G²C

Conseil et assistance en sécurité

Comment enclencher réellement la mise en mouvement des organisations au niveau Sécurité Opérationnelle

Gérard GAUDIN
Consultant international indépendant (G²C)
Président du Club R2GS France et Europe

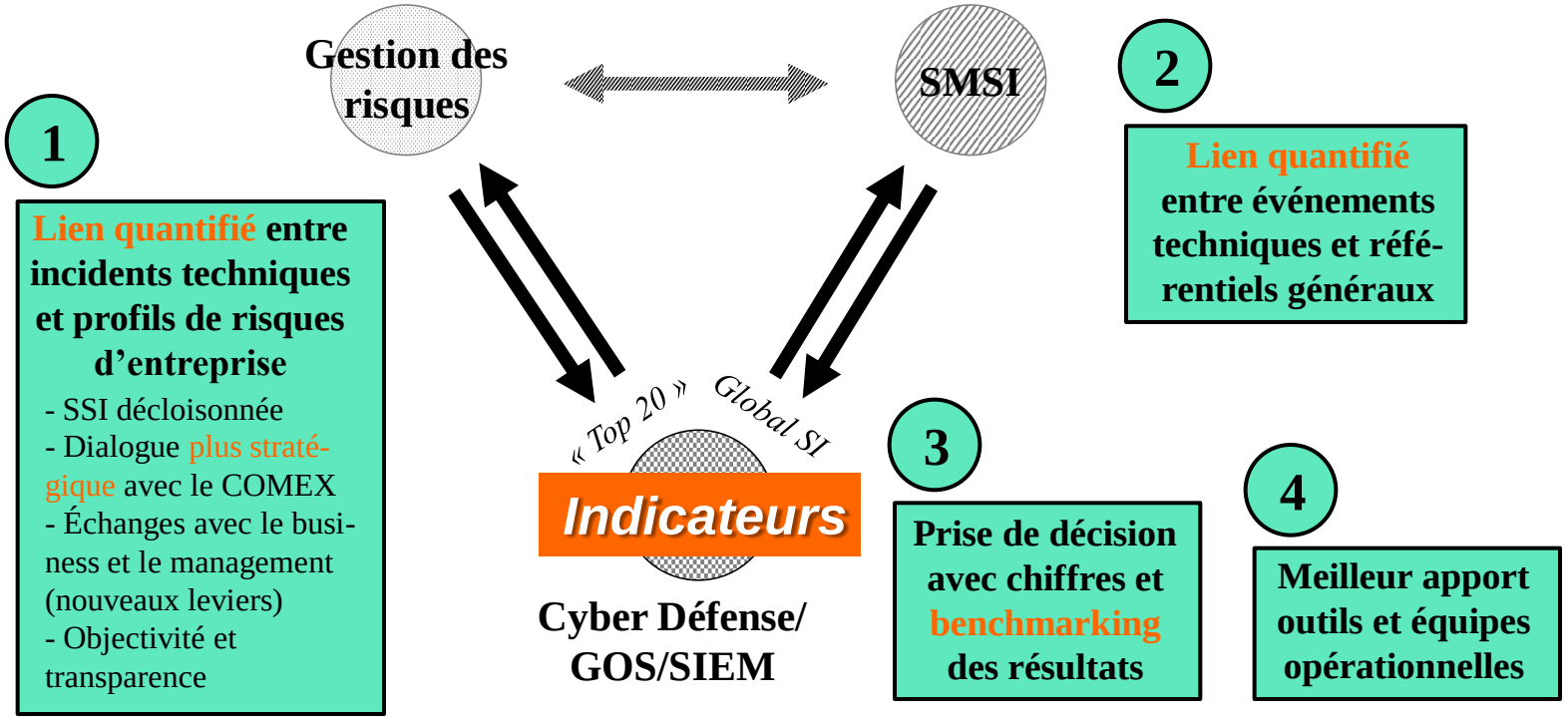
