NOMBREUSES

- Transformation numérique des entreprises
- Déploiement large des technologies dans le grand public

03 EXPERTISE ACCESSIBLE

- Compétences largement disponibles
- Marché noir des outils d'attaques
- Structuration mafieuse

02 RISQUES FAIBLES

- Anonymisation / absence de traces
- Réponse judiciaire complexe

01 GAINS IMPORTANTS

- Revenue de données CB : 3 à 50$
- Revente de données personnelles : 0,3 à 2$
- Fraudes métiers / espionnage : millions de $

Une menace de plus en plus présente au quotidien

Phishing

60 %

des mails échangés dans le monde

Source : Kaspersky Lab's Q1 2015 analysis

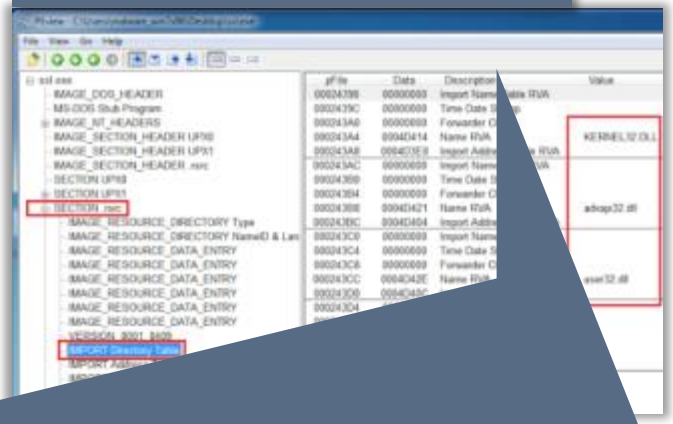
Ransomware

30%

nombre de DSI ayant déjà dû gérer un attaque par un ransomware

Source : Webroot, 2015

Malwares bancaires



x 5

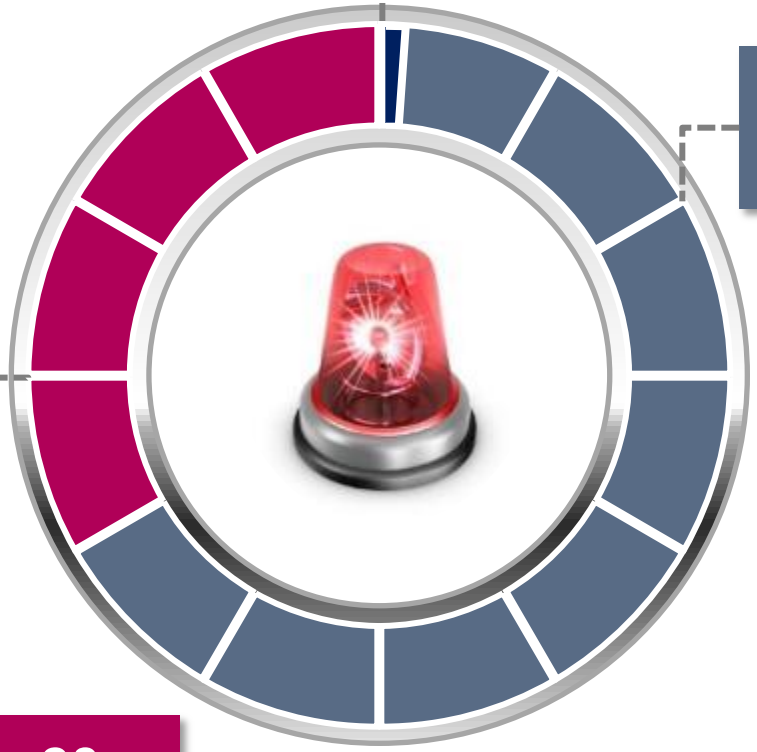
augmentation du nombre malwares bancaires enregistrés en un an

