CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

L'apport clé d'un standard d'indicateurs de sécurité pour benchmarker le niveau de sécurité de son système d'information

Gérard GAUDIN

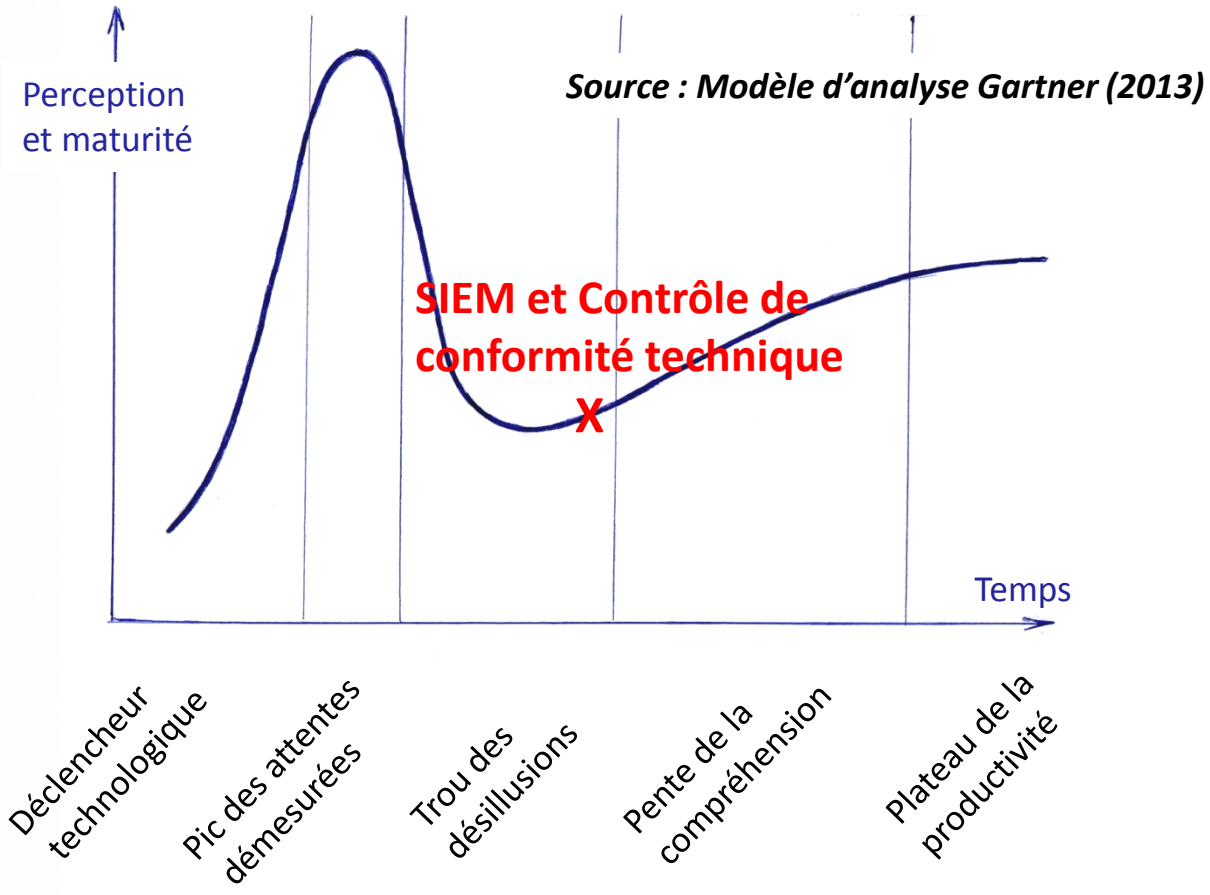
(Consultant indépendant G²C et
Président du Club R2GS)

Club R2GS

Sommaire

- État et maturité du domaine Cyber défense et SIEM
- Le besoin de passer d'une culture qualitative à une culture quantitative
- Besoin d'un nouveau standard en Cyber défense
- Des chiffres statistiques d'état de l'art disponibles
- Huit usages clés au carrefour « expertise/management »
- Une démarche globale de gestion de la sécurité en cours d'adoption rapide en France et en Europe
- Conclusion

État et maturité du domaine Cyber Défense et SIEM



Le besoin de passer d'une culture qualitative à quantitative en Cyber sécurité

- Des initiatives tous azimuts pour de maigres résultats, mais tout n'a pas encore été fait …
- 2 axes restent à développer
  - Chiffres statistiques d'état de l'art neutres, partagés et incontestés (Incidents et vulnérabilités)
  - Meilleur dialogue RSSI avec Top management pour mobiliser l'entreprise (70 % des incidents impliquant l'humain)

