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.
Président de ETSI ISG ISI)

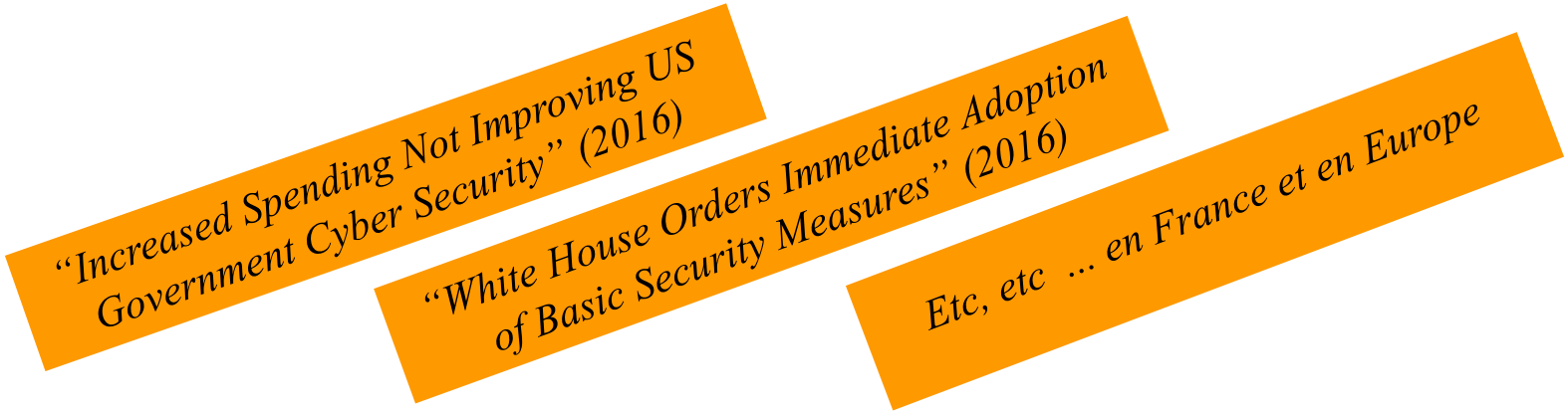
Le 10 novembre 2017

Colloque Institut Mines-Telecom

SOMMAIRE

1. Mise en mouvement des organisations encore faible au niveau Sécurité Opérationnelle

De bien maigres résultats malgré une mobilisation globale inégalée de la profession et au-delà



- De nombreux incidents continuent à exploiter des vulnérabilités de base et pourraient être facilement évités (DBIR 2016)
  - ✓ Référentiels d'hygiène encore peu appliqués malgré incitation SOCs
- Une certaine résistance des Directions de production IT
- Efficacité de la détection restant faible
- Réaction tardive et approximative (peu structurée)

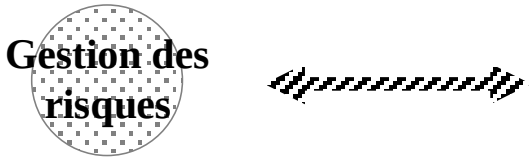
2. Quelques initiatives récentes nouvelles dans le domaine de la Sécurité Opérationnelle

Des espoirs placés sur le thème de la « Cyber intelligence »

- Avoir un niveau d'organisation et d'échanges au sein de la profession se rapprochant de celui des attaquants
- Exemples se multipliant :
  - ✓ Service nouveau proposé par Swift pour les banques
  - ✓ Services avec des valeurs ajoutées croissantes
  - ✓ Nombreux secteurs d'activités ayant développé des ISACs (USA, et maintenant en Europe)
- Mais encore une approche exclusivement technique et de spécialistes …
- Quelle Valeur Ajoutée réelle dans l'écosystème de plus en plus complexe de la détection ?

