

CNAM-TS

Direction des Systèmes d'Information
Département Infrastructure, Réseaux et Sécurité



Constitution et mise en place d'une équipe sécurité

La CNAM-TS en quelques chiffres

- 70 % des remboursements maladie des assurés sociaux
- + de 120 Milliards € de remboursements / an

- 150 Organismes juridiquement indépendants (CTIR, CPAM, CGSS, URCAM, UGECAM...)
- 1700 sites géographiques
- 90 000 postes de travail
- 2000 serveurs Windows
- 200 serveurs Unix

Département Infrastructure, Réseaux et Sécurité

- Conception et mise à disposition des infrastructures mutualisées (dns, annuaire, messagerie...)
- Centre National de Gestion du Réseau (exploitation des « tuyaux », dns, pare-feux, proxy)
- Conception des infrastructures et outils nécessaire à la sécurité

Pourquoi une équipe dédiée Sécurité ?

- La gestion de la sécurité est répartie
 - ✓ Le Réseau
 - ✓ Le Bureau d'Etudes
 - ✓ Les Centres de Traitements Informatiques Régionaux
 - ✓ Les Organismes de bases

- Multiples interlocuteurs

- Pas de tableaux de bord généraux

Objectifs

- Disposer d'un pôle d'expertise reconnu
 - ✓ Intégration dans les applications
 - ✓ AntiVirus / AntiSpam
 - ✓ Durcissement des Systèmes
 - ✓ Évaluation des vulnérabilités

- Fédérer les actions liées à la sécurité

- Mettre en place des outils de reporting de la sécurité

Sécurité Applicative

- ✓ Réponse aux dossiers sécurité
- ✓ Respect des exigences du S.D.S. pendant cycle de vie des projets
- ✓ Intégration des différents outils dans l'infrastructure applicative
- ✓ Mise en œuvre politique d'identification / authentification pour l'accès sécurisé aux applications



Experts « solutions » pour le développement

La Sécurité à la CNAM-TS

Sécurité Applicative

- ✓ Réponse aux dossiers sécurité
- ✓ Respect des exigences du S.D.S. pendant cycle de vie des projets
- ✓ Intégration des différents outils dans l'infrastructure applicative
- ✓ Mise en œuvre politique d'identification / authentification pour l'accès sécurisé aux applications



Experts « solutions » pour le développement

Sécurité Infrastructure

- ✓ Responsabilité globale de la sécurité de l'infrastructure
- ✓ Validation des solutions de sécurité
- ✓ Conception et évolution des outils spécifiques A.M. (IGC, transfert sécurisé, anonymisation, ...)
- ✓ MOE des outils des serveurs et postes de travail



Experts « solution sécurité - infrastructure »