Source : Crédit Agricole, 2015

Une menace avec laquelle il faut apprendre à vivre et à se préparer

c'est la durée qu'il faut à 84 % des attaques pour **réussir**

1 jour



205 jours

c'est la durée moyenne pour **détecter** une attaque ciblée

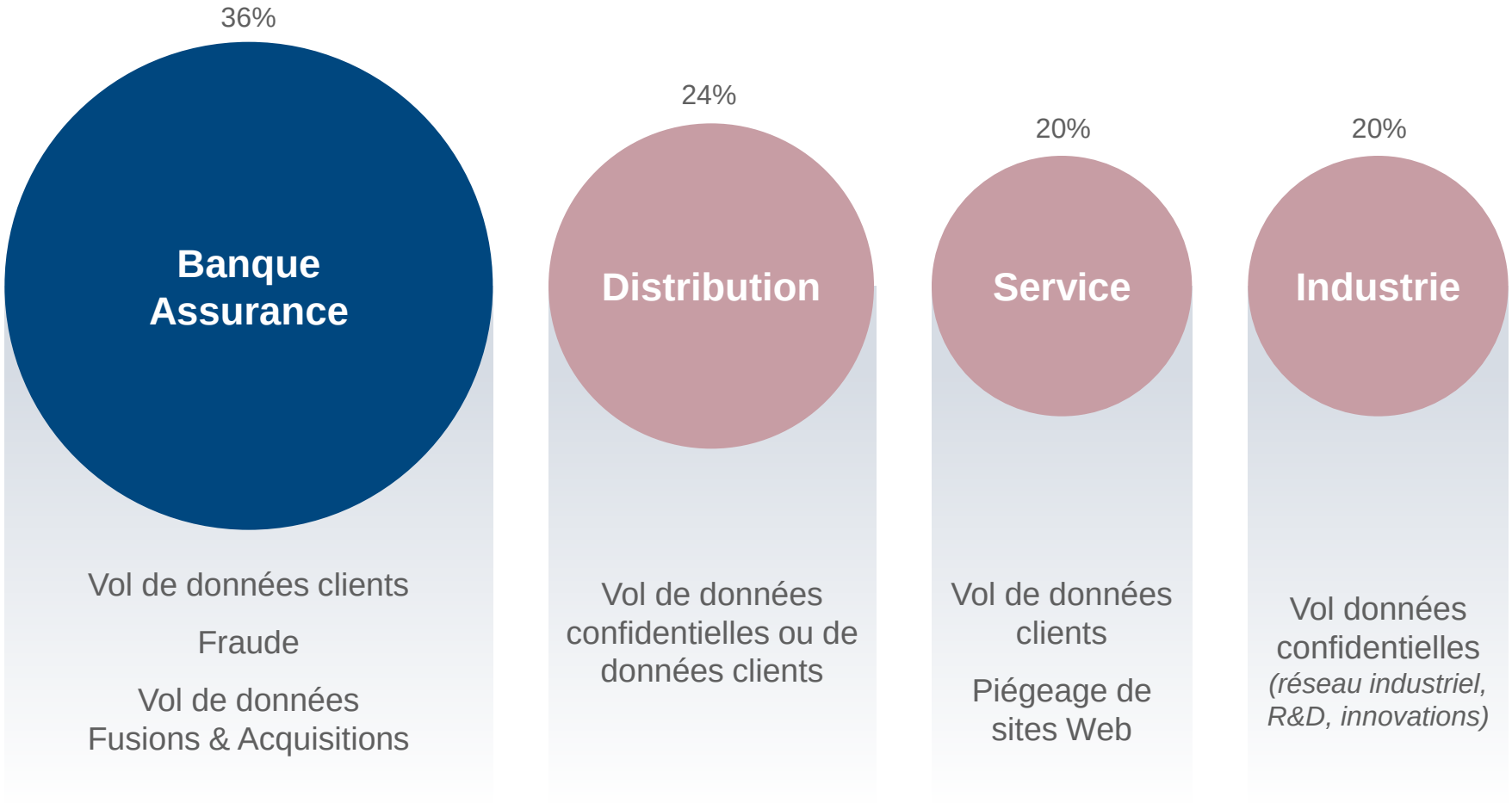
31 %

des attaques **décelées en interne**

c'est la délai moyen pour **reconstruire** un SI après une attaque ciblée

90 jours

Tous les secteurs sont touchés !



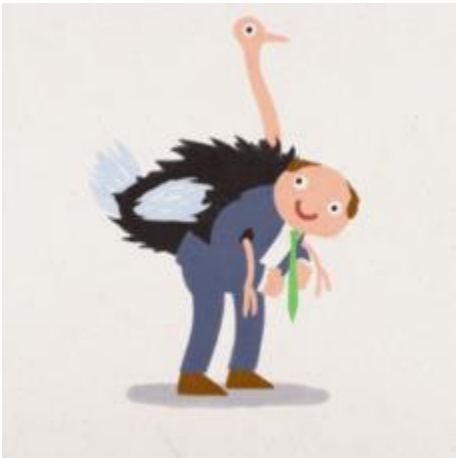
Source : Verizon 2013

Changer d’attitude vis-à-vis de la cybersécurité !

