MÉTHODOLOGIE D'ANALYSE DES SYSTÈMES D'INFORMATION

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Cyril Segretain

04/12/2018

Plan des cours

1. **Risques et sécurité du système d'information**
2. **Méthodologies d'analyse de risques**
3. **Normes ISO 27k**
4. **Politiques de sécurité des systèmes d'information**
5. **Conformité : les législations importantes (LPM, GDPR)**

MÉTHODOLOGIE ANALYSE DE RISQUES

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Présentation des principales méthodologies françaises

MEHARI	EBIOS
Méthode Harmonisée d'Analyse de RIsques	Expression des Besoins et Identification des Objectifs de Sécurité
Créée par le CLUSIF en 1993	Créée par l'ANSSI en 1995
Similaire à ISO 27005 – Appréciation des risques – Traitement des risques – Gestion des risques	Conforme à la norme ISO 27001
Mise à jour en 2017	Dernière version en 2010

MÉTHODOLOGIE D'ANALYSE DES RISQUES

EBIOS

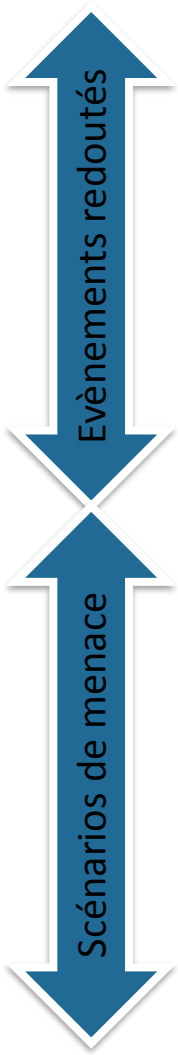
INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

EBIOS par l'exemple

Actualité

- Un étudiant « pirate » le système informatique de son école pour améliorer ses notes.
- Cet étudiant s'est introduit dans le système d'information de son école mais n'a pas pu modifier ses notes.
- Dépité de n'avoir pu atteindre ce but, l'étudiant a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité du SI pendant quatre jours.

EBIOS par l'exemple



Biens essentiels	• Résultats/notes (besoin d'intégrité fort) • Services (besoin d'accès sous 24h)
Impacts	• Image de l'école • Paralysie des activités
Sources de menaces	• Etudiant agissant par cupidité • Etudiant agissant par vengeance
Menace	• Modification après intrusion dans le SI (intégrité) • Envoi massif de mails (disponibilité)
Biens supports	• Système d'information de l'école • Messagerie de l'école

Risque 1

Altération des résultats

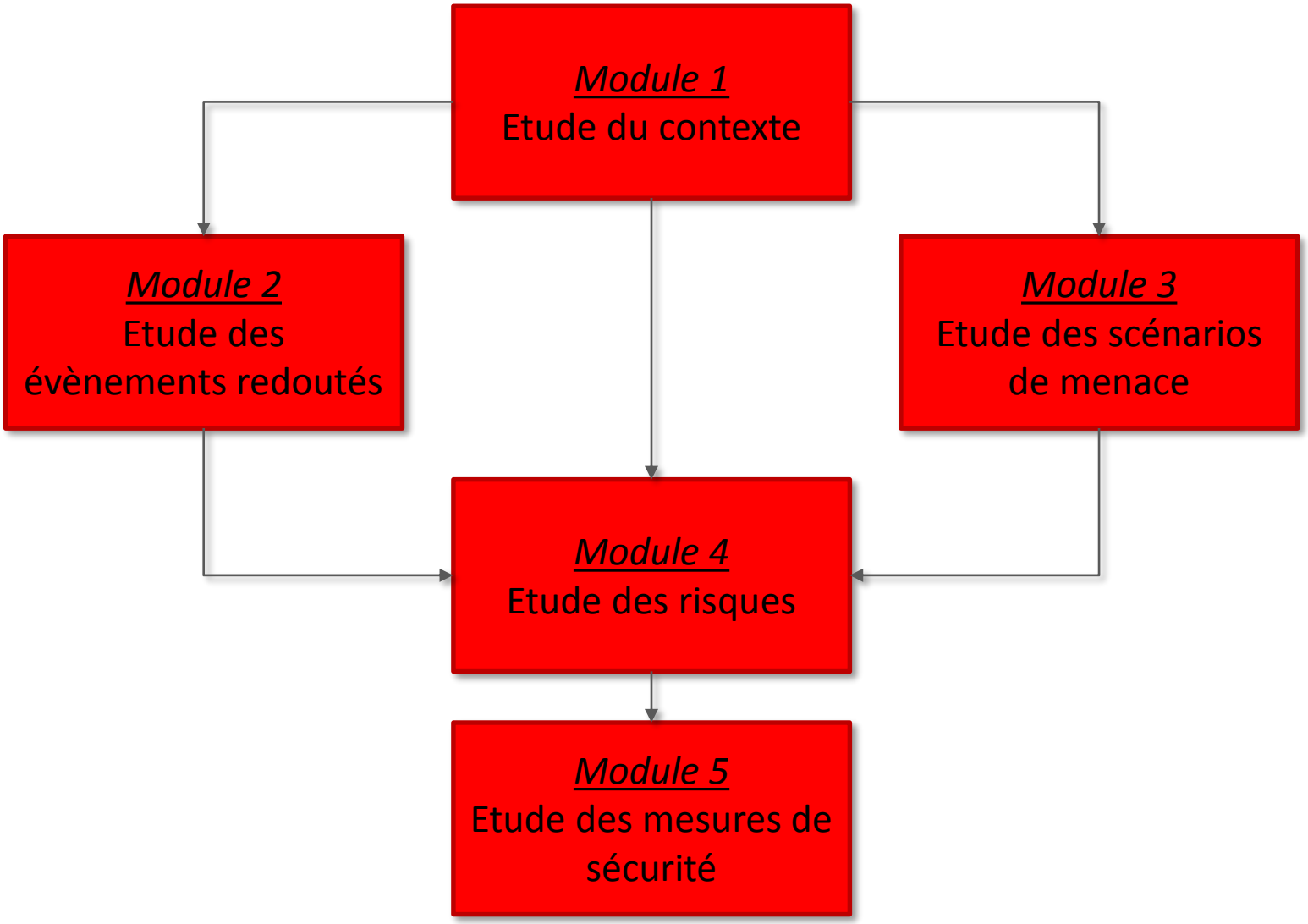
Un étudiant agissant par cupidité s'introduit dans le système d'information de l'école et modifie ses notes, ce qui ternit l'image de l'école.

