De l'utilisation de la supervision de sécurité en Cyber-Defense ?

Orange Business Services

Direction de la sécurité

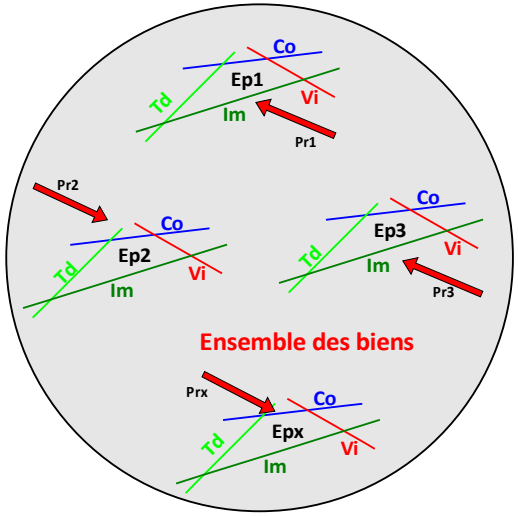
JSSI 2011
Stéphane Sciacco

Sommaire

Introduction

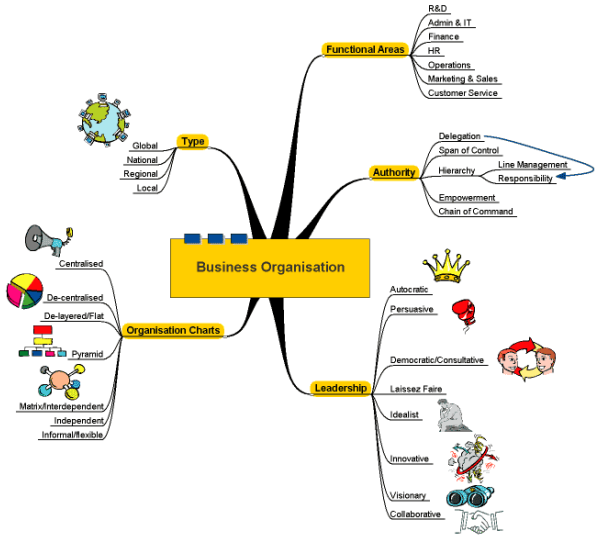
« Postulats de base »

- **Elément prioritaire à superviser**
  - Analyse de risque global sur l'ensemble des « actifs » d'une entreprise
    - définir ceux à superviser « **en priorité** »



- **Projet de supervision de sécurité intègre**
  - Une organisation humaine
  - Des processus métiers

- **En dernier des outils**
  - Exemple un SIEM
  - **Et pas l'inverse**



SOC c’est quoi ?

SOC = S(ecurity) O(perating) C(enter)

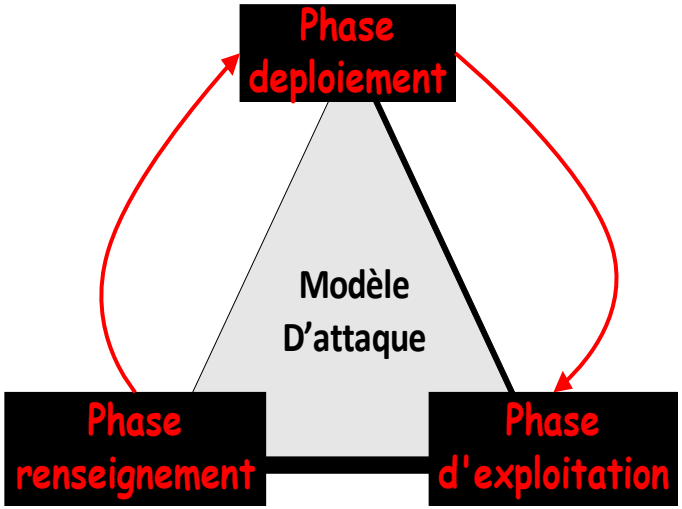
- **Ce n'est pas**
  - Un Call center
  - Des opérationnels qui réalisent des actions de corrections
  - Du monitoring technique
  - Un service d'archivage/reporting

- **C'est une équipe qui :**
  - Prend en compte une **expression de besoin** de supervision de sécurité
  - Met en mise en place des **solutions** de **détection**
  - D**étecte et qualifie** des événements de sécurité
  - Fournit des **plan de réaction**
  - **Intégrée** dans l'organisation sécurité d'une entreprise

Localisation de la supervision de sécurité

« Modèle d'attaque »

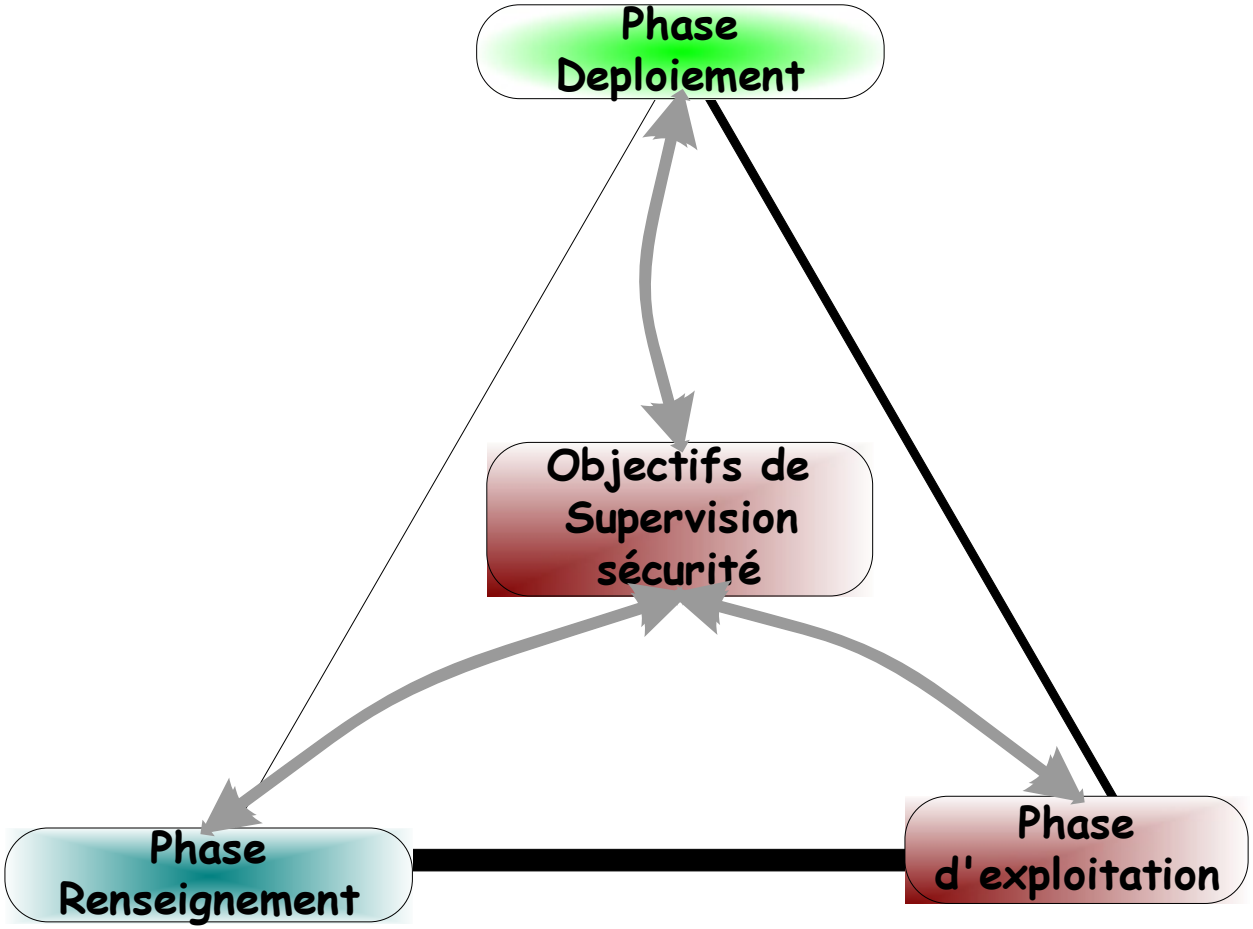
- **Simplification d'une attaque**
  - **Re =** phase de renseignement (découverte)
  - **De =** phase de déploiement/planification (intrusion)
  - **Ex =** phase d'exploitation (vol, Dysfonctionnement,…)



