



Eric Bornette
Analyse de risque, analyse de la menace

Introduction.

- Eric BORNETTE
- DGA MI
- eric.bornette@laposte.net



Plan général

- Introduction, présentation générale du cours.
- Objectifs de l'analyse de risque.
- Les différentes étapes et tâches de l'analyse de risque.
- Les méthodes d'AR, focus sur EBIOS.
- Mise en œuvre des outils et des savoir faire, projet.
- Restitution.
- Conclusion, fin du cours.



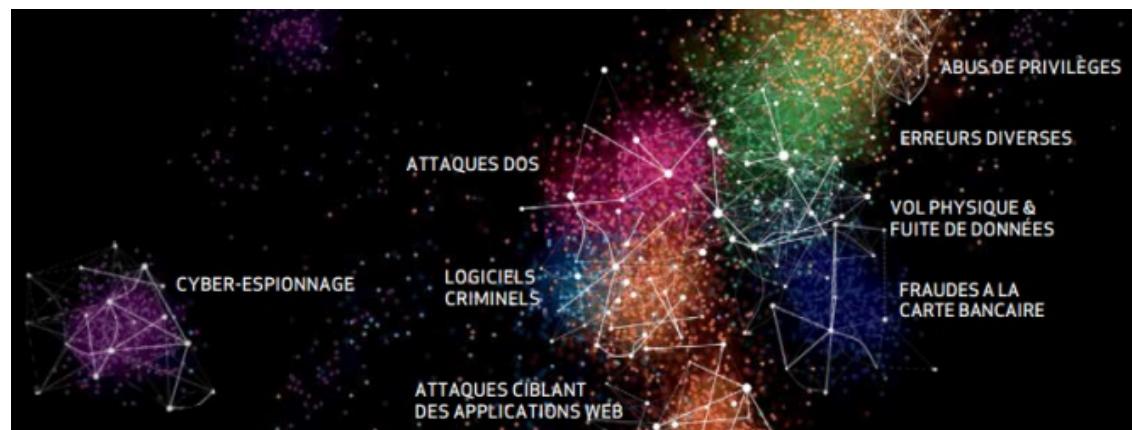
Plan

- Introduction, présentation générale du cours.
- **Objectifs de l'analyse de risque.**
- Les différentes étapes et tâches de l'analyse de risque.
- Les méthodes d'AR, focus sur EBIOS.
- Mise en œuvre des outils et des savoir faire, projet.
- Restitution.
- Conclusion, fin du cours.



Objectifs de l'AR

- Etat des lieux de la sécurité (SSI, Cyber sécurité...) :
 - Besoin (cycle de vie sécurité).
 - Compréhension
 - Coût
 - Métrique
 - Evolution de la menace
 - ...



Objectifs de l'AR

- ↗ Expliquer
- ↗ Clarifier
- ↗ Orienter
- ↗ Benchmark
- ↗ Formaliser
- ↗ Relativiser
- ↗ Pondérer
- ↗



Objectifs de l'analyse de risque.

- Le dictionnaire (petit Robert) apporte les définitions suivantes :
 - (1) Danger éventuel plus ou moins prévisible.
 - (2) Éventualité d'un événement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage. Par ext. Événement contre la survenance duquel on s'assure.
 - (3) Fait de s'exposer à un danger (dans l'espoir d'obtenir un avantage).



Objectifs de l'analyse de risque.

↗ Les experts sécurité nous disent que :

- ↗ Le risque est l'exposition à un danger, un préjudice, un événement dommageable lié à une situation voulue ou hasardeuse.
- ↗ Le risque est défini par la probabilité d'existence de cet événement, de ses conséquences (périmètre et profondeur). Le risque concerne les biens, les personnes, les organisations...
- ↗ Le risque est une combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque et de l'impact sur des éléments essentiels et sur l'organisme.

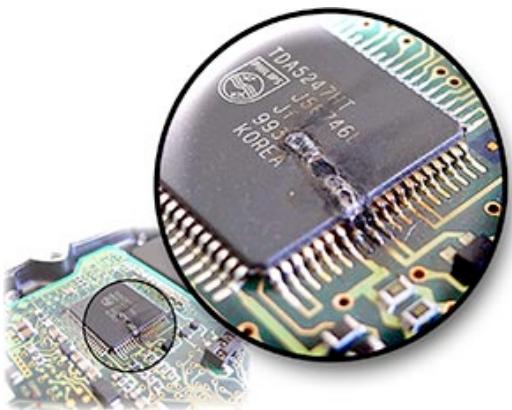


Objectifs de l'analyse de risque.

- ↗ L'analyse de risque de risque est un domaine à part entière qui a deux grands cadres d'application pour les systèmes :
 - ↗ La sûreté de fonctionnement.
 - ↗ La sécurité des systèmes d'information.



Objectifs de l'analyse de risque.



Panne informatique majeure dans une banque de Singapour

INFRASTRUCTURE SERVEUR

Pannes



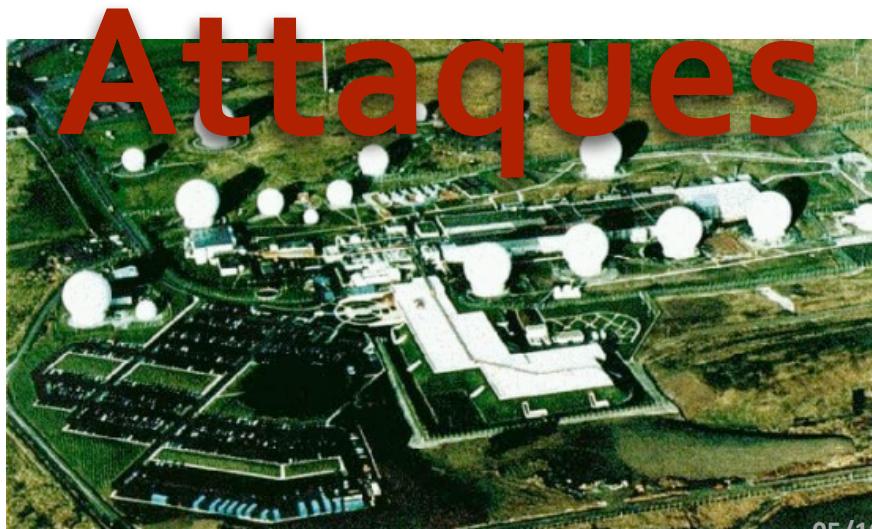
Edition du 06/07/2010 - par Guillaume Garnier avec IDG NS

[Imprimer](#) [Envoyer](#) [Contact](#) [Rss](#) [Partager](#)

Une des plus importantes banques de Singapour, la DBS, a subi lundi, pendant près de sept heures, une panne de tout son système informatique en partie externalisé chez IBM.

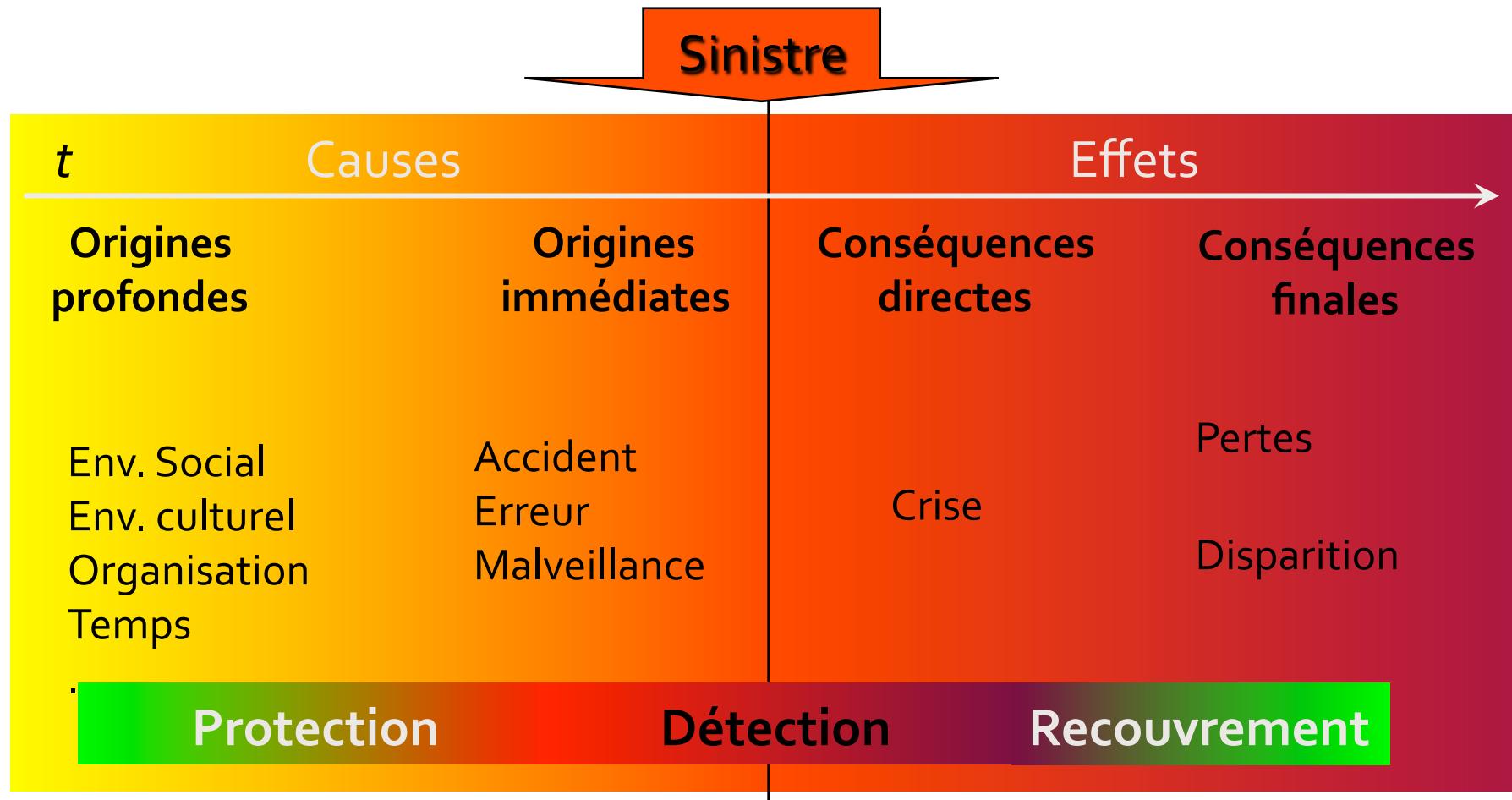
La défaillance a touché le back-end du système informatique de la DBS Bank, rendant impossible pour ses clients de retirer de l'argent dans les distributeurs lundi matin. « Nous avons su qu'il y avait un problème dès 3h du matin (heure de Singapour), et à 10h, tous nos sites et distributeurs de billets étaient redevenus opérationnels. Nous menons pour l'heure une enquête afin de déterminer la cause du problème d'hier, et nous ne sommes donc pas en mesure de commenter sur ce sujet pour le moment » a écrit Jenny Lee, porte-parole de la banque, dans un email.

10



05/10/17

Objectifs de l'analyse de risque.



Objectifs de l'analyse de risque.

- **Synthèse :**

- Que veut-on protéger ?
- Contre quoi ?
- Contre qui ?
- A quel prix, quel niveau d'effort ?
- Avec quels moyens et quelle stratégie.
- ...



Objectifs de l'analyse de risque.

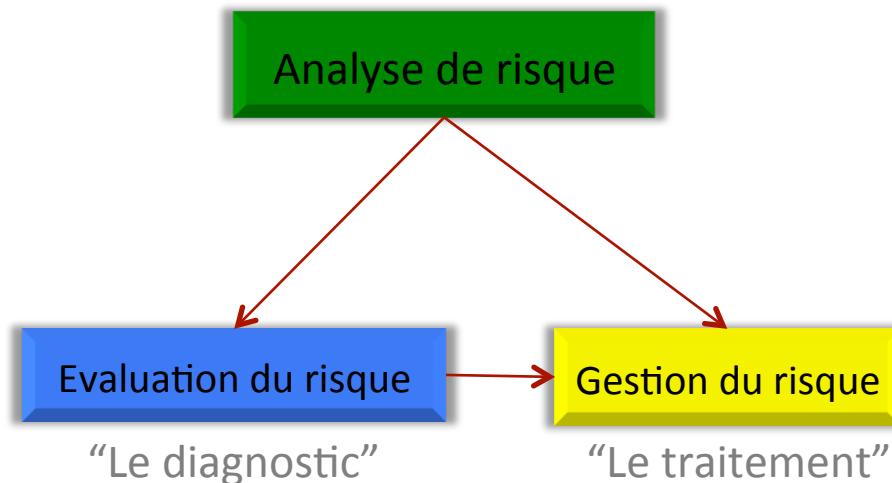
↗ L'analyse de risque est un processus qui peut être mis en œuvre dans différents cas d'utilisation :

- ↗ Mise en politique de sécurité.
- ↗ Evolution de la politique de sécurité.
- ↗ Evolution d'organisation.
- ↗ Evolution de contexte.
- ↗ Mise en place d'un nouveau système.
- ↗ Etude pour décision stratégique.
- ↗ Externalisation, outsourcing.
- ↗ ...



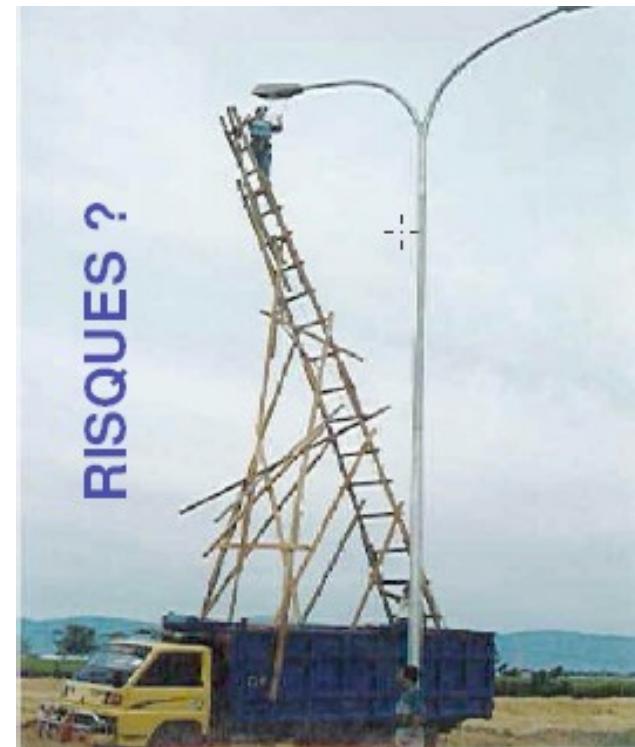
Objectifs de l'analyse de risque.

- L'**analyse de risque** est une discipline analytique destinée à permettre l'implémentation d'une politique de sécurité en tenant compte du ratio coût/bénéfice dans un environnement réel et complexe. Elle est composée de deux branches : l'évaluation du risque et la gestion du risque (REF2 – Bursztein, 2008).



Objectifs de l'analyse de risque.

- **L'évaluation des risques** consiste à :
- identifier les risques présents au sein d'un système, leurs conséquences et à évaluer l'efficacité des parades associées (REF2 – Bursztein, 2008).



Objectifs de l'analyse de risque.

- **La gestion des risques** consiste à sélectionner les parades qui minimisent l'exposition aux risques tout en prenant en compte les contraintes fonctionnelles ainsi que les contraintes pragmatiques d'ordre social, politique et financier (REF2 – Bursztein, 2008).



Objectifs de l'analyse de risque.