Animation des RSSI

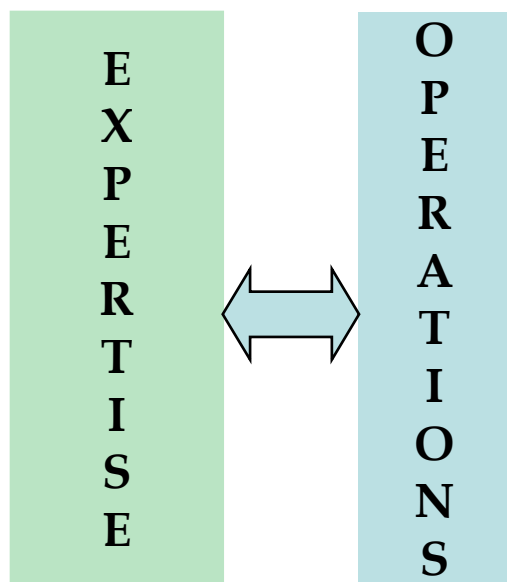
Animation des RSSI

E
X
P
E
R
T
I
S
E

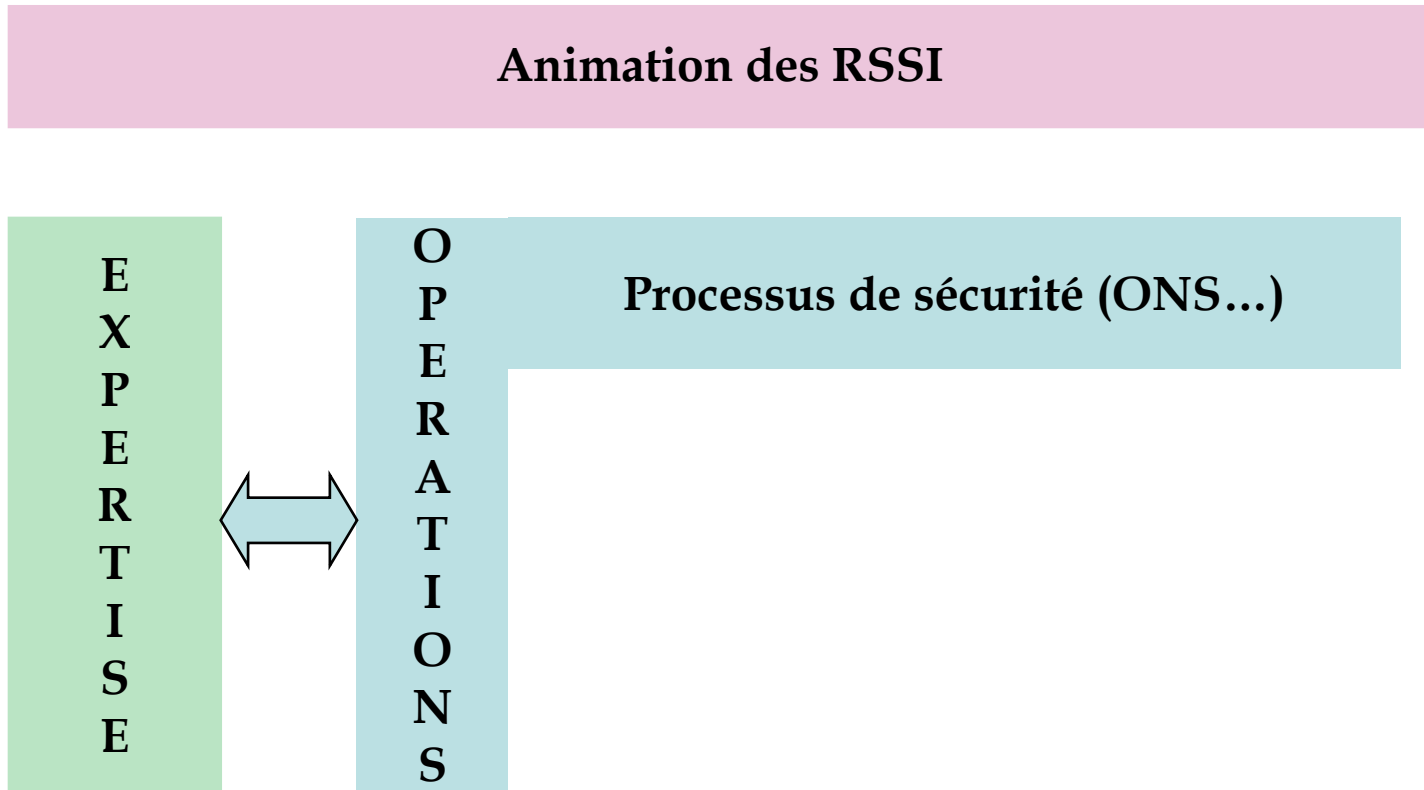
Conception de produits
propres à l'AM : IGC,
anonymisation, transfert
sécurisé...