- **Modèle proposée d'attaque**
  - **Attaque** = Combinaison (**Re, De, Ex**)

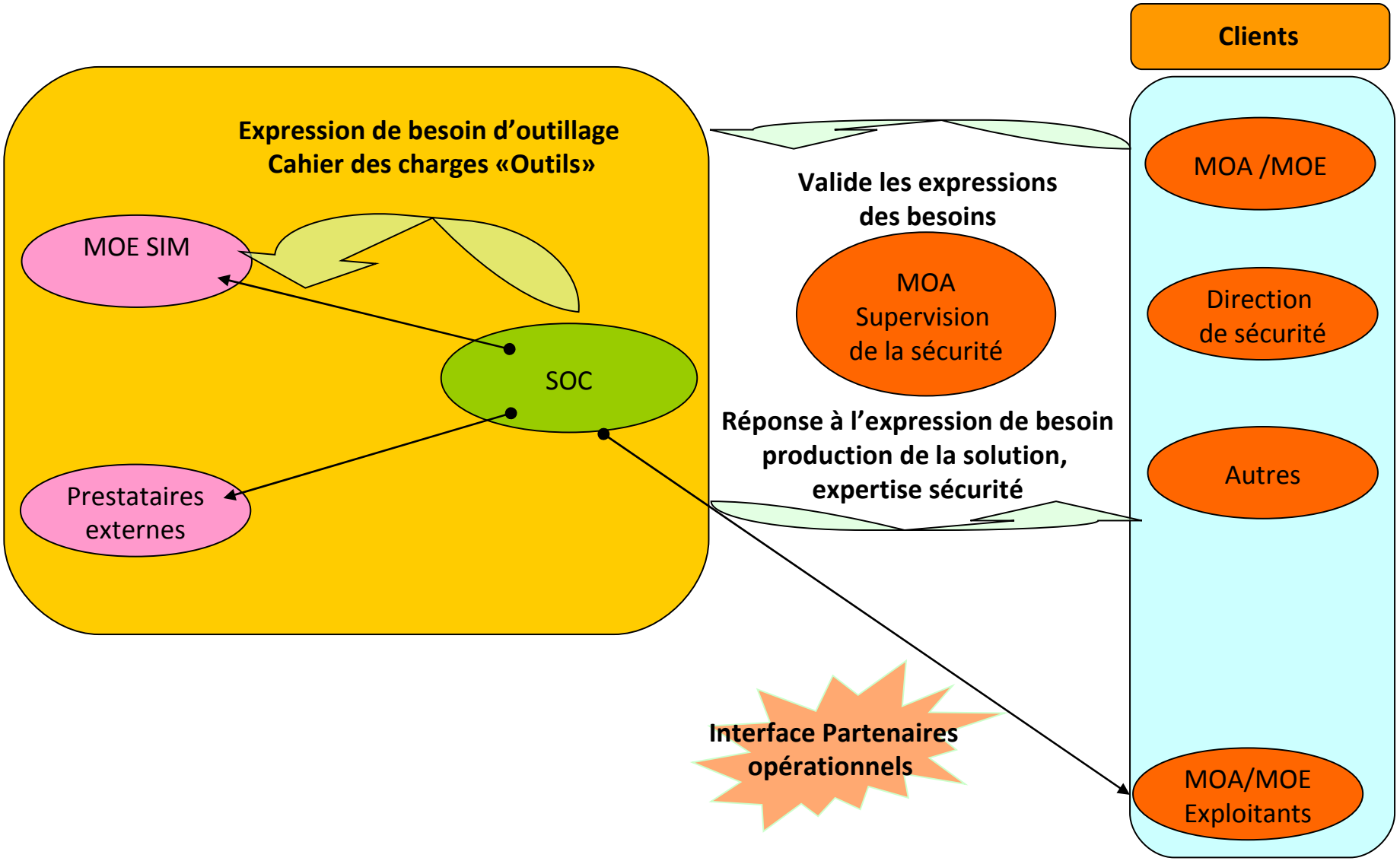
Objectifs de supervision de la sécurité

- **La supervision de sécurité**
  - une contre-mesure possible




Organisation

Synergie inter-entités



Supervision sécurité : qui ?

- **Instance de pilotage**
  - « MOA » global de supervision de sécurité
    - Gestion global du service de supervision de la sécurité
  - Rôles
    - Consolidation des demandes
      - Agrégation, capitalisation
    - Priorisation des services à mettre en supervision
      - Processus d'aide à la décision
    - Aide à la rédaction du cahier des charges
      - Support au demandeur (MOA/MOE)
  - « Connaissances »
    - Des métiers MOA/MOE
    - Des possibilités du SOC

Supervision sécurité : qui ?

- **Les métiers MOA/MOE/Exploitant**
  - Implication
    - Rédaction du cahier des charges de supervision de sécurité
      - Connaissances des éléments critiques et des risques
  - Intégration du SOC dans le service
    - Au même titre qu'un service standard de mise en exploitation
      - « évolution des mentalités »
  - Actions temps réel
    - Prise en compte des notifications pour corrections ou pas
      - Par les exploitants
  - Actions temps différée
    - Amélioration de la sécurité en fonction des remontées du SOC
      - Erreur de configuration, faux positif, tendances,……

Supervision sécurité : qui ?

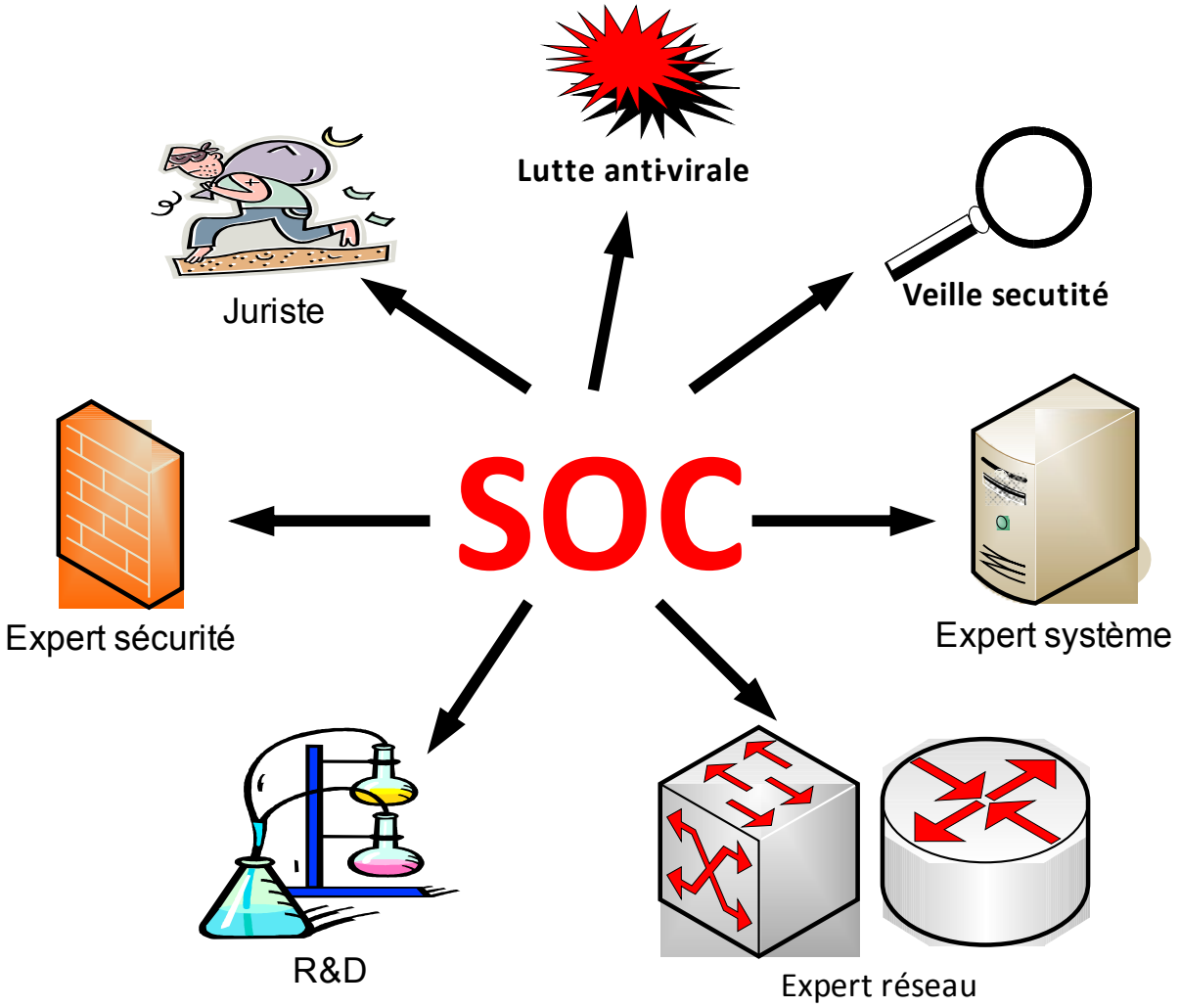
- **Le SOC**

Rôles	Responsabilité	Expertise
Brigadier	Intervention en HNO réaction sur fiche consigne	« Superviseur» Niveau 1
Analyste sécurité	Intervention en HO et astreinte qualification Ingénierie de la solution technique	« Expert sécurité » (Niveau 2/3)
Responsable	Transverse	Validation du cahier des charges et de la solution technique