- L'analyse de risque est un élément central du processus de sécurité des systèmes d'information (SSI).
 - Objectifs de l'analyse de risque :
 - Réduire le risque.
 - *Je fume moins.*
 - Accepter le risque.
 - *Je fume et je sais que je peux tomber malade.*
 - Eviter le risque.
 - *Je fume pas.*
 - Transférer le risque.
 - *J'offre mes cigarettes à mes collègues.*

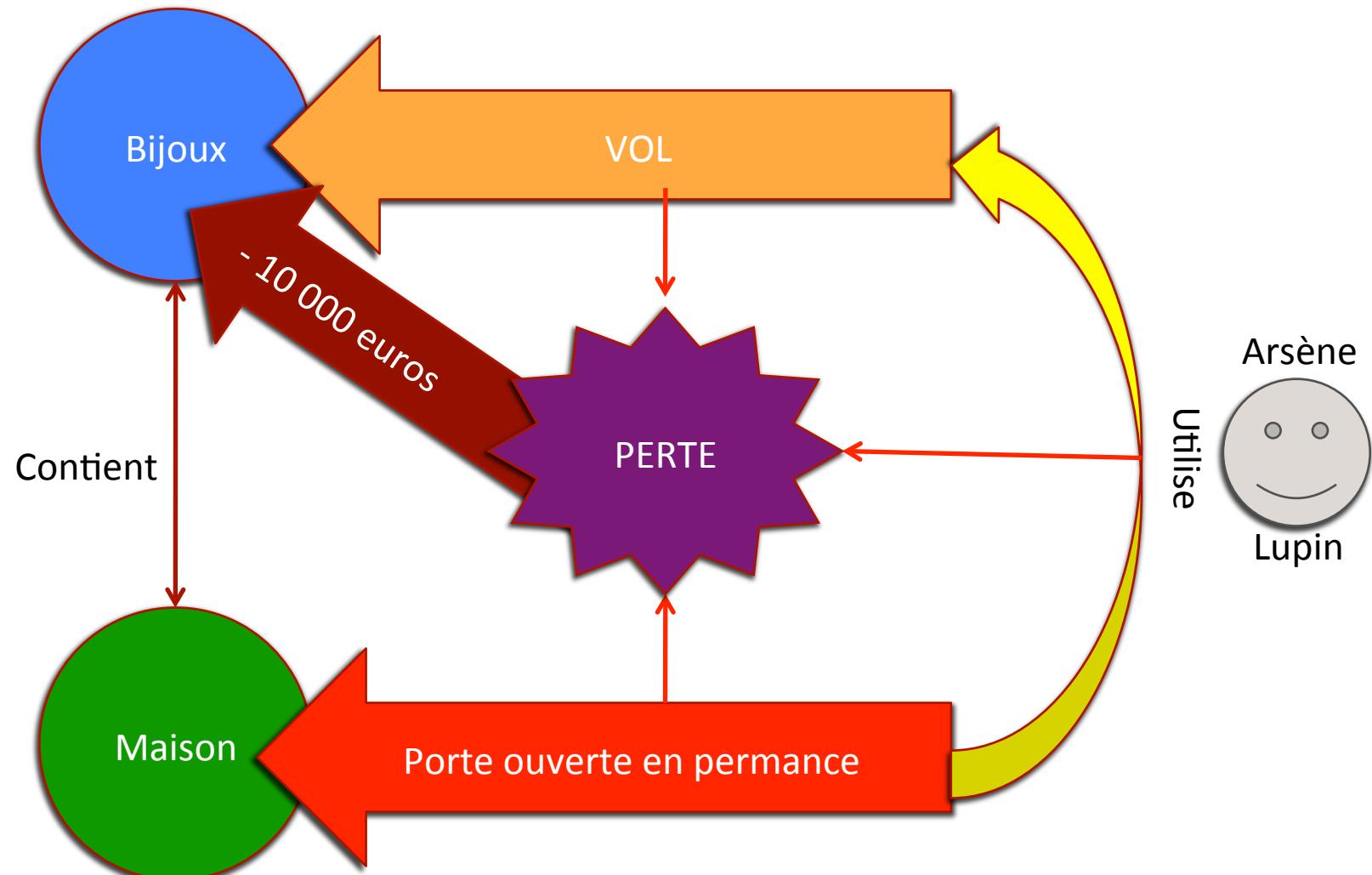


Plan

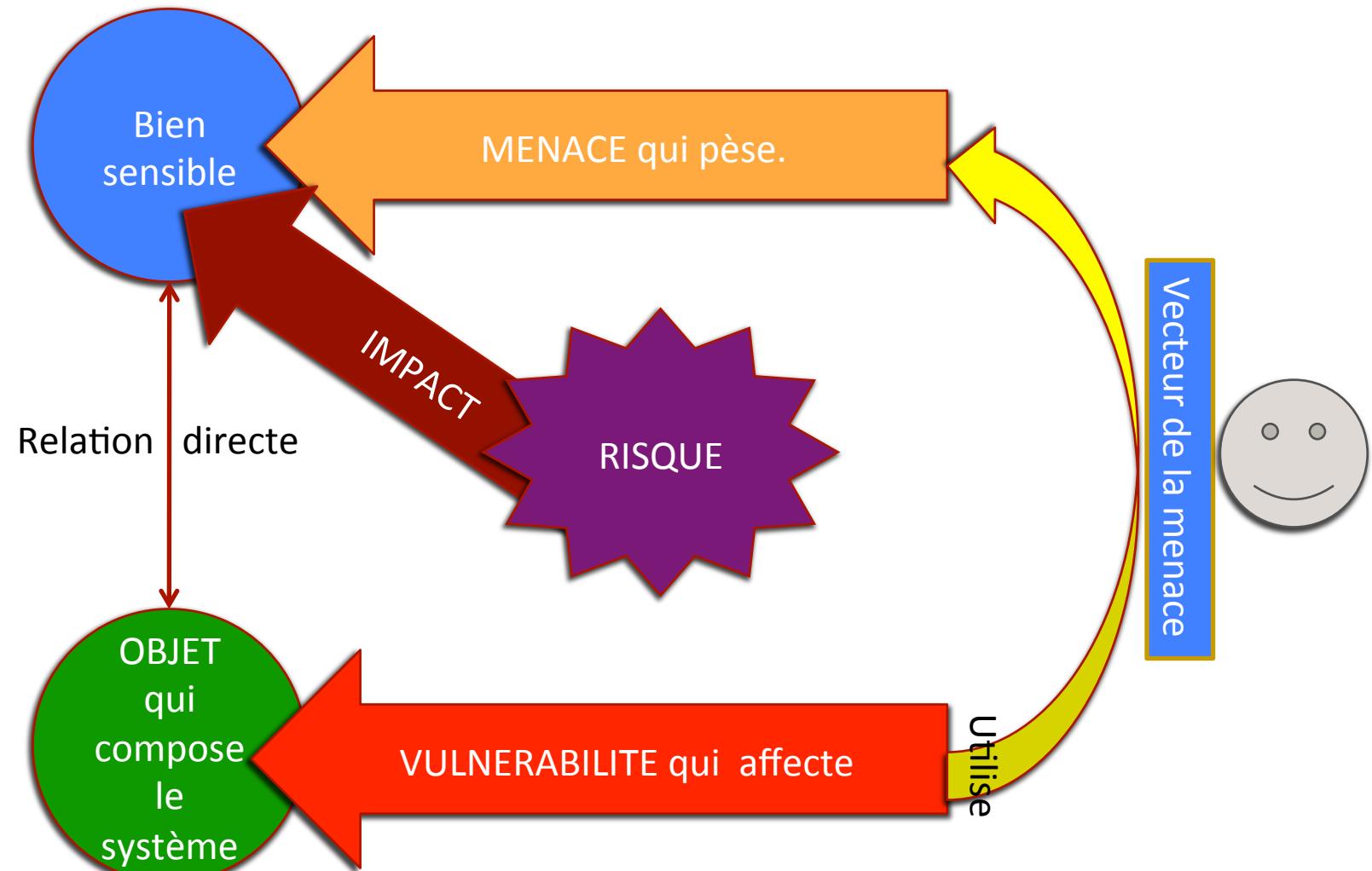
- Introduction, présentation générale du cours.
- Objectifs de l'analyse de risque.
- **Les différentes étapes et tâches de l'analyse de risque.**
- Les méthodes d'AR, focus sur EBIOS.
- Mise en œuvre des outils et des savoir faire, projet.
- Restitution.
- Conclusion, fin du cours.



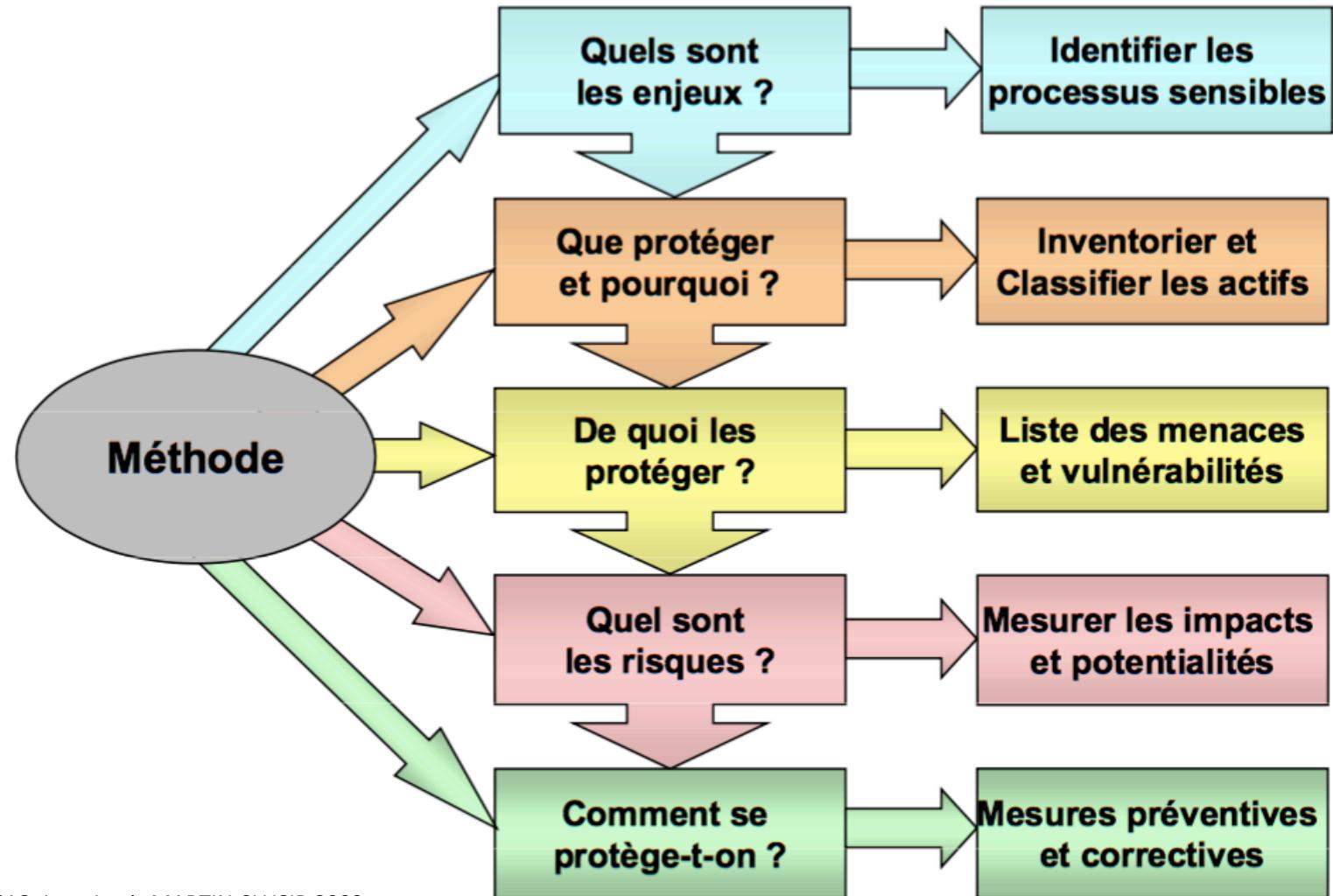
Etapes et tâches de l'analyse de risque.



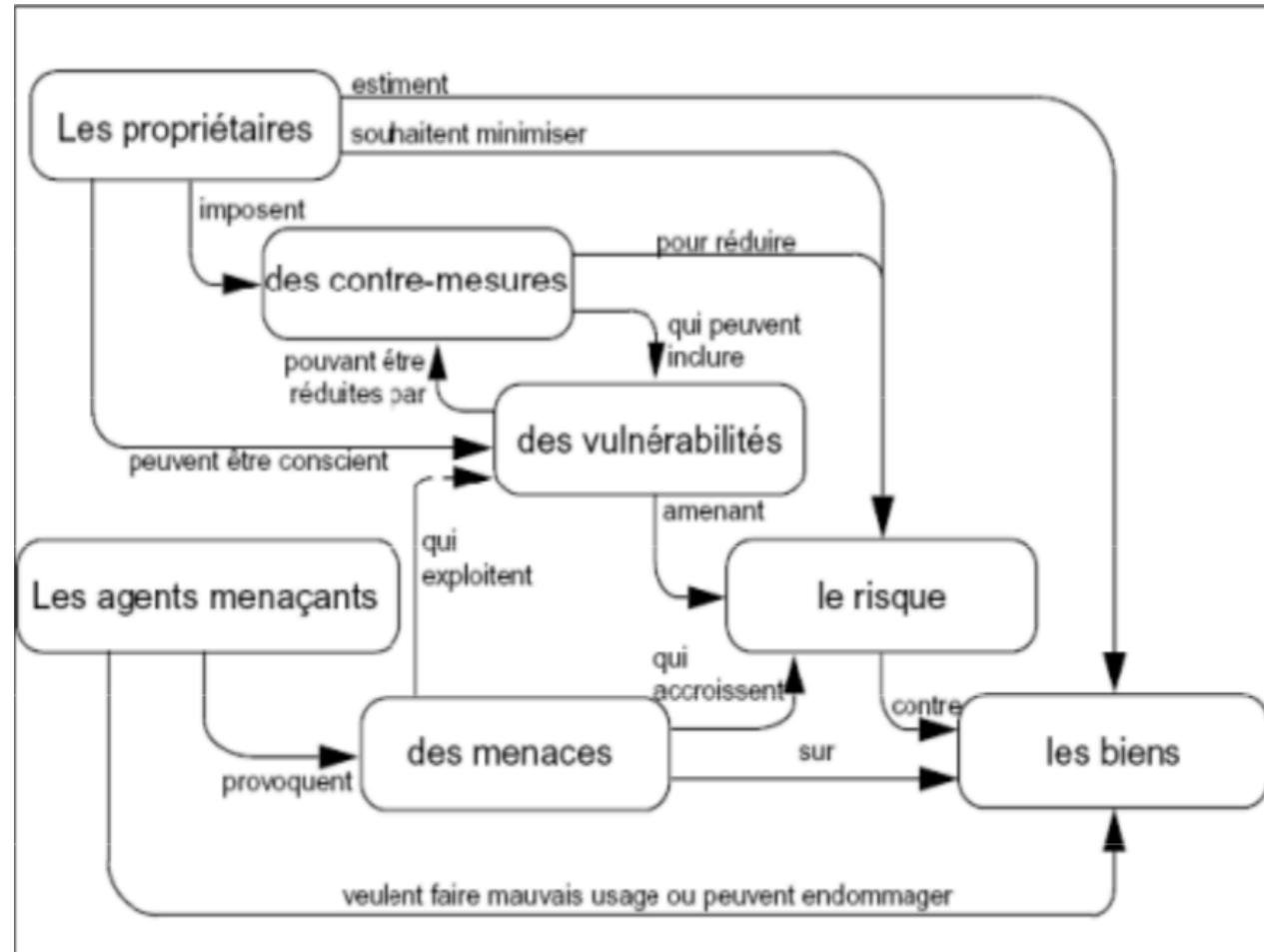
Etapes et tâches de l'analyse de risque.