3. Deux valeurs ajoutées pour aider au déblocage de cette situation frustrante

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



A

Lien quantifié entre incidents techniques et profils de risques d'entreprise

- SSI décloisonnée
- Dialogue plus stratégique avec le COMEX
- Échanges avec le business et le management (nouveaux leviers)
- Objectivité et transparence

B

Lien quantifié entre événements techniques et référentiels généraux

« Top 20 » Global SI

Indicateurs

Cyber Défense/ GOS/SIEM

C

Prise de décision avec chiffres et benchmarking des résultats

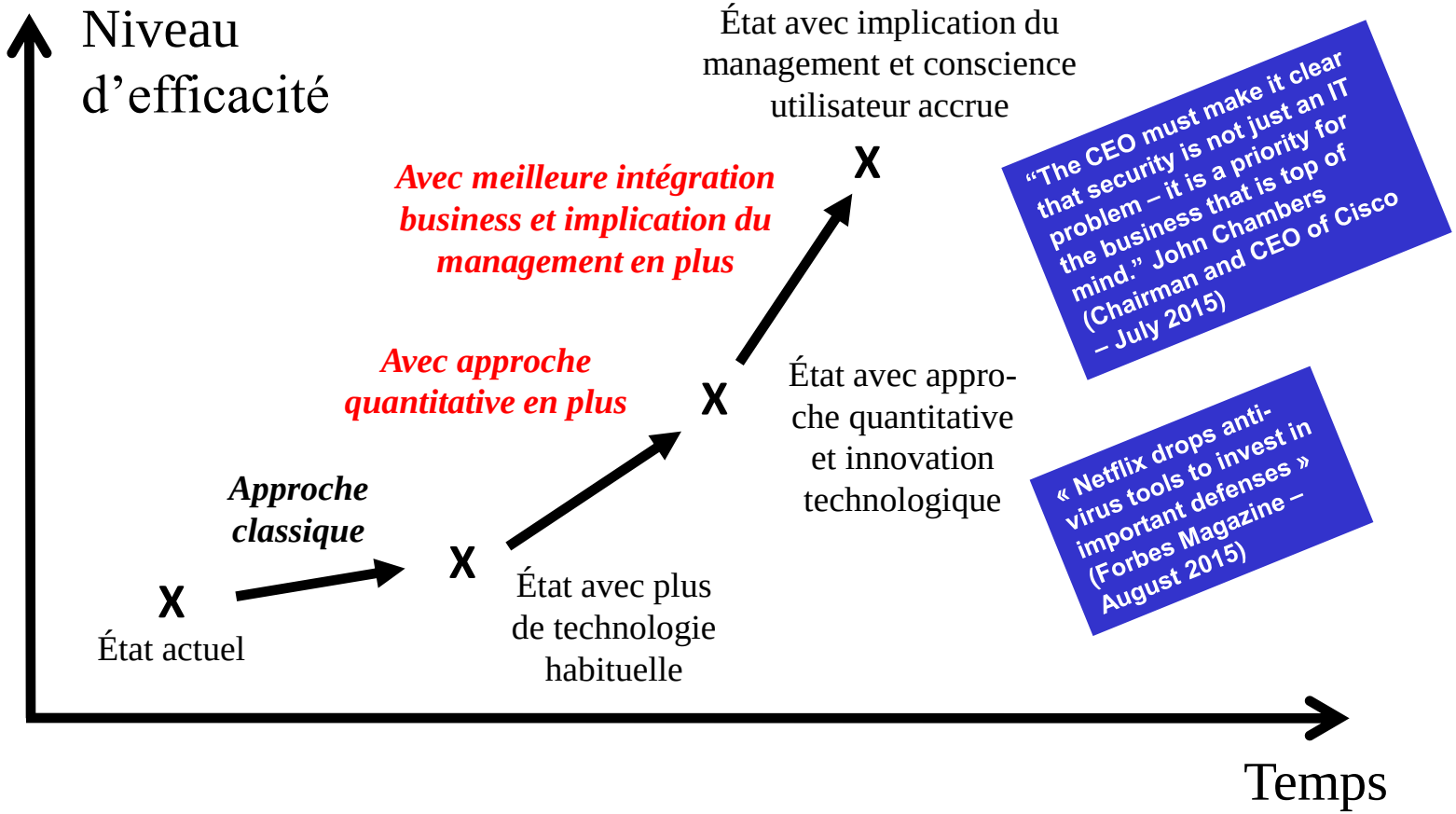
D

Meilleur apport outils + équipes opérationnelles, et « awareness » + utilisateurs