Risque 2

Indisponibilité des services

Par vengeance, un étudiant sature la messagerie par un envoi massif de mails, ce qui bloque les services de l'école et paralyse ses activités.

Les modules EBIOS



1. Etude du contexte

Quel est le sujet de l'étude ? Quel service doit être analysé ?

1. Gestion du risque

- Circonscrire le périmètre et définir le cadre dans lequel l'étude va être réalisée

2. Définir les métriques

- Fixer les paramètres et les échelles utiles pour l'analyse et la gestion des risques de l'étude

3. Identifier les biens

- Déterminer les biens essentiels et supports dans le périmètre ainsi que les liens entre eux
- Identifier les mesures de sécurité existantes

➢ *Définir les biens et les outils pour continuer l'analyse de risques*

2. Étude des événements redoutés

Quels sont tous les évènements craints ?

1. Apprécier les évènements redoutés

- Déterminer les scénarios métiers craints
- Identifier la valeur de ce que l'on souhaite protéger
- Mettre en évidence les sources de menaces et les impacts des sinistres
- Évaluer les évènements redoutés

➢ *Définir le DICP de chaque bien essentiel en terme de besoins et d'impacts*

3. Etude des scénarios de menaces

Quels sont tous les scénarios craints ?

1. Apprécier les scénarios de menaces

- Identifier les modes opératoires pouvant porter atteinte à la sécurité
- Mettre en évidence les menaces
- Identifier les vulnérabilités
- Évaluer les scénarios de menaces

➢ *Définir les scénarios de menaces et leur vraisemblance*

4. Étude des risques

Quel est la matrice des risques ? Comment les traiter ?

1. Apprécier les risques

- Faire la corrélation entre les évènements redoutés et les scénarios de menaces
- Mettre en évidence les scénarios les plus pertinent
- Qualifier leur niveau de criticité

2. Identifier les objectifs de sécurité

- Traiter les risques
- Envisager les risques résiduels

➢ *Etablir les scénarios de risques et choisir le traitement des risques*

5. Étude des mesures de sécurité

Quelles mesures de sécurité appliquer ? Quels sont les risques résiduels réels ?

