CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS


# Quand Monsieur SOC rencontre Monsieur CARTO

**« L'ignorance est mère de tous les maux »,**
**Rabelais (1564)**

Jean OLIVE (jean.olive@cgi.com - 06 74 33 29 42)

Thibault CHEVILLOTTE (Thibault.chevillotte@cgi.com 06 13 04 33 94)

CGI | Business Consulting

# Besoins du SOC

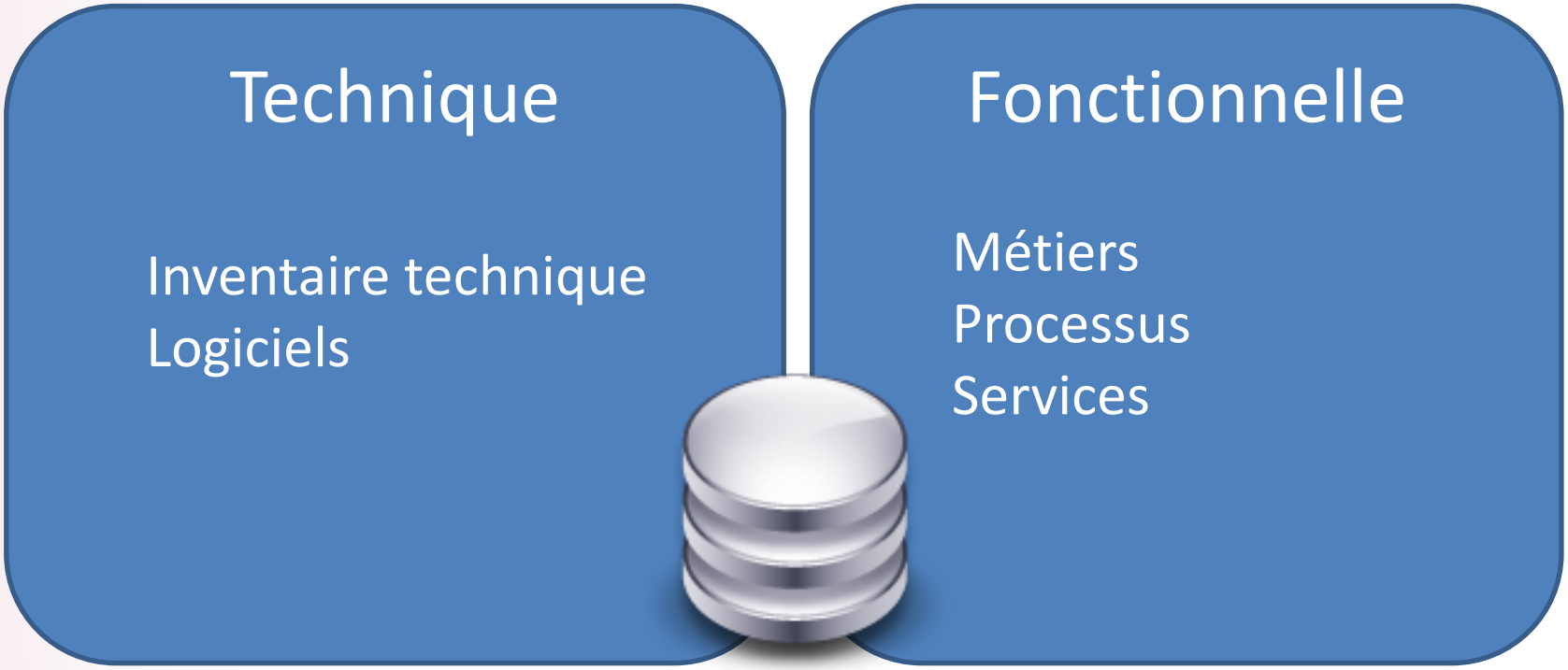
## Analyser et traiter les évènements de sécurité

- Détecter des anomalies à partir des évènements
- Qualifier les anomalies en incidents de sécurité
- Réagir à ces incidents
  - Circonscrire le problème
  - Qualifier les impacts
  - Restaurer
  - Eviter la récurrence