« C’est une problématique technique »

« Je suis unbreakable »

« Trop compliqué ! »



« Cela n’arrive qu’aux autres »

Comprendre les motivations des attaquants

Idéologie

- Interruption de service
- Messages idéologiques
- Divulgation

Gains financiers

- Vols de données stratégiques et de secrets industriels
- Vols de cartes de crédit
- Vols de données personnelles

Déstabilisation

- Destruction logique et/ou physique
- Vols de données stratégiques

Obtention de capacité d'attaques

- Vols de mécanismes d'authentification / certificats
- Vols de code source
- Écoute de données

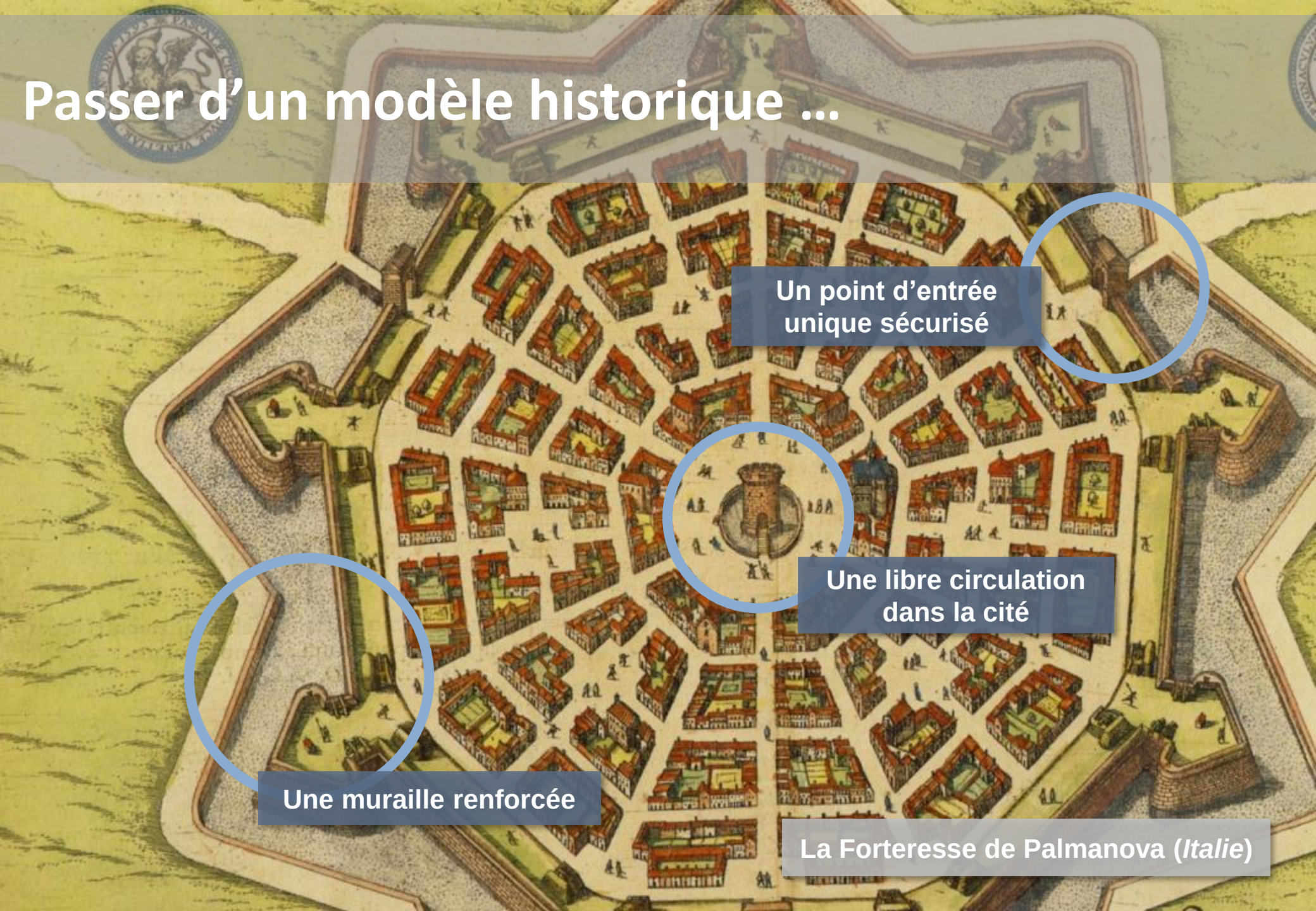
Répondre suivant 3 piliers

PROTEGER

DETECTER
REAGIR

RESPONSABILISER

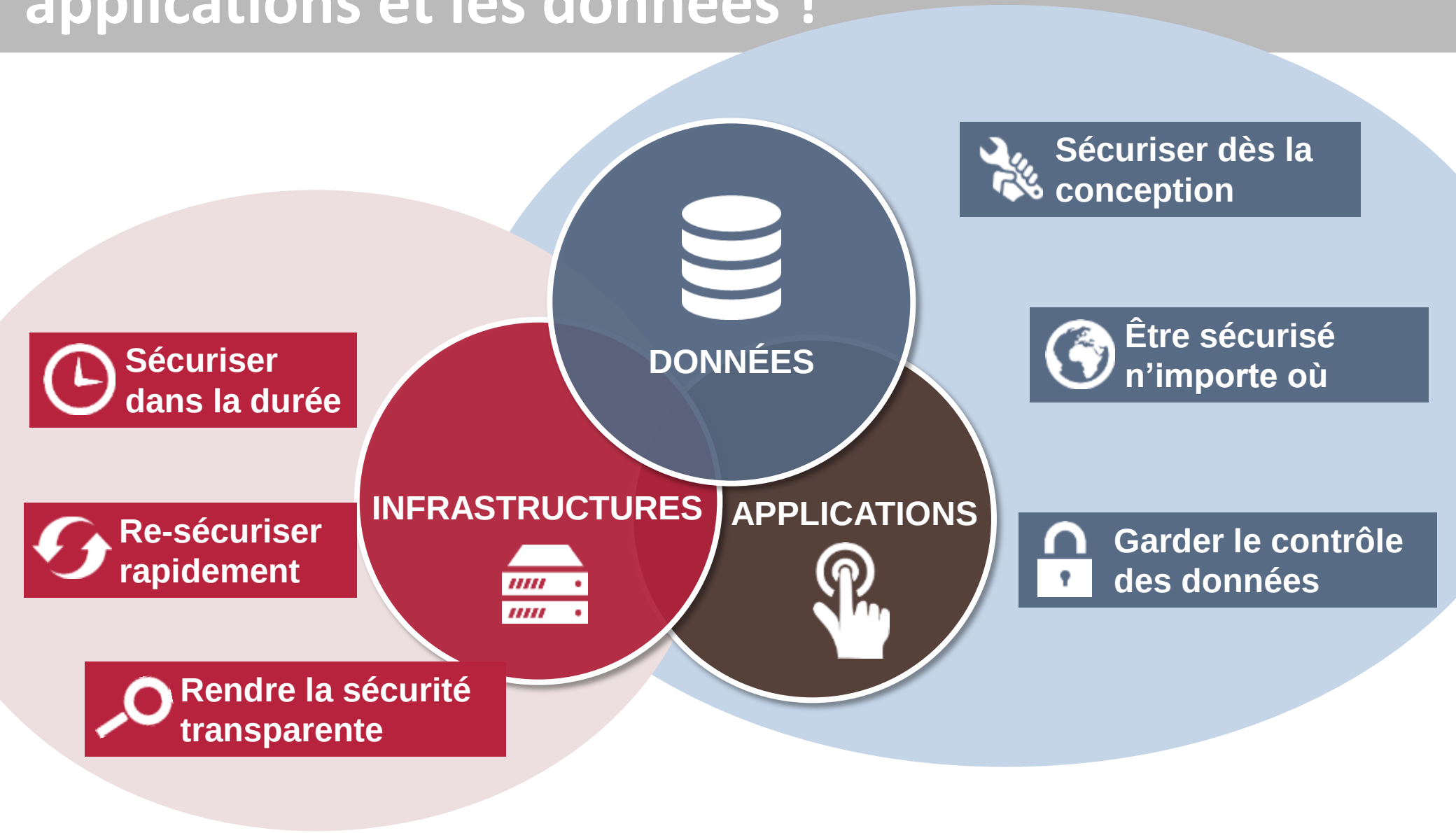
Passer d’un modèle historique …



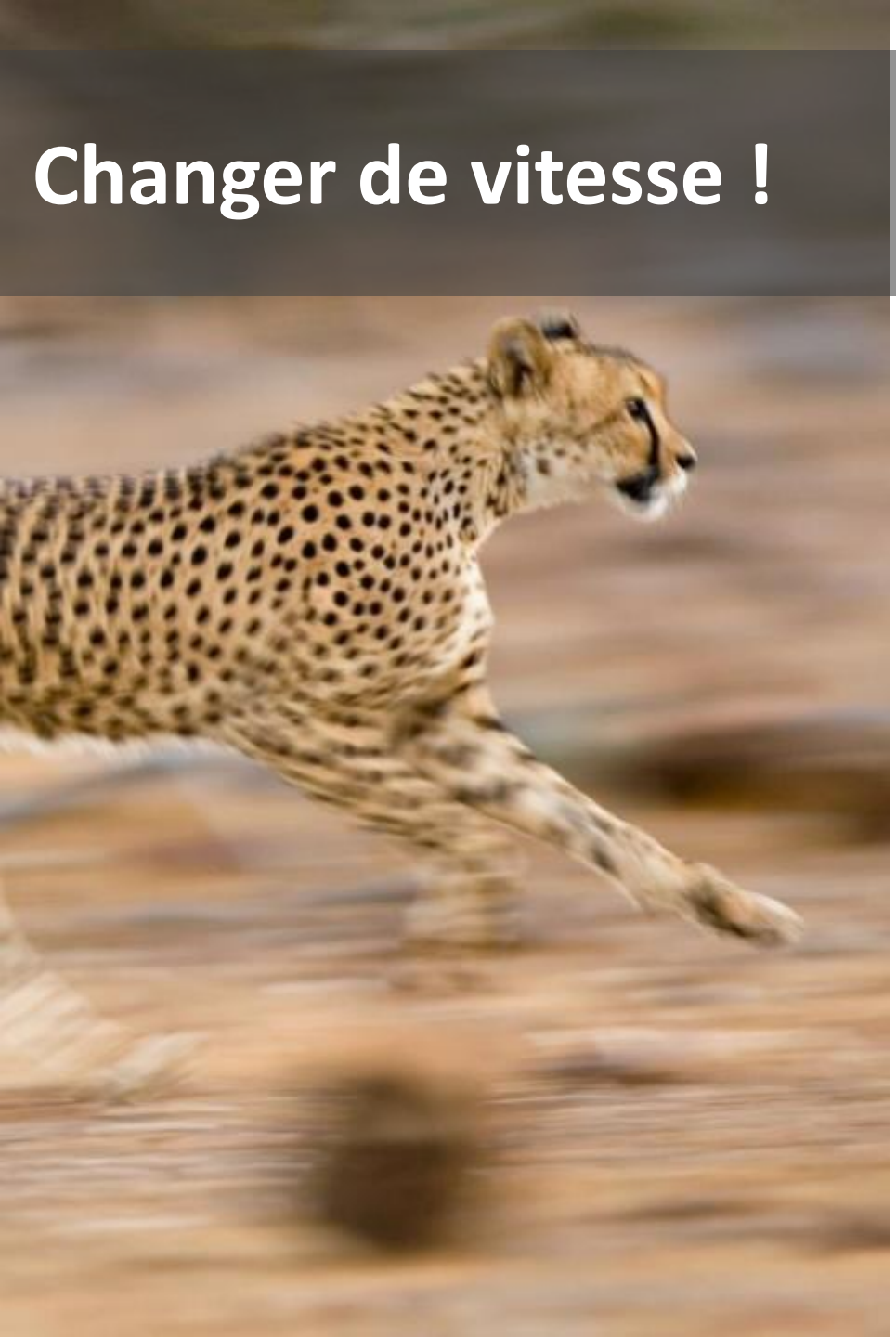
La Forteresse de Palmanova (*Italie*)

… à un nouveau modèle

Protéger les infrastructures… mais surtout les applications et les données !



Changer de vitesse !



TO DO LIST

- ❑ Organiser un **exercice de crise cyber** chaque année
- ❑ Mener un **audit réellement intrusif « read team »**
- ❑ Étudier la **cyberassurance**
- ❑ Construire son **SOC** & **CERT**
- ❑ Revoir les **points d'accès Internet**
- ❑ Revoir la protection des **données critiques**

Cybercriminalité : s'organiser et s'entraîner

Frédéric GOUX
Partner cabinet Solucom
Frederic.GOUX@solucom.fr

Salma BENNANI
Responsable Solucom Maroc
Salma.BENNANI@solucom.fr

SECURITYINSIDER
Le blog des experts sécurité Solucom

@secuinsider

www.securityinsider-solucom.fr