CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Panorama des référentiels et clés pour initier une démarche de sécurité

Conférence du 18 décembre 2014

Gérôme BILLOIS, Senior Manager Solucom, Administrateur du CLUSIF
gerome.billois@solucom.fr Twitter @gbillois

Contributions à l'étude

Analyse réalisée par un groupe de travail pluriel :

- Alctatel-Lucent
- Amossys
- Andra Cigéo
- Cassidian
- Cabestan Consultants
- Conix
- Hervé Schauer Consultants
- Itekia
- Michelin
- Qualware Consulting
- RATP
- RTE
- Sogeti
- Solucom
- Trend Micro
- Verizon Enterprise Solutions
- Wallix

Le choix des sujets et les propos tenus n'engagent pas les entreprises et organismes ayant participé au groupe de travail. Certains participants n'ont pas souhaité apparaître.

Objectifs de l'étude

- **Construire un panorama des documents traitant de la sécurité des SI industriels**

- **Donner les clés pour démarrer une démarche de sécurisation des réseaux industriels**

Objectifs de l'étude

- **Construire un panorama des documents traitant de la sécurité des SI industriels**

- **Donner les clés pour démarrer une démarche de sécurisation des réseaux industriels**

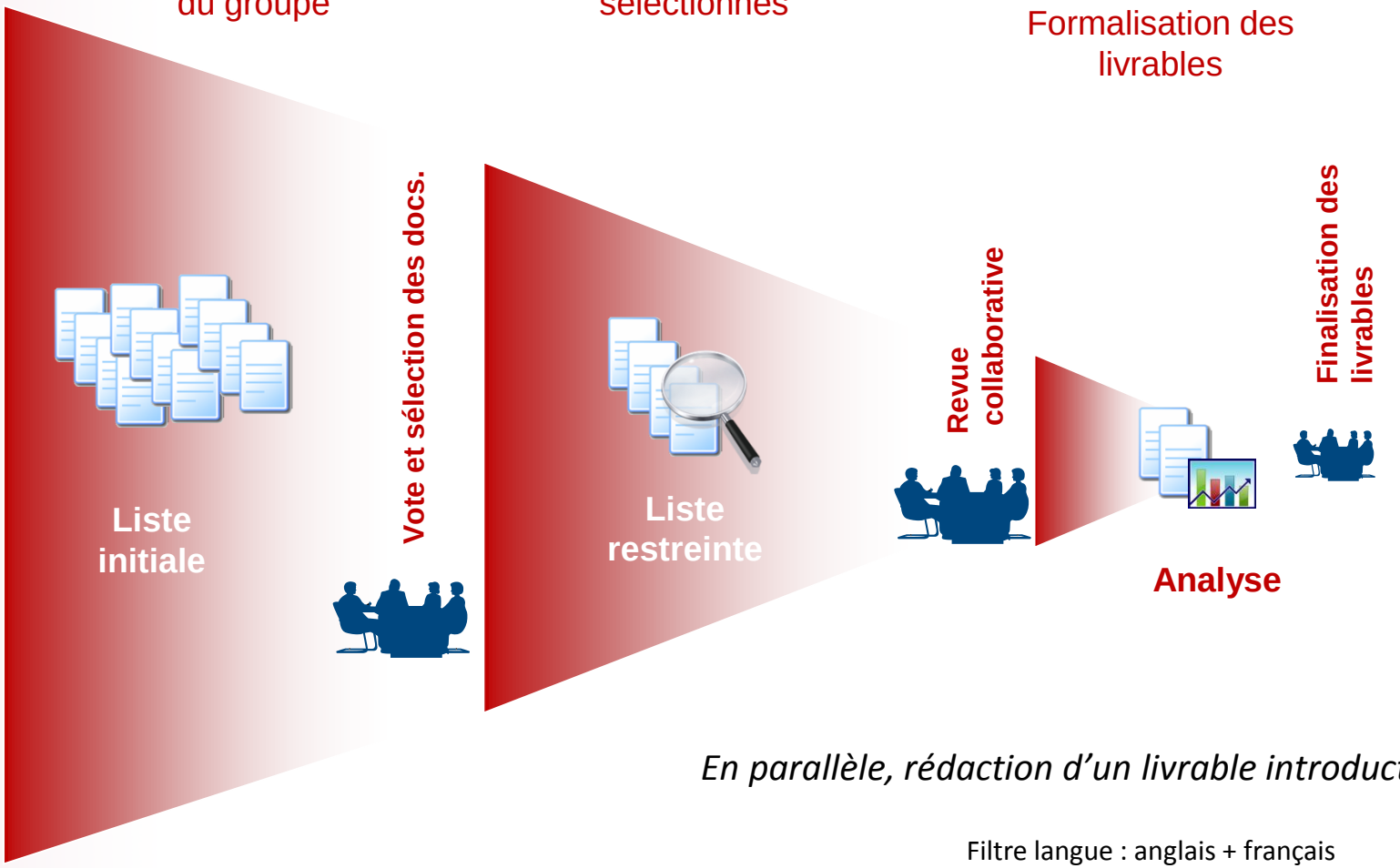
Méthodologie

Identification des documents par l'ensemble des membres du groupe

Relecture des documents sélectionnés