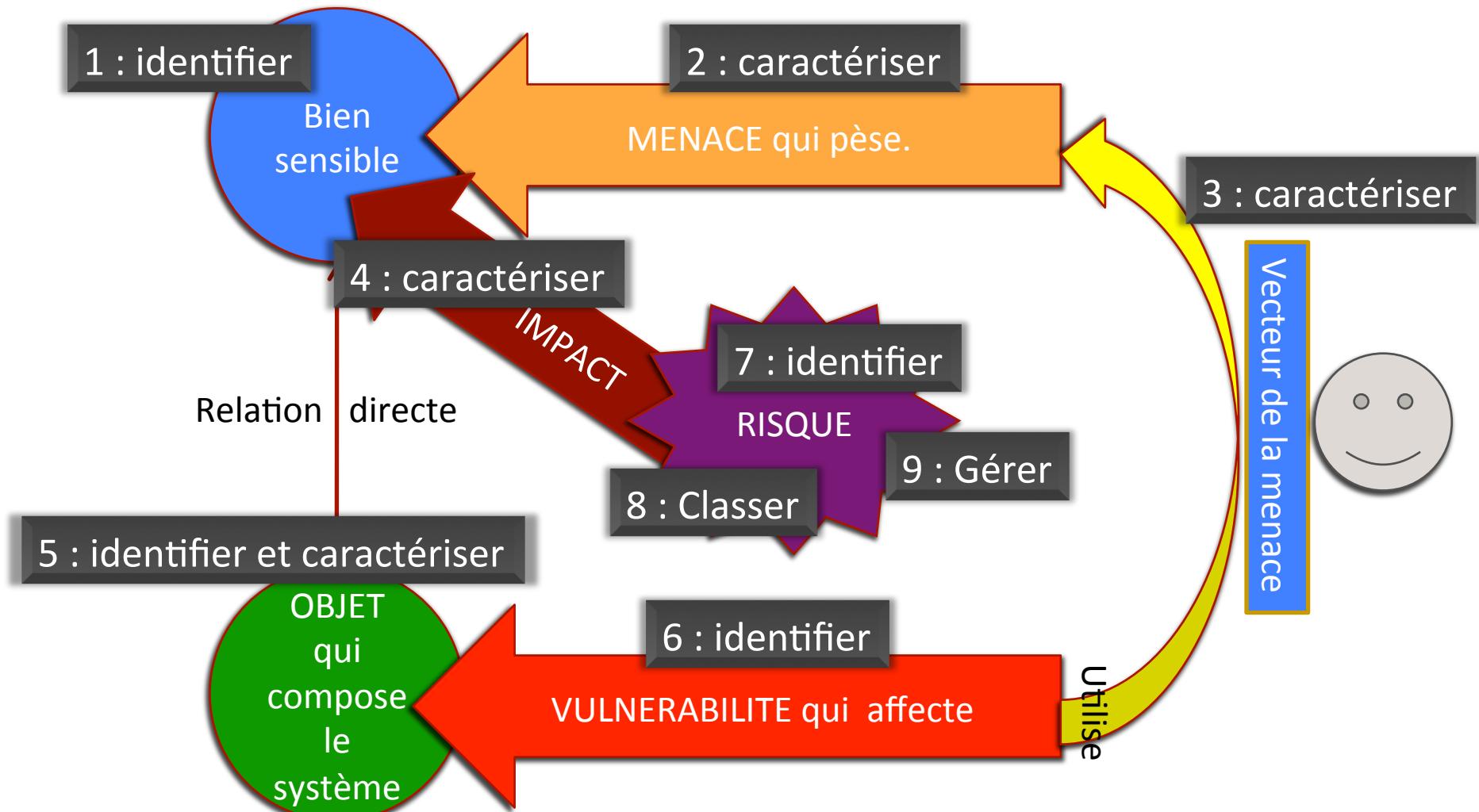
Etapes et tâches de l'analyse de risque.



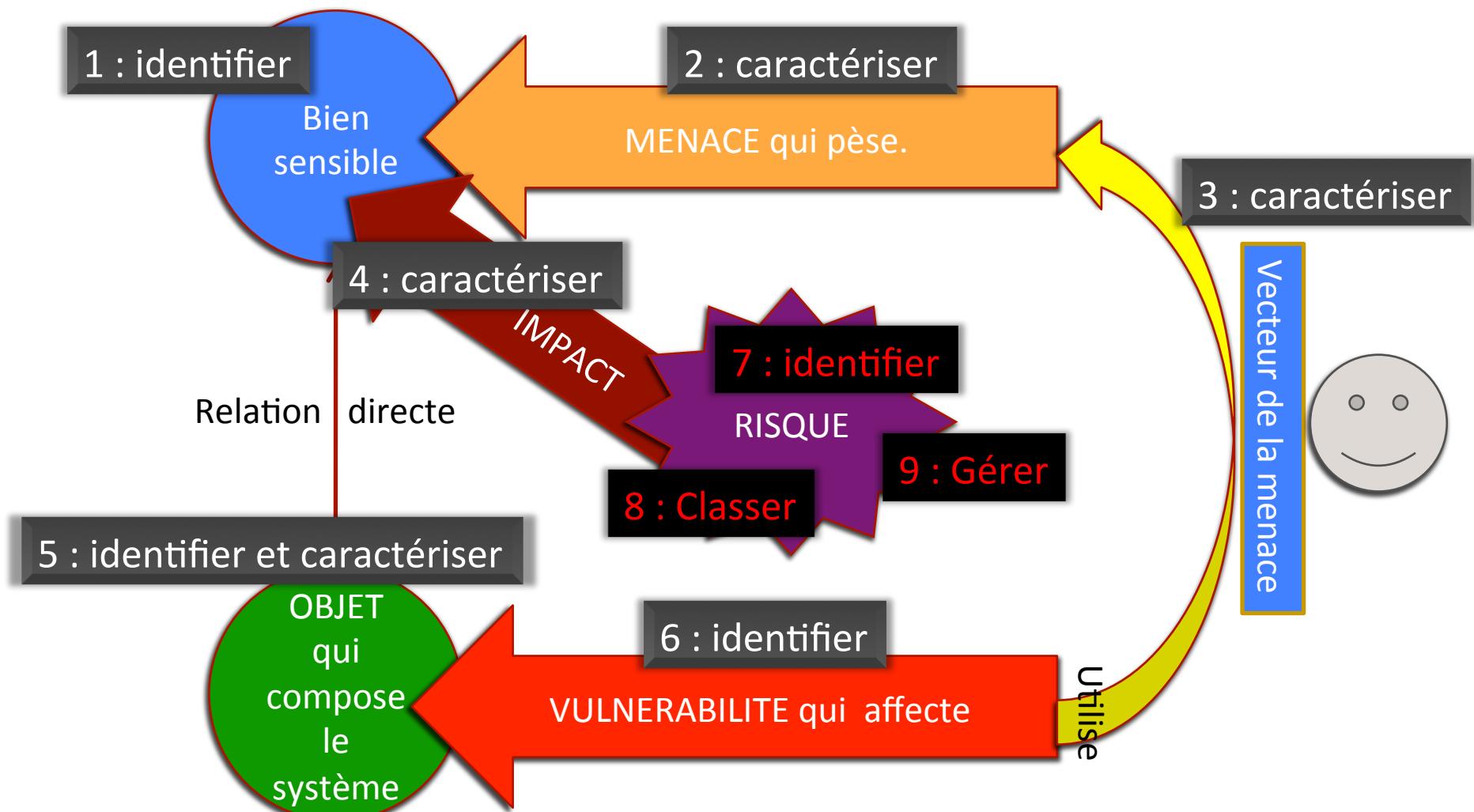
Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

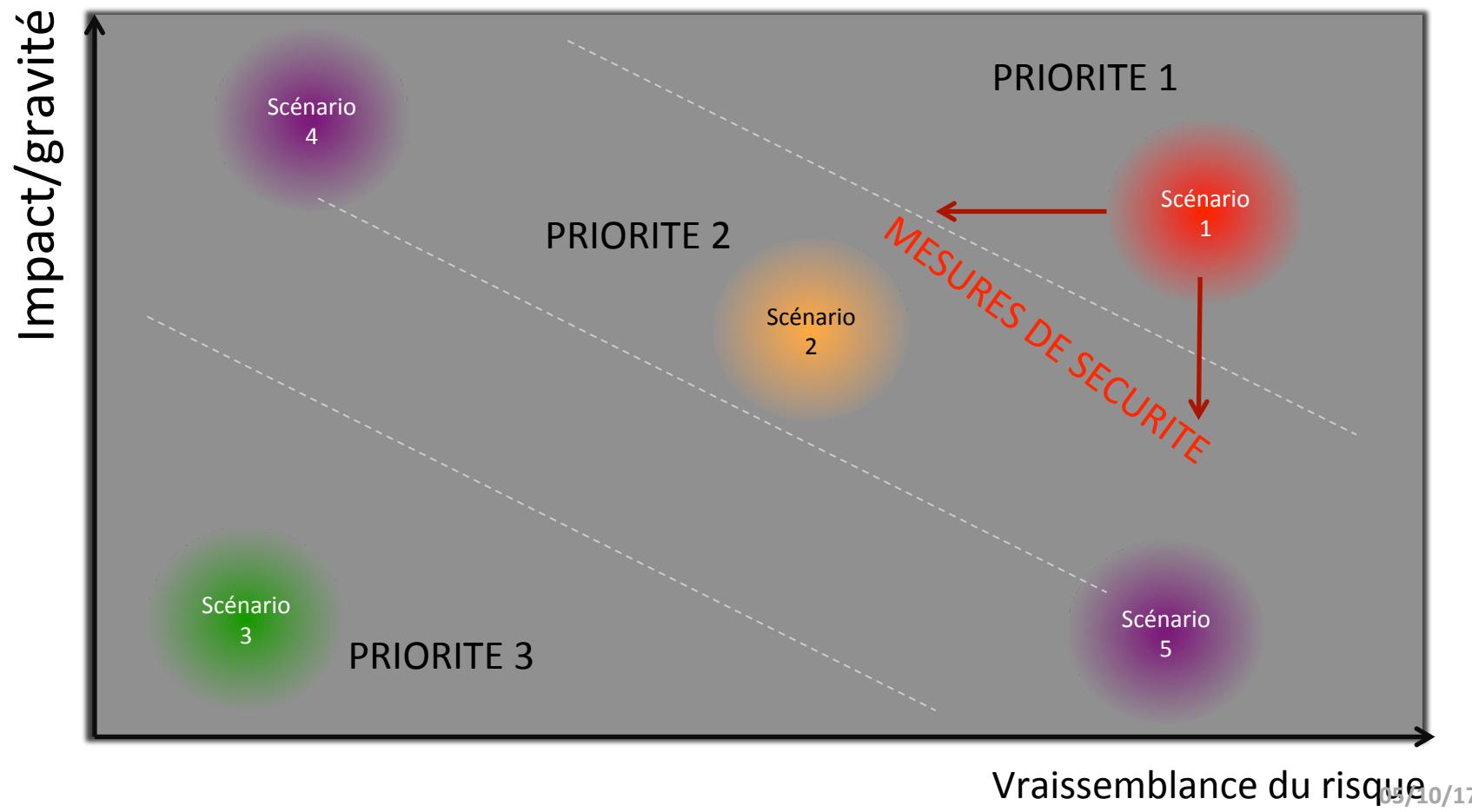


Etapes et tâches de l'analyse de risque.

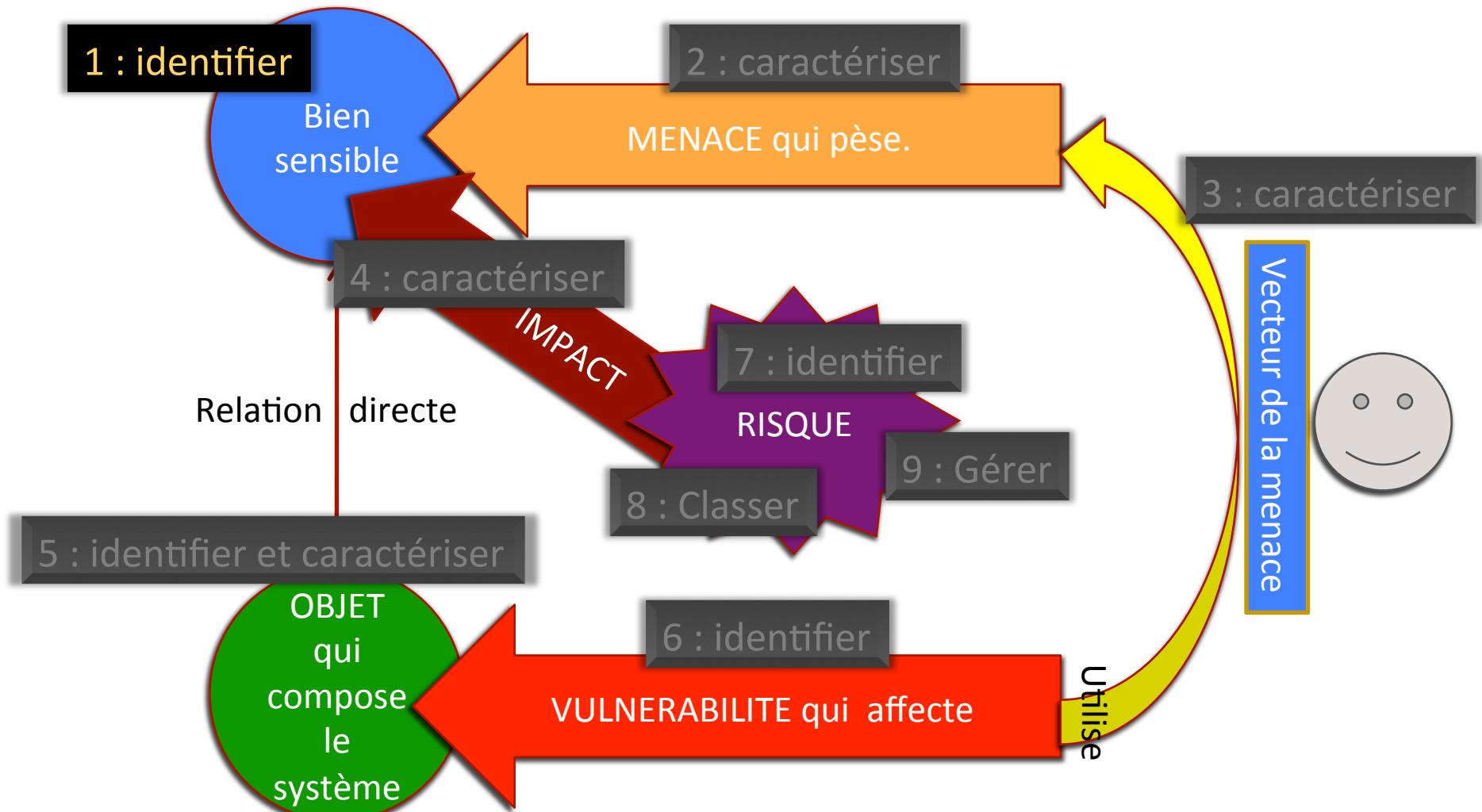


Etapes et tâches de l'analyse de risque.

Objectif de l'évaluation du risque.



Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

Objectif : répondre à la question « que doit-on protéger ».

Bien sensible :

- information ou fonction.
- immatériel.
- ne pas confondre un bien matériel et une fonction informatique qui participe à son « au cycle de vie ».