- **Expertise technique**
  - Système, réseaux, application,….
- **Compétences**
  - Sécurité, capteurs de sécurité, intrusion,…..
- **Relationnel**
  - Réponse au cahier des charges
  - Gestion de crise

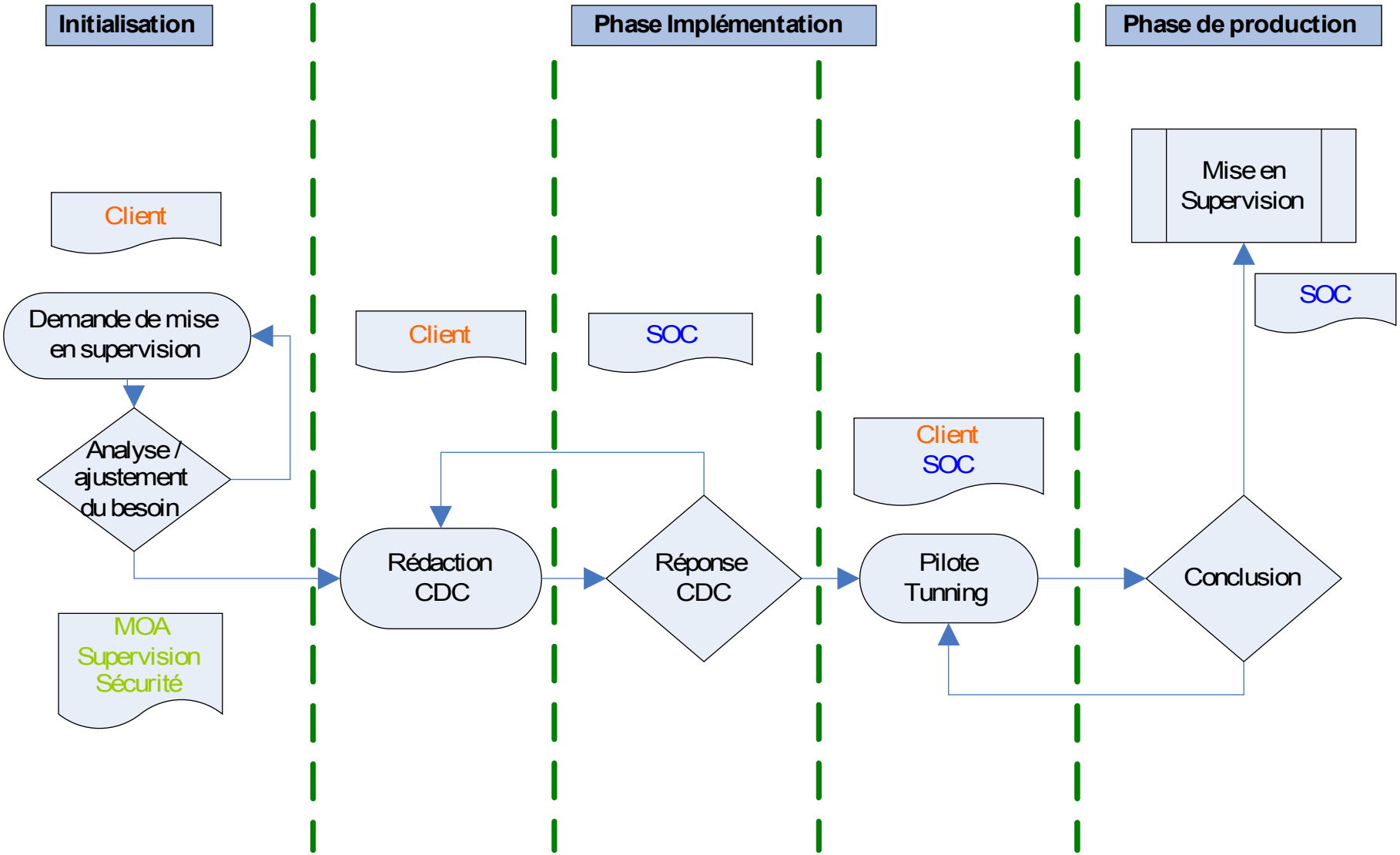
Supervision sécurité ouverture

- **« Partenaires »**
  - Un SOC ne doit pas vivre en autarcie



Processus

Processus global



Choix des « services » à superviser

- **Critères « services »**
  - Type et sensibilité des données
    - Bancaire, Santé,….
  - Outsourcing
    - Tout ou partie du service outsourcé
  - Niveau de sécurité des plates-formes
    - Audit, analyse de risque
  - Type de réseaux
    - Internet, MPLS/VPN
  - …..

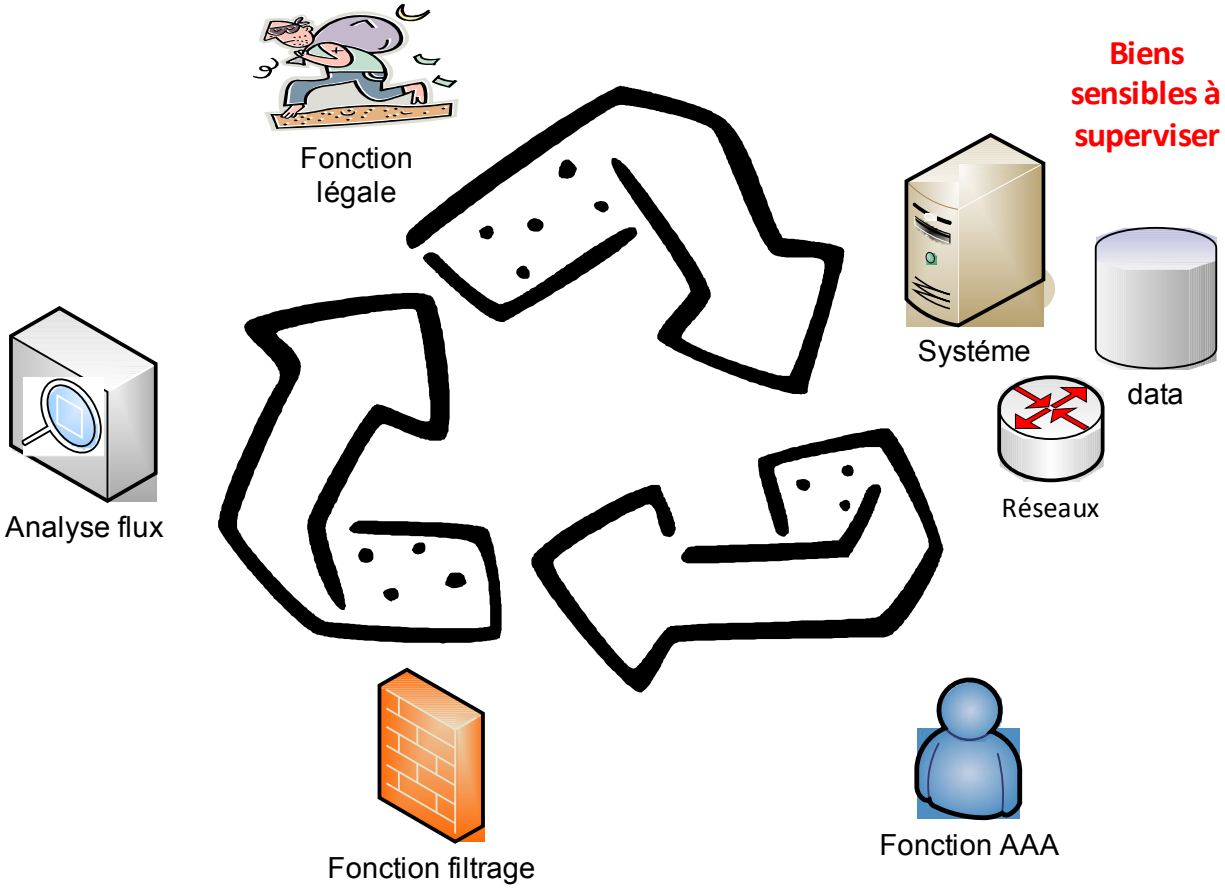
- **Critères normalisation , certification**
  - Eléments de preuve
    - ISO 20K, ISO 27K, PCI-DSS, SOX