Analyse des documents

Formalisation des livrables



En parallèle, rédaction d'un livrable introductif

Filtre langue : anglais + français

Panorama : Une littérature abondante et très variée

Un sujet clé pour de très nombreux organismes

- États, fournisseurs, organismes de normalisation…

Qui ont émis une multitude de documents

- 53 documents identifiés par les membres du groupe

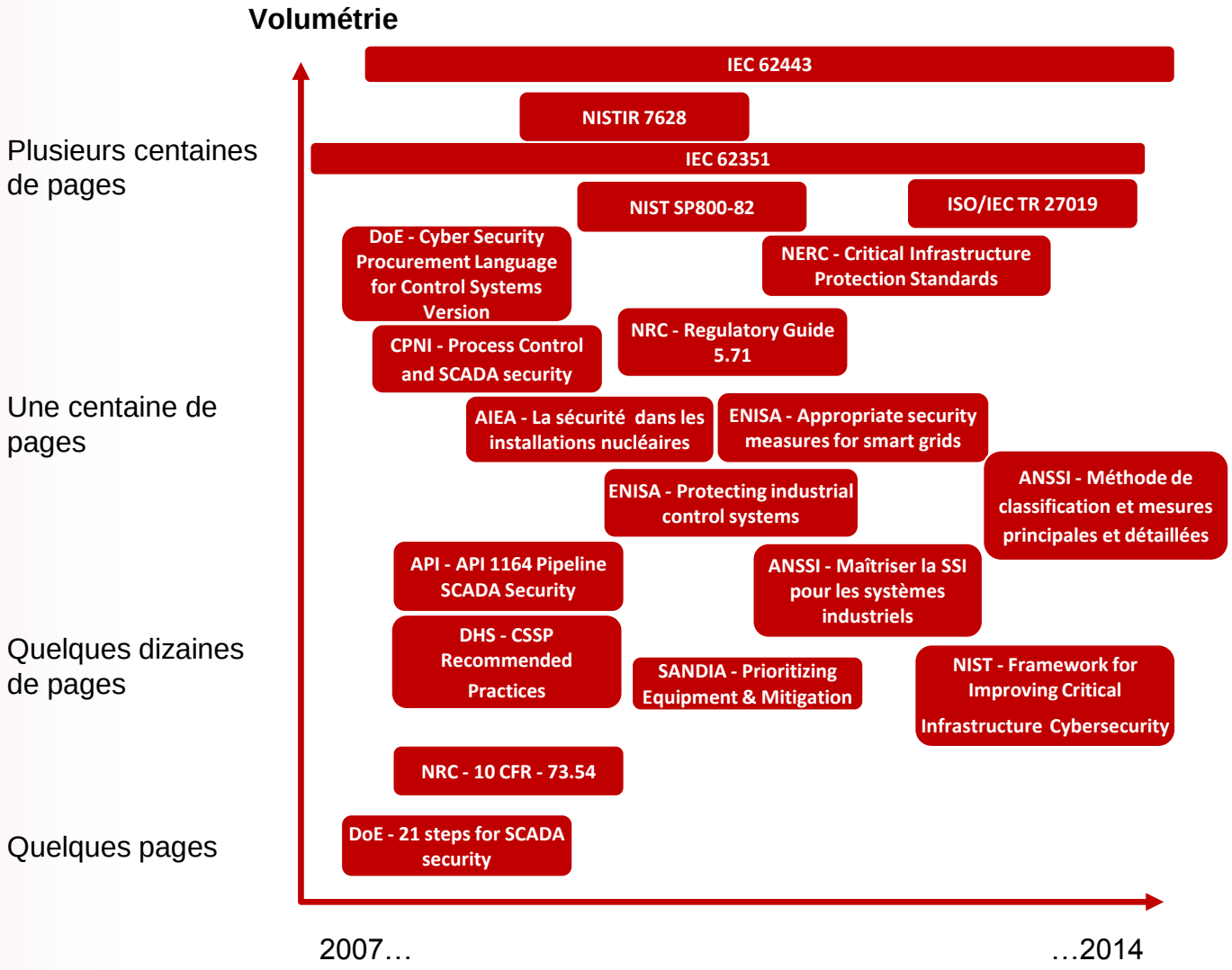
Au final 27 documents relus

- Plus de 4000 pages…

Et une sélection de 20

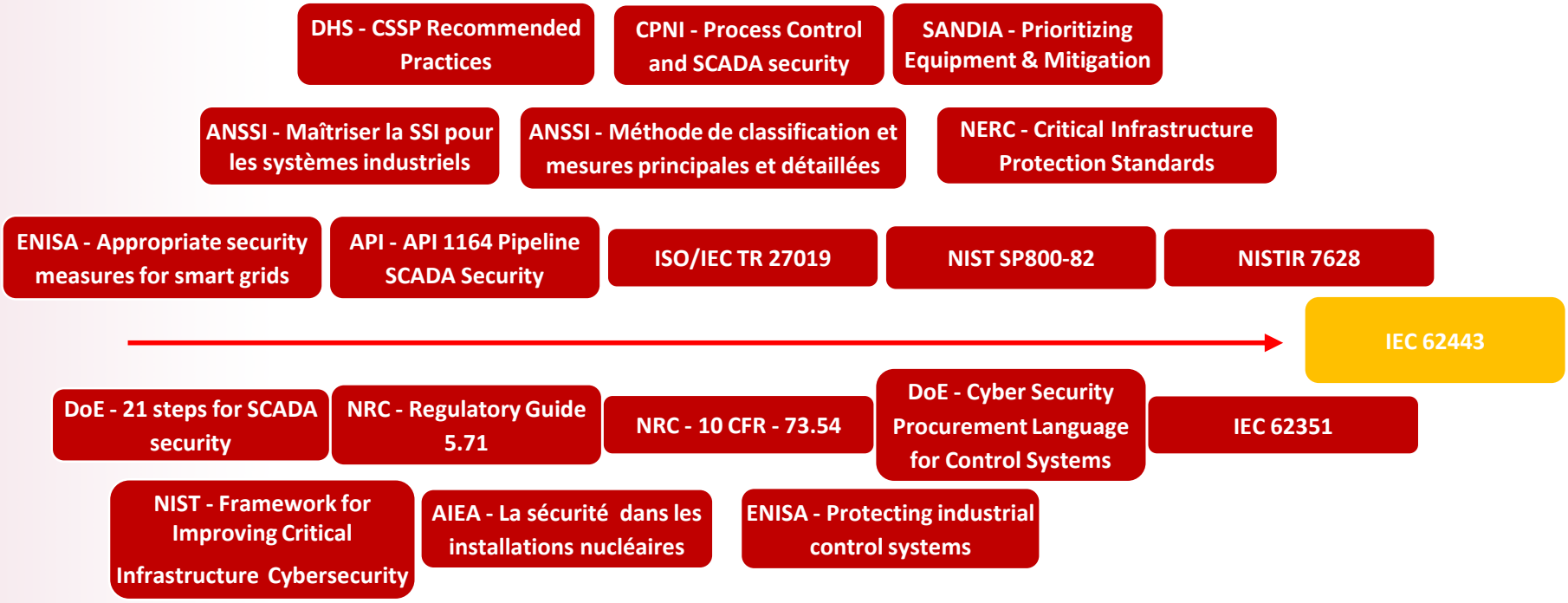
- En fonction de la pertinence de leur contenu, de leur lisibilité et de leur utilisation sur le terrain