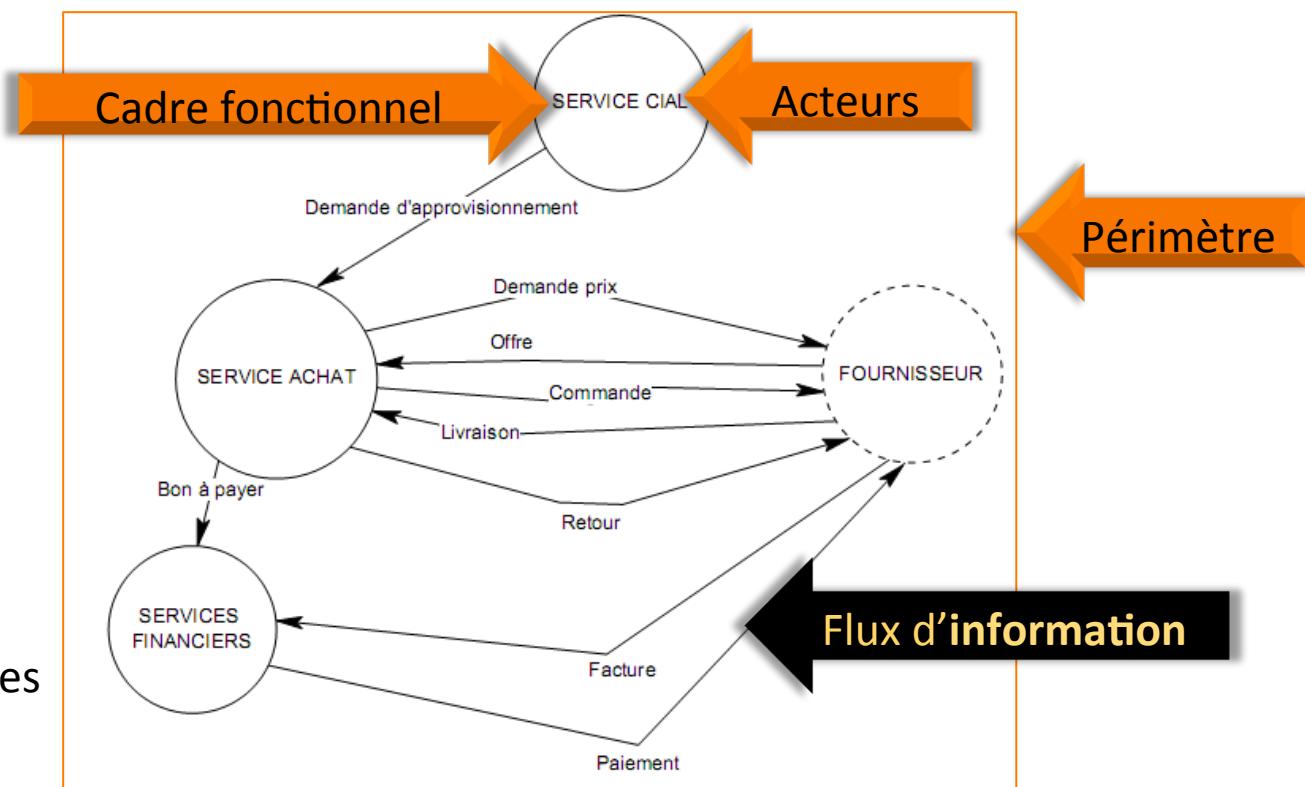
Caractérisation de la sensibilité :

- CID, impact, gravité...
- Permet de définir la sensibilité des composants du systèmes.



Etapes et tâches de l'analyse de risque.

- Définir le périmètre
 - Fonctionnel.
 - Organique.
 - Géographique.
 - ...
- Identifier les acteurs
- Auditer les acteurs
 - Cadre contractuel.
- Identifier les biens.
- Caractériser les biens.
 - Définir les métriques
- Faire valider.



Etapes et tâches de l'analyse de risque.

Biens essentiels

Processus métiers	Processus essentiels	Informations essentielles concernées	Dépositaires
Gestion des relations commerciales	Établir les devis (estimation du coût global d'un projet, négociations avec les clients...)	✓ Cahier des charges ✓ Catalogues techniques ✓ Contrat (demande de réalisation) ✓ Devis	Service commercial
Gestion des études	Créer des plans et calculer les structures	✓ Dossier technique d'un projet ✓ Paramètres techniques (pour les calculs de structure) ✓ Plan technique ✓ Résultat de calcul de structure	Bureau d'études
Gestion des études	Créer des visualisations	✓ Dossier technique d'un projet ✓ Visualisation 3D	Bureau d'études
Gestion des services web	Gérer le contenu du site Internet	✓ Informations société (contacts, présentation...) ✓ Exemple de devis ✓ Exemple de visualisation 3D ✓ Page Web	Directeur adjoint

Etapes et tâches de l'analyse de risque.

Les critères pour caractériser les fonctions et informations :

- CID.
- Autres éléments...



Critères de sécurité	Définition
Disponibilité	Propriété d'accessibilité au moment voulu au bien sensible
Intégrité	Propriété d'exactitude et de complétude du bien sensible
Confidentialité	Propriété du bien sensible de n'être accessible qu'aux utilisateurs autorisés.

Etapes et tâches de l'analyse de risque.

Les échelles de valeurs (besoin de sécurité) :

DISPONIBILITE

Niveaux de l'échelle	Description détaillée de l'échelle
Plus de 72h	Le bien essentiel peut être indisponible plus de 72 heures.
Entre 24 et 72h	Le bien essentiel doit être disponible dans les 72 heures.
Entre 4 et 24h	Le bien essentiel doit être disponible dans les 24 heures.
Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures.

CONFIDENTIALITE

Niveaux de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public.
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.
Réservé	Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées.
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.

INTEGRITE

Niveaux de l'échelle	Description détaillée de l'échelle
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée.
Maîtrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.
Intègre	Le bien essentiel doit être rigoureusement intègre.

Etapes et tâches de l'analyse de risque.

Exemple de production

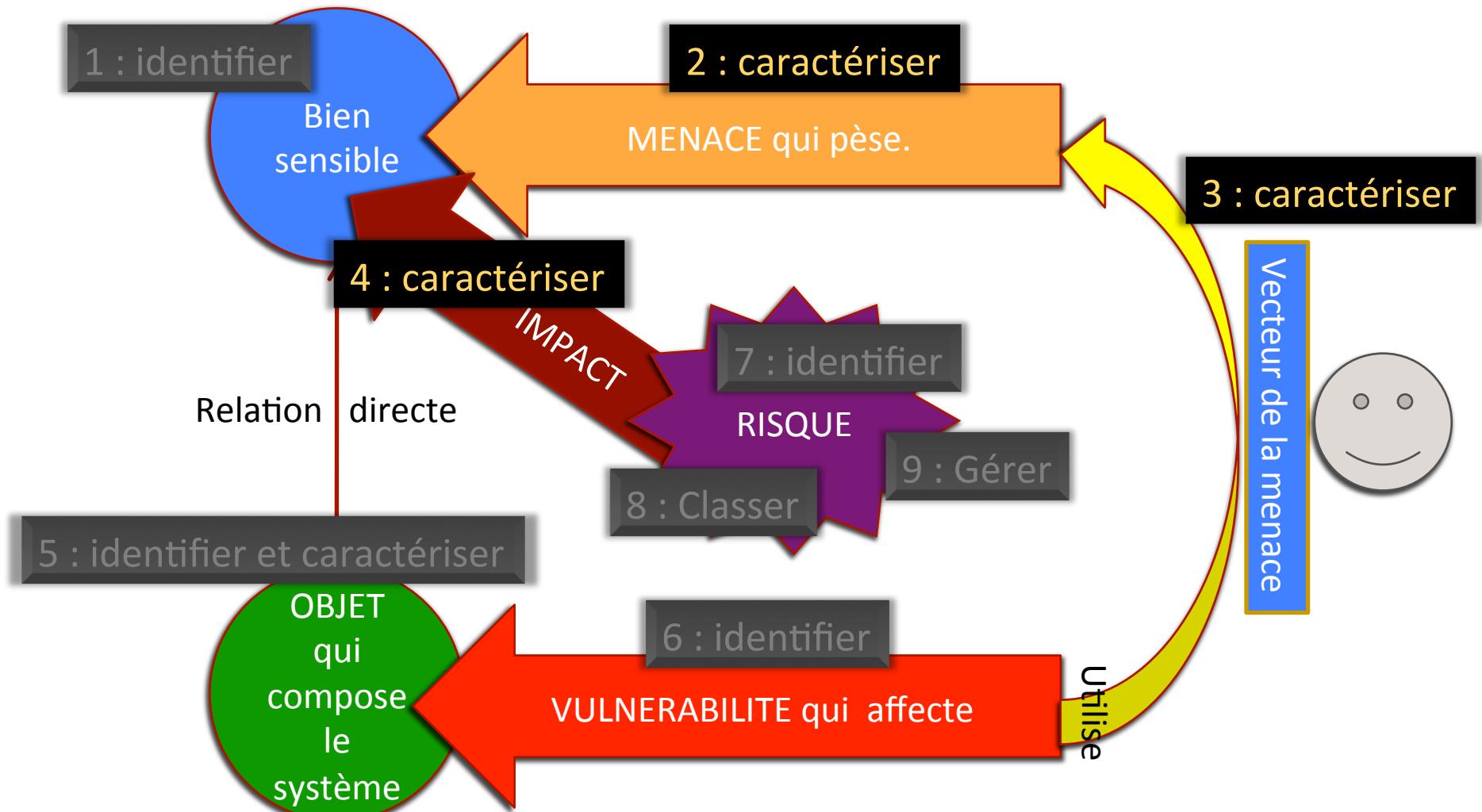
BS	Type	Nom	Description	C	I	D
BS1	Inf.	Design de composant	Masque utilisé pour la réalisation du composant. Comporte l'algorithme de chiffrement.	4	3	2
BS2	Inf.	Plan d'adressage du réseau de l'entreprise	Ensemble des adresses internet des services actifs sur le réseau de l'entreprise	3	3	4
BS3	Fct.	Paye des employés	Calcul des montants et préparation des virements. Comprend les informations E/S de la fonction.	3	3	1

Etapes et tâches de l'analyse de risque.

- ...l'appréciation d'un tel impact est nécessairement subjective. Elle dépend de l'entité qui formule cette appréciation, des valeurs qu'elle respecte et de l'importance qu'elle accorde au projet potentiellement compromis
- Impact :
 - Compromission d'information.
 - Divulgation du patrimoine informationnel de l'entreprise.
 - Perte de service.
 - ...
- Gravité :
 - Qualitative :
 - Négligeable : Le système surmontera les impacts sans aucune difficulté.
 - Limitée : Le système peut surmonter les impacts avec une difficulté modérée.
 - Importante : Le système peut surmonter les impacts mais en fragilisant sérieusement et durablement l'entité.
 - Critique : Le système ne peut pas surmonter les impacts.
 - Quantitative :
 - métrique \$\$\$, temps,...



Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

- **Une menace** est l'attaque possible d'un élément menaçant sur un bien d'un système.
 - Cette menace est liée à un élément hostile.
 - Il faut être prudent avec les approches classiquement présentées.
 - $R = M \times V$.
 - M omniprésente, permanente,...
 - $\rightarrow R = V$.



Etapes et tâches de l'analyse de risque.

- **Le vecteur de la menace est l'élément hostile par lequel la menace peut s'instancier sur le système.**
- **Capacité du vecteur de la menace : cadre d'analyse de la menace.**
- **Exemple :**
 - Menace : espionnage.
 - Vecteur de menace : Société concurrente.
 - Les concurrents de la société sont identifiés. Ce sont les sociétés....



Etapes et tâches de l'analyse de risque.

- Exemples menace :
 - Espionnage.
 - Vol.
 - Incendie.
- Exemples vecteur de la menace :
 - APT28.
 - Administrateur.
 - Feu accidentel.

```
or (int j = 0; j < loc; j++) res[j] = buf[j];
return res;
}
public void checkRes(int[] res) {
    for (int i = 0; i < res.length; i++) {
        if (res[i] != checkRes[i]) {
            System.out.println("Error at index " + i);
        }
    }
}
private int[] decodeMessage(int[] res) {
    int loc = 0, i = 0;
    if (res[0] == 0) {
        i = 0;
    } else {
        i = res[0];
    }
    if (i > res.length) {
        System.out.println("Error: i > res.length");
        return null;
    }
    int loc = i, i = 0;
    while (i < res.length) {
        if (buf[loc] <= MAX_RES_LEN) {
            res[i] = buf[loc];
            i++;
            loc++;
        } else {
            System.out.println("Error: buf[" + loc + "] > MAX_RES_LEN");
            return null;
        }
    }
    return res;
}
public int[] extractMessage(int[] res) {
    int loc = 0, i = 0;
    while (i < res.length) {
        if (buf[loc] <= MAX_RES_LEN) {
            res[i] = buf[loc];
            i++;
            loc++;
        } else {
            System.out.println("Error: buf[" + loc + "] > MAX_RES_LEN");
            return null;
        }
    }
    return res;
}
private void extractMessage(int[] res) {
    for (int i = 0; i < res.length; i++) {
        if (buf[i] <= MAX_RES_LEN) {
            res[i] = buf[i];
        } else {
            System.out.println("Error: buf[" + i + "] > MAX_RES_LEN");
        }
    }
}
```



Etapes et tâches de l'analyse de risque.

- ↗ Pas de réel référentiel de menace.
- ↗ Base générique de certaines méthodes.
- ↗ Impacts de la menace sur les caractéristiques de sécurité des biens sensibles.

39 - ABUS DE DROIT

Utilisation ou exploitation du système par une personne autorisée, dans but mal intentionné (exemples : pour un administrateur ou un exploitant : accord de droits d'administration ou d'exploitation à des personnes non habilitées, rapprochement de données ; pour un PS : accès selon un mode techniquement utilisable mais en dehors du contexte légitime d'emploi)

20 - VOL DE SUPPORTS OU DE DOCUMENTS

Vol de documents du système, vol ou substitution d'un support de stockage d'informations dans un site du système, dans un site de stockage (sauvegarde par exemple) lors d'un transport de support; ou lors de la restitution partielle ou totale du dossier sur support papier ou support informatique

18 - ESPIONNAGE A DISTANCE

Observation des activités d'exploitation ou d'administration du système par des personnes non autorisées (visiteurs, caméras cachées, observateurs par des fenêtres)

Etapes et tâches de l'analyse de risque.

- Pour chaque bien sensible :
 - Identifier la ou les menaces.
 - Identifier un ou plusieurs vecteurs de menace.
 - Evaluer l'impact si la menace se réalise sur le bien sensible.
 - WHAT IF ?
 - Impact direct + impact indirect.
 - Le cas échéant, recenser les mesures compensatrices.
 - Faire valider
- Fait redouté, à rapproché du scénario.

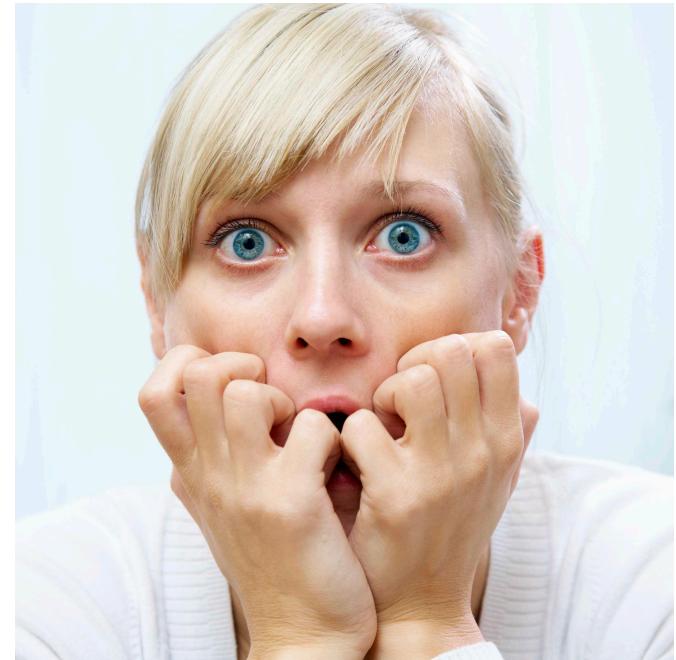


Etapes et tâches de l'analyse de risque.

