CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Retour d'expérience : convergence sécurité physique / sécurité de l'information

1. Contexte et enjeux
2. Méthodologie de déploiement et acteurs
3. Bilan du projet
4. Conclusion
5. Annexes

Damien CHAMINADE, expert indépendant sûreté/sécurité

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Retour d'expérience : convergence sécurité physique / sécurité de l'information

1. Contexte et enjeux
2. Méthodologie de déploiement et acteurs
3. Bilan du projet
4. Conclusion
5. Annexes

Damien CHAMINADE, expert indépendant sûreté/sécurité

Un contexte initial complexe…

Un groupe de 20 000 salariés…

Nombre important d'incidents
Vols, vandalisme, espionnage, intrusions, agressions, fraudes…

110 sites
R&D, usines, entrepôts, bureaux

… avec des enjeux Business forts

Projets R&D sensibles
Prototypes, bancs d'essai…

Fabrication de produits innovants
Savoir-faire industriel

Marché dynamique
Croissance externe, concurrence

Où les mesures de protection sont perfectibles…

Disposition des locaux et gestion des flux (véhicules, piétons), accès…

Gardiennage des sites

Déploiement non sécurisé des outils : vidéo, contrôle d'accès par badge…

15% des sites avec vidéo et/ou contrôle d'accès, 6 éditeurs différents, accès non autorisé aux outils…

… comme la gouvernance de la protection de l'information

Besoin de renforcer le pilotage global…

… de définir une architecture logicielle sécurisée…

… et de mieux appréhender la réglementation (ex. CNILen France)

=> renforcement de la Direction Sûreté et de la Direction de la Sécurité Informatique

… permettant de dégager 3 enjeux et 3 objectifs majeurs

Enjeux

- Le **coût des incidents** doit être réduit
- Les **informations et actifs sensibles** mieux protégées
- Les **synergies Business encouragées**

Objectifs

- La **sécurité physique** doit être renforcée sur les 110 sites
  - Via une architecture centralisée de contrôle d'accès par badge, de vidéo-protection et de détection d'intrusion
- La **sécurité logique** de la nouvelle architecture ne doit pas constituer un risque supplémentaire
  - Vigilance particulière sur la confidentialité, la disponibilité, l'intégrité, mais aussi la conformité à la réglementation
- Les **résidents** (salariés, visiteurs) doivent être **sensibilisés** sur les risques et les enjeux (incident = perte de chiffre d'affaires, voire menace sur l'emploi)