Le 1er décembre 2016

Séminaire Aristote

SOMMAIRE

1. Deux axes novateurs pour débloquer la mise en mouvement encore faible des organisations en GOS

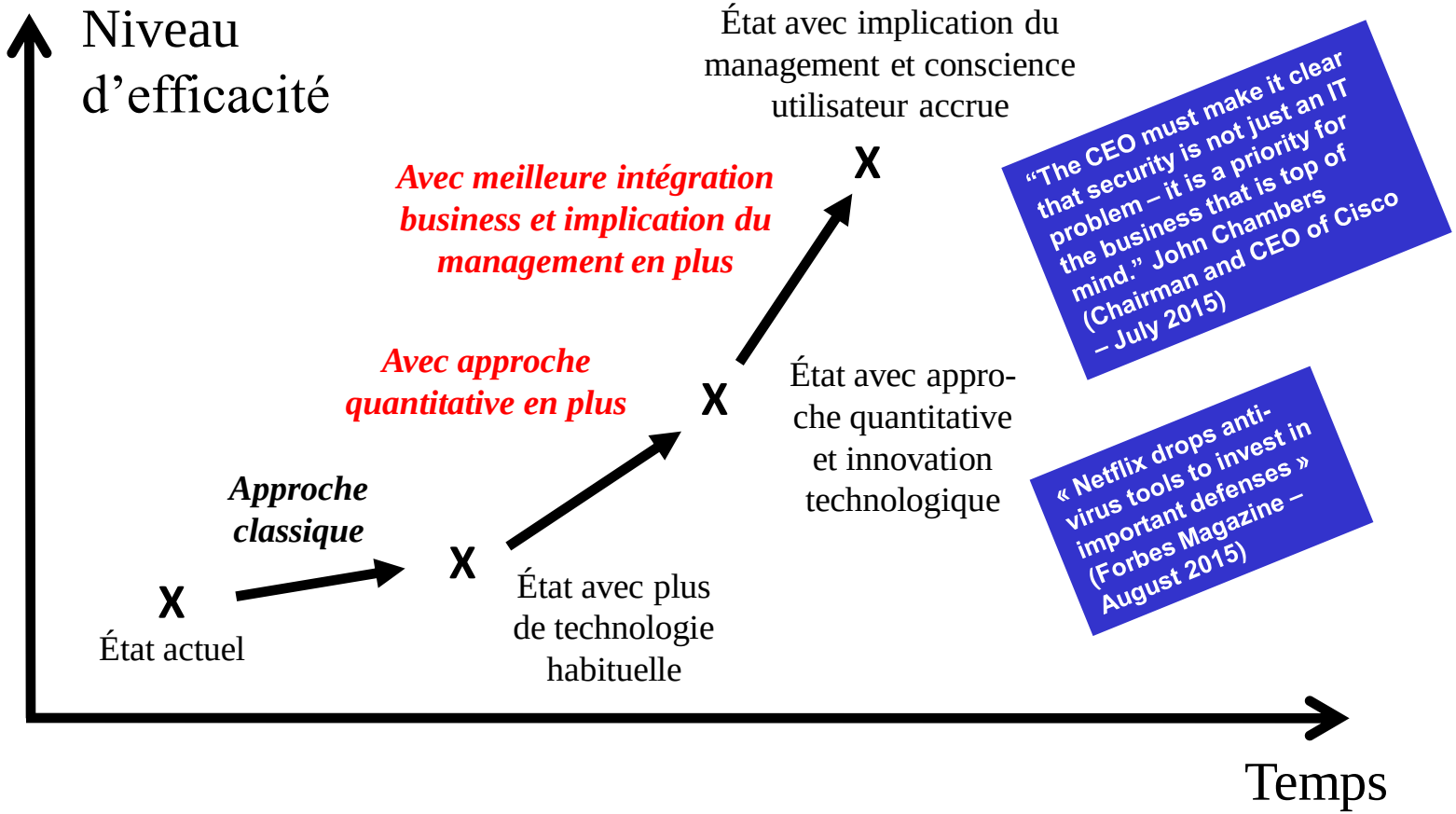
Indicateurs et chiffres + Mobilisation du management = les 4 effets « déverrouillants » de ces 2 axes