Security Supervision services criteria

Criteria	description	Validation	Cout	Pound	Priority result	Detail
Marketing	High priority	Yes	10	10	10	
	Normal priority	No		5		
	Regular TTM	No		5		
	Fast-track TTM	No		5		
	Innovation TTM	No		10		
	ITTM	Yes		5	2,5	
Normalisation	PCI-DSS	No		20		
	ISO 20000	No		10		
	ISO 27001	Yes	10	20	15	
	ISO 15408	No		20		
	SOX	No		20		
	RGS	No		20		
Services data	Data	Yes	10	5	7,5	
	Email	No		5		
	Files	No		5		
	Voices	No		10		
	Video	No		10		
	Customer data	No		10		
	Medical Data	No		20		
	Financial data	No		20		
	Human ressources data	No		15		
	Government/calssified data	No		20		
Partners ans subcontractors	Functional partner	No		10		
	Technic partner	No		20		
	Solution provider	No		20		
	Support maintenance sub-contractor	No		20		

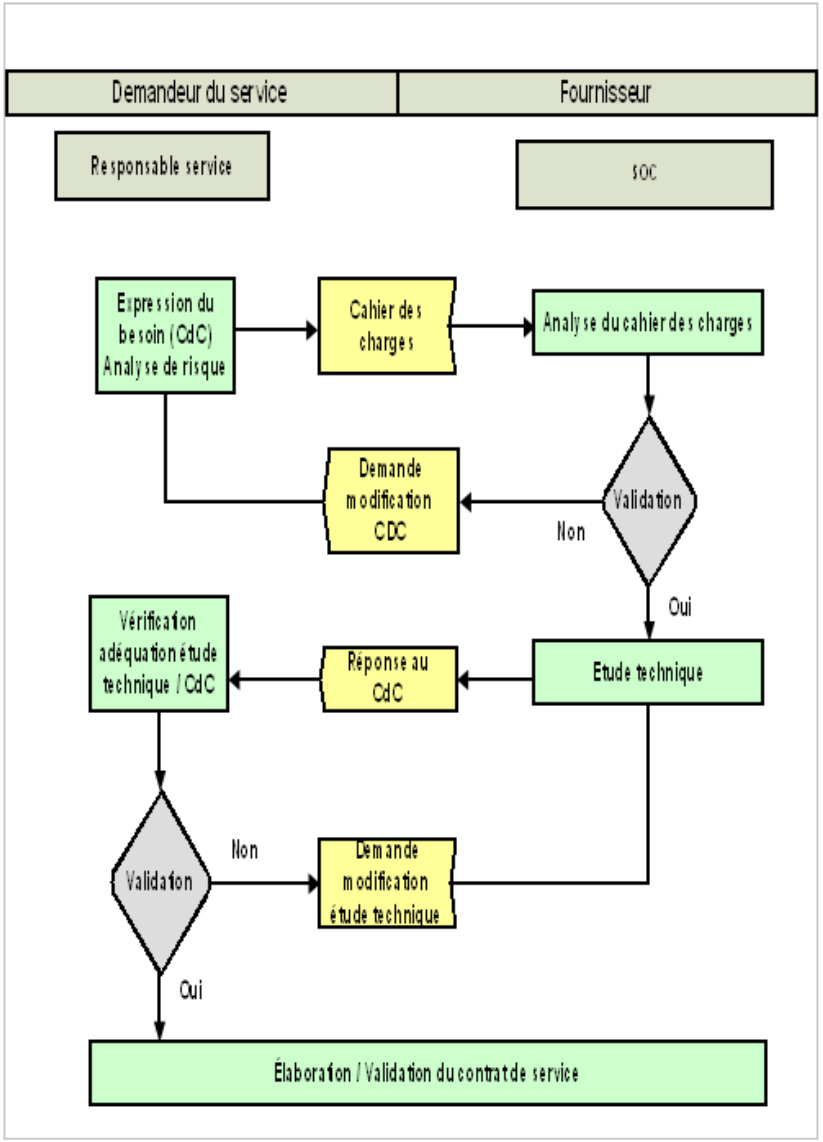
Le cahier des charges générique

- Rôles
  - Indiquer ce qui serait à superviser pas comment le superviser
  - Liste des « fonctions »



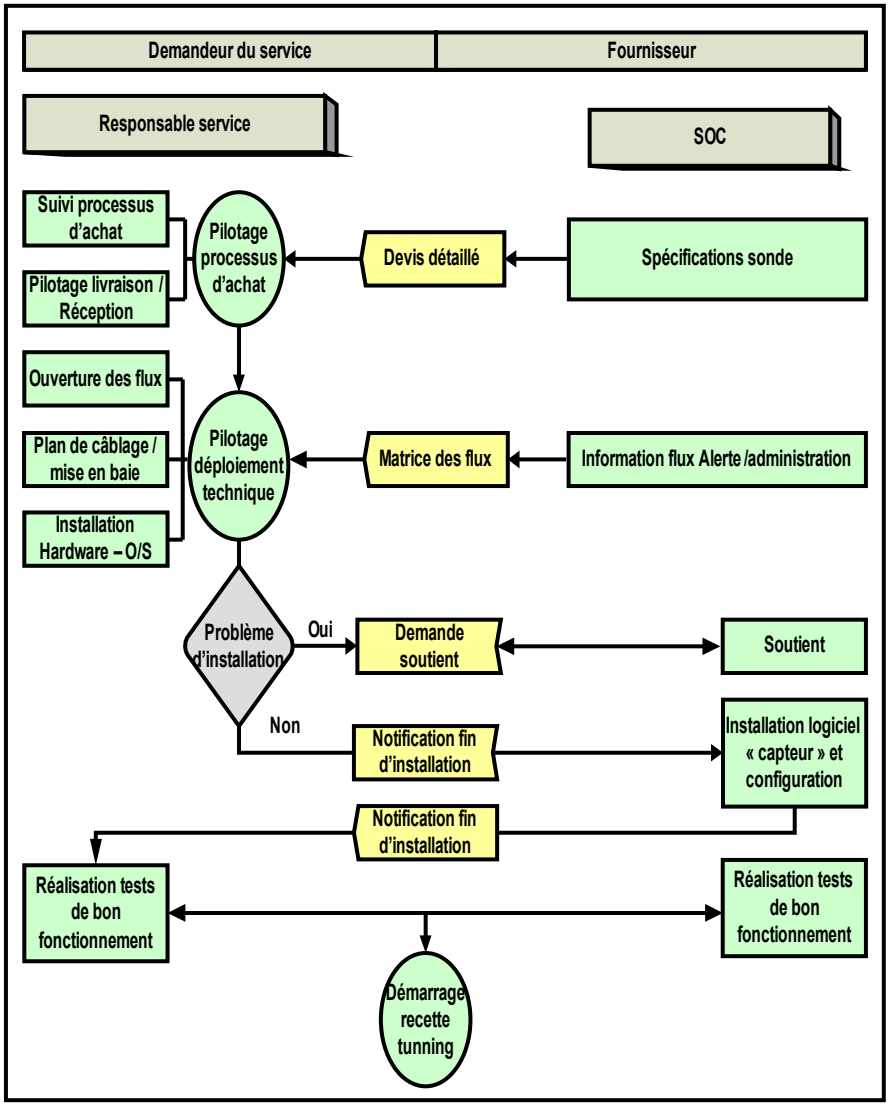
Validation et réponse

- **Fonction du CDC**
  - Réseaux
    - Ex : Protocole de routage
  - Authentification
    - Ex : contrôle d'accès
  - Vérification filtrage
    - Ex : ACL critiques
  - Analyse des flux
    - Ex : Flux autorisé attaque
- **Réponse du SOC**
  - Solution technique
    - Type de capteur
    - Jeux de règles
      - Recherche pour les logs
      - Signature IDS