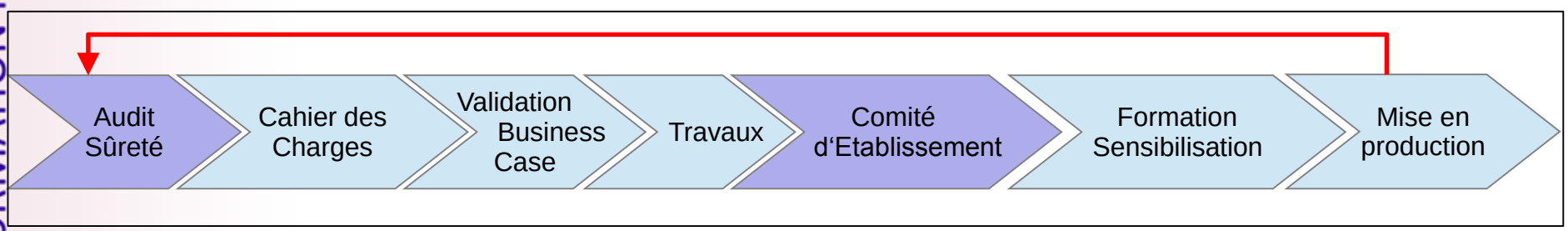
CLUSIF

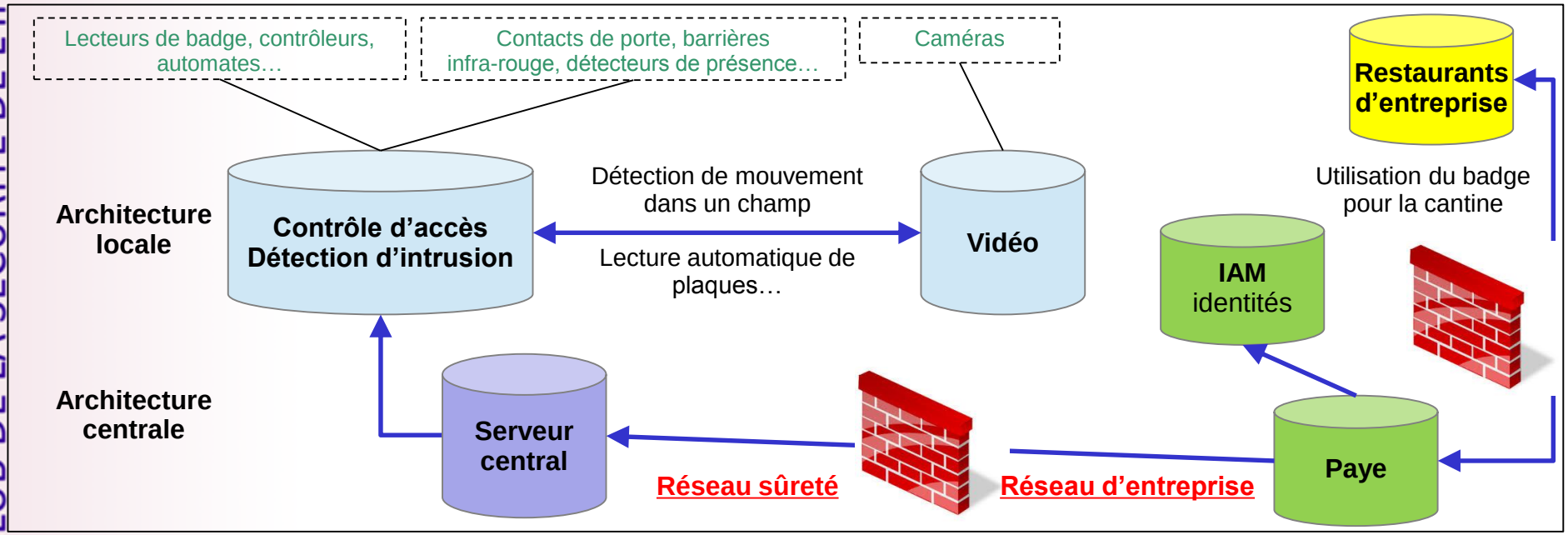
Retour d'expérience : convergence sécurité physique / sécurité de l'information

1. Contexte et enjeux
2. Méthodologie de déploiement et acteurs
3. Bilan du projet
4. Conclusion
5. Annexes

Damien CHAMINADE, expert indépendant sûreté/sécurité

Une méthodologie projets et une architecture sont définies, puis déployées…





… faisant intervenir de multiples acteurs internes et externes à l'entreprise

ACTEURS INTERNES

Direction Sûreté

- **Pôle audits, projets, investigations**
- **Pôle Exploitation & Maintenance**

Directions d'Etablissement => 110
(Usines, centres R&D, sites tertiaires, entrepôts)

- **Salariés**
- **CE et CHSCT d'Etablissement**
- **Agents de gardiennage, hôtesses d'accueil, télésurveilleurs**

Direction de la Sécurité Informatique

Correspondant CNIL

ACTEURS EXTERNES

Intégrateurs de solutions vidéo, contrôle d'accès et détection intrusion

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Retour d'expérience : convergence sécurité physique / sécurité de l'information

1. Contexte et enjeux
2. Méthodologie de déploiement et acteurs
3. Bilan du projet
4. Conclusion
5. Annexes

Damien CHAMINADE, expert indépendant sûreté/sécurité

Les objectifs sont atteints , au-delà des espérances

Sûreté renforcée => déploiement sur 90% des sites

- Réduction du nombre des incidents (-70%), vidéo = dissuasion
- Analyse post incident facilitée :~ 80% résolution
- Reporting centralisé
- Renforcement de la communauté des experts sûreté – outils et processus communs
- Couplage avec les logiciels d'armoires à clefs

