Quel apport de la normalisation à la Cybersécurité ?
Evaluation et qualification : la problématique de la Cybersécurité

Jean-Pierre Quémard
Président ACN (alliance pour la confiance numérique)
Président CN 27 SSI, Chairman CSCG,
Vice Chairman ETSI TC Cybersecurity

Le contexte spécifique de la cybersécurité

- La cybersécurité est transversale par nature tout traitement de données est potentiellement affecté
- Initialement pris en charge par les acteurs de l'IT (sécurité informatique ciblant les RSSI) a progressivement débordé et couvert tous les domaines d'applications du fait de la numérisation croissante de l'industrie et des services :
  - Santé,
  - Energie (smart grids, ..),
  - Transport
  - Smart cities,
  - Communication, ….
- Avec une préoccupation duale : Comment garantir la **sécurité** des personnes et des biens tout en garantissant les libertés individuelles (**notion de privacy**).

ISO

- L'ISO est l'un des trois organismes internationaux en charge de la standardisation avec l'ITU et l'IEC
- Au sein de l'ISO deux organismes principaux sont en charge de la sécurité :
  - L'ISO/IEC JTC1 SC27 IT Security Techniques
    - 149 standards publiés, 50 pays participants, 20 pays observateurs
    - 5 groupes spécifiques ISMS, Crypto, évaluation applications, privacy et biométrie
  - L'ISO TC 292 « Security and resilience » couvrant les autres aspects de la sécurité (infrastructures critiques, sécurité sociétale, gestion de crise lutte contre la fraude , …) la France est chairman du WG 6 homeland security.
  - Mais il y a également le SC17 Cards and personal identification , le SC37 Biometrics, le SC 38 Cloud Computing and Distributed Platforms, etc
  - Liaison du SC27 avec le TC 22 automotive : exemple de coopération trans working groups.

IEC/ITU

- L'IEC a également deux TC traitant de problèmes de sécurité.
- Le TC 65 (Industrial-Process Measurement, Control & Automation)
  - IEC 62443: Industrial Automation and Control Systems Security
  - Development in IEC TC65 WG10 (IEC 62443) and in the International Society of Automation (ISA) 99 (ANSI/ISA-62443)
  - Liaison existante avec le SC27
- Le TC 57 (POWER SYSTEMS management and associated information exchange)
  - IEC 62351: Data and communication security
  - Development in IEC TC57 WG15
  - Scope Power Automation and Smart Grids
- L'ITU a également le groupe ITU-T SG17 qui traite de problèmes de sécurité ainsi que le 3GPP SA3