Sécurité des Infrastructures

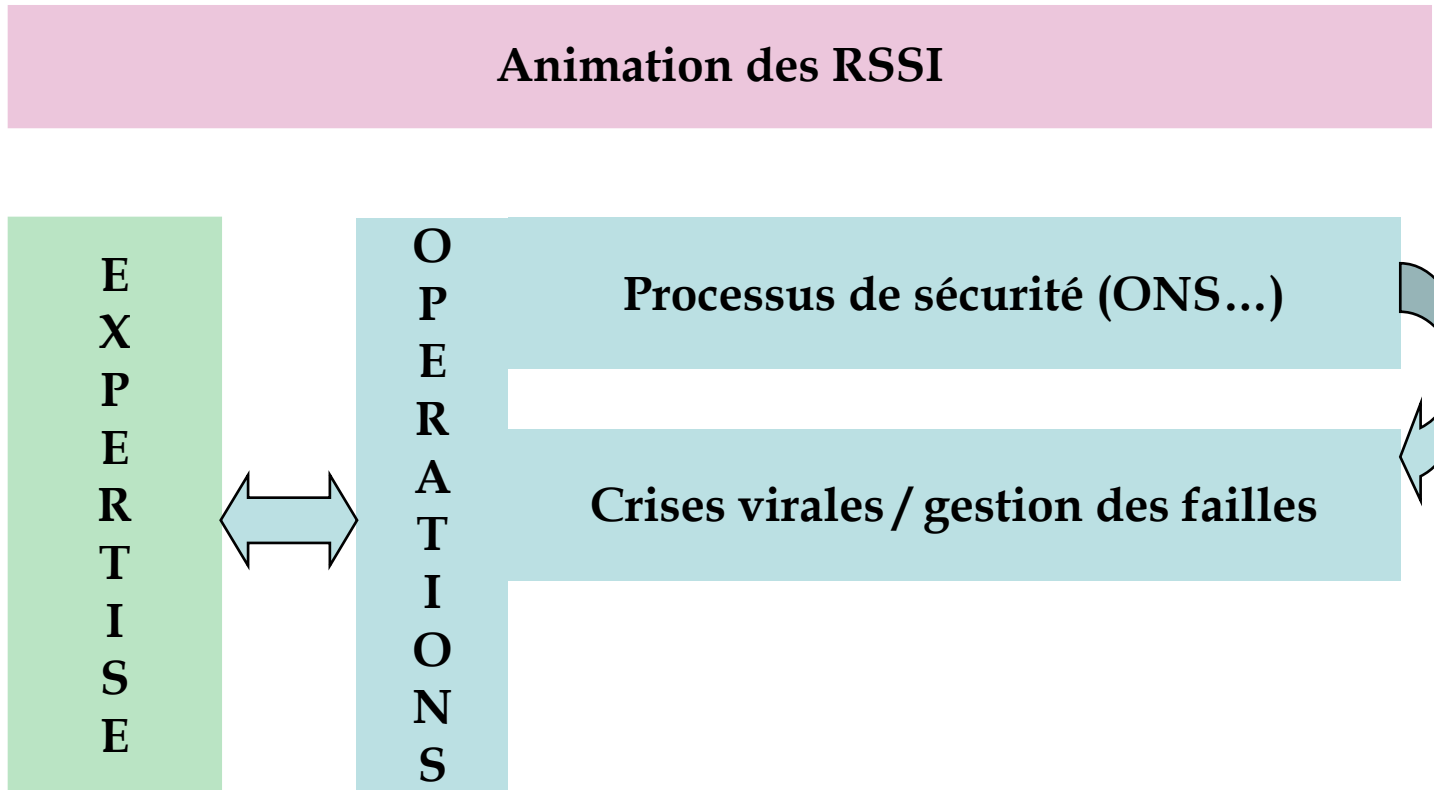
Animation des RSSI



Sécurité des Infrastructures

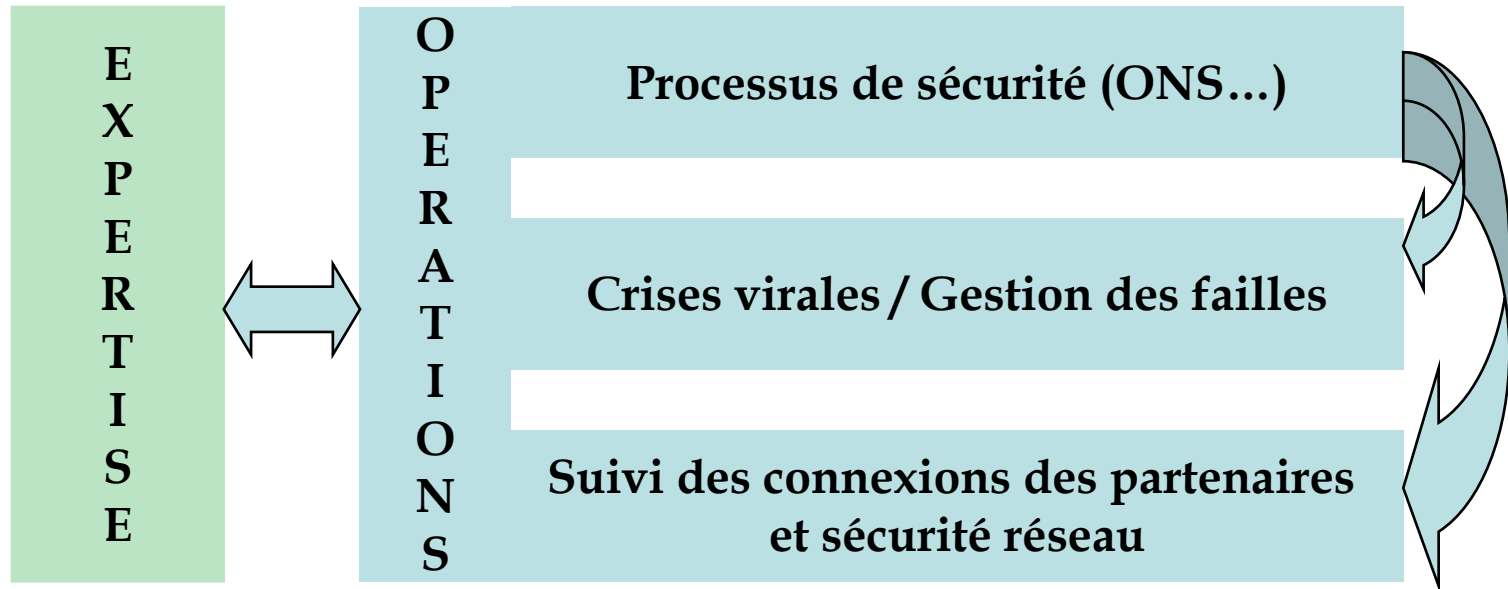


Sécurité des Infrastructures



Sécurité des Infrastructures

Animation des RSSI



La formation d'experts sécurité

- Largeur du scope de formation !
 - ✓ Administration
 - ✓ Réseau
 - ✓ Sécurité
 - ✓ Méthode
 - ✓ Développement

- Difficile de trouver le bon compromis en fonction du profil

La formation d'experts sécurité

- Difficile de trouver aussi le bon dosage entre théorie et pratique
- Effort constant, qui peut être partiellement comblé par de la veille technologique