- Sens véritable reconnu au niveau international des initiatives « Réseau européen Club R2GS » et « Standard ETSI ISG ISI »

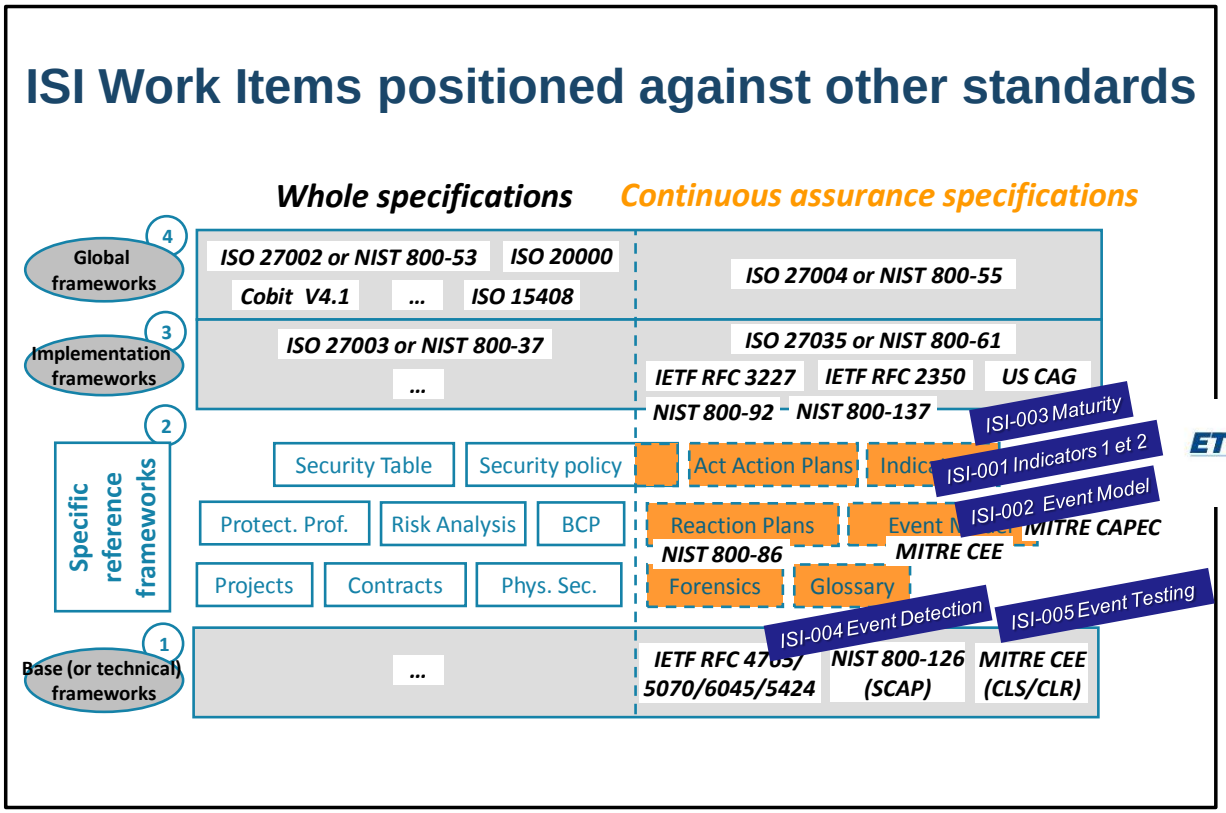
Club R2GS ETSI

- Et sens d'une nouvelle initiative relative au 2ème axe présentée dans le cadre du FIC 2014

FIC 2014 DIGITAL IDENTITY AND TRUST 6th International Forum on Cybersecurity

Atelier animé par DIA et G²C

Besoin d'un nouveau standard en Cyber Défense : un vide criant comblé en assurance Cyber sécurité continue



Des chiffres statistiques d'état de l'art disponibles : faisabilité de la démarche de benchmarking prouvée par G²C