4. Un chemin idéal de maturité croissante (1)

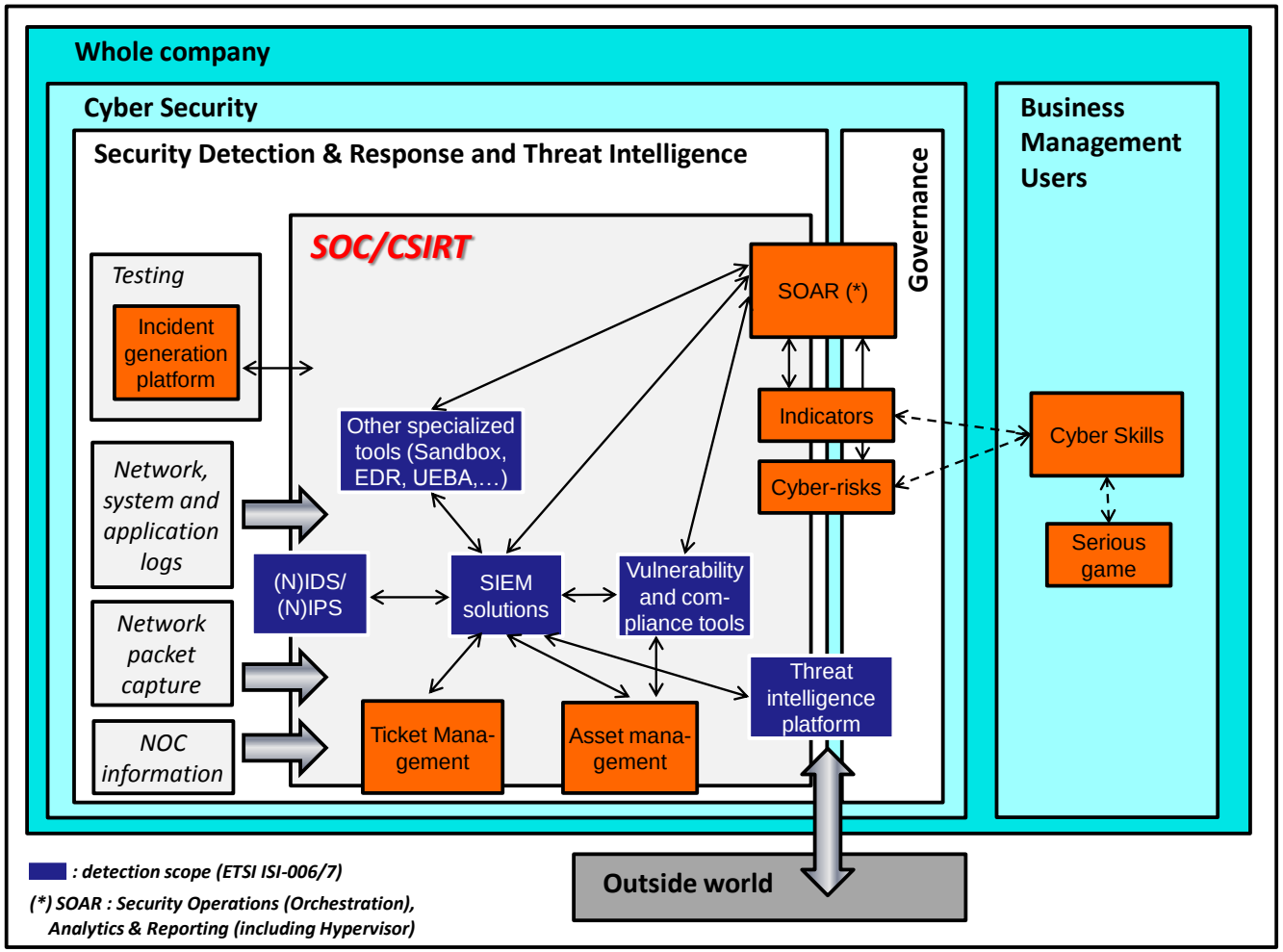
Des objectifs plus ambitieux atteignables