2. Un chemin idéal de maturité croissante (1)

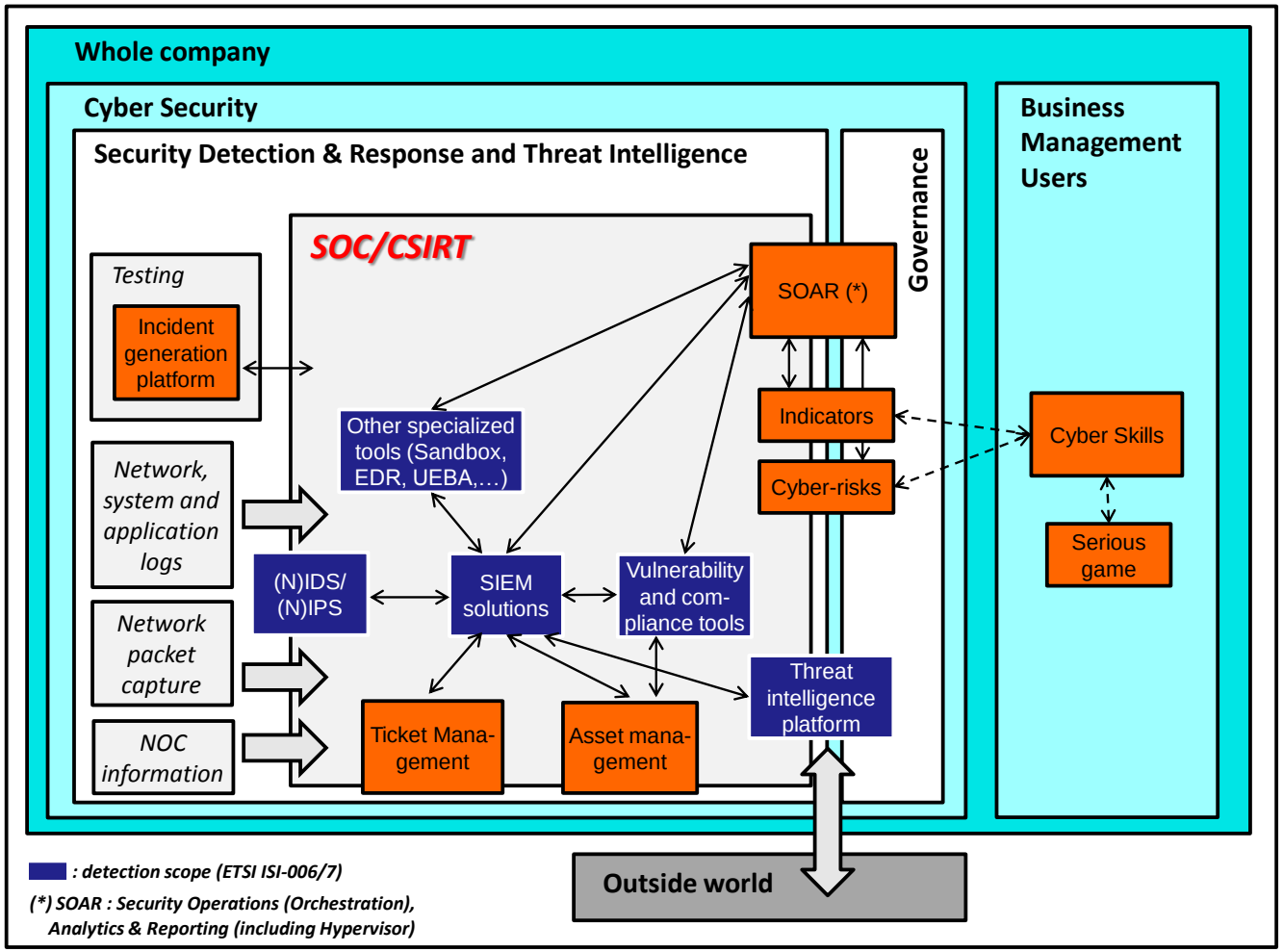
Des objectifs plus ambitieux atteignables