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Établir les devis				
Indisponibilité de devis	24-72h	✓ Employé peu sérieux ✓ Incendie des locaux ✓ Panne électrique	✓ Impossibilité de signer un contrat ✓ Perte d'un marché ✓ Perte de crédibilité	2. Limitée
Altération de devis	Intègre	✓ Employé peu sérieux	✓ Impossibilité de signer un contrat ✓ Perte d'un marché ✓ Impossibilité de remplir les obligations légales ✓ Perte de crédibilité	3. Importante
Compromission de devis	Limité	✓ Employé peu sérieux ✓ Concurrent	✓ Perte d'un marché ✓ Action en justice à l'encontre du cabinet ✓ Perte de crédibilité	3. Importante

Etapes et tâches de l'analyse de risque.

- Fait redouté :
 - Définition.
 - Utile pour :
 - Limiter le périmètre de l'analyse de risque.
 - Fournir des points d'entrée à l'analyse.
 - Etablir un cadre de communication dans le langage métier du commanditaire.
 - Guider la présentation de l'évaluation du risque.
 - Limites :
 - Souvent centré sur des actifs physiques → nécessite de faire le lien avec la composante système d'information (souvent une grande fonction).
 - Attention au « paradoxe du lampadaire ».

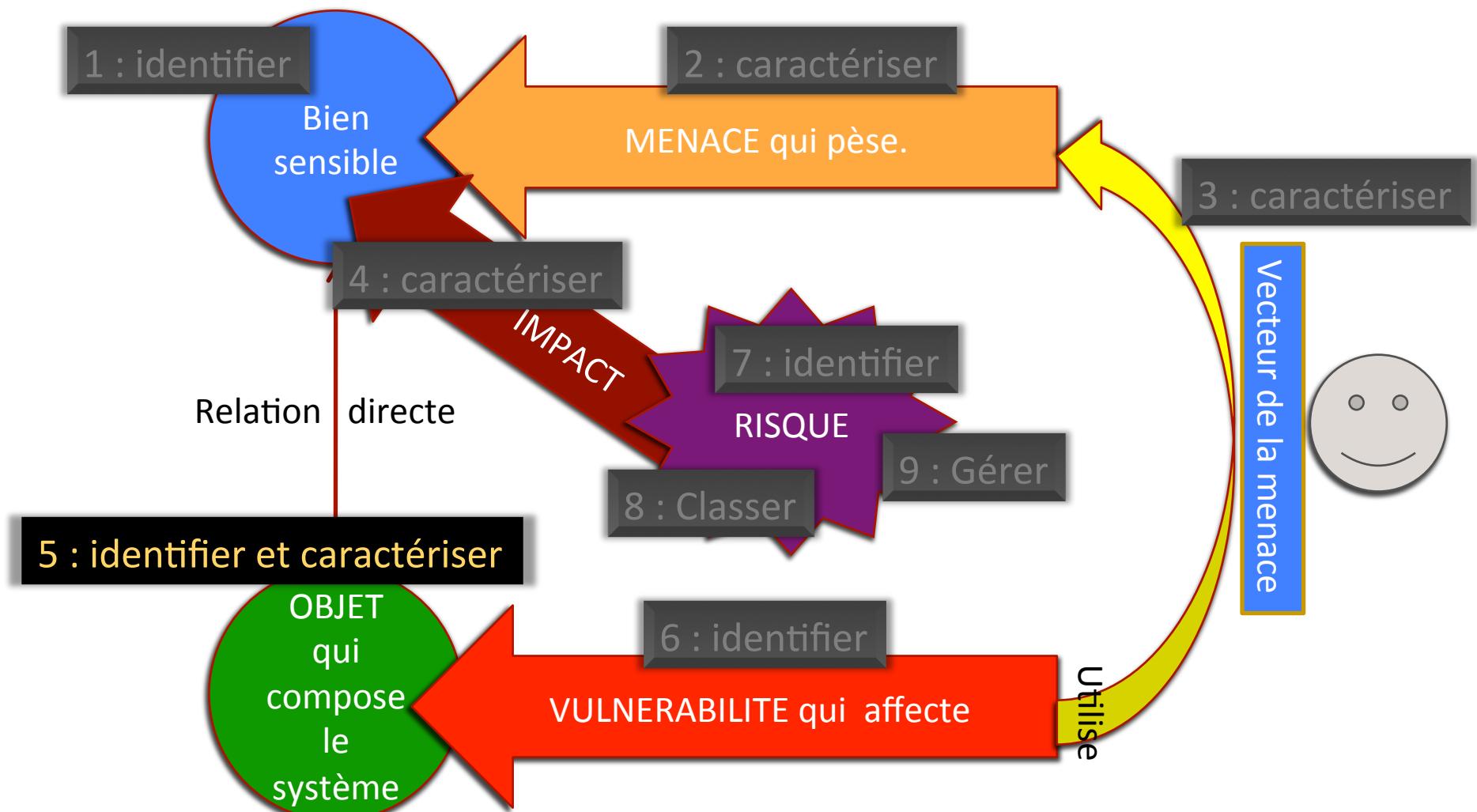


Etapes et tâches de l'analyse de risque.

- Exemple de fait redouté :
 - Nous redoutons qu'un afflux exceptionnel de client à l'ouverture des soldes provoque un dysfonctionnement majeur qui nous fasse perdre un nombre très important de commande.
 - Reformulation AR :
 - Menace : DOS
 - Fonction : prise de commande.
 - Impact : perte de commandes (10^6 € pour 600 s).
 - Gravité : importante.
- Scénario...



Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

Objet sensible :

- essentiellement informatique, il stocke, traite, transporte, réalise un bien sensible.



1000\$

- l'objet hérite de la sensibilité



10000000\$

Héritage multiple.

Etapes et tâches de l'analyse de risque.

- Pour tous les biens sensibles :
 - Identifier les composants du système qui sont en relation directe avec eux et jouent un rôle essentiel dans leur cycle de vie.
 - Un même composant du système peut avoir une relation directe avec plusieurs biens sensibles.
 - Localiser ces composants sur une vue du système, généralement une vue topologique ou une vue d'architecture physique.
 - Identifier les mécanismes de sécurité présents sur ces composants mais aussi en périphérie.
 - Recenser l'ensemble de ces composants et les relations avec les biens sensibles dans un tableau.
 - Pour chaque composant du système, définir son besoin de sécurité par héritage des caractéristiques des biens sensibles avec lesquels il est relation.
 - Faire valider.



Sensibilité nulle.
Valeur : 600€

CLIENTS.DBF	
No_Client	Nom
10	Bowen Jones
12	Steve Smith
13	Mary Ann Chan
11	Lise O'Brien



+



Etapes et tâches de l'analyse de risque.

- Différents types d'objet du système :

PER – Personnes

Ce type de biens supports est constitué de l'ensemble des individus, catégories d'individus ou groupes sociaux homogènes, qui ont accès à tout ou partie des biens essentiels.



MAT – Matériels

Ce type de biens supports est constitué de l'ensemble des éléments physiques d'un système informatique (*hardware* et des supports de données électroniques) participant au stockage et au traitement de tout ou partie des biens essentiels.



CAN – Canaux interpersonnels

Ce type de biens supports est constitué de l'ensemble des circuits organisationnels (canaux et processus organisationnels) et des échanges verbaux en face à face, qui transportent tout ou partie des biens essentiels.



LOG – Logiciels

Ce type de biens supports est constitué de l'ensemble des programmes participant au traitement de tout ou partie des biens essentiels (*software*).



ORG – Organisations

Ce type de biens supports est constitué de la combinaison de personnes (PER), de supports papier (PAP) et des canaux interpersonnels (CAN) en interaction, organisées pour satisfaire les objectifs d'un organisme (en réalisant des activités métiers spécifiques) et manipulant tout ou partie des biens essentiels.



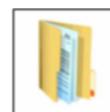
LOC – Locaux

Ce type de biens supports est constitué des infrastructures immobilières hébergeant, et nécessaires au bon fonctionnement, des systèmes informatiques (SYS) et des organisations (ORG), dans lesquels sont utilisés tout ou partie des biens essentiels.



PAP – Supports papier

Ce type de biens supports est constitué de l'ensemble des supports statique non électronique contenant des données.



RSX – Canaux informatiques et de téléphonie

Ce type de biens supports est constitué de l'ensemble des vecteurs physiques de communication et de télécommunication qui transportent tout ou partie des biens essentiels.

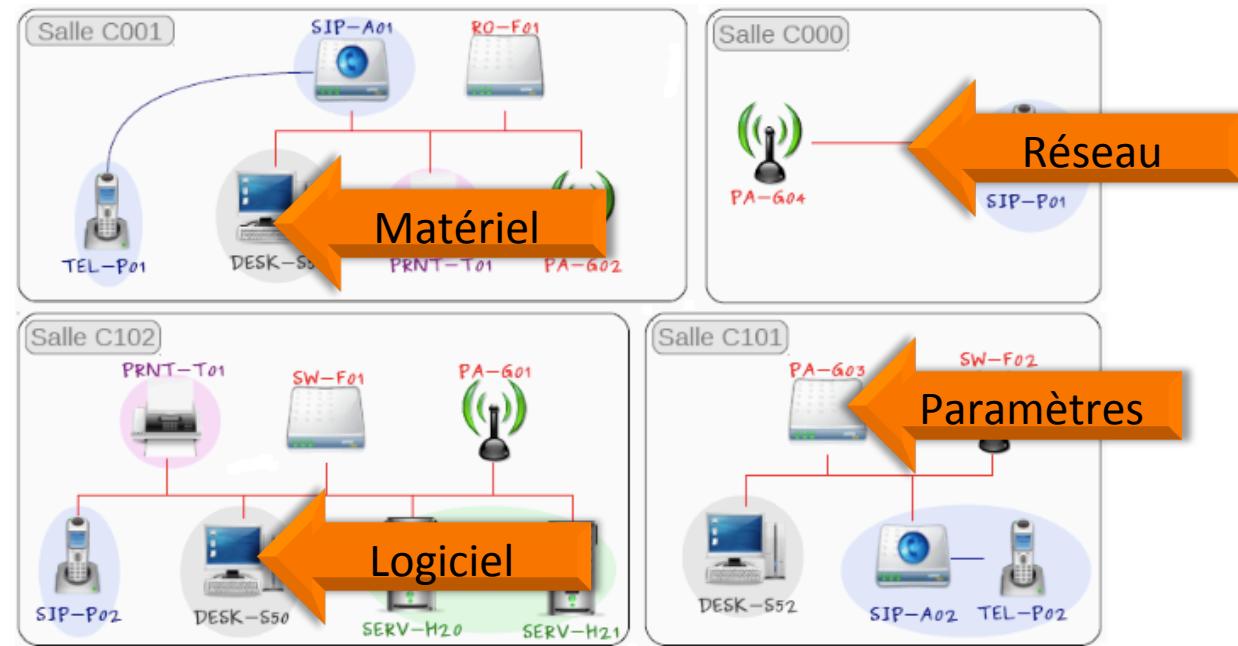


- A adapter en fonction de la cible de l'analyse !

Etapes et tâches de l'analyse de risque.

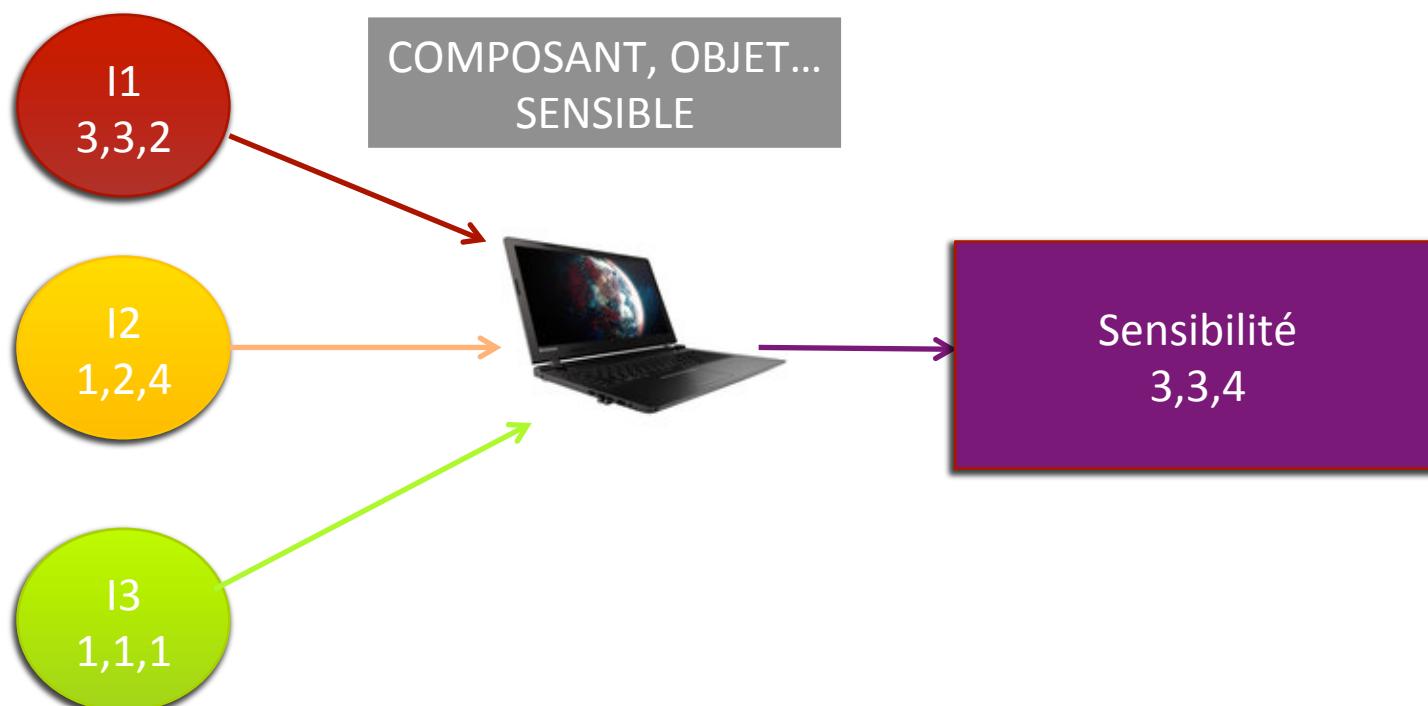
- Vue topologique (automatique, manuel)

Matériel
Logiciel
RZO
Supports info.