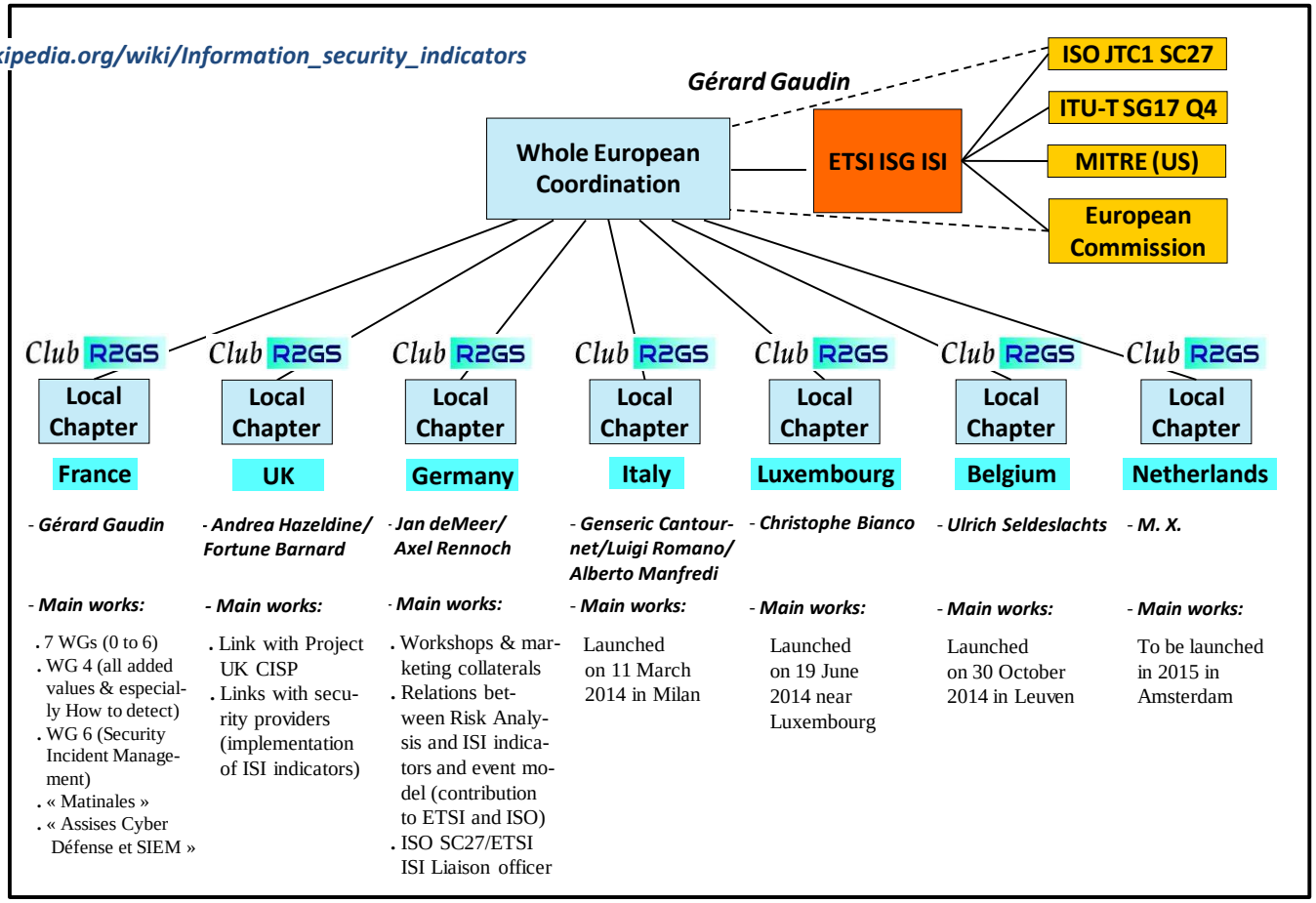
	État de l'art (par mois)	Écart pays	Niveau de dispersion	Degré d'impré-cision (1)	Périmètre de l'indi-cateur	Source (s)	Pério-dicité
IEX_ PHI.1	33 cam-pagnes (3)	Oui (uni-que ment Fr & All)	100 % par rapport à état de l'art (entre -70 % et +50 %)	1	(2)	RSA + chiffres complé mentaires sur typo-logie (4)	Trimes-triel
IEX_ DOS.1	0,008 attaque DDoS	Non	80 % par rapport à état de l'art (entre -50 % et +50 %)	1	Par site Web	CSI et Panel de 15	Annuel + affi-nage tri-mestriel
IEX_ MLW.4	1,5 malware installé avec suc-cès sur des serveurs (8)	Non	80 % par rapport à état de l'art (entre -35 % et +65 %)	3	Par ensem-ble de 10.000 serveurs	CSI et Panel de 15	Annuel + affi-nage tri-mestriel
VCF_ UAC.3	6 comptes non conformes	Non	50 % par rapport à état de l'art (entre -60 % et +40 %)	3	Par base de données ou par applica-tion	Panel de 15	Trimes-triel

Huit usages clés au carrefour « expertise/ management » : pourquoi les indicateurs GS ISI-001 sont utilisés avec un succès croissant

- 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

Une démarche globale de gestion de la sécurité en cours d'adoption rapide en France et en Europe

Link: http://en.wikipedia.org/wiki/Information_security_indicators



Des raisons d'espérer en une résolution des défis posés, avec un chemin aujourd'hui 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
- La volonté politique de faire face des États se développe (Occident)
- 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