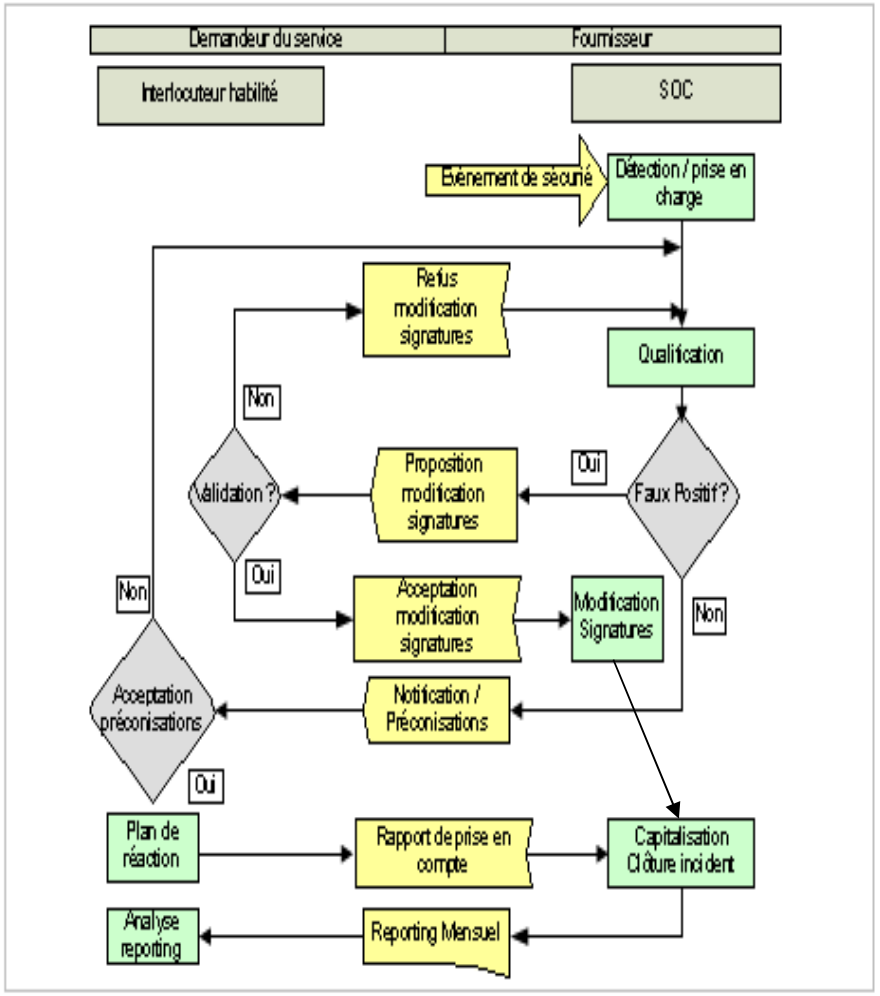
Processus de déploiement

- Installation
  - Mise en place des capteurs sécurité
    - Capteurs, règles
- Tunning
  - Affiner les règles des capteurs
    - Sélection humaine
    - « Proposition » capteur
- Phase pilote
  - Réduction du bruits
    - Erreur configuration
    - Faux positifs
  - Rédaction des fiches consignes



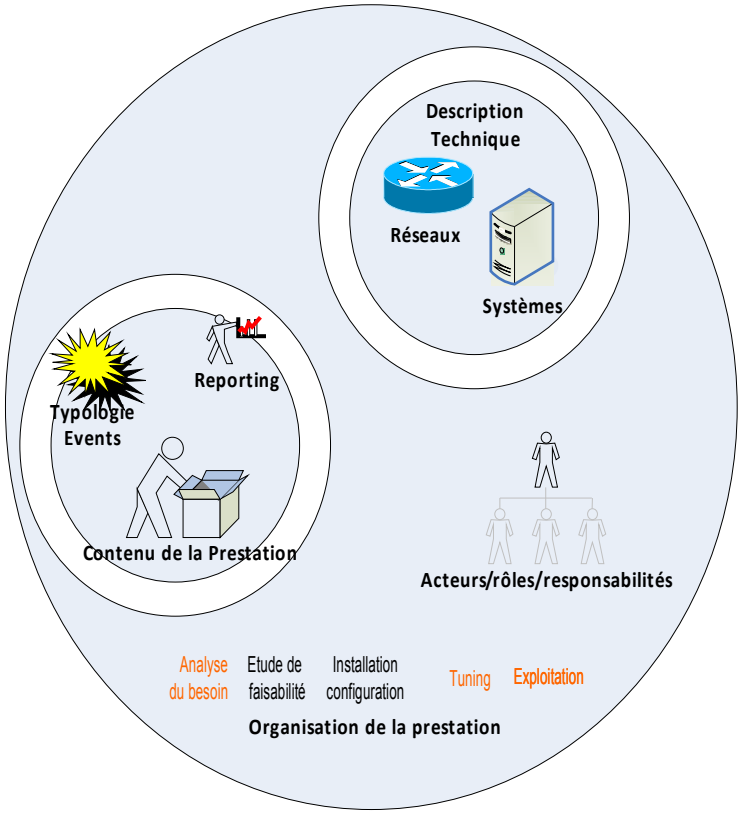
Détection / Qualification / plan d'action

- **Détection**
  - Réception des événements de sécurité
  - Prise en charge
- **Qualification**
  - Expertise
  - Connaissance du contexte
  - Enrichissement source externe
  - Modification des signatures
  - Notification
- **Plan d'action (préconisation)**
  - Fourniture d'un plan d'action
  - Participation aux cellules de crise
  - Capitalisation de l'événement
  - Voir analyse à froid