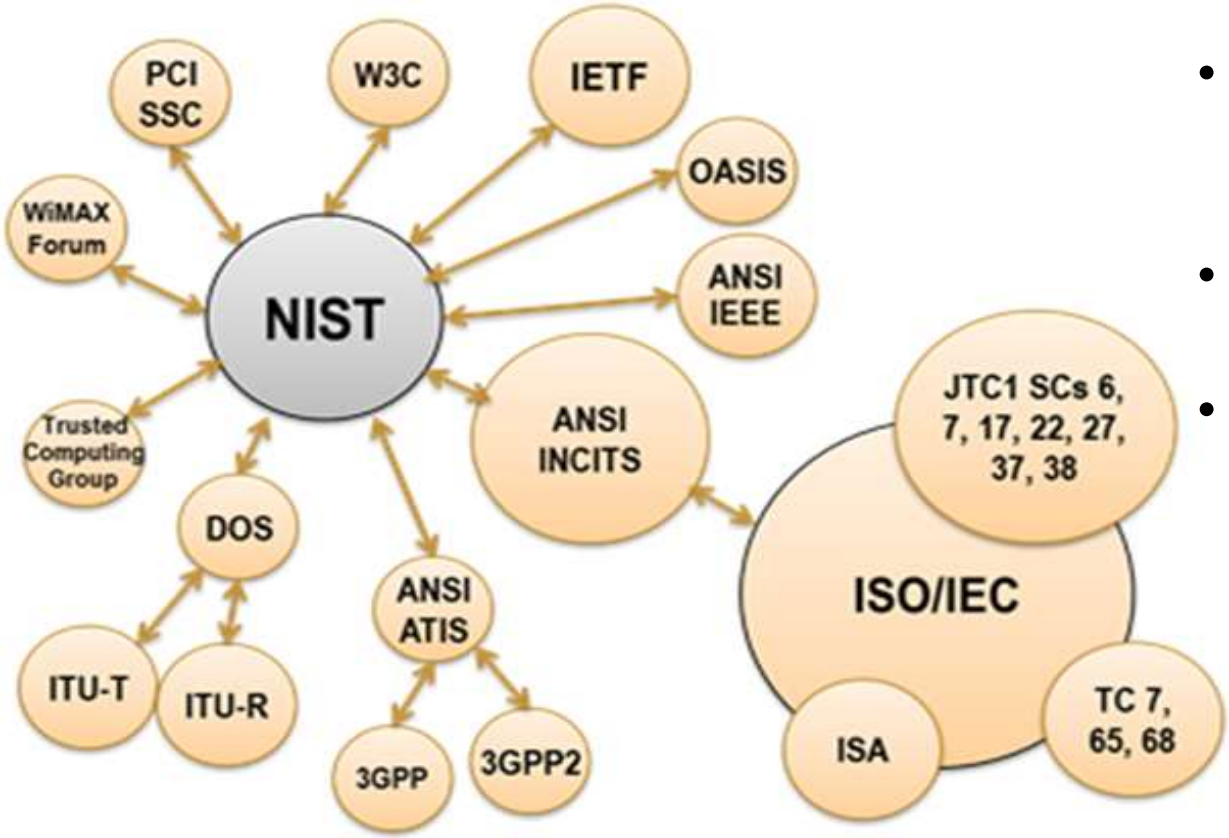
Le niveau Européen

- Trois ESO (European standardisation organisation) sont en charge de la standardisation CEN, CENELEC et ETSI. Fonctionnement sur mandat de la commission européenne. Structure différente entre CEN, CENELEC et ETSI
  - Exemple le mandat M530 sur le privacy by design confié au JWG 8 du CEN/CENELEC avec le support de l'ETSI
  - ou le CEN TC 391 « sécurité sociétale et protection du citoyen »
  - Le TC Cybersecurity de l'ETSI sujets traités : le post quantum computing , security assurance by default, structured information sharing, ..
- Une structure légère de coordination le focus CSCG cyber Security Coordination group sous tutelle CEN/CENELEC avec la participation des DG Connect et Grow ainsi que de l'ENISA (Agence de sécurité Européenne)

Le niveau national

- L'AFNOR est le National Body (NB) représentatif officiel au titre du schéma national de normalisation géré par la DGE au sein du Ministère de l'industrie
- A ce titre l'AFNOR anime les comités miroirs de normalisation pour l'ISO et le CENELEC
- La CN 27 SSI est le miroir du JTC1 SC 27 et du JWG 8 dépendant du COS (Comité d'orientation stratégique) ICN
- Le CoFIS (Comité de filière des industries de la sécurité) anime une sous commission normalisation sous co-présidence CICS/DGE.

Le niveau international un exemple le NIST



- Organisme Américain équivalent « commercial » de la NSA dépend du DoC
- Le NIST est très actif dans le domaine de la cybersécurité
- L'ANSI est l'équivalent US de l'AFNOR

Les apports de la normalisation

- Définir des mécanismes, protocoles, processes, méthodes, .. reconnus largement au niveau national, européen ou international.
- Favoriser l'interopérabilité
- Protéger la propriété intellectuelle
- Eviter les duplications d'efforts
- Tirer parti d'un réseau d'experts vaste et reconnus

Un enjeu stratégique :la qualification des produits et services

- Comment évaluer les produits et services ?
- Quels niveaux de sécurité ?
- Quelles méthodes ?
- Comment reconnaitre les certifications entre différents pays ?
- Les pistes :
  - Certification critères communs ISO/IEC 15408/18045
  - Certifiaction de type CSPN
  - Auto certification pour les niveaux le plus bas mais reposant sur des standards connus

Conclusion

- Le paysage de la standardisation en cybersécurité est complexe,
- Beaucoup d’acteurs et d’intervenants a tous niveaux, verticaux det tranversaux
- La Normalisation est un bon point d’entrée pour avoir une vision globale.

Merci de votre attention.

Questions ?