FRC 2017
La cybersécurité opérationnelle

M. Jean-Marc MISERT

Socle de sécurité opérationnel et relation avec la production

La filière SI du groupe

Introduction

Répartition géographique et par branche des effectifs de la filière SI

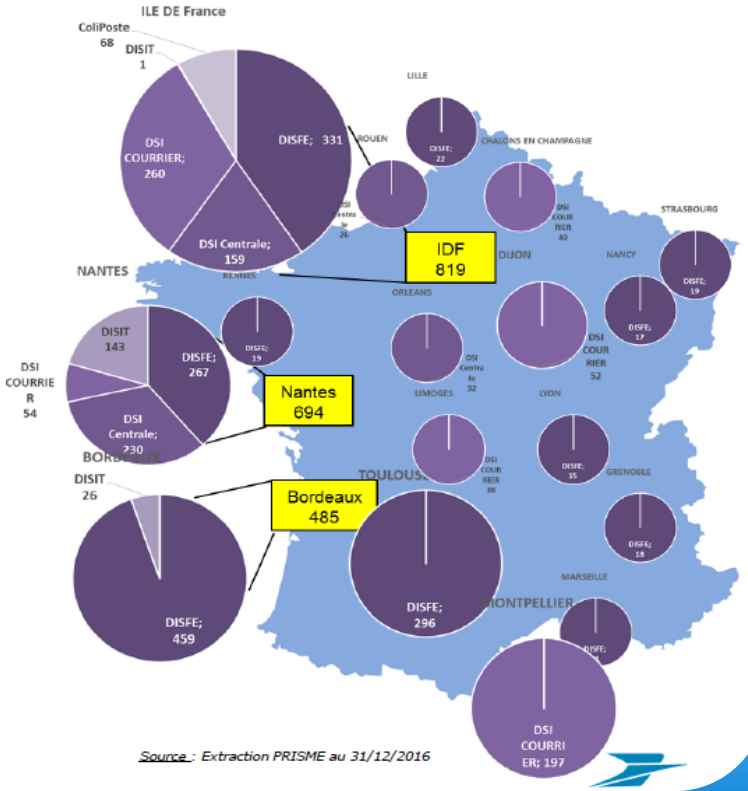
Répartition des effectifs par Branche

A fin décembre 2016, la filière SI du Groupe La Poste regroupait 4 436 EUTC

Effectifs à fin décembre 2016 par Branche (en EUTC)	
DSEM	1146
DISFE	1676
DSI BSCC	892
GROUPE (*)	672
Numérique	50
TOTAL Groupe	**4436**

(*) DSI Centrale, DISIT, DSI Groupe

Répartition des effectifs hors DSEM



Source : Extraction PRISME au 31/12/2016

Zoom sur le département sécurité de la production informatique

Nos missions :

- Garantir la sécurité opérationnelle : prévention, détection, réaction
- Garantir la continuité des SI

Quelques unes de nos contraintes

- Lois et règlements : LPM, NIS, RGPD, Bâle 3, ..
- La PSSI du groupe, de la banque
- L'effet volume
- La variété technologique
- Les compétences à maintenir ou développer

Mais surtout

- La production doit « tourner »

On fait comment ? Illustration avec quelques cas d'usage

- En phase de construction
  - Comment maintenir à jour la PSSI ?
  - Comment intégrer la sécurité dans les projets ?
- En phase récurrente
  - Comment surveiller nos SI et réagir ?
  - Comment assurer une veille sur les vulnérabilités ?
  - Comment garantir le « MCS » ?

Comment maintenir à jour la PSSI ?

- Un process est appliqué
- Périodiquement les RSSI émettent des propositions de mises à jour
- Au sein de la DPI, **une dizaine** de référents sur nos activités clés sont sollicités

- Chacun doit estimer **l'impact et la faisabilité** des maj
- Une réunion de concertation aboutit sur une synthèse
- Le PLUS : une PSSI plus en prise avec la réalité du terrain, qui peut mieux s'appliquer **de bout en bout**.

Comment intégrer la sécurité dans les projets ?