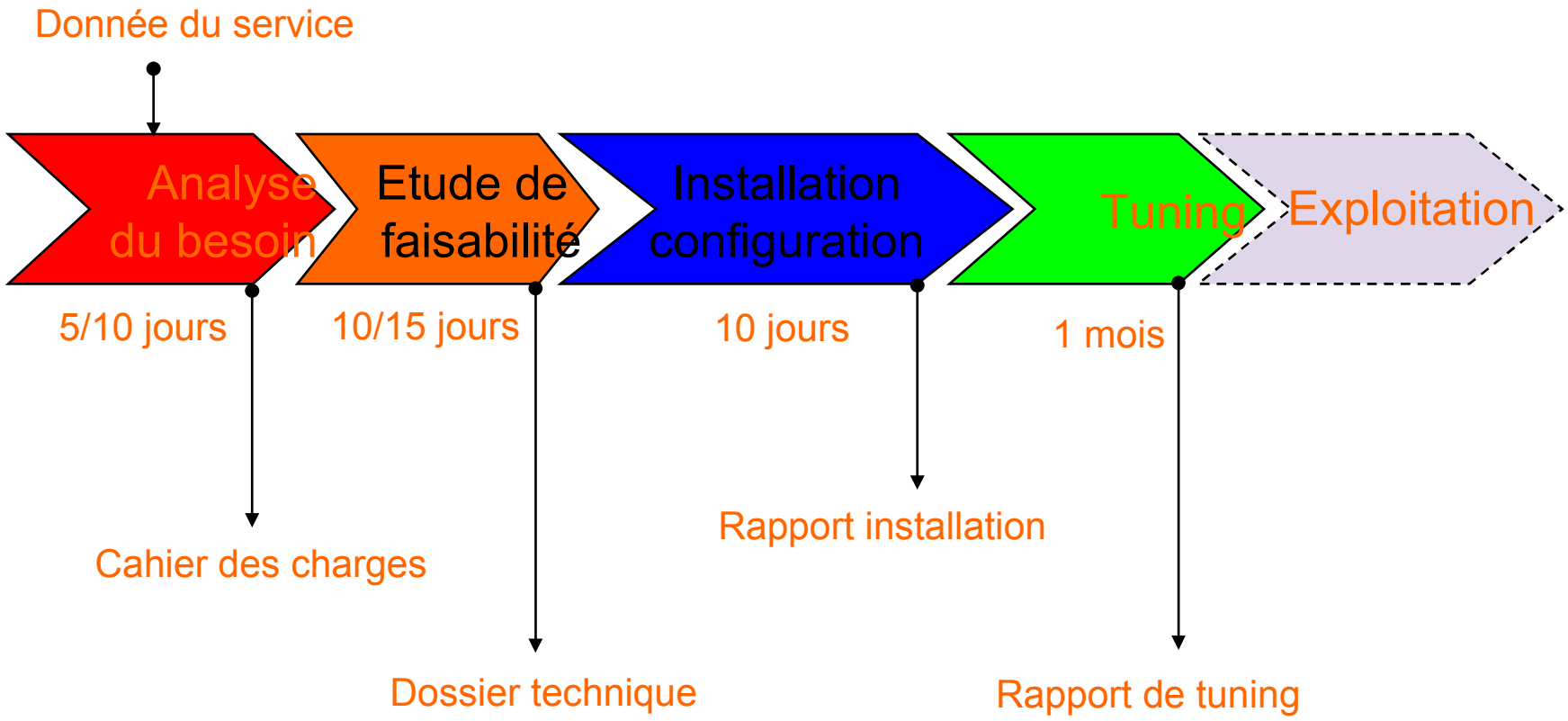


Contrat : cadrer la prestation

- Description technique
  - Réseaux/système/application
    - Volumétrie
    - Sensibilité (DIC)
    - Inventaire,…
- Intervenants
  - Listes des acteurs
  - Rôles (MOA, exploitants,…)
  - Responsabilité
    - Gestionnaire de crise
    - Application des corrections,....
- Contenu de la prestation
  - Typologie des événements
  - Délais de réaction (échelle 4 niveaux)
  - Reporting (type, fréquence, destinataire)



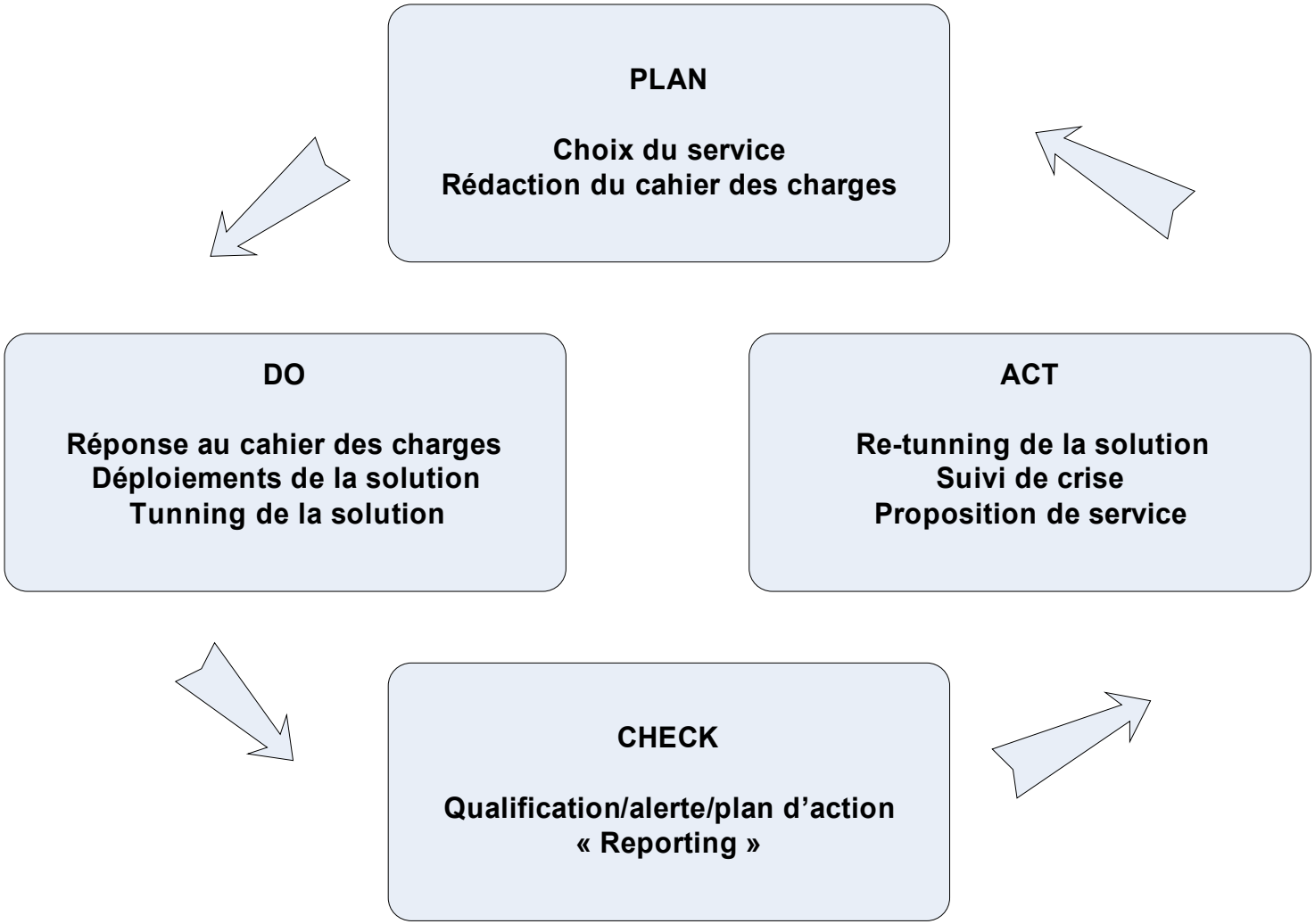
Synchronisation des phases



Processus connexes

- **« Exercices »**
  - Tests organisationnels
    - Réactivité des équipes
      - Qualification des événements
      - Amélioration des compétences
    - Durcissement des processus
      - Améliorations de la chaine complète
        - Rupture de la chaine
  - Tests techniques
    - Efficacité IDS
      - Jeux de signatures
      - Techniques d'évasions
    - Efficacité logs
      - « complétude » de logs collectées
    - Framework de test
      - Metasploit,….

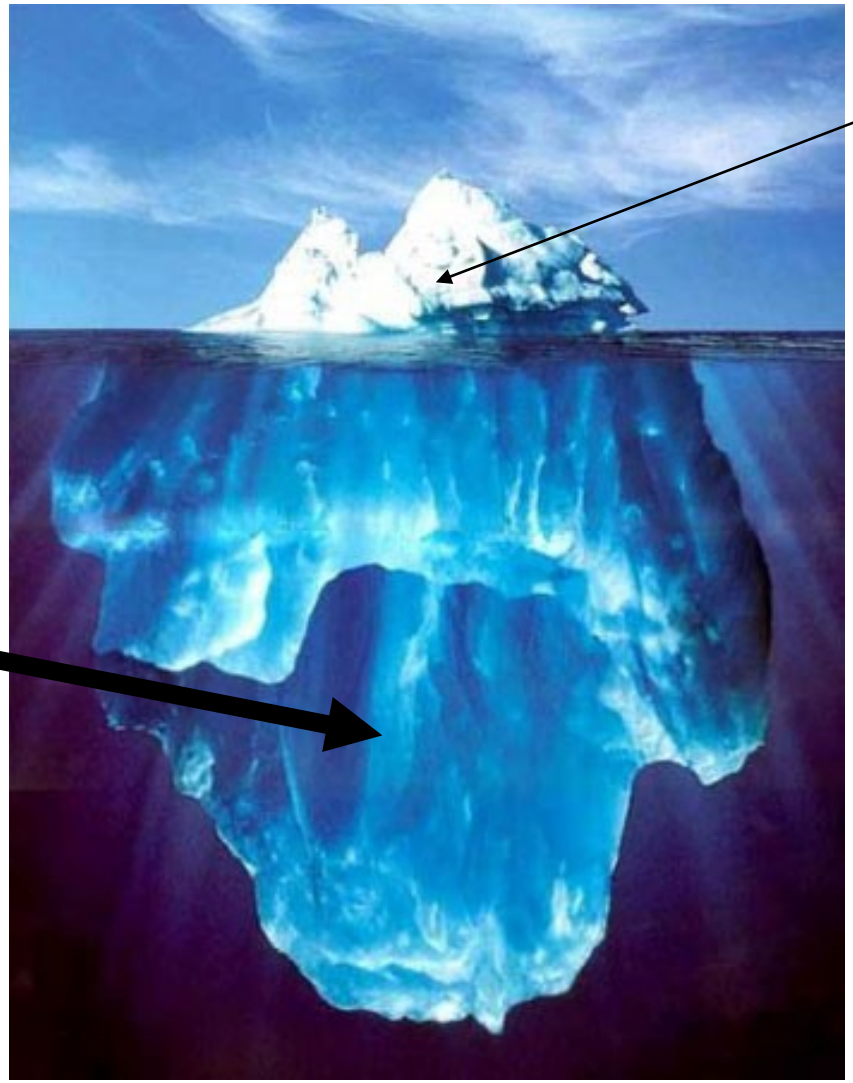
Supervision de sécurité et PDCA modèle ☺