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



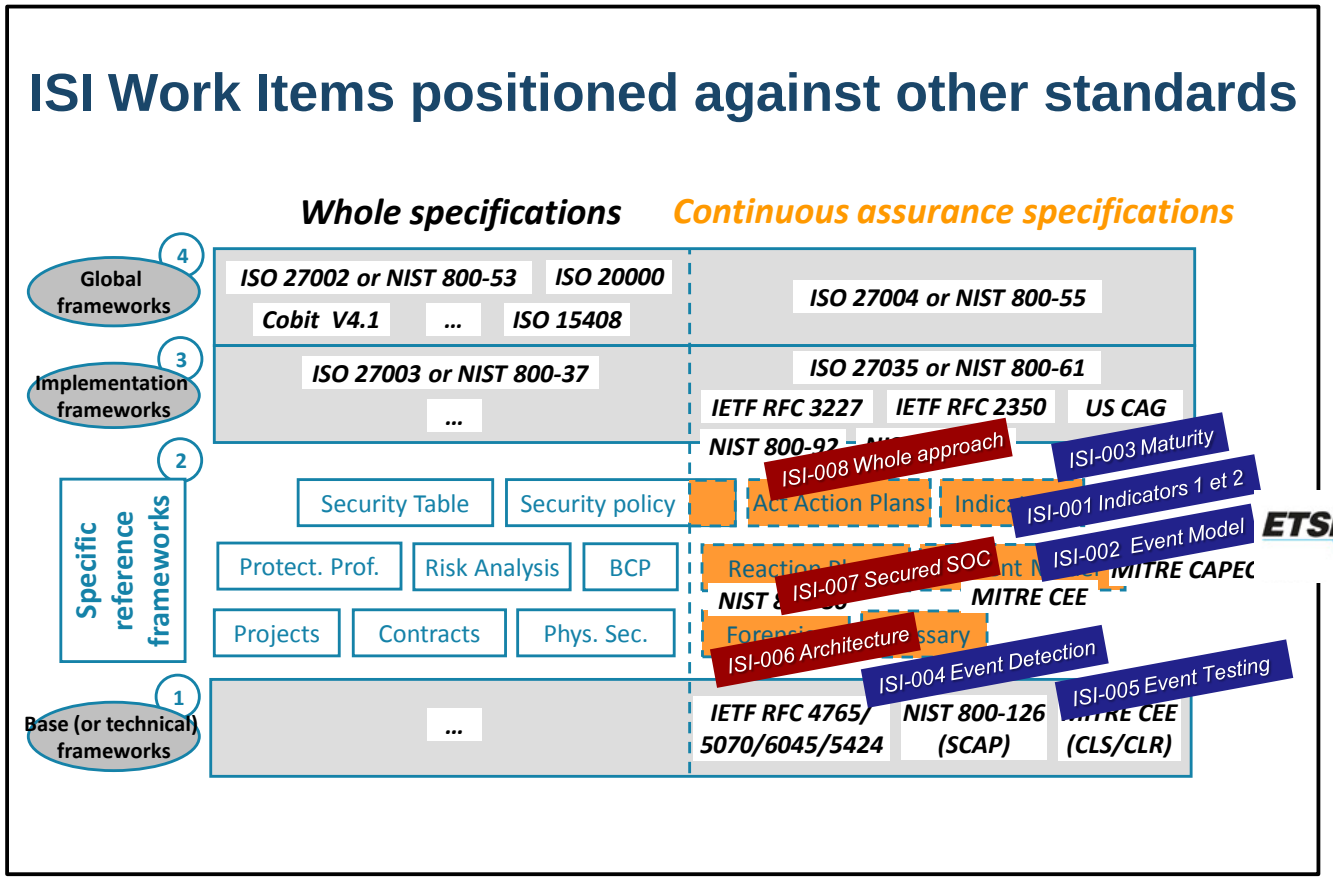
4. Un chemin idéal de maturité croissante (2)