Mais aussi

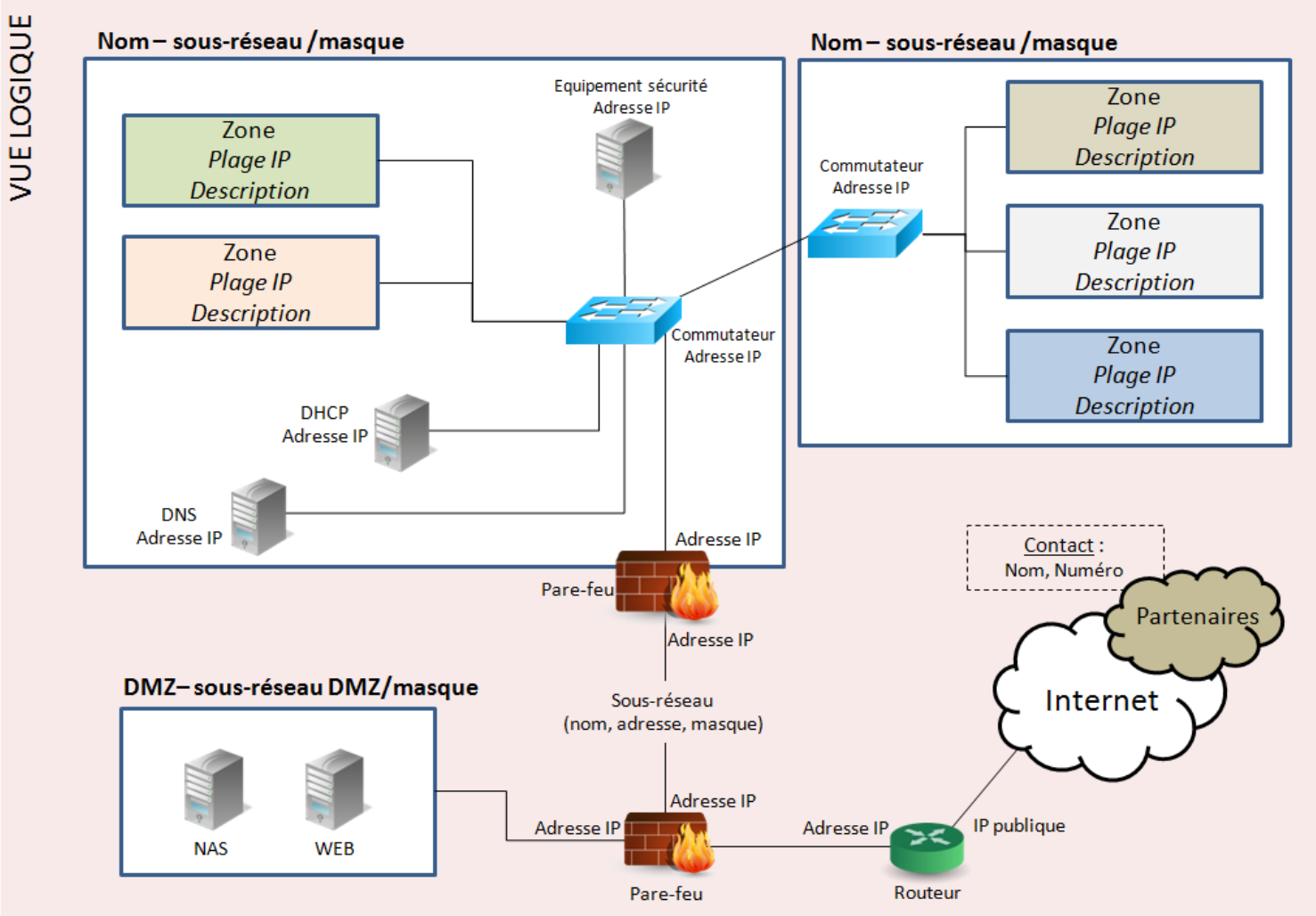
- Présenter un état des lieux de la sécurité sur la base d'indicateurs
- Assurer la cohérence des mesures