Architecture sécurisée

- Mise à niveau aux standards sécurité IT du groupe
- Réseau distinct => optimisation de la bande passante (MAN)
- Sécurité physique des locaux informatiques renforcée

Efficacité accrue de la politique de sécurité globale

Ressources humaines

- Visites inter sites facilitées
- Gestion automatique des départs / arrivées – interface avec la paye : < 5% d'anomalies (One GoodBye)
- Badge unique déployé en 2 ans - sentiment accru d'appartenance à l'entreprise

Coûts réduits

- Réduction des coûts de maintenance (-40%)
- Réduction du coût des incidents (-95% sur certains sites)
- Réduction des primes d'assurances (~ M€)
- Réduction des impressions
- Réduction des notes de frais (cantine)

Facility management optimisé

- Réduction des coûts de climatisation et optimisation de l'occupation des salles de réunion – géolocalisation anonyme du support de badge

Conformité réalisée

- 100% de conformité
- Implication des représentants du personnel (définition des besoins)
- Centralisation des demandes d'extractions => réduction du risque

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Retour d'expérience : convergence sécurité physique / sécurité de l'information

1. Contexte et enjeux
2. Méthodologie de déploiement et acteurs
3. Bilan du projet
4. Conclusion
5. Annexes

Damien CHAMINADE, expert indépendant sûreté/sécurité

La convergence est effective entre sécurité physique et sécurité de l'information… et donc?

- La convergence a permis *in fine* de **réduire considérablement les risques de malveillance,** avec un **Retour sur Investissement rapide**
- Toutefois, elle a créé de **nouveaux risques**, la règlementation française exigeant par exemple de désactiver le contrôle d'accès en cas d'alerte incendie avérée!
- N'oublions pas non plus la **composante humaine** : 1 salarié correctement sensibilisé est plus efficace qu'une caméra et un lecteur de badge réunis
- Enfin, pas de déploiement efficace sans une **gouvernance centralisée** ou *a minima* une **attention sur l'adhésion** (top management, utilisateurs, salariés…), surtout dans un contexte matriciel

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Retour d'expérience : convergence sécurité physique / sécurité de l'information

1. Contexte et enjeux
2. Méthodologie de déploiement et acteurs
3. Bilan du projet
4. Conclusion
5. Annexes

Damien CHAMINADE, expert indépendant sûreté/sécurité

Rappels sur les exigences réglementaires

- 3 obligations majeures (parmi d'autres) – déploiement vidéo
  - ***consulter* les représentants des salariés** (Comité d'Établissement)
  - faire une **déclaration à la CNIL** (déploiement vidéo) et **en préfecture**
- Risques particuliers
  - **finalités des demandes d'extraction de données personnelles** (ex. historique d'utilisation d'un badge)

Textes applicables

- *Loi relative à l'informatique, aux fichiers et aux libertés,* n°78-17 consolidée en 2010
- *Loi d'orientation et de programmation pour la sécurité*, n°95-73 modifiée en 2009, article 10
- Circulaire INTD9600124C (vidéosurveillance)
- Décret n°96-926 (vidéoprotection)

Quelques exemples de prise en compte de la sécurité logique

Infrastructure	• **Mise en place d'un réseau dédié – distinct du MAN** • **Gestion spécifique des flux vidéo** • **Administration via SNMP**
Réseau	• **Cryptage des données (interfaces, flux vidéo)** • **Suppression des mots de passe dans les scripts** • **Modification des mots de passe éditeur** • **Génération et analyse des logs, notamment en cas de détournement de finalité de l'utilisation de la vidéo**
Sécurité des données	• **Refonte de l'architecture de réplication et de sauvegarde**
Continuité d'activité	• **Suppression des protocoles faibles : ftp, telnet…**
Gestion de parc	• **Mise en place d'une gestion par parc pour les mises à jour (anti-virus, migrations logicielles, changement de version de systèmes d'exploitation…)** • **Sécurisation des locaux (baies…) et des équipements (caméras, automates…)** • **Accès aux salles informatiques par badge, surveillance vidéo** • **Installation de contacts de porte et détecteurs de présence**