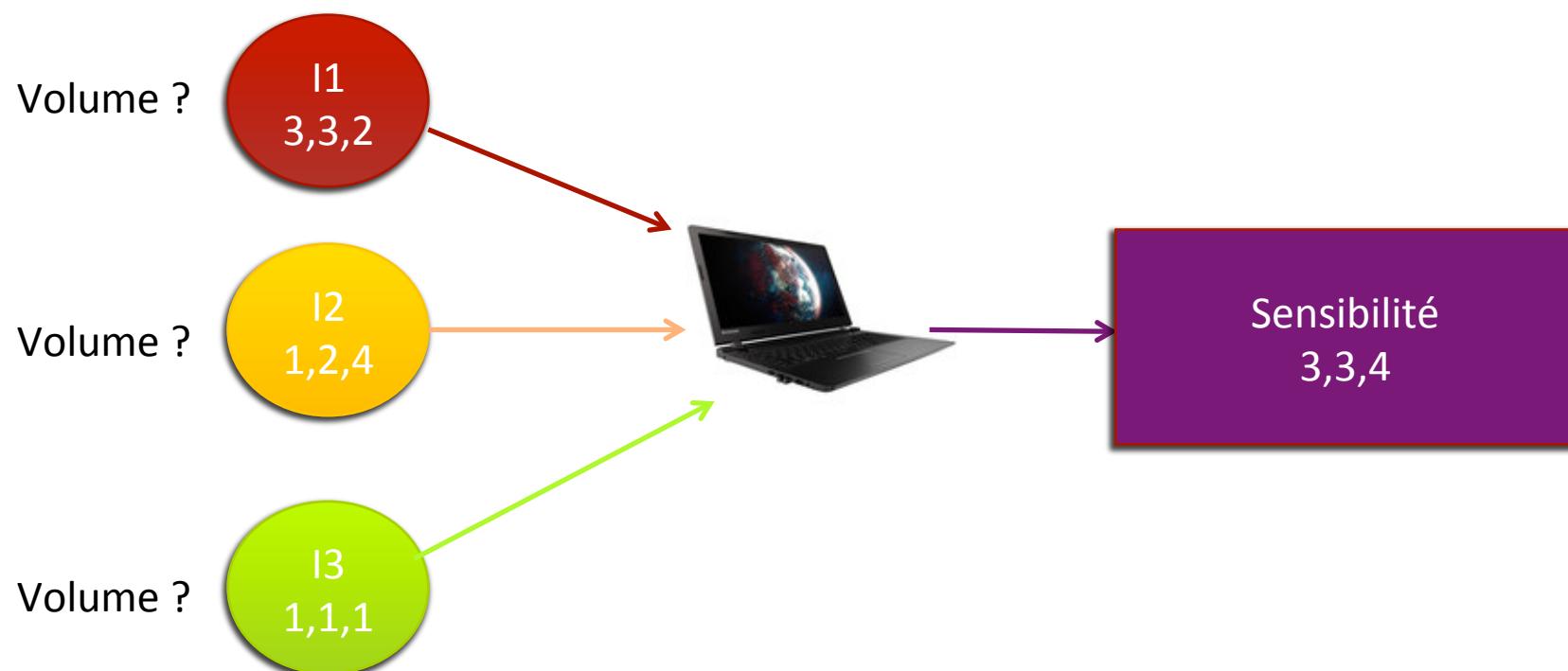
Etapes et tâches de l'analyse de risque.

- Pour tous les biens sensibles :



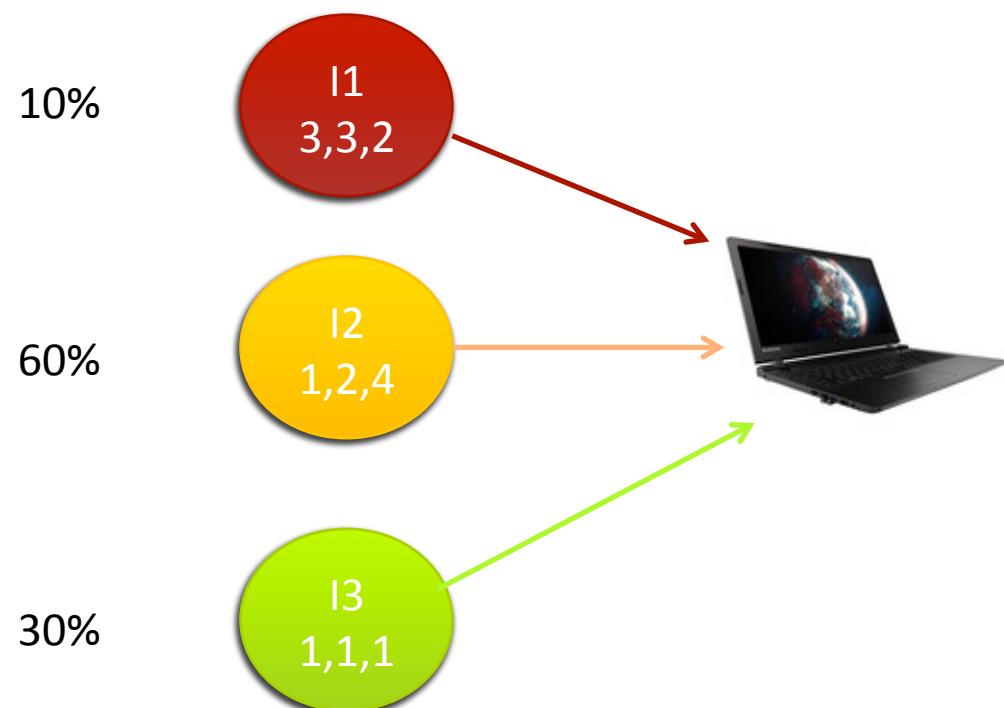
Etapes et tâches de l'analyse de risque.

- Pour tous les biens sensibles :



Etapes et tâches de l'analyse de risque.

- Pour tous les biens sensibles :



Etapes et tâches de l'analyse de risque.

- Pour tous les biens sensibles :



Etapes et tâches de l'analyse de risque.

Types de relation entre BS et OCS.

	Information	Fonction
Matériel	Contenir	Réaliser
Logiciel	Produire, nécessiter, ...	Réaliser
Bâtiment		
Réseau	Transmettre	
Personne	Utiliser	Réaliser
Organisation	Produire, utiliser...	Utiliser
Support	Contenir	

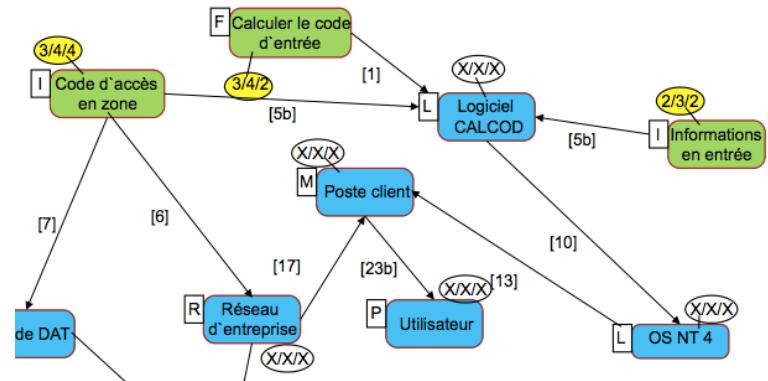
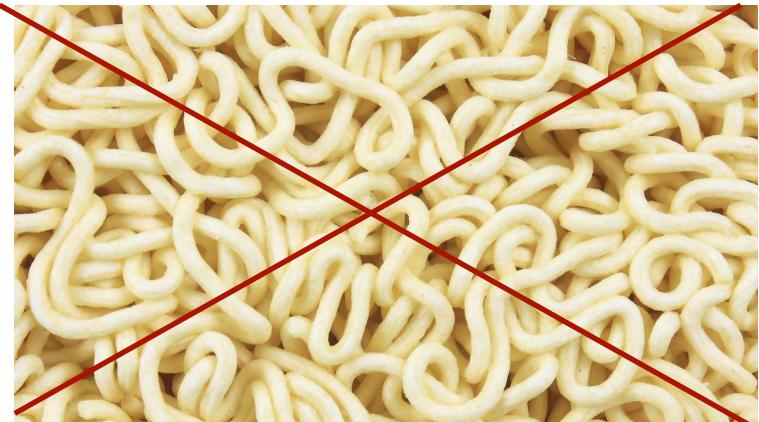
Etapes et tâches de l'analyse de risque.

Types de relation entre BS BS

↗	Matériel	Logiciel	Bâtiment	Réseau	Personne	Orga.	Support
Matériel	Contenir	Contenir	Contenir	Connecter	Accéder	Posséder	Connecter
Logiciel		Utiliser			Accéder		
Bâtiment	Contenir		Contenir	Contenir	Abriter	Accueillir	Contenir
Réseau	Connecter		Contenir	Connecter			
Personne	Accéder	Accéder	Accéder	Accéder		Appartenir	Posséder
Organisation	...						
Support	...						

Etapes et tâches de l'analyse de risque.

- Conseils pour garder une vue utile et utilisable :
 - Privilégier les relations directes.
 - Cas particulier du type « bâtiment ».
 - Généraliser, regrouper les composants identiques.
 - Supprimer les éléments superflus en fonction du contexte de l'analyse (exemple sécurité physique).
 - Simplifier dès que possible... Sauf cas particulier, les mesures de sécurité sont



Etapes et tâches de l'analyse de risque.

- Comment gérer la complexité d'un système :
 - Approche top down de l'analyse.
 - Découpage fonctionnel ou organique.
 - Traitement par décomposition successive des sous ensembles (fonctionnels ou organiques).
 - Pas d'obligation d'avoir le même niveau de détail pour chaque sous ensemble.
 - Limiter l'analyse de risque à une sélection de faits redoutés.
 - La qualité de l'analyse n'est que rarement liée au niveau de détail...

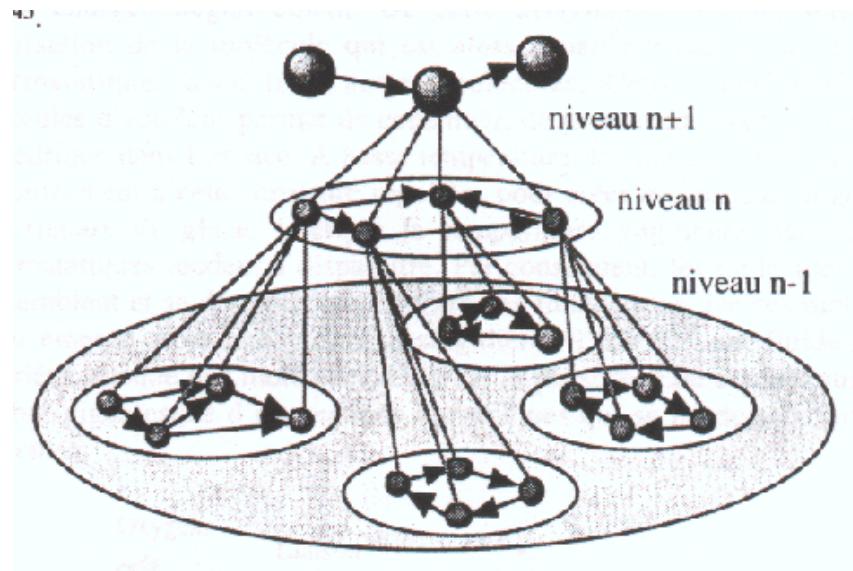
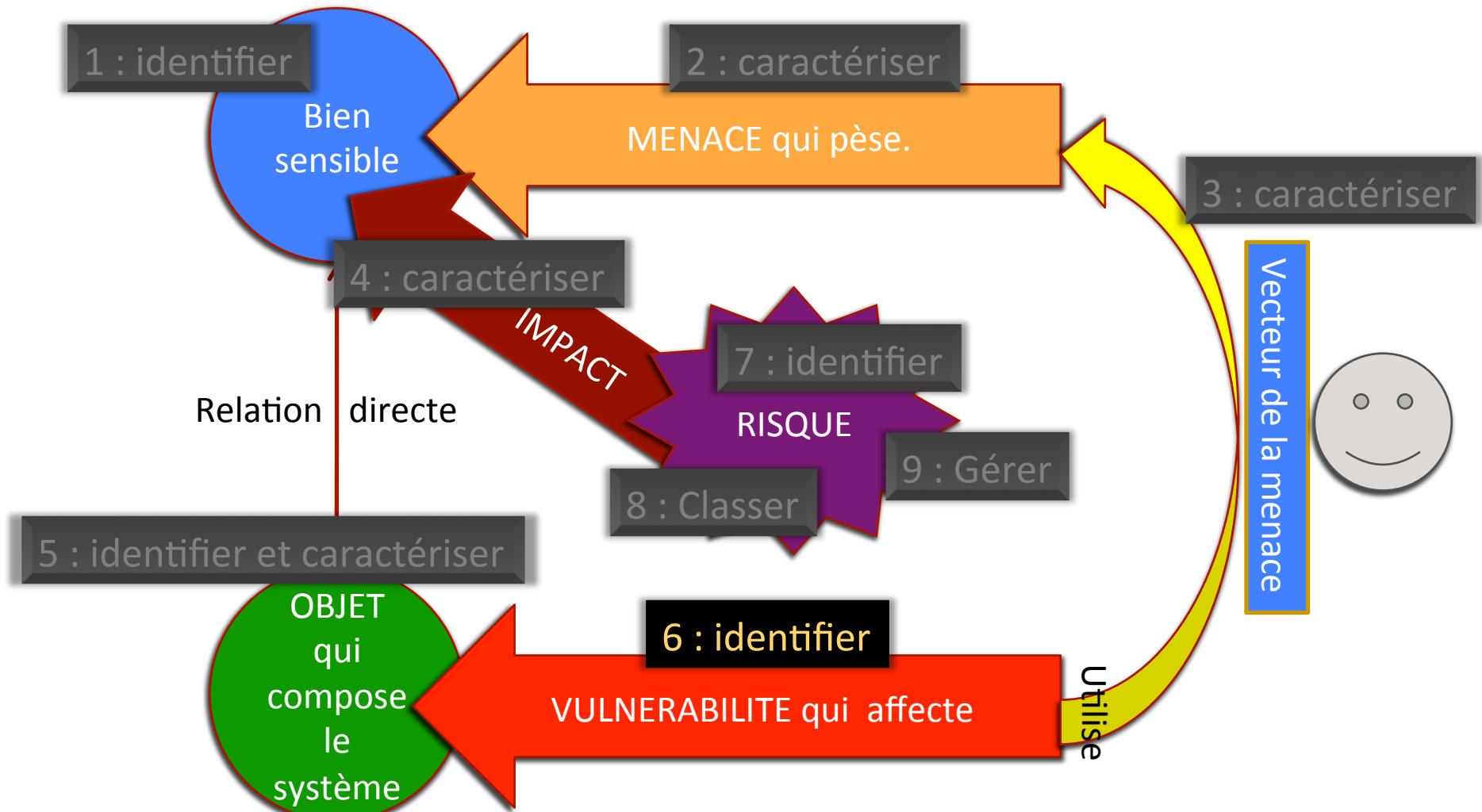


Figure 2.2. Représentation en réseaux d'une pyramide de complexité

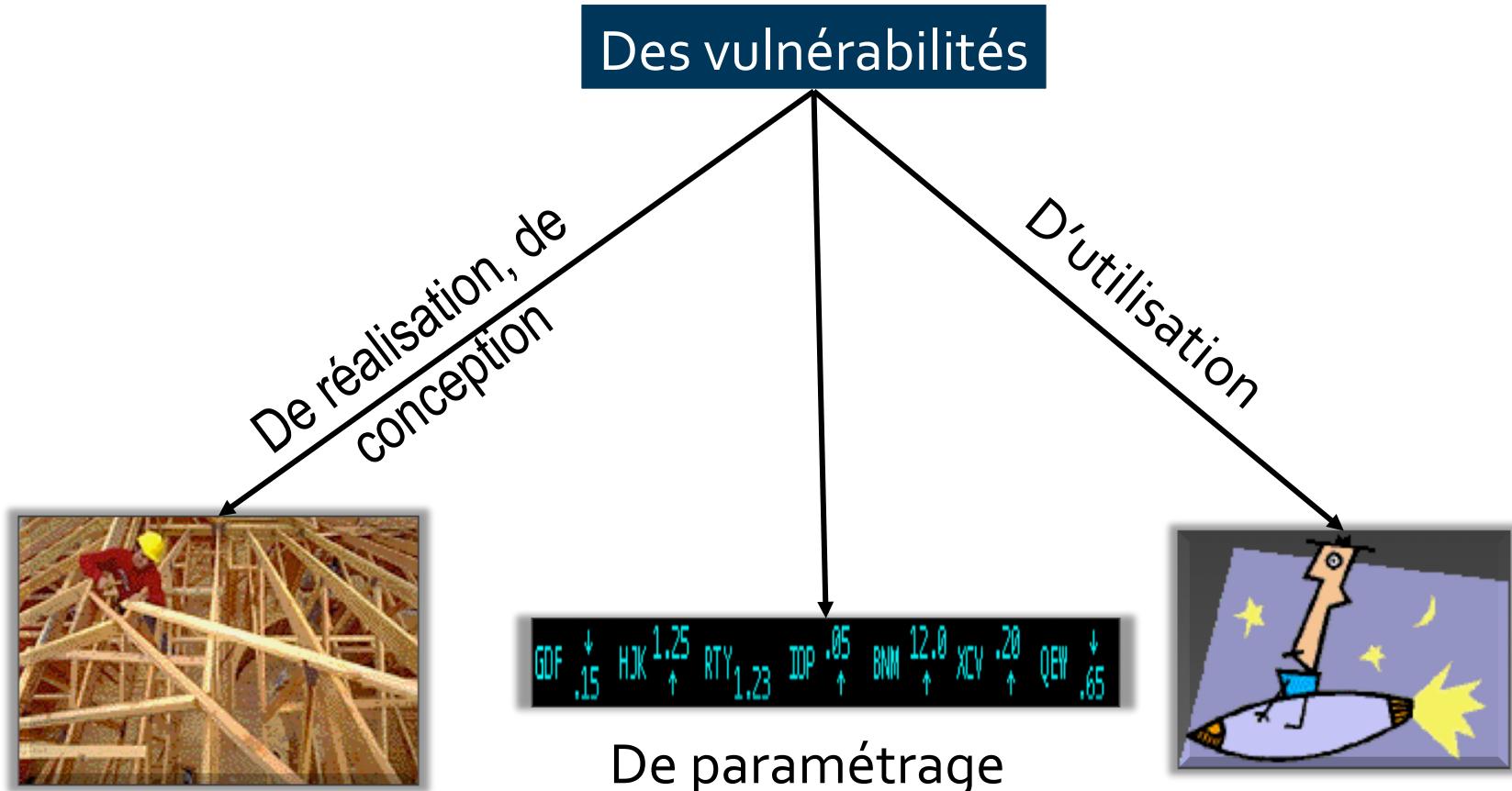
Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