1. Formaliser les mesures de sécurité à mettre en œuvre

- Déterminer les mesures de sécurité (techniques, fonctionnelles, organisationnelles) permettant de traiter les risques
- Etudier les mesures de sécurité
- Identifier les risques résiduels

2. Mettre en œuvre les mesures de sécurité

- Définir le plan d'action de mise en place des mesures de sécurité
- Mettre en place les mesures de sécurité
- Réaliser l'homologation de sécurité

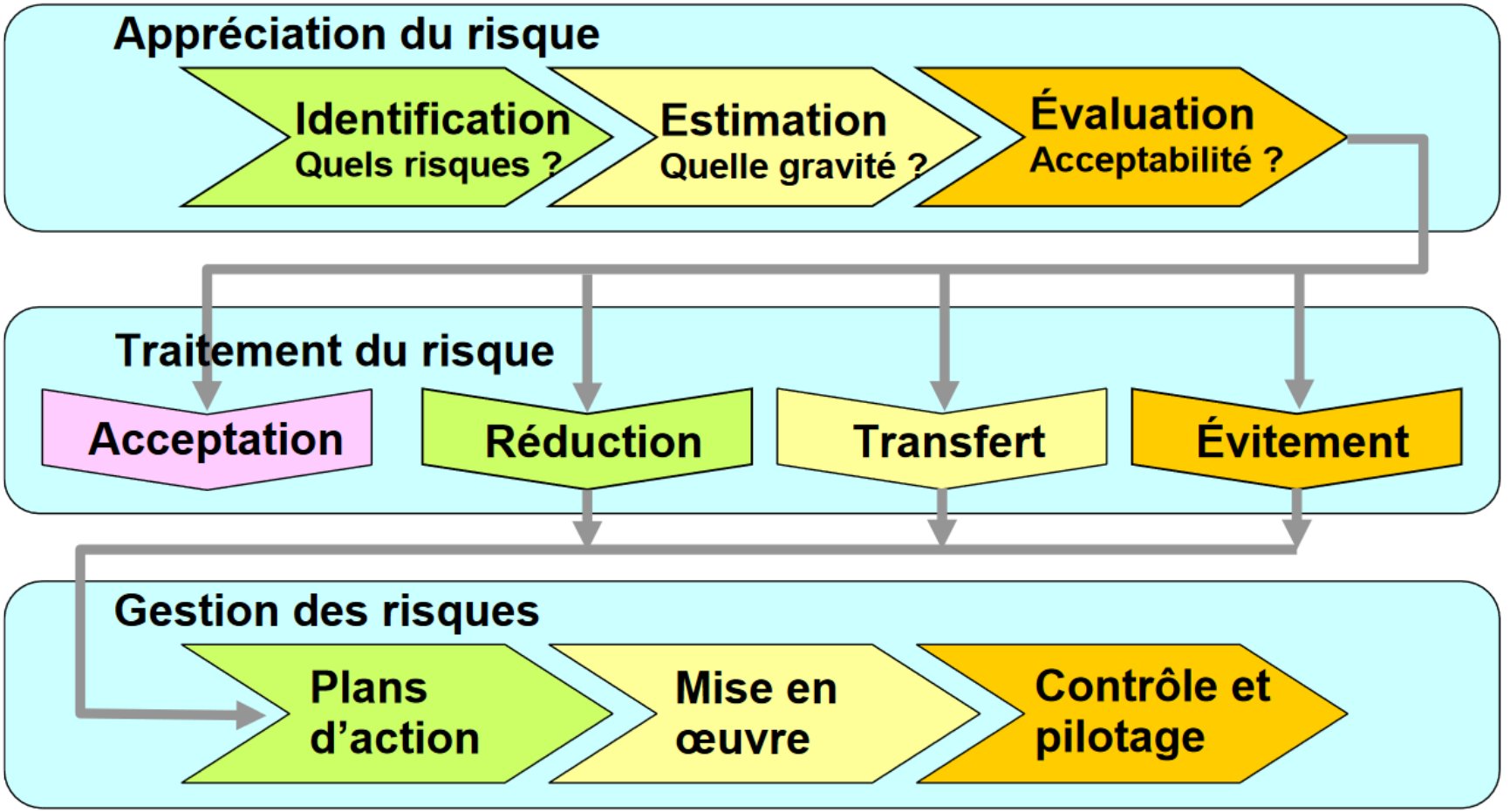
➢ *Mettre en place une sécurité adaptée et déterminer les risques résiduels*