# Deux approches



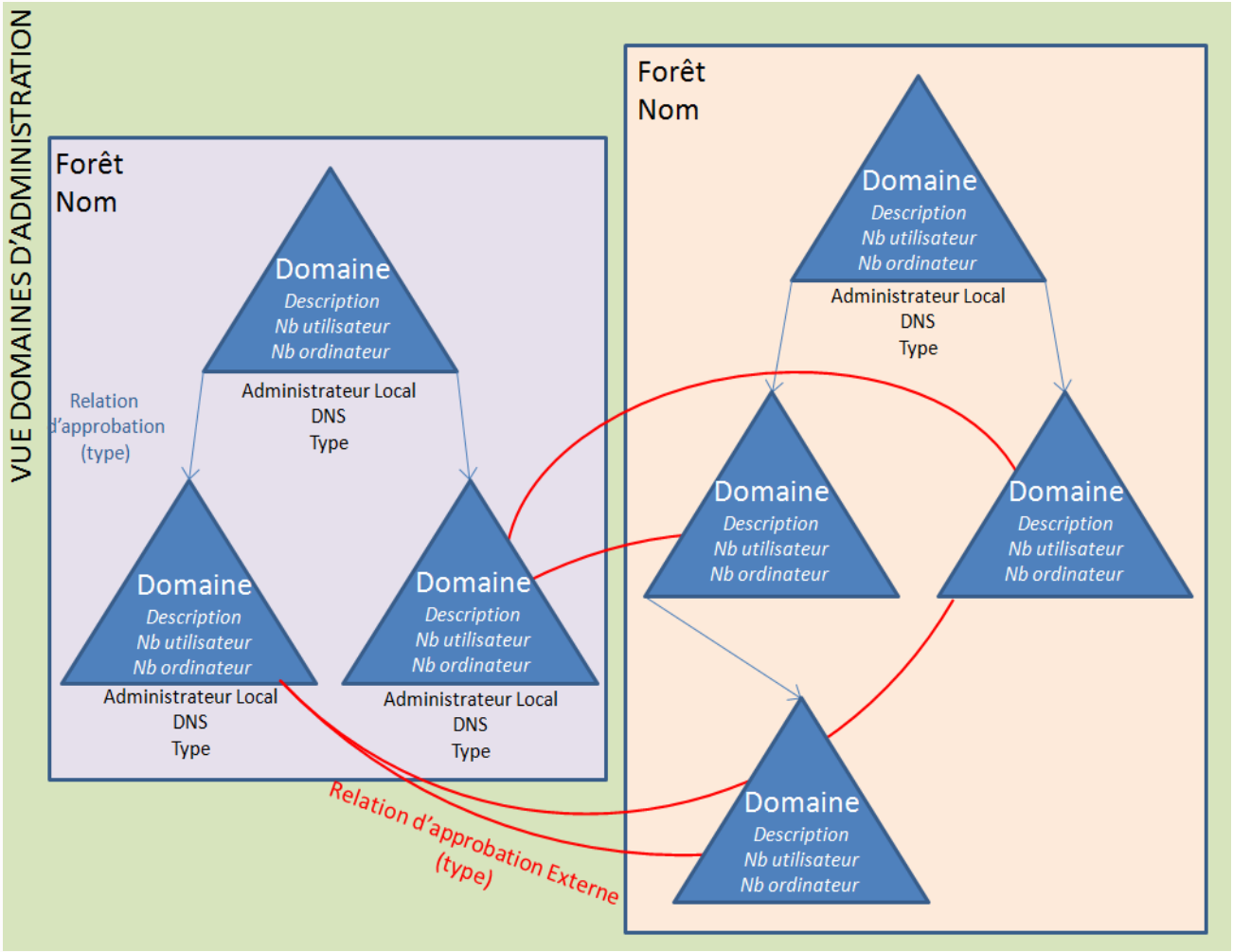

Catalogue d'applications

# Vision des points d'accès



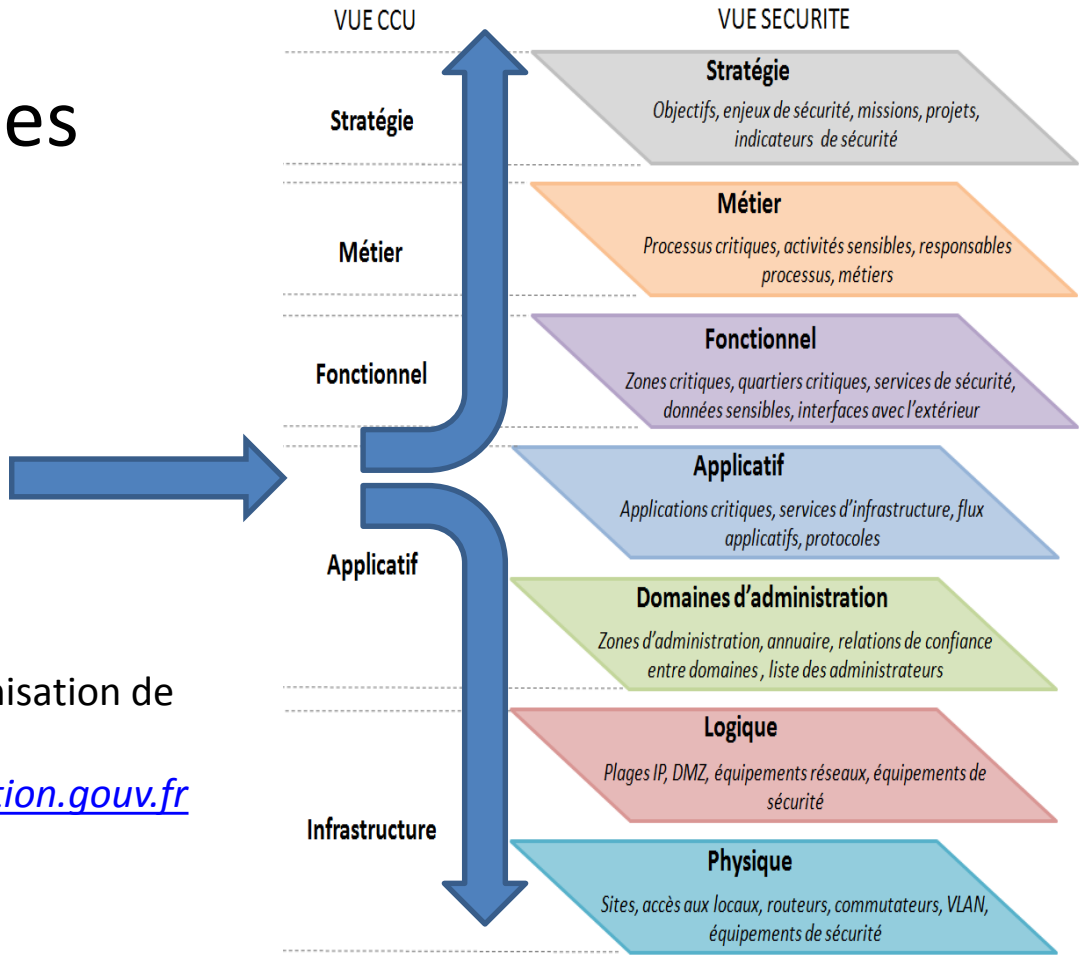

CGI Business Consulting

# Vision des domaines AD



# Modélisation par couche

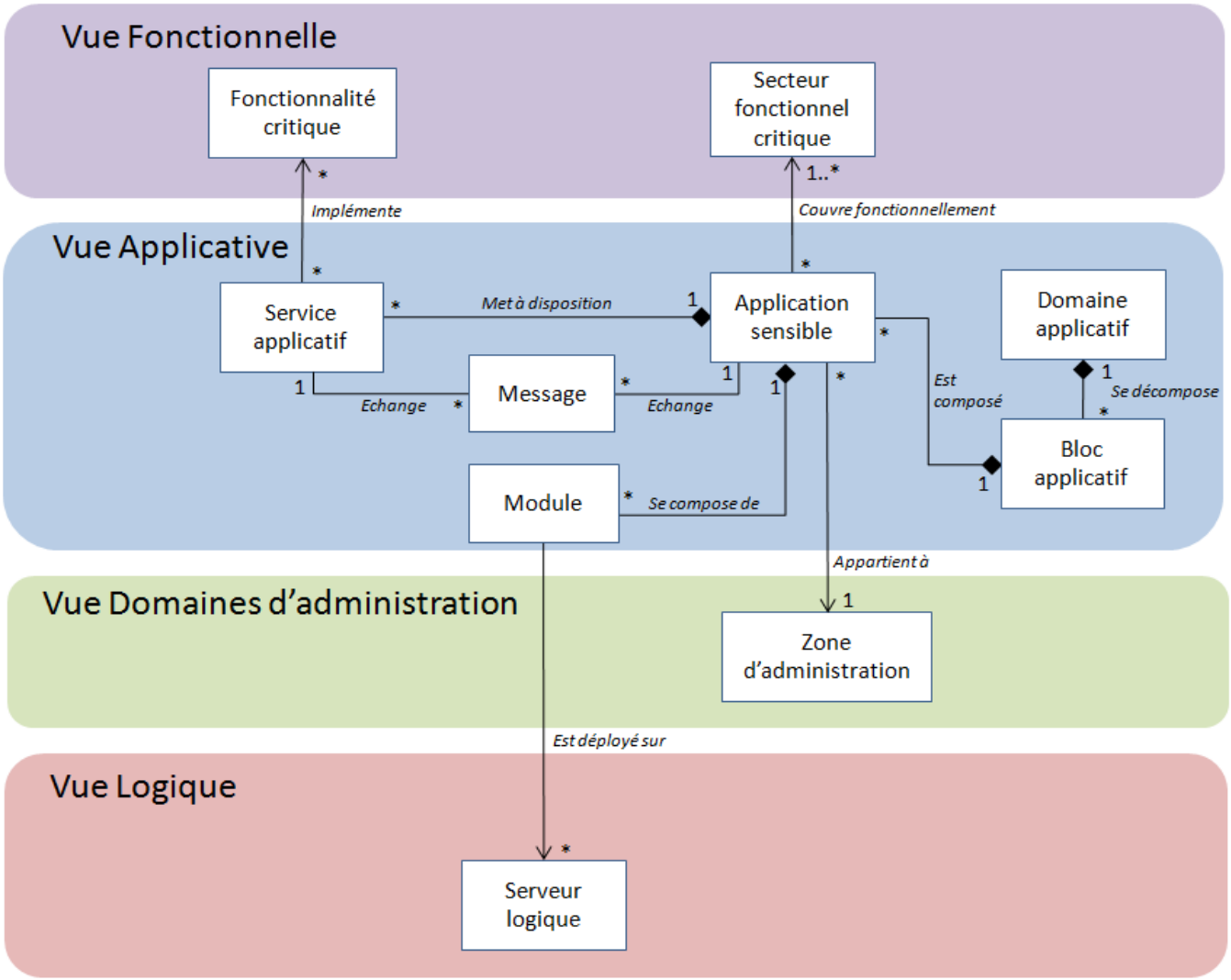
- Inventaires des objets
- Schémas
- Liens




CCU : Cadre Commun d'Urbanisation de l'Etat – DISIC – 2012 - https://references.modernisation.gouv.fr

CGI Business Consulting

# Modélisation des liens



# Par où commencer ?

- Périmètre
- Niveau d'abstraction
- Nombre de liens

Liens de dépendance

| Vues représentées | Niveau 0 | Niveau 1 | Niveau 2 | Niveau 3 | Niveau 4 |
|---|---|---|---|---|---|
| *Liste de contacts* | *X* | X | X | X | X |
| Stratégique | | | | | X |
| Métier | | (X) | X | X | X |
| Fonctionnelle | | (X) | | | X |
| Applicative | | (X) | X | X | X |
| Administration | | X | X | X | X |
| Logique | | X | X | X | X |
| Physique | | | | X | X |

SOC seul

CGI Business Consulting

CLUSIF

# Au minimum …

- Annuaire des contacts
- Biens critiques
- Points d'accès externes
- Domaines d'administration

# La cartographie doit permettre de …

- Positionner les sources de logs et les collecteurs
- Qualifier un incident et réagir
- Faire apparaître des indicateurs dans leur contexte

CGI Business Consulting