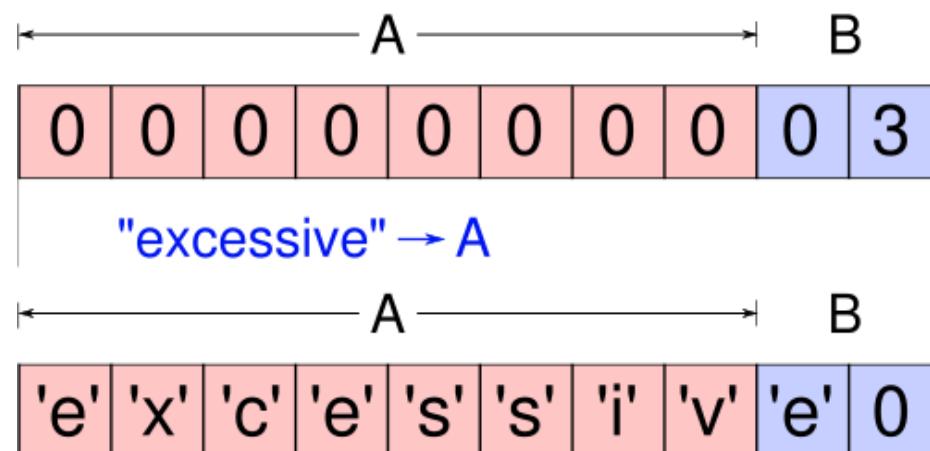
- ↗ **Une vulnérabilité** est une caractéristique d'une entité « du système » qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.
- ↗ On considère trois types de vulnérabilités.

Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

- Dans le cadre des vulnérabilités de conception ou de réalisation on est en présence d'un objet mal réalisé, dont le comportement est déficient. Ce comportement a un impact systémique. L'objet menace directement la politique de sécurité.



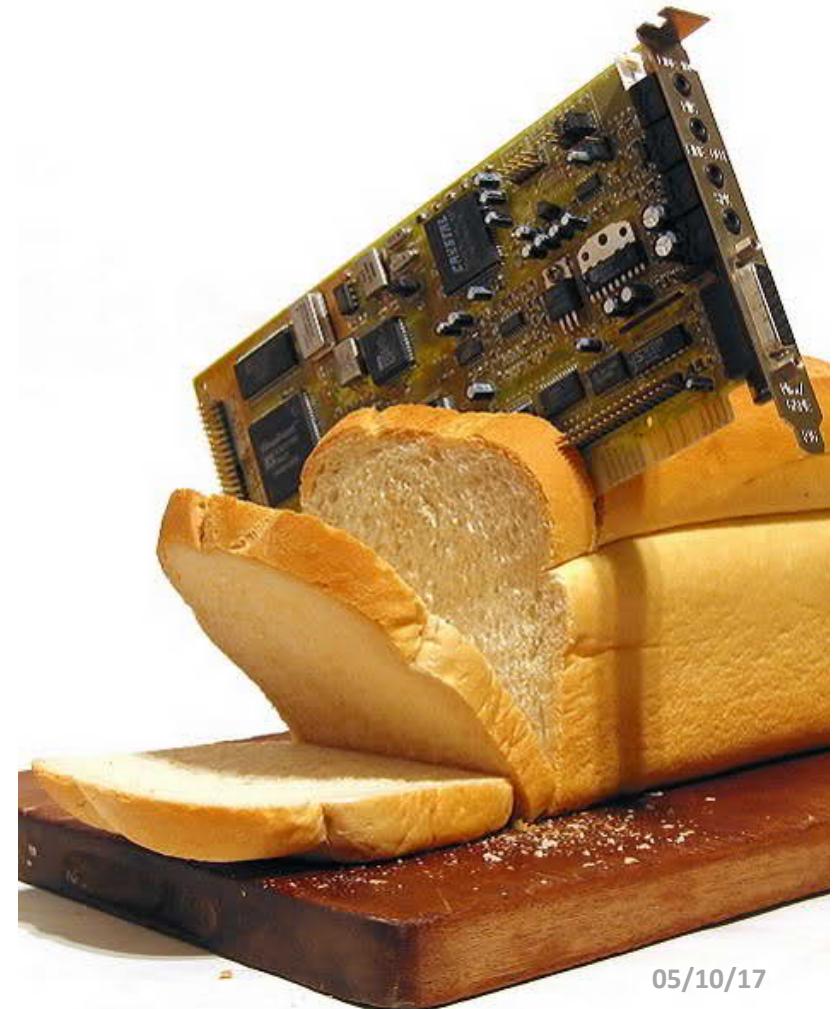
Etapes et tâches de l'analyse de risque.

- ↗ Pour les **vulnérabilités de paramétrage** les objets sont mal intégrés dans leur contexte d'emploi. Ils n'offrent pas un comportement compatible avec la politique de sécurité. Ce comportement impacte l'état des objets qui lui sont connexes. Il affaiblit la politique de sécurité du système dans lequel il est intégré.



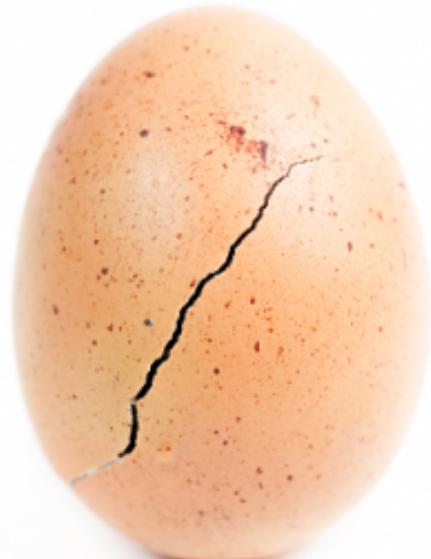
Etapes et tâches de l'analyse de risque.

- ↗ Pour les **vulnérabilités d'utilisation**, l'objet est bien réalisé. Il est intégré comme conformément à l'état de l'art dans son contexte. Dans la manière dont il est utilisé, l'objet ne respecte pas la politique de sécurité du système dans lequel il est intégré car l'utilisation qui en est faite n'est pas conforme avec ses spécifications d'origine.



Etapes et tâches de l'analyse de risque.

- Analyse de vulnérabilité.
- On doit répondre à la question :
 - Quelles sont les vulnérabilités des objets sensibles du système.
 - Nécessite l'utilisation d'un référentiel adhoc.



Etapes et tâches de l'analyse de risque.

- Référentiel de vulnérabilités des composants numériques.
- Sources :
 - Référentiel générique méthode.
 - Analyse de vulnérabilités.
 - Audit, pentest...
 - Sources ouvertes.
 - Référentiels industriels.
 - Référentiel spécialisé
 - Gratuit.
 - Payant.
 - Reverse engineering.
 - Marché des vulnérabilités.

The screenshot shows the homepage of the CERT-FR website. At the top, there's a header with the logo of the Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) and the text "Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques". Below the header, there are sections for "Informations utiles", "ACTUALITÉS", and "ALERTE". The "ALERTE" section is titled "ALERTE (LES 5 plus récentes)" and lists five recent alerts. The "ALERTE" section also includes a note about alert documents being issued to prevent immediate danger. Below this, there's a "Avis (LES 20 plus récents)" section listing 20 recent notices. The footer contains links for RSS feeds and contact information.



Etapes et tâches de l'analyse de risque.

- L'analyse de vulnérabilité :
 - S'applique aux objets sensibles (composant du système en relation directe avec un bien sensible).
 - Sur les objets de type :
 - Technologique.
 - Organisationnel.
 - A réaliser dans l'ordre de sensibilité et à traiter par type de composant technologique.
 - Peut être manuelle ou automatisée.
 - Conduite entre deux phases :
 - Identification.
 - Confirmation.
 - Caractérisation.
 - Nécessite d'adapter le référentiel en fonction du contexte de l'analyse.

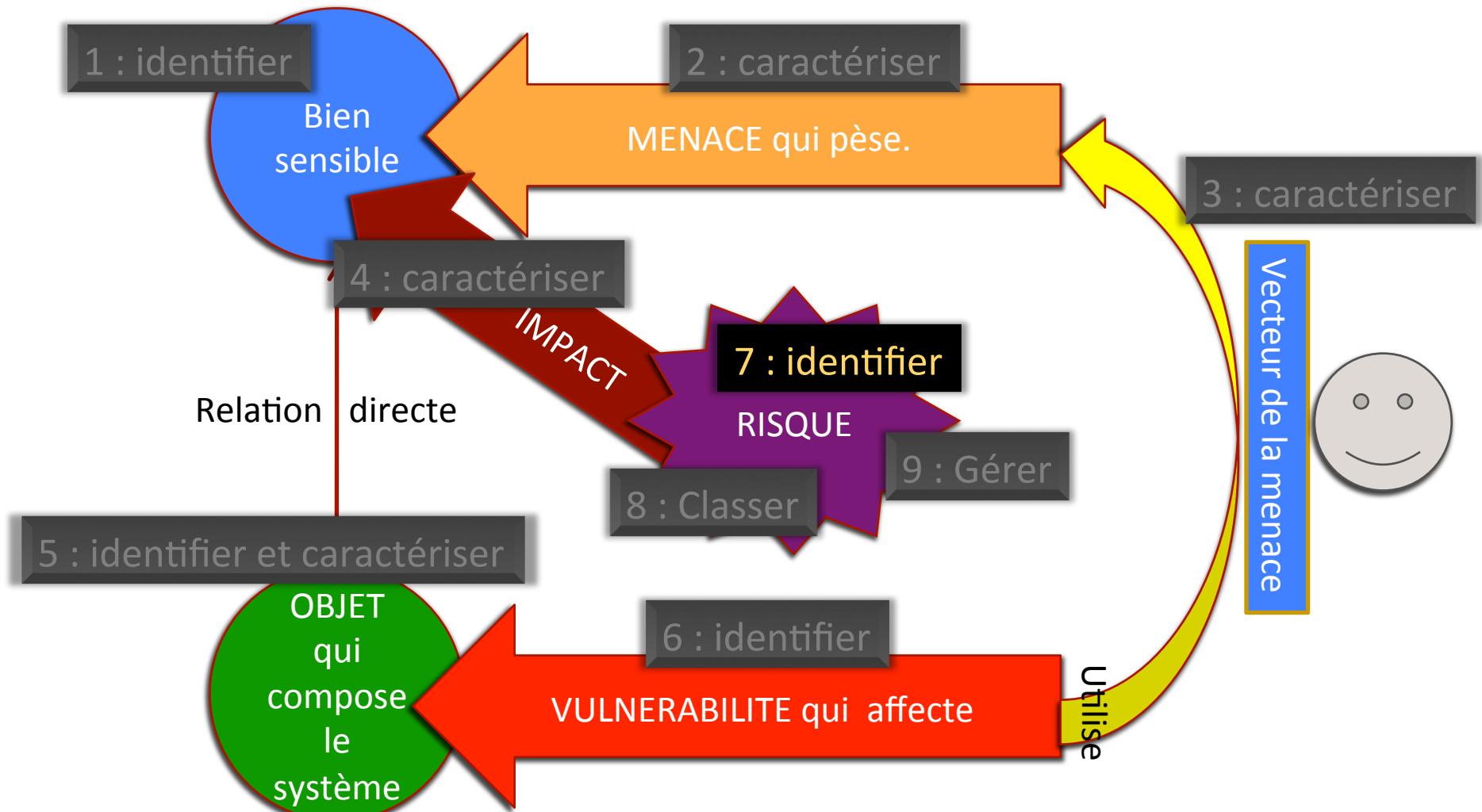


Etapes et tâches de l'analyse de risque.

- Caractérisation des vulnérabilités (exemple).
 - Nécessaire pour l'évaluation du niveau de risque.
 - Traduit la réalité de la vulnérabilité pour l'objet concerné.
 - Vulnérabilité constatée sur le système.
 - La vulnérabilité existe mais n'est pas présente sur l'objet concerné.
 - Vulnérabilité existante sur version antérieure.
 - Vulnérabilité existante sur type d'objet de même nature.
 - Vulnérabilité type sur type d'objet.



Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

- Le scénario est l'outil principal pour identifier les risques → on parle de scénario de risque.
- Ce n'est pas du cinéma ☺
- Étude méthodique qui, à l'aide de données multiples fournies à l'analyste, permet de formuler diverses hypothèses (évaluation) afin d' identifier les décisions possibles et de prévoir leurs conséquences, dans une situation de fait redouté.
- Nécessaire pour :
 - Mettre en dimension les vulnérabilités.
 - Formaliser les risques.
 - Regrouper les risques...
- Scénario risque != scénario de menace.

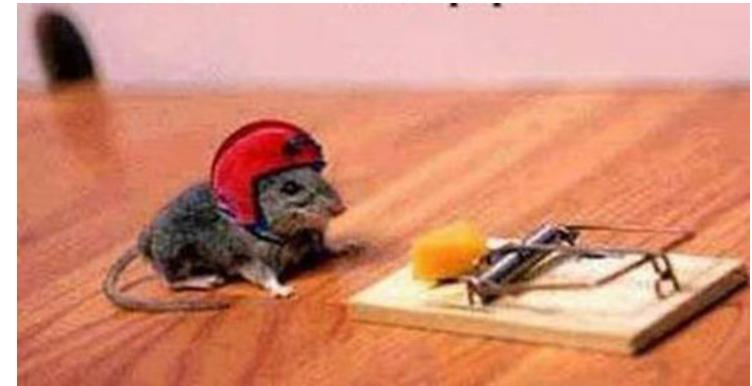


Etapes et tâches de l'analyse de risque.

- Scénario de risque :
 - Un bien sensible.
 - Une menace.
 - Un vecteur de menace.
 - (vulnérabilité, objet sensible) → vraisemblance.
 - Gravité/impact.

Comment identifier les scénarios de risques ?

Quel niveau de raffinement ?



Scénario de risque = (fait redouté, scénario de menace)

Etapes et tâches de l'analyse de risque.

- Le vocabulaire, exemple EBIOS :
 - Scénario de risque , avec un niveau donné, combinant un événement redouté (fait redouté) et un ou plusieurs scénarios de menaces.
 - Événement redouté : Scénario, avec un niveau donné, représentant une situation crainte par l'organisme.
 - Scénario de menace : Scénario, avec un niveau donné, décrivant des modes opératoires.