- 40 % d'incidents « basiques »
+ 30 % de taux de détection
- 30 % de temps de réponse



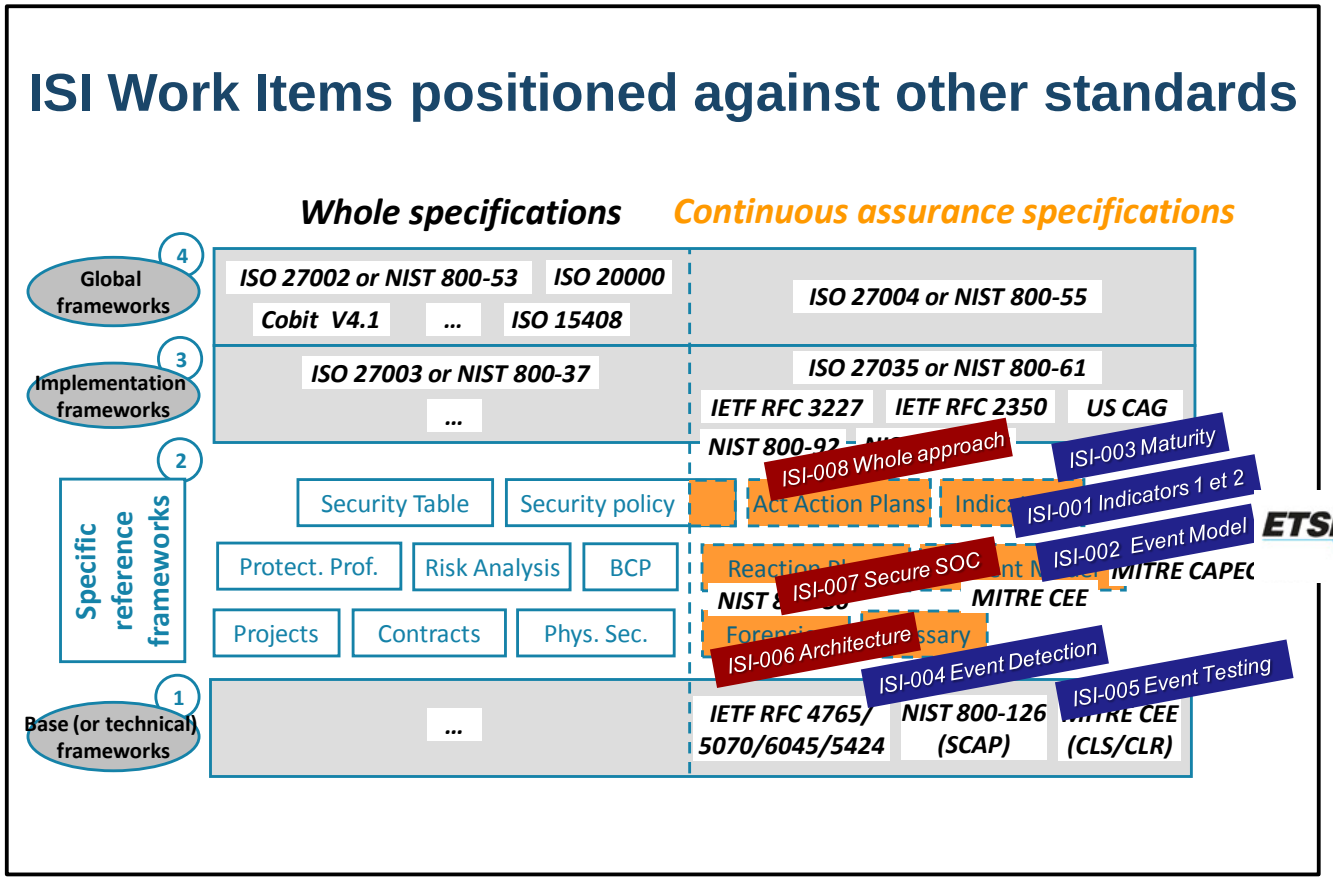
2. Un chemin idéal de maturité croissante (2)