La nécessité croissante d'un framework d'intégration en détection



5. Potentialité du standard ETSI ISI (1)

3 nouveaux standards ISI en développement (Phase 2)



5. Potentialité du standard ETSI ISI (2)

Un usage de base pour évaluer les niveaux de conformité et d'assurance relatifs à des référentiels généraux

ISO 27002 control areas	ISO 27006 technical control areas	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
A5				Non-continuous checking
A6				Purely organisational issues
A7		IWH_UNA.1	VTC_NRG.1 VOR_PRT.1	Information classification + asset management
A8	x	IMF_LOM.1 IDB_UID.1 IDB_RGH.1 to 7 IDB_IDB.1 IDB_MIS.1 IDB_IAC.1 IDB_LOG.1	VBH_PRC.1 to 6 VBH_IAC.1 to 2 VBH_FTR.1 to 3 VBH_WTI. 1 to 6 VBH_PSW.1 to 3 VBH_RGH.1 VBH_HUW.1 to 2	Focus on deviant internal behaviours
A9	x	IEX_PHY.1	VTC_PHY.1	Marginal topic for a SIEM approach
...	...	...	...	...
A15	**XX**	IMF_TRF.2 to 3	VBH_IAC.2 VBH_WTI.2 VBH_WTI.6 VBH_RGH.1 VCF_DIS.1 VCF_TRF.1 VCF_FWR.1 VCF_ARN.1 VCF_UAC.1 to 3 VTC_IDS.1	Focus on configuration vulnerabilities or non-conformities

5. Potentialité du standard ETSI ISI (3)

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

Niveau haut
- ✓ Commissaires aux Comptes
- ✓ Dirigeants
- ✓ DSI/RSSI
- ✓ Ressources humaines/management

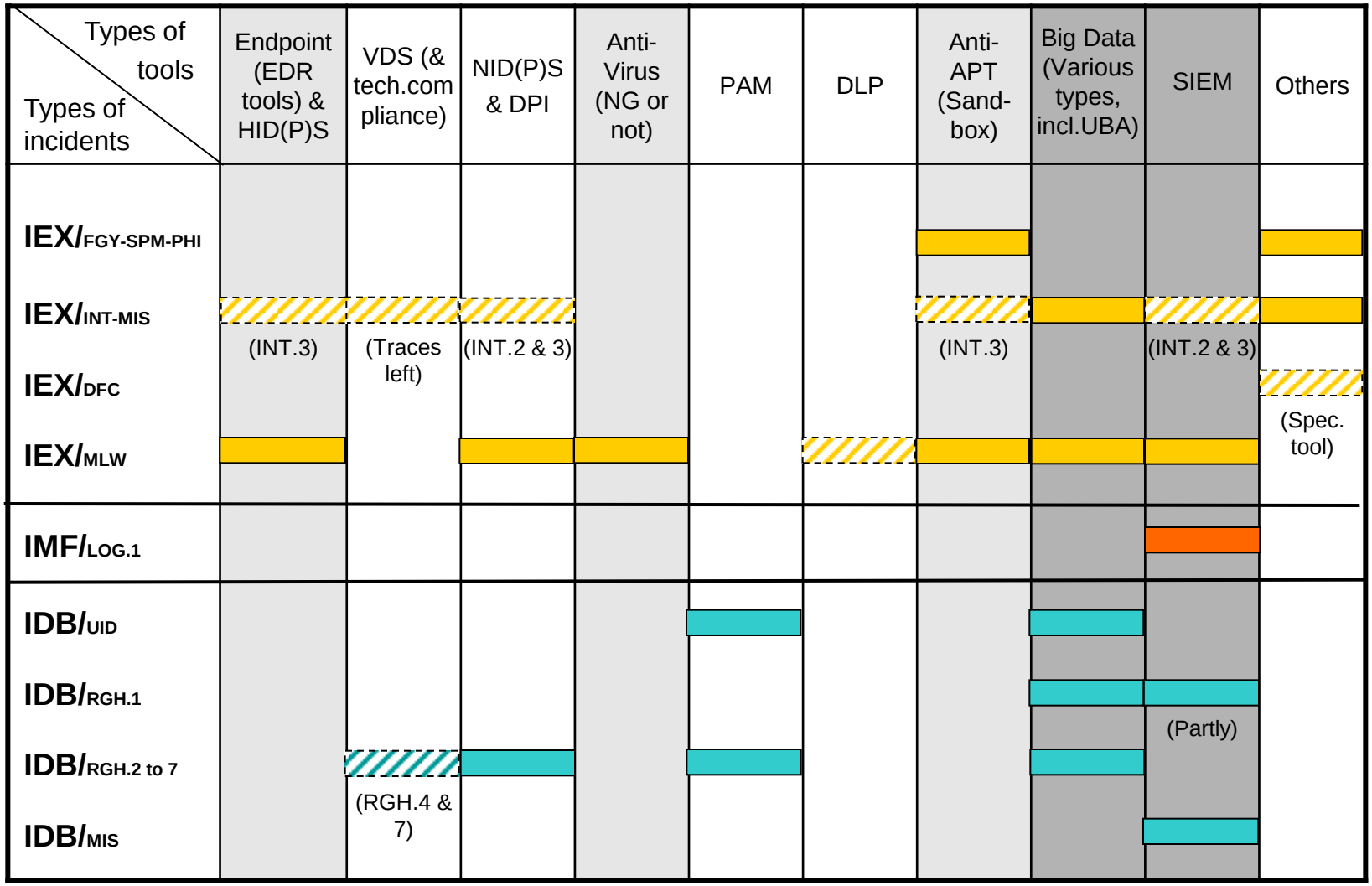
Niveau bas
- ✓ Responsables Opérations IT
- ✓ Responsables Ingénierie IT