MÉTHODOLOGIE D'ANALYSE DES RISQUES MEHARI

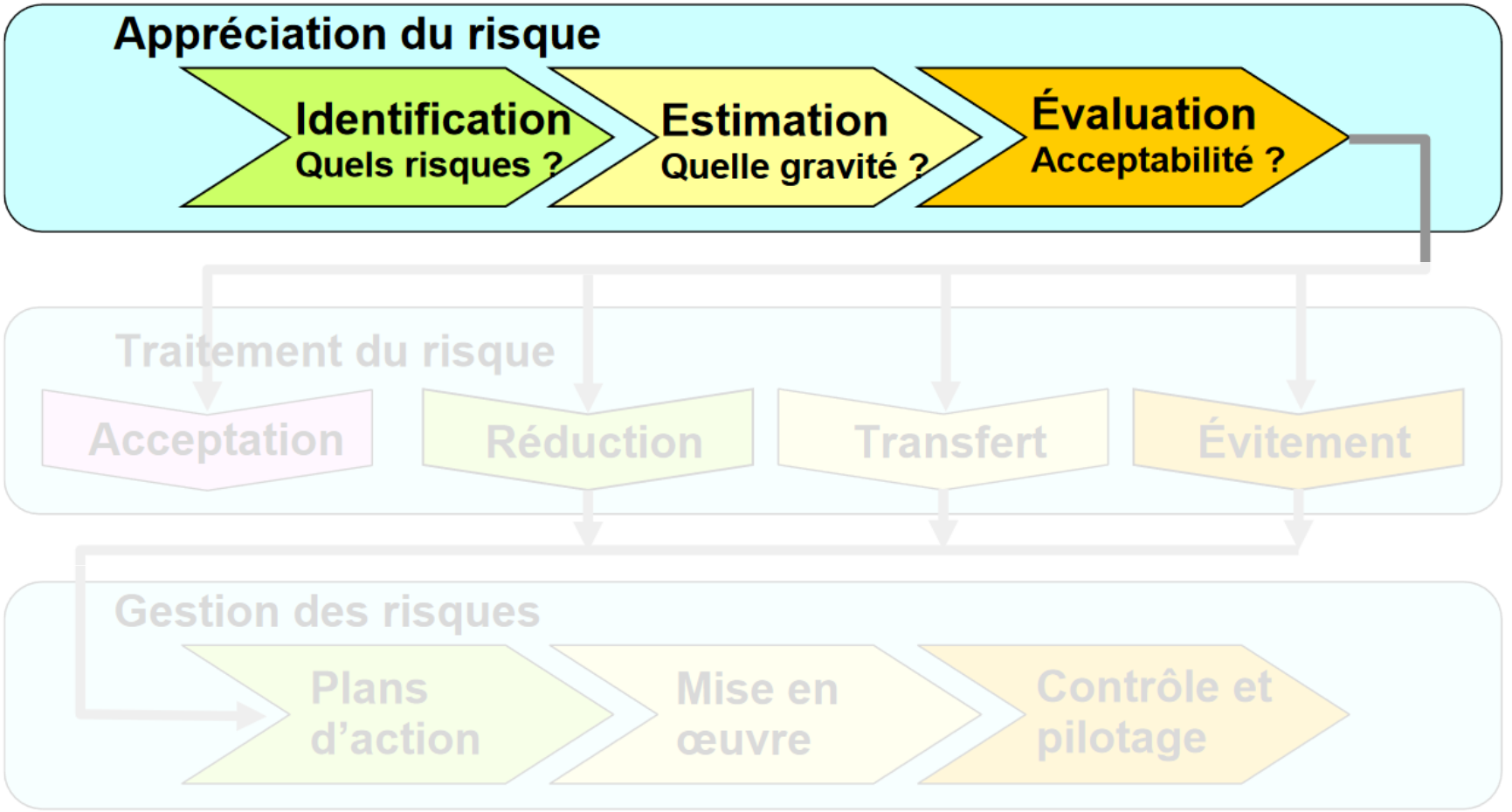
INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Présentation globale de la méthode