- La sécurité est « fondue » dans la méthode de conduite de projets
- Les ADR sont systématiques, ceci est validé en comité (CVP)
- Lors des phases de conception, il est demandé aux CDP de nous fournir un fichier « SecuOp »

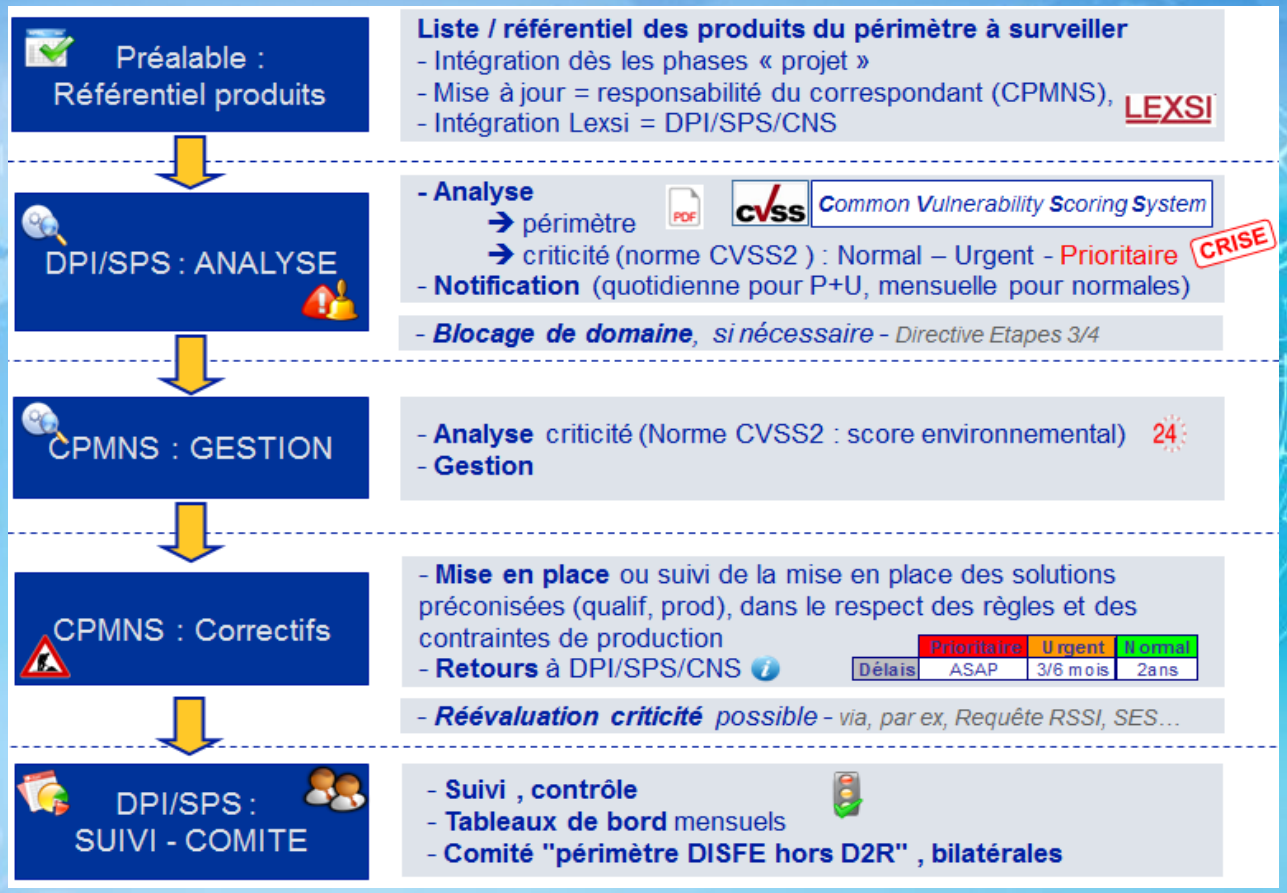
- Ce fichier nous permet de savoir lesquels de nos outils vont être mis en œuvre
- Le PLUS : **une vision de bout en bout** en assurant le lien entre exigences de sécurité et capacité à faire

Comment surveiller nos SI et réagir ?

- Nous disposons d'un CERT et SOC interne (24/7)
- Ce qu'il faut surveiller est défini dans la PSSI, et mis en œuvre par les architectes

- Chaque typologie d'alerte fait l'objet d'une « DTS »
- Une alerte est à minima un incident (ITIL) mais peut être un déclencheur de crise (cellule dédiée)
- Le PLUS : **le bout en bout** entre une description « littérale » dans la PSSI jusqu'aux actions précises de réaction(s)

Comment assurer une veille sur les vulnérabilités ?



Le PLUS : process **de bout en bout** de la déclaration d'un composant sur notre SI au suivi de ses mises à jour

Comment garantir le MCS ?

- La **double** problématique de base, avoir un niveau de sécurité de départ « conforme » **et** qui ne se dégrade pas dans le temps !
- Pour le niveau de sécurité de départ, chaque nouveau serveur voit l'affectation d'une tâche ITIL
- Pour les serveurs déjà en production : des campagnes de contrôles « massives » 4 fois par an.
- *Le PLUS : **le bout en bout** du contrôle sur l'ensemble du cycle de vie de l'équipement*

Conclusion et remerciements

Au **bout** de cette présentation, un message :

« raisonner de **BxxT en BxxT** »

Merci pour votre attention !