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

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

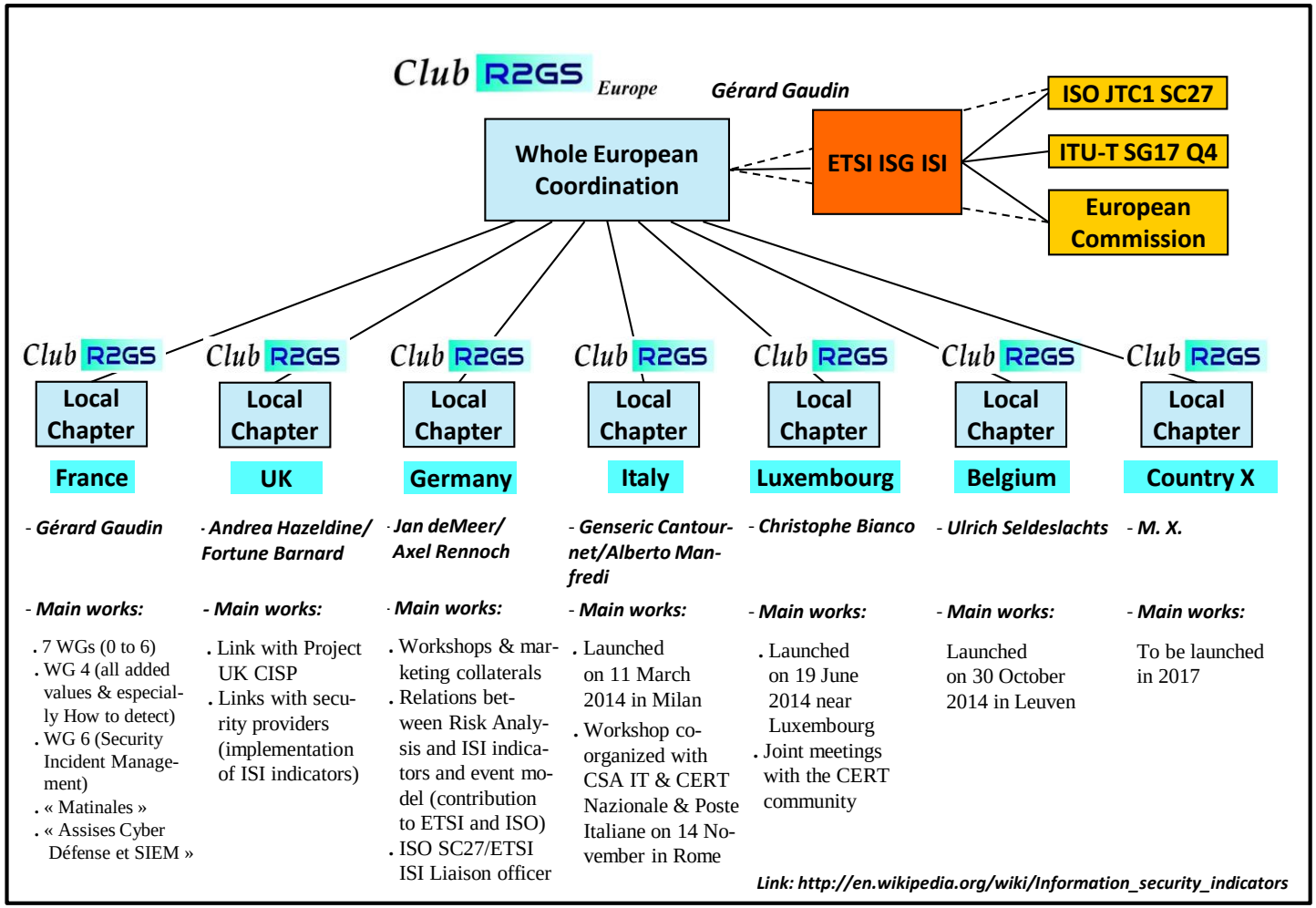
5. Potentialité du standard ETSI ISI (4)