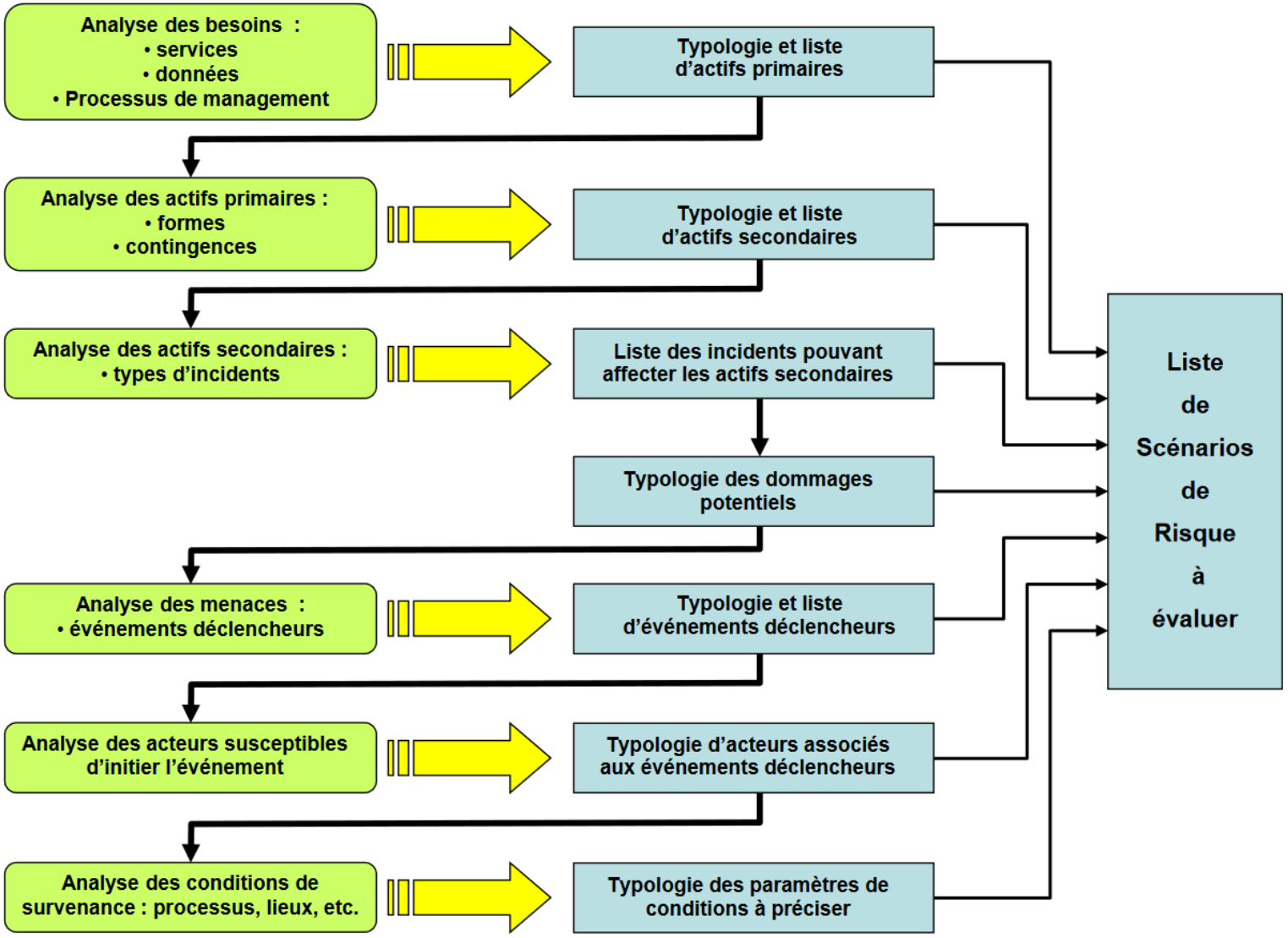
- Les 3 grandes étapes de MEHARI :