La veille technologique

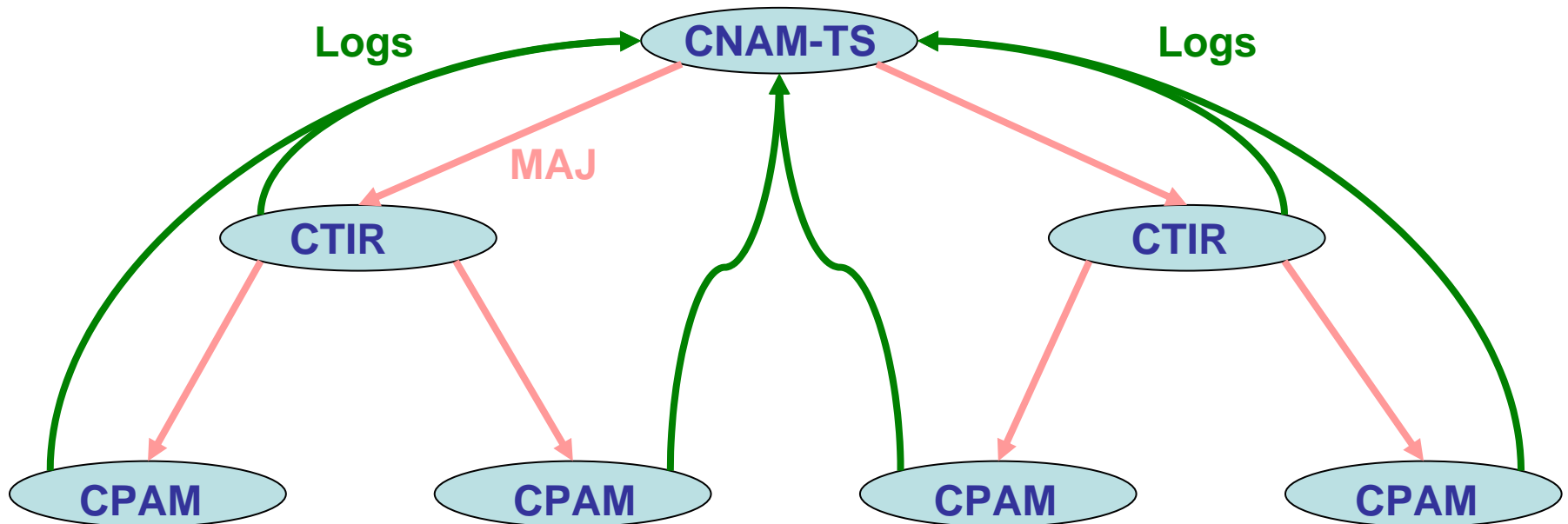
- C'est coûteux et il y a peu ou pas de retour sur investissement visible
- Mais indispensable => ne pas l'oublier dans les plans de charge !
- Interne ou externalisée ?
 - ✓ Nouveaux produits
 - ✓ Vulnérabilités

La veille technologique - Vulnérabilités

- Facilement externalisable
- Ne pas céder à la folie du patch systématique
- Nécessite donc une cellule pour évaluer les risques en interne

Les premiers résultats - AntiVirus

- Centralisation des mises à jour
- Centralisation des alertes



Les premiers résultats - ONS

- Définition des circuits d'alimentation
 - ✓ Quels évènements ?
 - ✓ Remontés par qui ?

- Définition des circuits d'action
 - Qui alerter ?
 - Vers qui escalader ?

- Rédaction du cahier des charges en cours

Les premiers résultats – Vulnérabilités

- Qualification de la gravité de la vulnérabilité par l'équipe sécurité



- Transfert au BE pour étude d'application du patch



- Qualification / diffusion par le CNQD

Les premiers résultats – Authentification LDAP

- Coupler un annuaire LDAP avec le système AccessMaster
- Permettre aux applications clients légers d'utiliser les standards
- Sortir progressivement du client/serveur
- Maquette en cours de réalisation.

Les futurs projet

- Refonte du système d'identification / authentification
- Migrer les technologies internes vers les standards
- Mise en place de proxy de sécurité pour interopérabilité avec les autres régimes

Constitution d'une équipe dédiée sécurité

- Travail de longue alène
- Bien évaluer les besoins en formation
- Impliquer tous les acteurs potentiels
- Prévoir les outils de reporting
- Ne pas négliger la veille technologique

Constitution d'une équipe dédiée sécurité

Des questions ?

Merci beaucoup...