Une littérature abondante et très variée

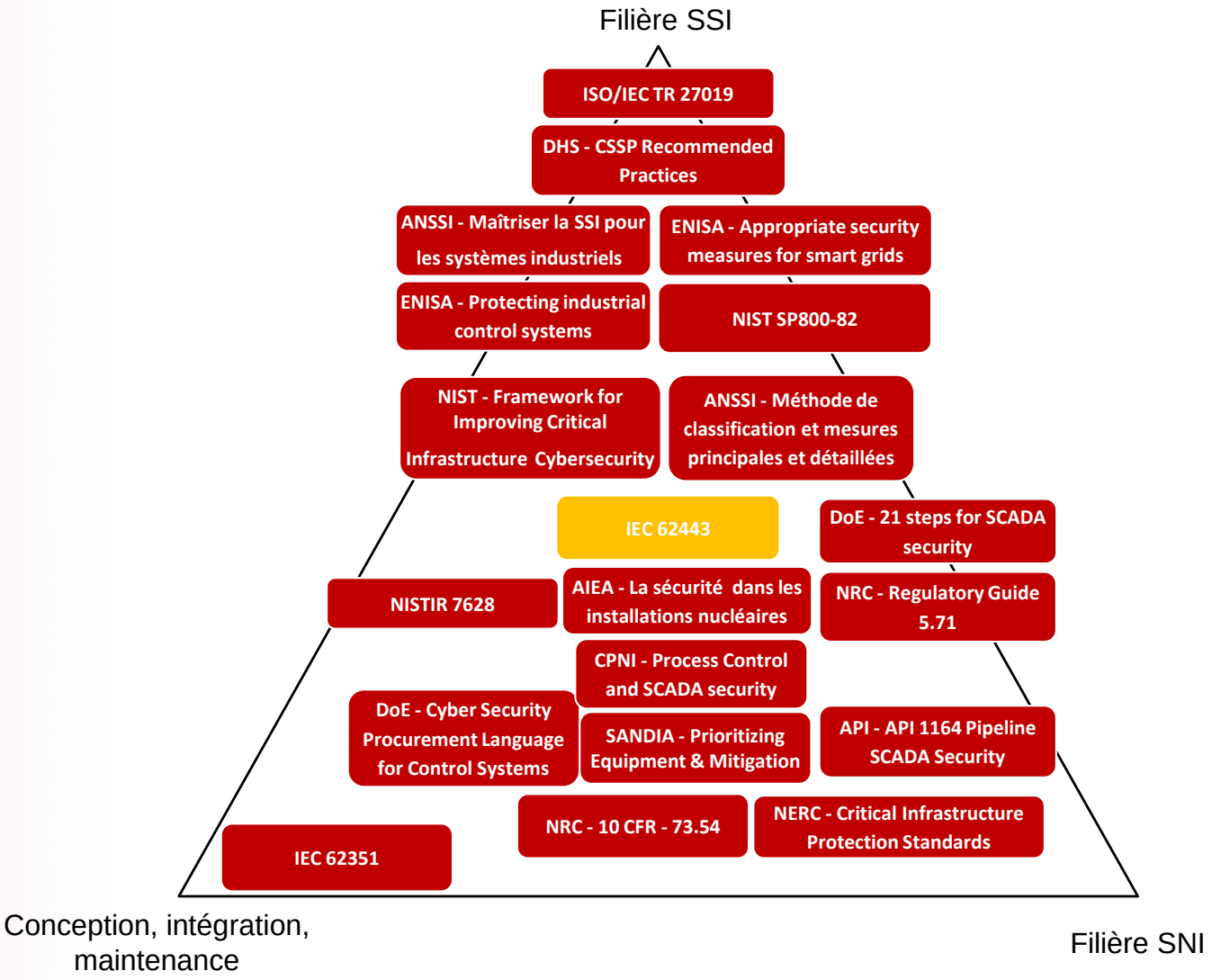


Des typologies de documents très variables

De l'introductif… …au plus spécialisé



Des documents utiles pour des populations différentes



Des incontournables

Les incontournables pour démarrer

- ANSSI - Maîtriser la SSI pour les systèmes industriels
- NIST SP800-82
- DHS - CSSP Recommended Practices

Les incontournables pour implémenter / évaluer

- ANSSI - Méthode de classification et mesures principales et détaillées
- ISO/IEC TR 27019
- IEC 62443-2-1
  IEC 62443-3-3
- ENISA - Appropriate security measures for smart grids
- NIST - Framework for Improving Critical Infrastructure Cybersecurity

Les incontournables pour approfondir

- NERC - Critical Infrastructure Protection Standards
- ENISA - Protecting industrial control systems
- NRC - 10 CFR - 73.54
- AIEA - La sécurité dans les installations nucléaires
- NISTIR 7628
- SANDIA - Prioritizing Equipment & Mitigation
- IEC 62351
- DoE - Cyber Security Procurement Language for Control Systems
- CPNI - Process Control and SCADA security
- API - API 1164 Pipeline SCADA Security
- NRC - Regulatory Guide 5.71
- DoE - 21 steps for SCADA security

En conclusion

Aujourd'hui une multiplicité de référentiels, sans « vainqueurs » désignés

Le manque d'un minimum de vocabulaire et de principes communs

Un besoin de monter en maturité… les années aideront !