Outils

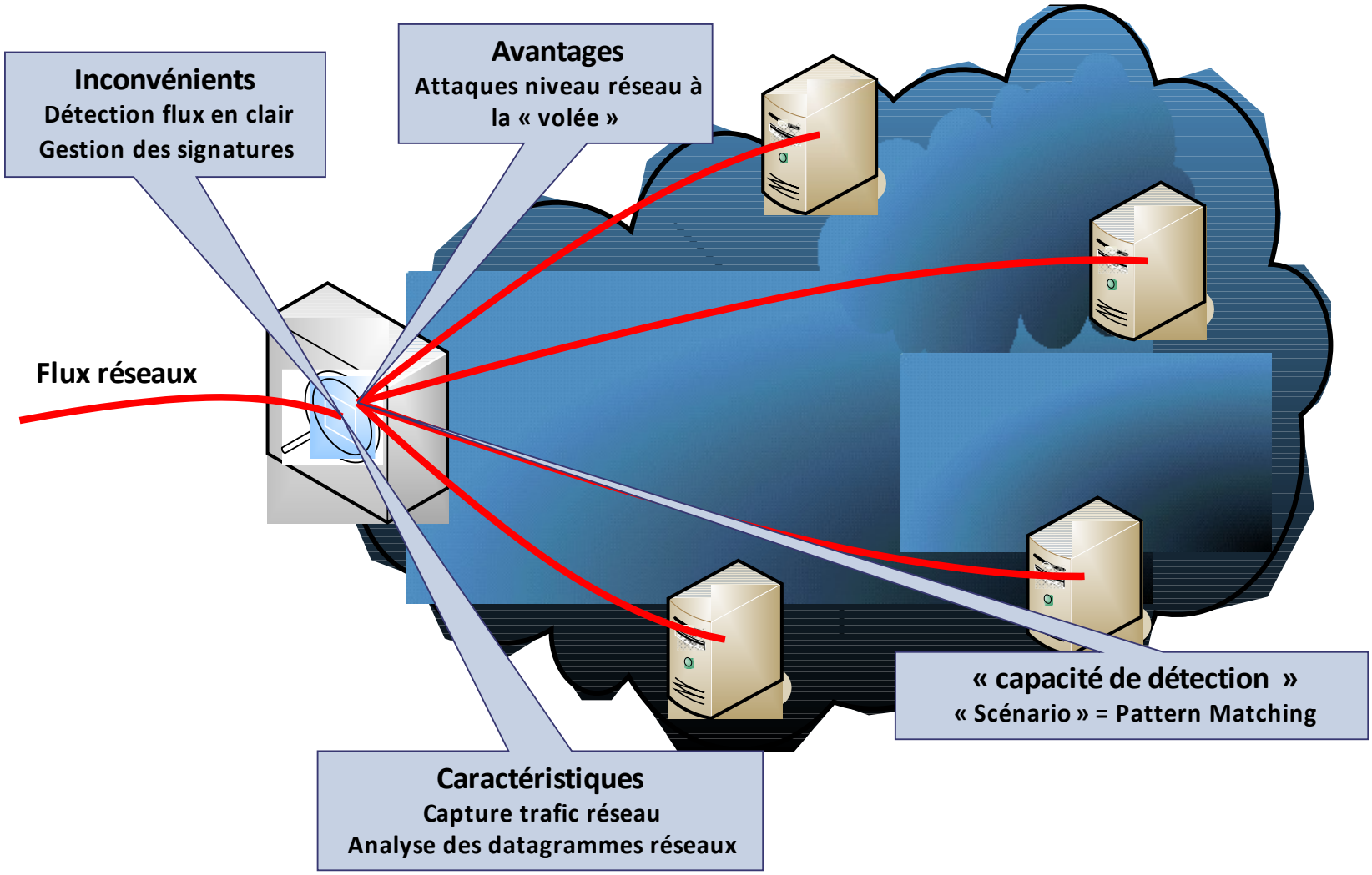
Warning !

- **Règles de l'iceberg**



IDS

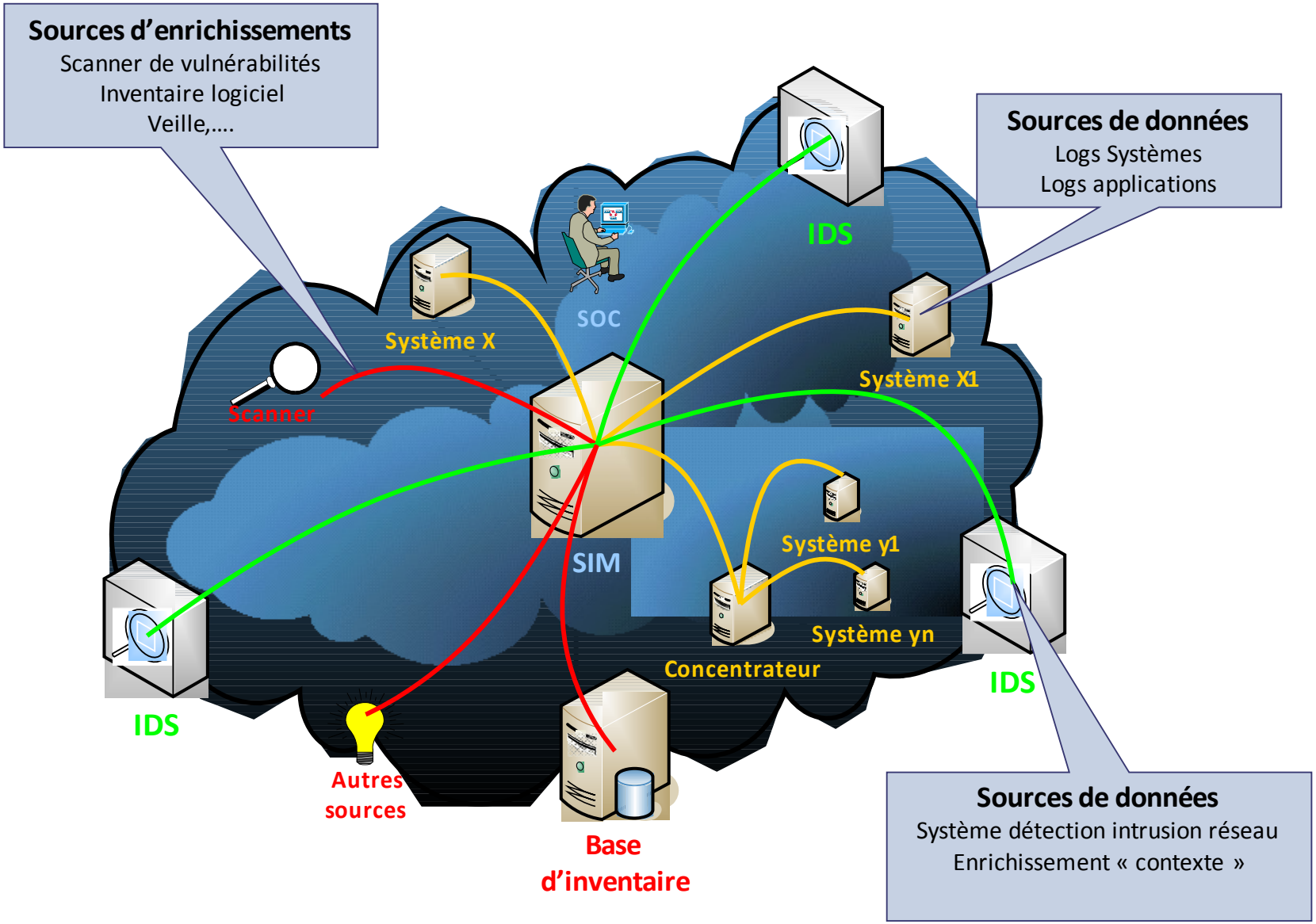
- Système de détection d'intrusion



Outil SIM/SIEM

- **Ce n'est pas :**
  - Concentrateur de log (archivage)
  - Outil spécifique de fourniture de tableau de bord
- **Fonction de base**
  - Acquisition des données qui peuvent contenir des « événements de sécurité »
    - Logs systèmes/applications
    - sondes spécifiques ,…
  - Acquisition des données « source d'enrichissement »
    - Scanner de vulnérabilité
    - base d'inventaire des cibles protégées
    - Base de vulnérabilités
  - Corrélation
    - Fréquence/statistique
    - Modélisation de scénario
    - « Croissement »
    - Déviance