Illustration avec le positionnement des10 types d'outils principaux



5. Potentialité du standard ETSI ISI (5)

Usages promus par le réseau Européen de Club R2GS



5. Potentialité du standard ETSI ISI (6)

Relation avec les réglementations en France et en Europe

- LPM volet Cyber et NIS Directive
  - ✓ 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), et pour élaborer des statistiques en Europe
- 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 (ETSI ISI recommandé, et futur standard ISI-007)
  - ✓ Réponse PRIS
- Règlement EU sur les données à caractère personnel
  - ✓ Apport de ETSI ISI pour catégoriser et notifier les incidents, et élaborer des statistiques
- Effet levier des relations entre certains Etats
- ETSI ISI salué lors du 1er Colloque ENISA/Cen-Cenelec/ETSI/Commission EU du 19 septembre 2017

6. Repenser la démarche globale en Cyber sécurité

Besoin d'un changement radical de paradigme : les 3 composantes clés d'une démarche repensée

- Impliquer le *management* de l'entreprise *à tous les niveaux*
  - ✓ Abord des cyber risques comme les autres risques majeurs (avec une vision synthétique objective et quantifiée des risques)
  - ✓ Rendre l'ensemble du management plus concerné, en impliquant les dirigeants dans la valorisation des employés les plus participatifs …
  - ✓ … et en mettant dans les mains des managers des méthodes et outils nouveaux (PPI et Team building) pour les pousser à s'engager (Approche plus bottom-up)
- Jouer sur des *leviers de motivation* innovants pour mobiliser et engager, avec mesure nécessaire des progrès en hygiène informatique (30 indicateurs possibles)
- Montrer volonté de changement des responsables SSI
  - ✓ Prise en compte meilleure des besoins business et de facilité d'usage
  - ✓ Simplification des processus IT associés

7. Des raisons d'espérer en une résolution des défis posés

Un chemin aujourd'hui mieux balisé pour permettre à l'entreprise de se protéger plus efficacement

- Une communauté d'utilisateurs avancés (en France, et progressivement en Europe) partage, se coordonne et veut progresser
- Les instances patronales commencent à se saisir du sujet
- Volonté politique de faire face des États se développe (Occident)
- Monde de l'assurance (cyber) commence à bouger

→ *Mais le handicap des usages de plus en plus libres et personnels persistera (le plus gros challenge)*

→ *Et les Directions Générales restent encore souvent à convaincre de l'importance de leur implication plus nette*