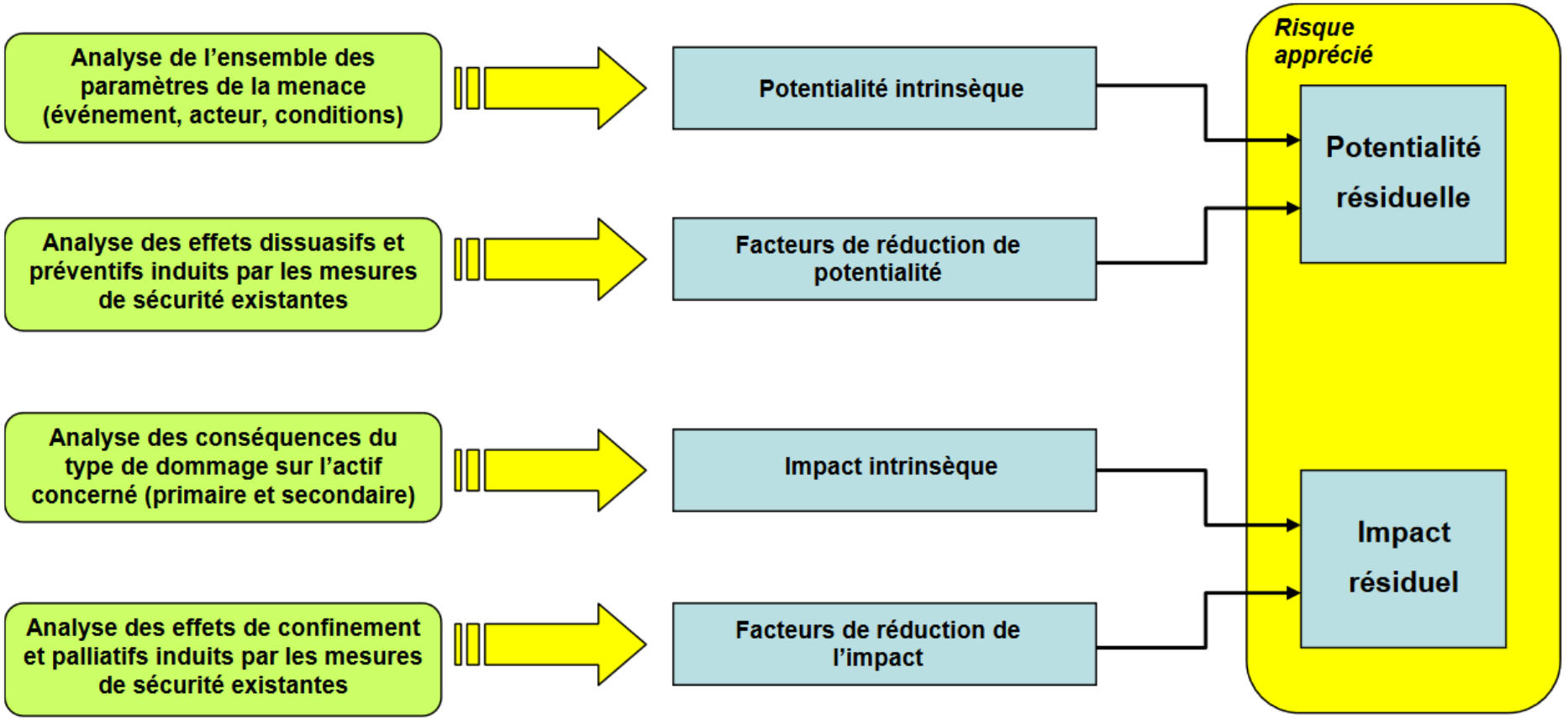
Traitement des risques



Identification des risques

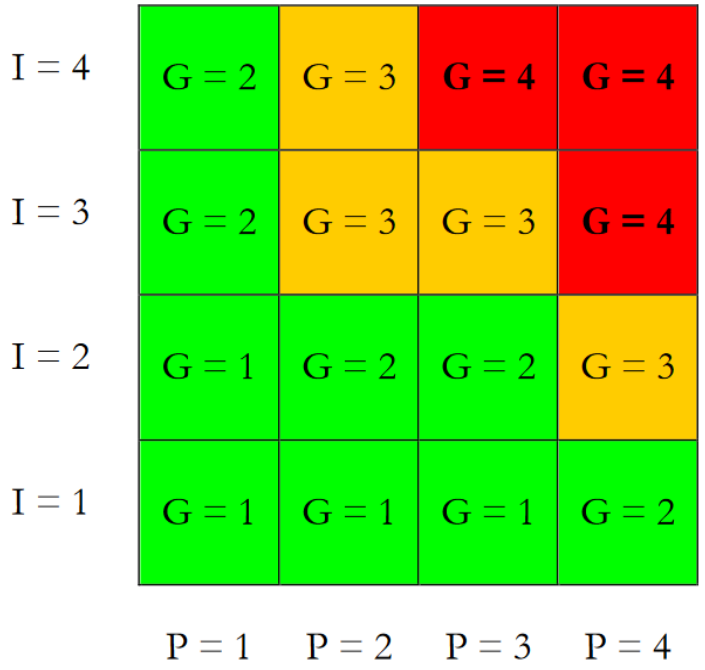


Appréciation des risques

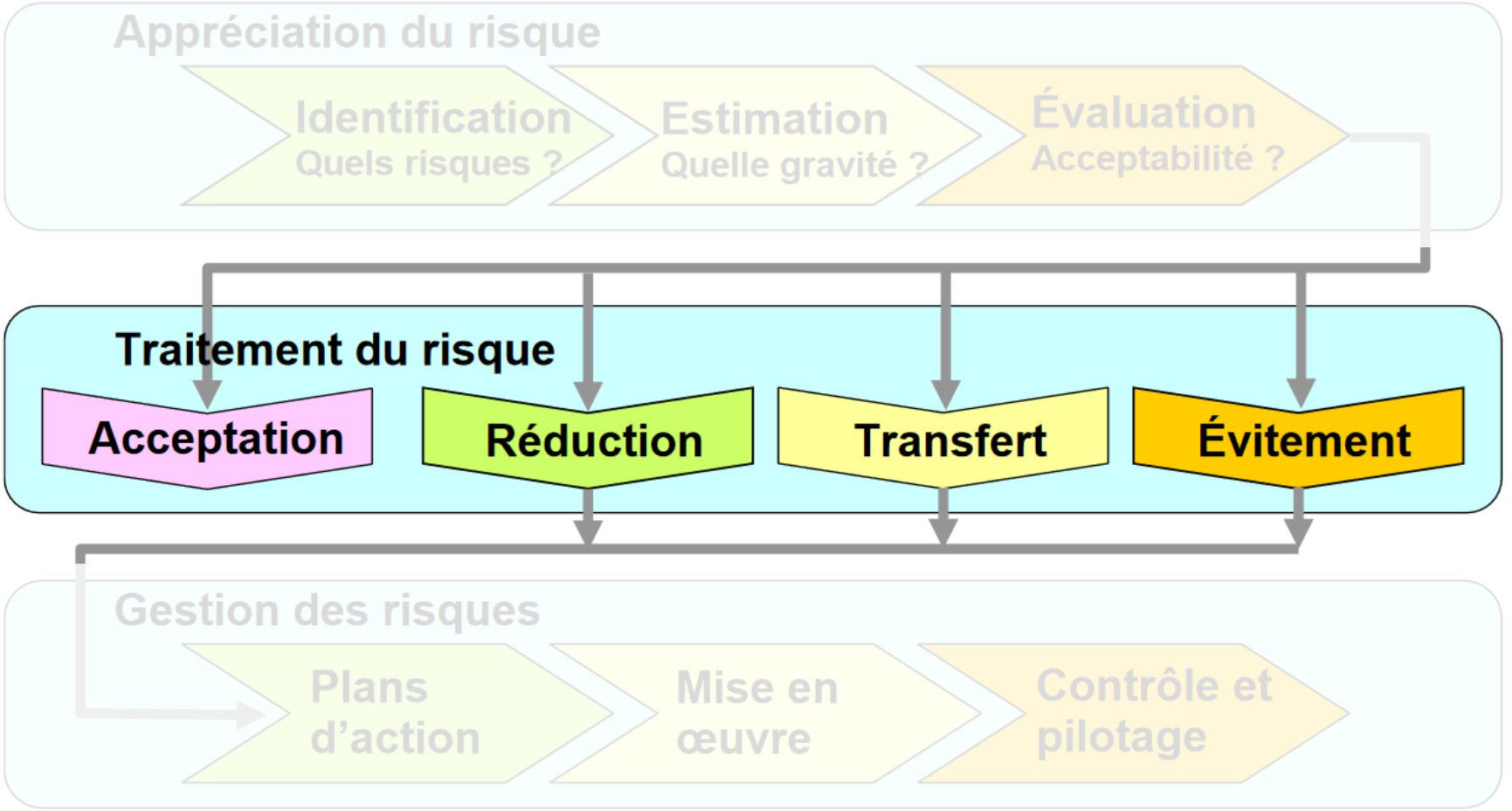


Acceptabilité des risques

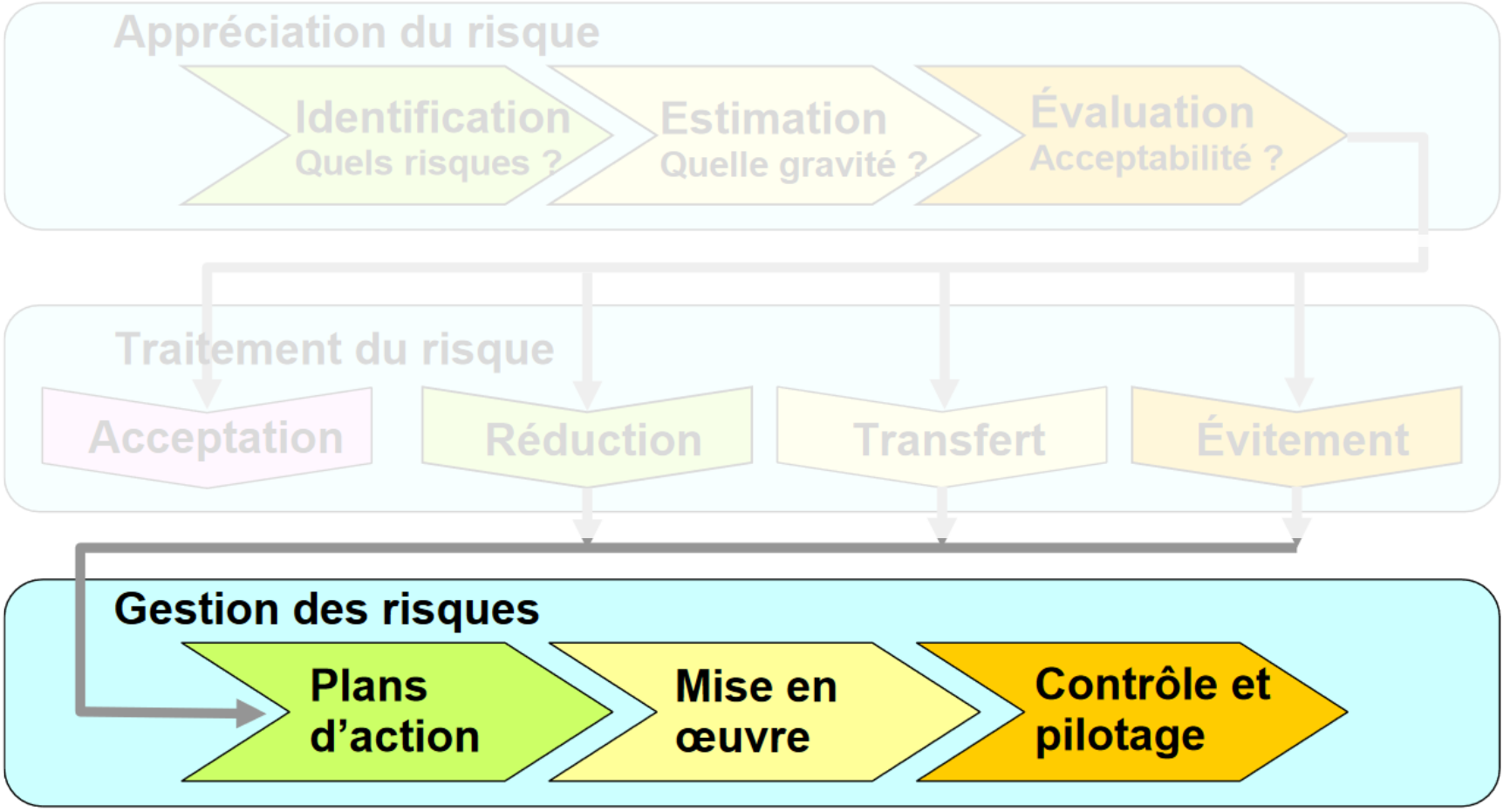
- MEHARI propose de définir trois types de risques :
  - Les risques insupportables, qui devraient faire l'objet de mesures d'urgence, en dehors de tout cycle budgétaire.
  - Les risques inadmissibles qui devraient être réduits ou éliminés à une échéance à déterminer, donc à prendre en compte dans une planification (plan de sécurité).
  - Les risques tolérés.