La nécessité croissante d'un framework d'intégration



3. Potentialité du standard ETSI ISI (1)

8 standards ETSI ISI (dont 3 en développement)



3. Potentialité du standard ETSI ISI (2)

Pourquoi les indicateurs GS ISI-001 sont utilisés avec un succès croissant (8 usages au carrefour de l'expertise et du management)

■ Accélérer les progrès en Cybersécurité à travers une approche solide alignée sur les préoccupations du management

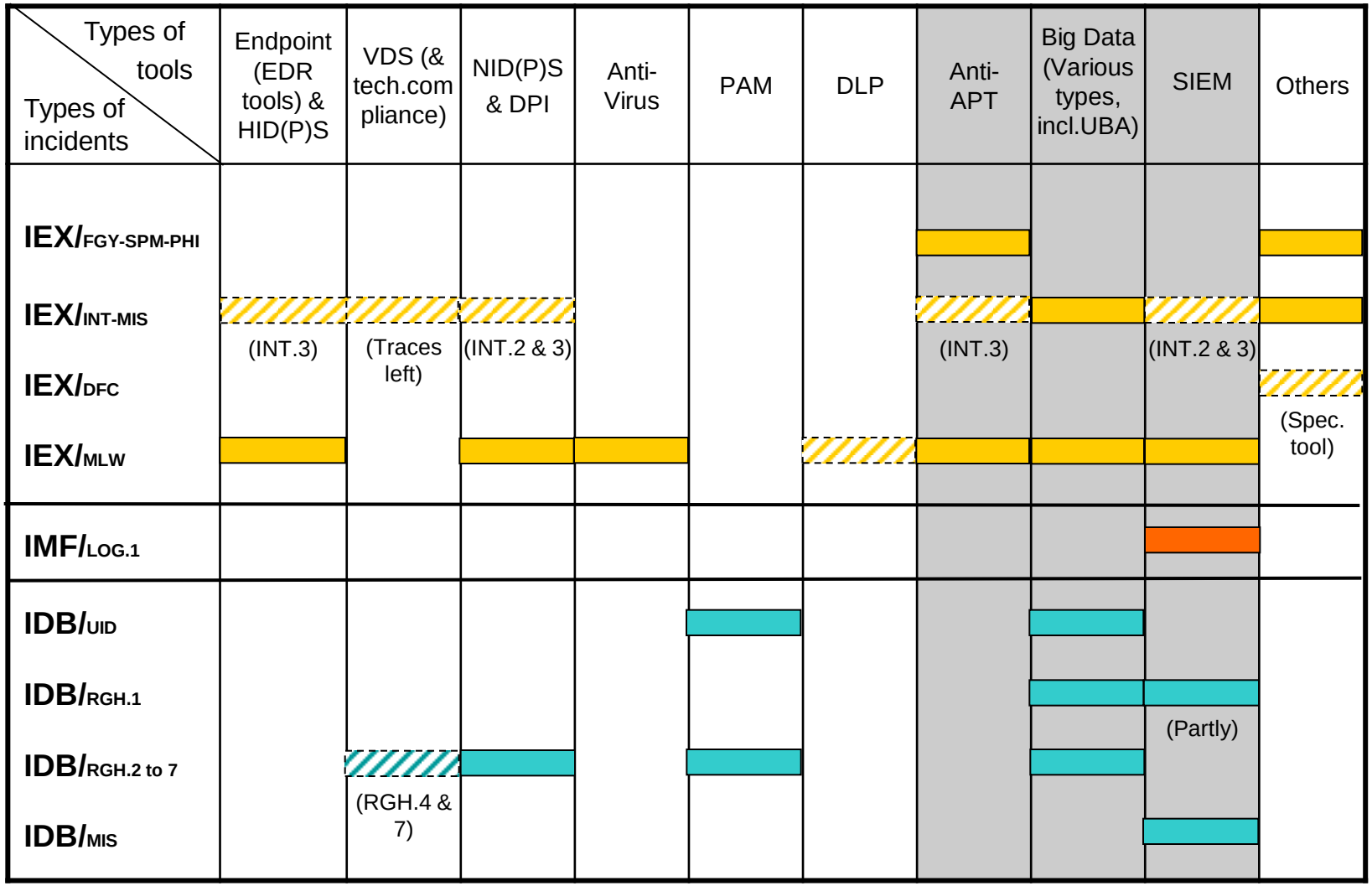
- ✓ Commissaires aux Comptes
- ✓ Dirigeants
- ✓ Responsables Opérations IT
- ✓ Responsables Ingénierie IT
- ✓ Management général et RSSI
- ✓ Ressources humaines/management