Objectifs de l'étude

- **Construire un panorama des documents traitant de la sécurité des SI industriels**

- **Donner les clés pour démarrer une démarche de sécurisation des réseaux industriels**

Les 5 phases clés vers la sécurisation d'un SI Industriel (1/4)

PHASE 1

Assimiler le métier industriel de l'entreprise et réaliser un état des lieux de la sécurité. Deux axes :

- Définir un échantillon représentatif d'installations à auditer, sur la base des activités métiers industrielles de l'entreprise
- Cartographier le périmètre d'audit et évaluer le niveau d'exposition aux cyber-risques

PHASE 2

Sensibiliser le comité de direction aux vulnérabilités informatiques induisant des risques industriels

- Mettre en avant les impacts humains, environnementaux, opérationnels, financiers, de réputation, et de non-conformité réglementaire
- Démontrer par l'exemple
- Proposer un plan d'actions pragmatique et applicable à court terme

Les 5 phases clés vers la sécurisation d'un SI Industriel (2/4)

PHASE 3

Élaborer la Politique de Sécurité des Systèmes d'Information Industriels

- Créer un groupe de travail impliquant le personnel référent opérationnel (Responsable d'exploitation et de maintenance, Automaticiens, Architecte SII, etc.)
- Structurer les résultats du groupe de travail en adoptant une approche graduée basée sur le concept de niveaux de risque, tel que peuvent le proposer l'IEC, l'AIEA ou encore l'ANSSI
- Élaborer un référentiel d'application de la PSSI-I

PHASE 4

Décliner la PSSI-I au niveau opérationnel

- Nommer la chaîne fonctionnelle cybersécurité industrielle et mettre en place une instance de gouvernance du projet ou du programme.
- Mettre en place des « Quick Wins » et mener la démarche dans un premier temps sur les sites critiques

Les 5 phases clés vers la sécurisation d'un SI Industriel (3/4)

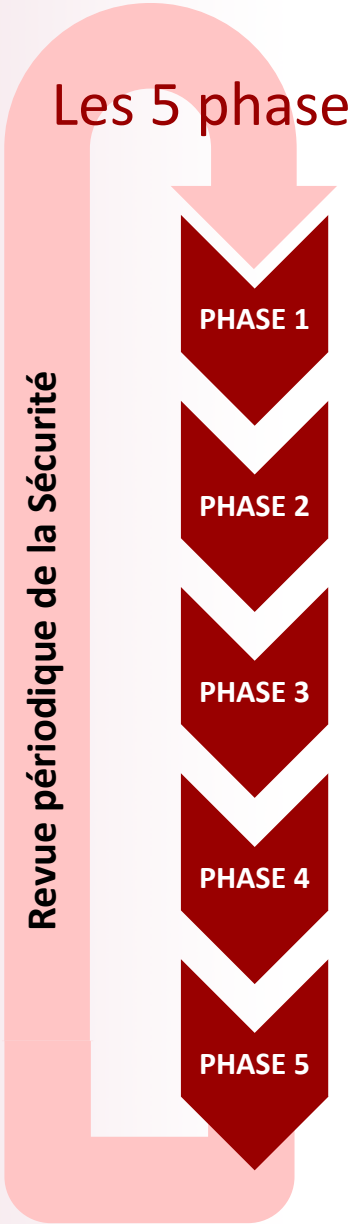
PHASE 5

Maintenir sous contrôle les cyber-risques

- Gérer les cyber-risques et assurer une veille continue
- Former/Sensibiliser tous les membres du personnel
- Intégrer la sécurité dans les projets et les évolutions. Une sélection des projets les plus sensibles pourra être réalisée pour initier le processus.
- Gérer les incidents de sécurité des SII
- Auditer et assurer un contrôle interne pour veiller à la conformité
- Piloter les plans d'actions élaborés suite aux constats d'audits ou lancés pour faire face à de nouvelles menaces ou vulnérabilités détectées.
- Réaliser des revues de direction périodiques

Une démarche à faire vivre dans le temps !

Les 5 phases clés vers la sécurisation d'un SI Industriel (4/4)



- **Assimiler le métier industriel de l'entreprise et réaliser un état des lieux de la sécurité**
- **Sensibiliser le comité de direction aux vulnérabilités informatiques induisant des risques industriels**
- **Élaborer la Politique de Sécurité des Systèmes d'Information Industriels**
- **Décliner la PSSI-I au niveau opérationnel**
- **Maintenir sous contrôle les cyber-risques**

Questions / réponses