Traitement des risques



Gestion des risques



Il existe une multitude de méthodologies d'analyses de risques.
Certaines grandes entreprises ont une méthodologie interne.

Il faut avoir une sensibilité globale sur le déroulement d'une analyse de risques et ensuite s'adapter au contexte.

- Il est important d’avoir une sensibilité risque (c’est la spécialité de l’école)
- Il faut comprendre le raisonnement d’une analyse de risques
- Il faut connaitre les méthodologies existantes et savoir en appliquer une
- Il faut pouvoir utiliser un outil et l’adapter aux besoins de l’entreprise

FIN DE LA 2ÈME PARTIE

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

ANNEXES

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Annexes

- EBIOS
  - https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf
  - https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf
- MEHARI
  - http://meharipedia.org/
  - http://meharipedia.x10host.com/wp/wp-content/uploads/2017/10/MEHARI-Principes-Specifications-2017-valid%C3%87.pdf

Annexes : autres méthodologies analyses de risques

Méthode	Création	Auteur	Secteur	Pays
EBIOS	1995	DGSSI	Gouvernement	France
Melisa		DGA	Armement	France
Marion	1980	CLUSIF	Association	France
Mehari	1995	CLUSIF	Association	France
Octave	1999	Carnegie Mellon	Universitaire	Etats-Unis
Cramm	1986	Siemens	Gouvernement	Angleterre
SPRINT	1995	ISF	Association	Angleterre
SCORE	2004	Ageris Consulting	Secteur privé	France
CALLIO	2001	CALLIO Tech.	Secteur privé	Canada
COBRA	2001	C&A Sys. Security	Secteur privé	Angleterre
ISAMM	2002	Evosec	Secteur privé	Belgique
RA2	2000	Aexis	Secteur privé	Allemagne

Veille sécurité

- CERT FR - ANSSI
  - Centre Gouvernemental de veille, d'alerte et de réponses aux attaques informatiques
  - https://www.cert.ssi.gouv.fr/
- CERT USA
  - https://www.us-cert.gov/
- Undernews : site actualité
  - https://www.undernews.fr/
- ZATAZ : site d'actualité, protocole d'alerte
  - https://www.zataz.com/
- Krebs on Security : Blog actualité
  - https://krebsonsecurity.com/
- Wired Security : actualités + dossiers approfondis
  - https://www.wired.com/category/security/
- Korben (technique), CERT Orange (vulnérabilités), Silicon (actu), …

Veille Twitter

- @UnderNews_fr
- @ANSSI_FR
- @argevise
- @selenalarson
- @gbillois
- @x0rz
- @hackerfantastic
- @josephfcox
- @Data_Cyber
- @InfoSecHotSpot