■ Stimuler les échanges au sein de la profession au-delà de ceux existant dans les communautés sécurité actuelles

- ✓ Collecter et partager l'expérience
- ✓ Faciliter la notification aux autorités

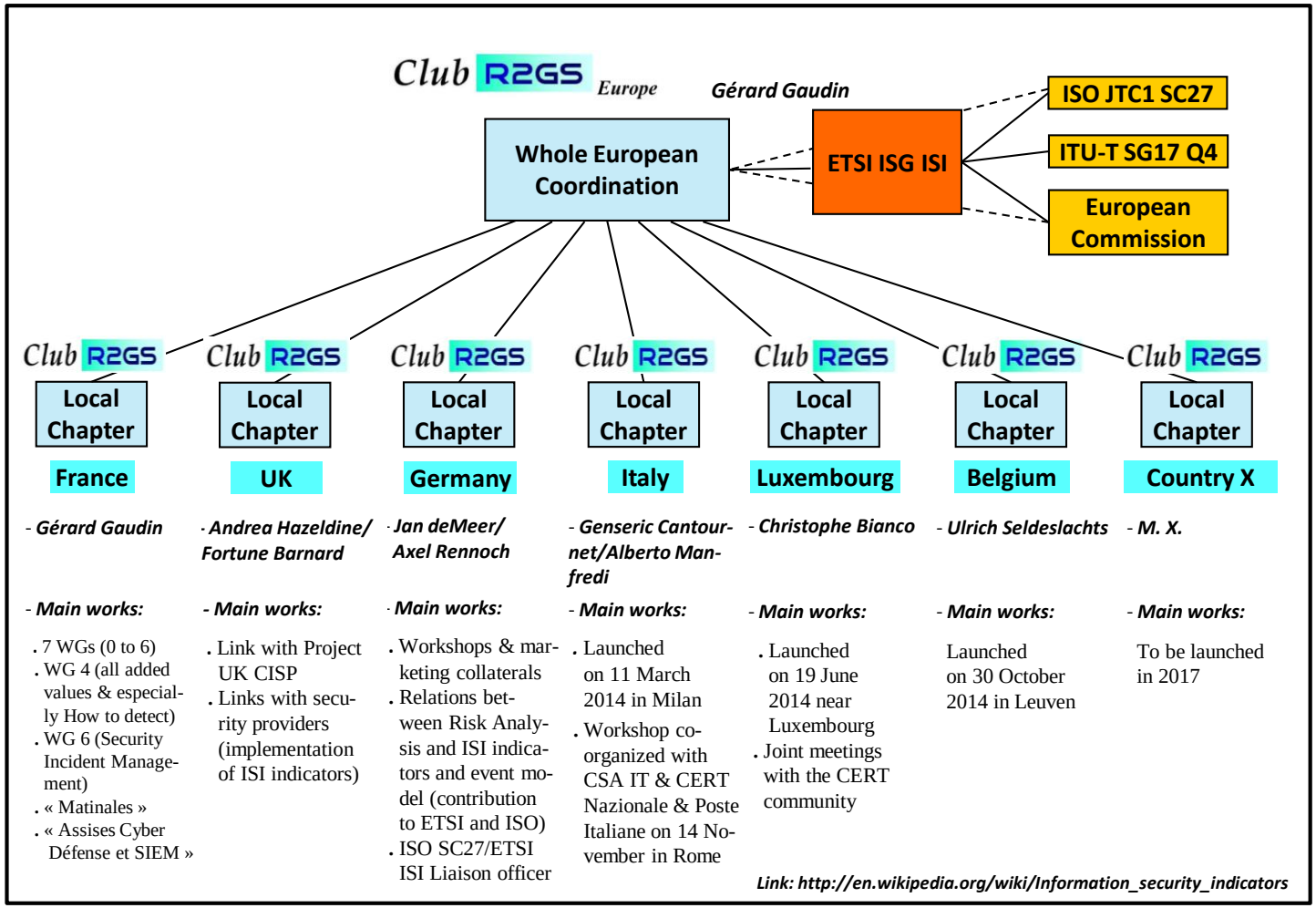
3. Potentialité du standard ETSI ISI (3)