SIM contexte



Outils

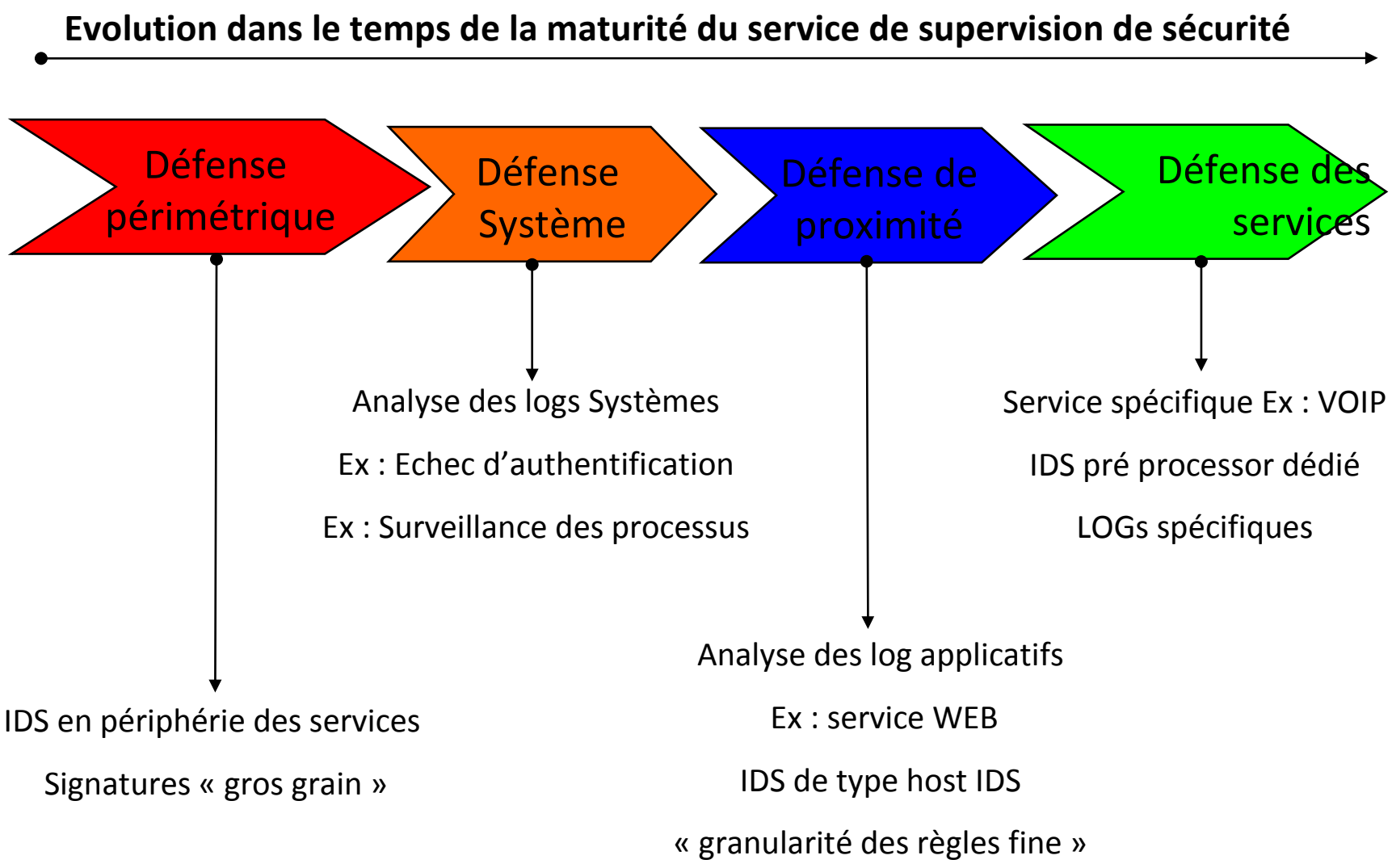
- **Complexités/difficultés des outils**
  - Règles de corrélation
    - Complexité de modélisation = expertise = ressources
  - Installation/paramétrage
    - Nécessite une très bonne expertise du produit
  - Ajustement constant
    - Moteur de corrélation sophistiqué = mise à jour = ressources
  - Cout de l'outils
    - Cher donc doit être en adéquation avec l'expression du besoin de supervision de sécurité

Outils connexes

- Base d'inventaires des systèmes/applications à superviser
  - Enrichissement de la qualification
- Base de connaissance
  - Capitalisation sur les incidents de sécurité
- Scanner de vulnérabilités
  - Ex : Nessus
- Cleanpipe/blackholing
  - Analyse comportementale
  - Dépassement de seuil
  - Outils spécifique
- Visualisation graphique
  - Ex : PICWIZ


Evolution

Evolution de maturité

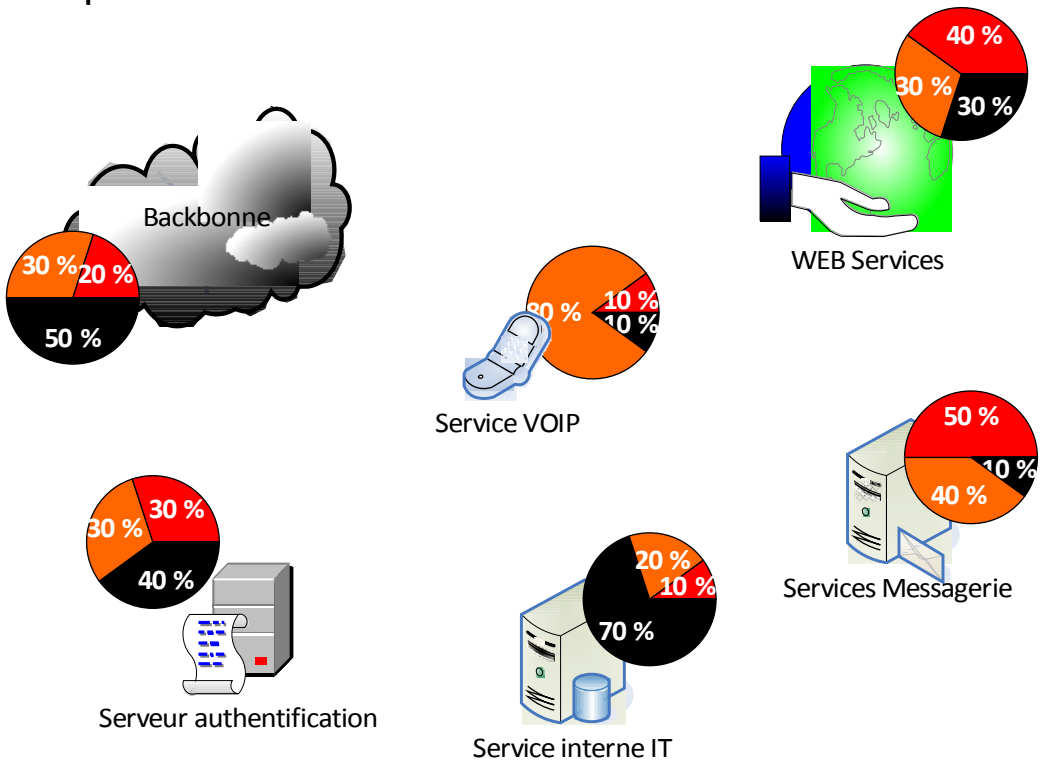



Piste

Piste de réflexion

Météo

- Définition d'un météo d'attaque sur l'ensemble des services en supervision de sécurité de type
  - Attaque avec impact = rouge
  - Attaque sens impact = orange
  - Faux positif = noire



« Conclusion »

Avantages/inconvénients

- **Facteurs de succès**
  - Définition des processus métier du service de supervision de sécurité
  - Identification claire de rôles et responsabilités coté client et SOC
  - Impliquer le métier MOA/MOE
  - De l'expertise donc des ressources humaines
  - De la patience = travail de fourmis

- **Pièges**
  - Vouloir stocker de millions de lignes de logs
  - Déployer des centaines de capteurs sans analyse du besoin
  - Vouloir faire supporter au SOC l'ensemble de la sécurité d'une entreprise
  - Se reposer sur les outils et pas sur l'expertise humaine

Merci