Club de la sécurité de l'information français

CLUSIF

Les travaux du GT SOC

Martine GUIGNARD
Imprimerie Nationale, Responsable du GT SOC au CLUSIF

Travail réalisé par le GT SOC

- Réalisation du document 'Comment déployer un SOC'
  - Nombreux participants au GT
  - Des réunions intéressantes et des débats animés
  - Nous attendons les retours des membres du CLUSIF.

- Constats
  - Peu de documents de référence
    - Le document du MITRE
    - Les référentiels PDIS et PRIS de l'ANSSI
  - Pas d'offres clairement définies
  - Des outils en plein essor
  - Ce document non dogmatique devrait permettre aux DSI, RSSI, Directeurs opérationnels de se faire une idée du déploiement d'un SOC et de ses impacts dans l'entreprise.

Le sommaire du document

- Objectif d'un SOC
  - Le SOC répond aux objectifs de l'entreprise
  - Il n'est pas constitué que de technologies mais comporte aussi une organisation humaine
  - Le SOC doit être sécurisé
- Catalogue de services et fonctions d'un SOC
  - Prévention, Détection, Réaction, Administration
- Structure et fonctionnement d'un SOC
  - Processus, ressources humaines, pilotage, moyens
- Mise en place d'un SOC
  - Définir le projet, le vendre, le mettre en place, en faire le bilan et continuer à améliorer

Catalogue de services et fonctions

Prévention

Protéger le SI en renforçant les fondamentaux pour réduire les possibilités d'attaque.
Préparer la détection et la réaction pour être prêt lors de l'attaque.

Détection

Se doter de capacités à déceler toute attaque portant sur le périmètre du SI.
Être exhaustif et instantané dans la découverte d'attaques du SI.

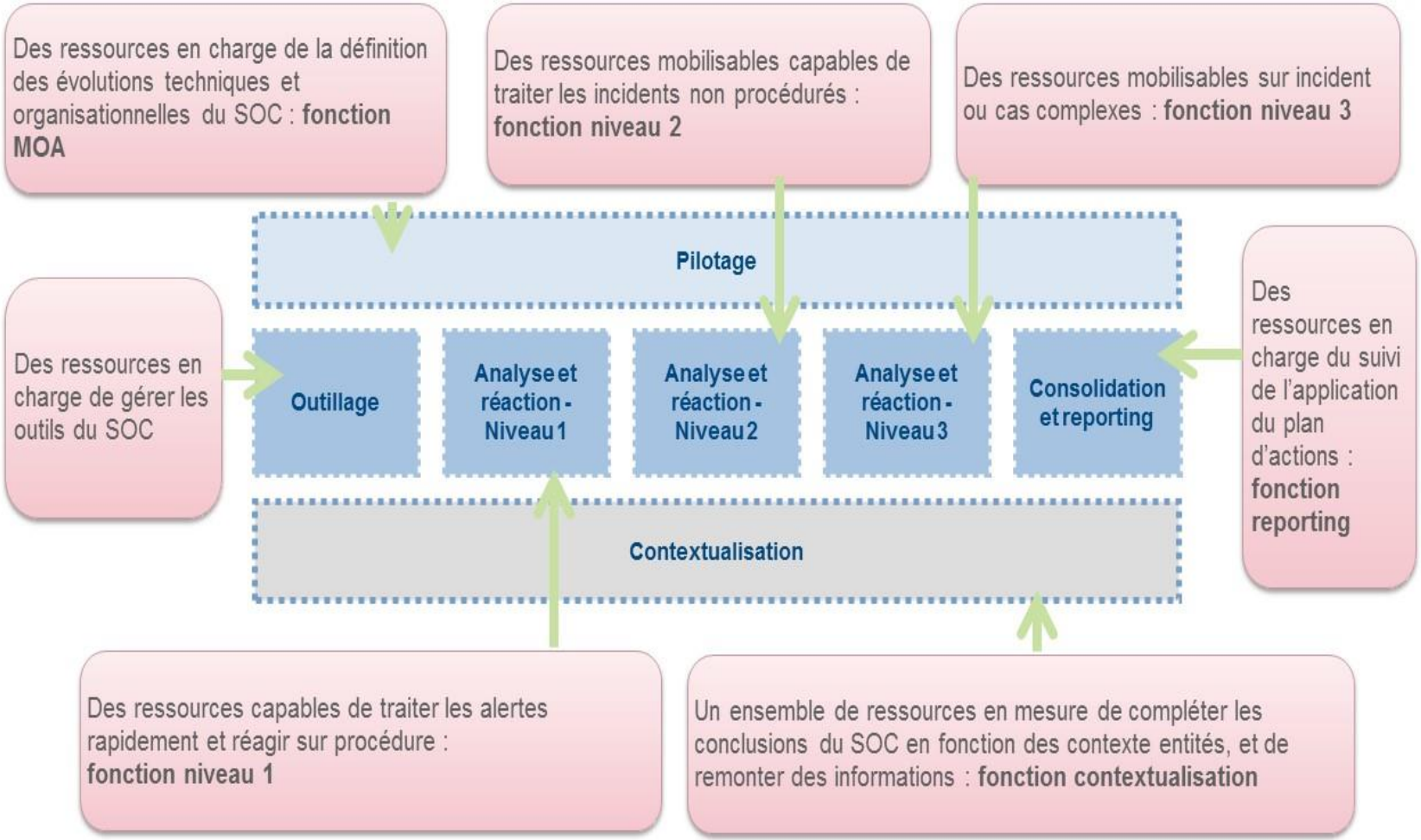
Réaction

Assurer une prise en compte totale (périmètre, impact et temporalité) de l'attaque.
Interface technique d'une cellule de cyber crise.

Administration sécurité

Administration fonctionnelle des outils de sécurité avancés

Structure et fonctionnement d'un SOC



Mise en place d'un SOC