Illustration avec le positionnement des10 types d'outils principaux



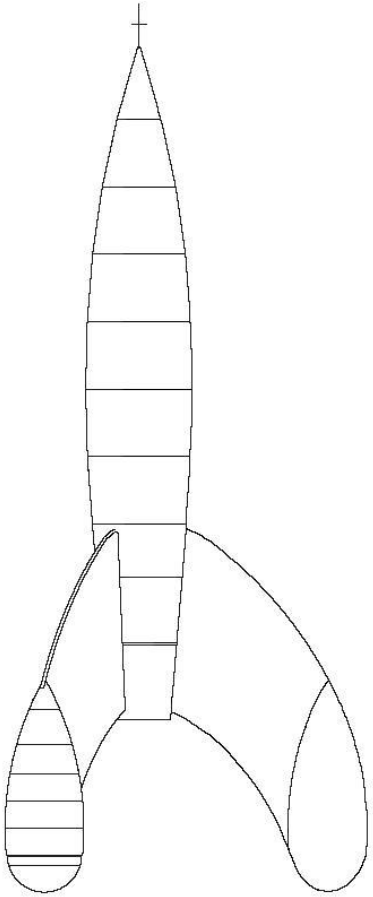
3. Potentialité du standard ETSI ISI (4)

Usages promus par le réseau Européen de Club R2GS



3. Potentialité du standard ETSI ISI (5)

Accélérer l'adoption de ETSI ISI en Europe : les 3 étages de la fusée



– 3 –
Coordination avec Agences SSI nationales (PPP) et éditeurs à partir de 2016

– 2 –
Europe et standard ETSI à partir de 2012

– 1 –
Club R2GS France (base OIV) à partir de 2009

3. Potentialité du standard ETSI ISI (6)

Relation avec réglementations en France et en Europe

- LPM volet Cyber et NIS Directive (projet)
  - ✓ Une impulsion nouvelle sur la détection des incidents
  - ✓ Apport du standard ETSI ISI pour catégoriser et notifier les incidents concernés (complémentaire de IDMEF/IODEF ou STIX/CyBox)
- Des prestataires de type MSSP à l'état de l'art encouragés par la publication de nouveaux référentiels ANSSI avec une dimension européenne potentielle
  - ✓ Détection PDIS (standard ETSI ISI recommandé)
  - ✓ PDIS base du futur standard ETSI ISI-007 (« Guidelines for building and operating a secure SOC »)
  - ✓ Réponse PRIS
- Règlement EU sur les données à caractère personnel
  - ✓ Apport de ETSI ISI pour catégoriser et notifier les incidents
- Effet levier des relations entre certains Etats