Etapes et tâches de l'analyse de risque.

- La base pour identifier les scénarios de risque est le fait redouté, c'est à dire l'association d'un bien sensible et d'un impact.
- Le fait redouté est un concept facilement appréhendé par l'organisme qui possède le système.
- Il s'exprime de façon littérale sans difficulté, souvent avec le vocabulaire métier utilisateur du système.
- Essentiel dans le cadre des échanges entre l'analyste et les référents métier.

Créer des plans et calculer les structures				
Indisponibilité de plans ou de calculs de structures	24-72h	<ul style="list-style-type: none">✓ Employé peu sérieux✓ Virus non ciblé✓ Personnel de nettoyage (soudoyé)✓ Personnels de maintenance✓ Panne électrique	<ul style="list-style-type: none">✓ Perte de crédibilité	2. Limitée

Etapes et tâches de l'analyse de risque.

- Exemple de fait redouté :
 - Du point de vue du métier :
 - Nous craignons qu'un attaquant projette notre drone sur un bâtiment public, en prenant son contrôle à distance provoquant ainsi des morts.
 - Du point de vue de l'analyste de risque SSI :
 - Perte de contrôle.
 - Système de command control.
 - Hacker.
 - Destruction d'un actif physique
→ gravité maximale.



Etapes et tâches de l'analyse de risque.

- Pour chaque fait redouté, rechercher les enchainements potentiels et en évaluant leur vraisemblance (scénario de menace).
- Un scénario de menace combine :
 - les sources de menaces susceptibles d'être à l'origine ➤ ex. : l'adolescent de 15 ans,
 - un bien support ex. : système informatique du collège,
 - un critère de sécurité ➤ ex. : intégrité,
 - des menaces ex. : intrusion, élévation de privilèges et modification de contenu,
 - les vulnérabilités exploitables pour qu'elles se réalisent ex. : facilité d'accès aux données, possibilité de modifier les données.



Etapes et tâches de l'analyse de risque.

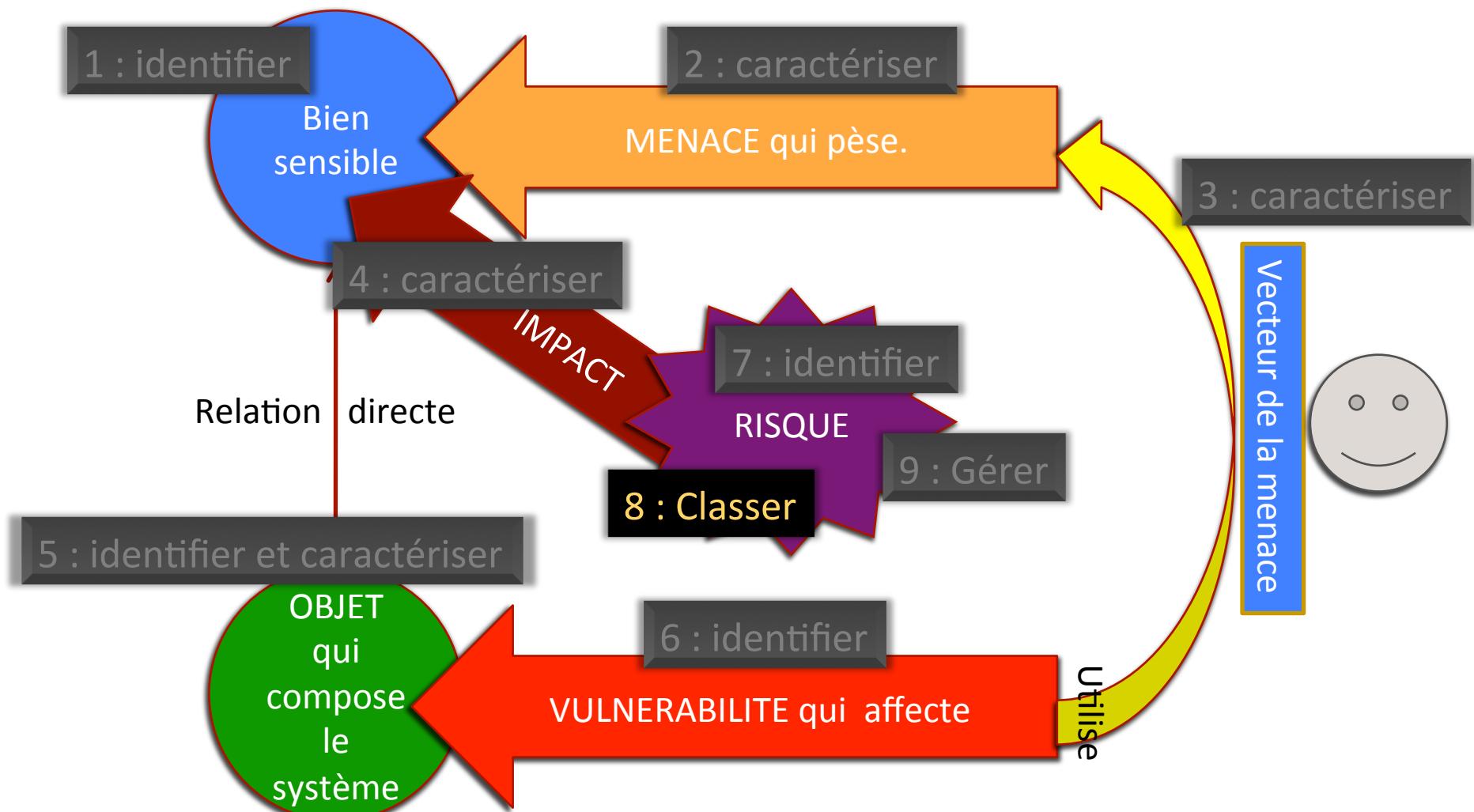
- Référentiel pour les scénarios de menace :
 - Il n'y en a pas.
 - Processus de veille.
 - Attention : tonneau des danaïdes.
 - Les limites de la preuve par l'exemple.
 - Quelques pistes de documentation.
 - Les rapports CLUSIF.
 - Les rapports annuels des majors de Cyber sécurité.
 - La presse spécialisé.
 - Des colloques, bien choisi.
 - La capitalisation interne.
 - Le BSP.



Sauron/Strider : la nouvelle attaque étatique débusquée par Symantec et Kaspersky

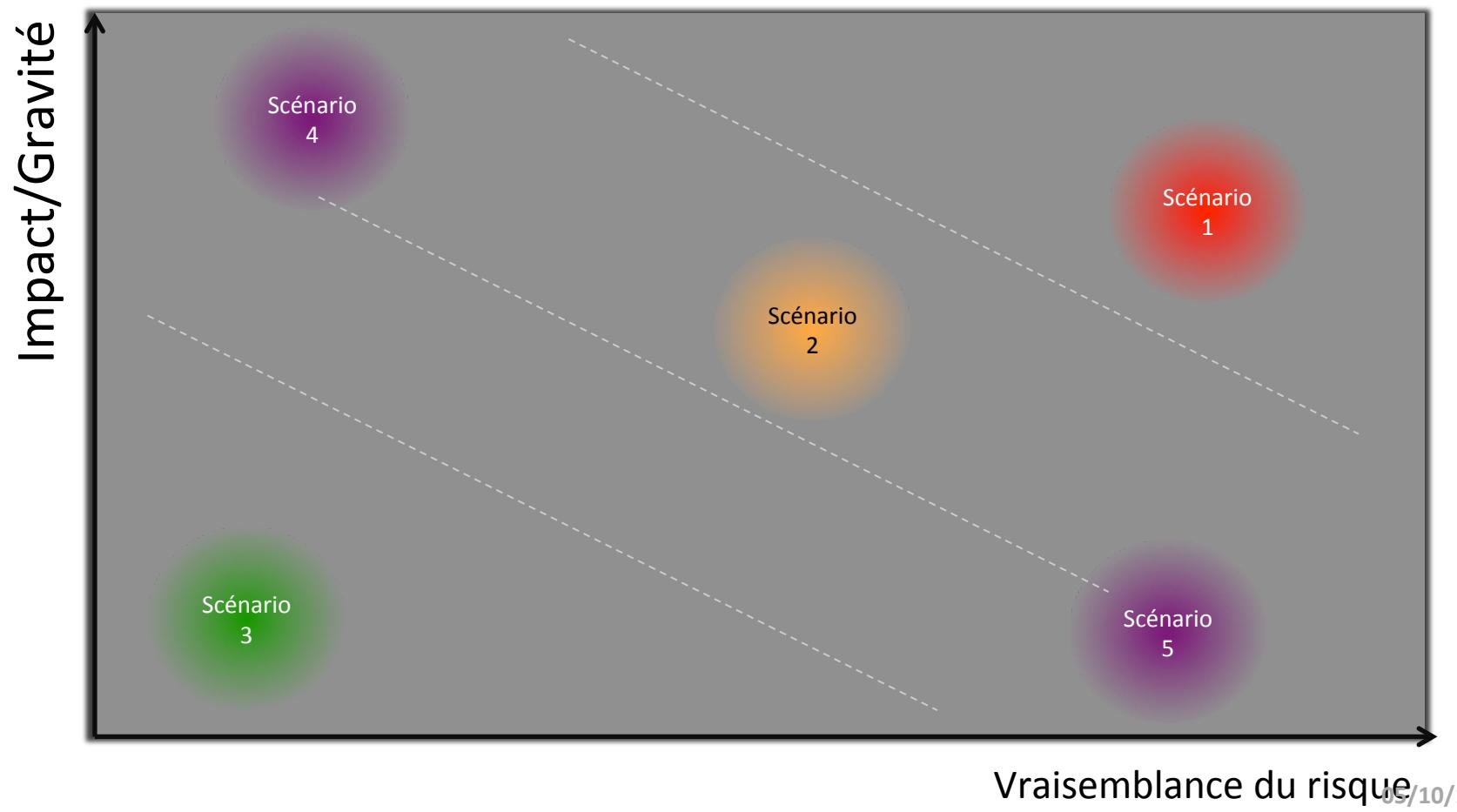
Sécurité : Symantec et Kaspersky publient coup sur coup deux études portant sur un même acteur cybercriminel identifié par leurs chercheurs. Les deux sociétés soupçonnent qu'un acteur étatique se dissimule derrière ce groupe, qui s'attaque à des cibles situées notamment en Russie et en Iran.

Etapes et tâches de l'analyse de risque.



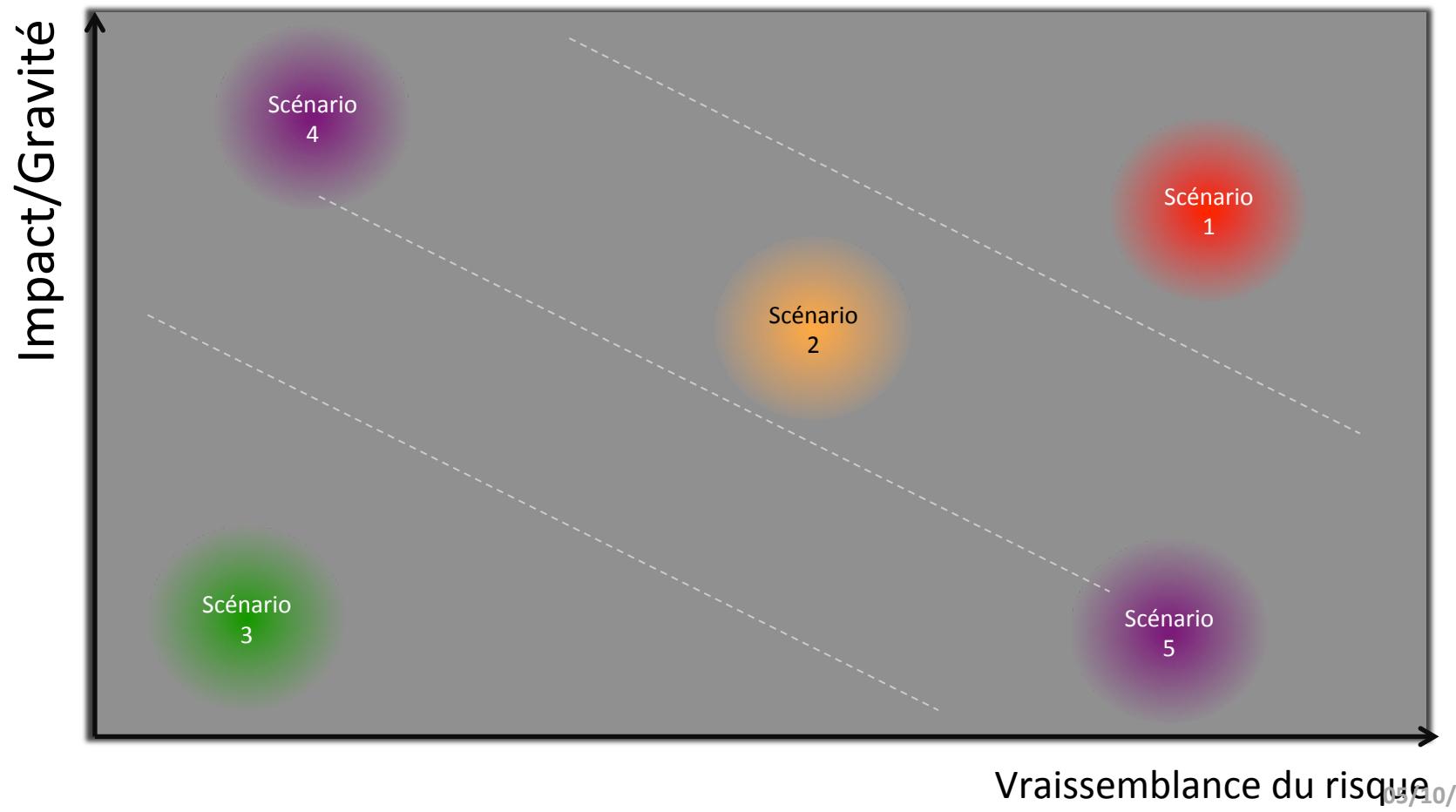
Etapes et tâches de l'analyse de risque.

- Ce que l'on veut faire



Etapes et tâches de l'analyse de risque.

Objectif de l'évaluation du risque.



Etapes et tâches de l'analyse de risque.

- **Gravité :**
 - Estimation de la hauteur des effets d'un évènement redouté ou d'un risque. Elle représente ses conséquences.
 - Elle dépend essentiellement de la hauteur et du nombre des impacts, de la valeur du bien considéré, de la motivation des sources de menaces.
- **Vraisemblance :**
 - Estimation de la possibilité qu'un scénario de menace ou qu'un risque se produise. Elle représente sa force d'occurrence.
 - Elle dépend essentiellement de l'exposition aux menaces
 - considérées :
 - de l'existence plus ou moins avérée de vulnérabilités,
 - de la motivation des sources de menaces.
 - de la facilité d'exploitation des vulnérabilités identifiées,
 - de la capacité des sources de menaces.



Etapes et tâches de l'analyse de risque.

- **Gravité :**

- Estimation de la hauteur des effets d'un évènement redouté ou d'un risque. Elle représente ses conséquences.
- Elle dépend essentiellement de la hauteur et du nombre des impacts, de la valeur du bien considéré, *de la motivation des sources de menaces*.

DIRECTEMENT LIÉE A LA NATURE DU BIEN SENSIBLE

- **Vraisemblance :**

- Estimation de la possibilité qu'un scénario de menace ou qu'un risque se produise. Elle représente sa force d'occurrence.
- Elle dépend essentiellement de l'exposition aux menaces
- considérées :
 - de l'existence plus ou moins avérée de vulnérabilités,
 - de la motivation des sources de menaces.
 - de la facilité d'exploitation des vulnérabilités identifiées,
 - de la capacité des sources de menaces.



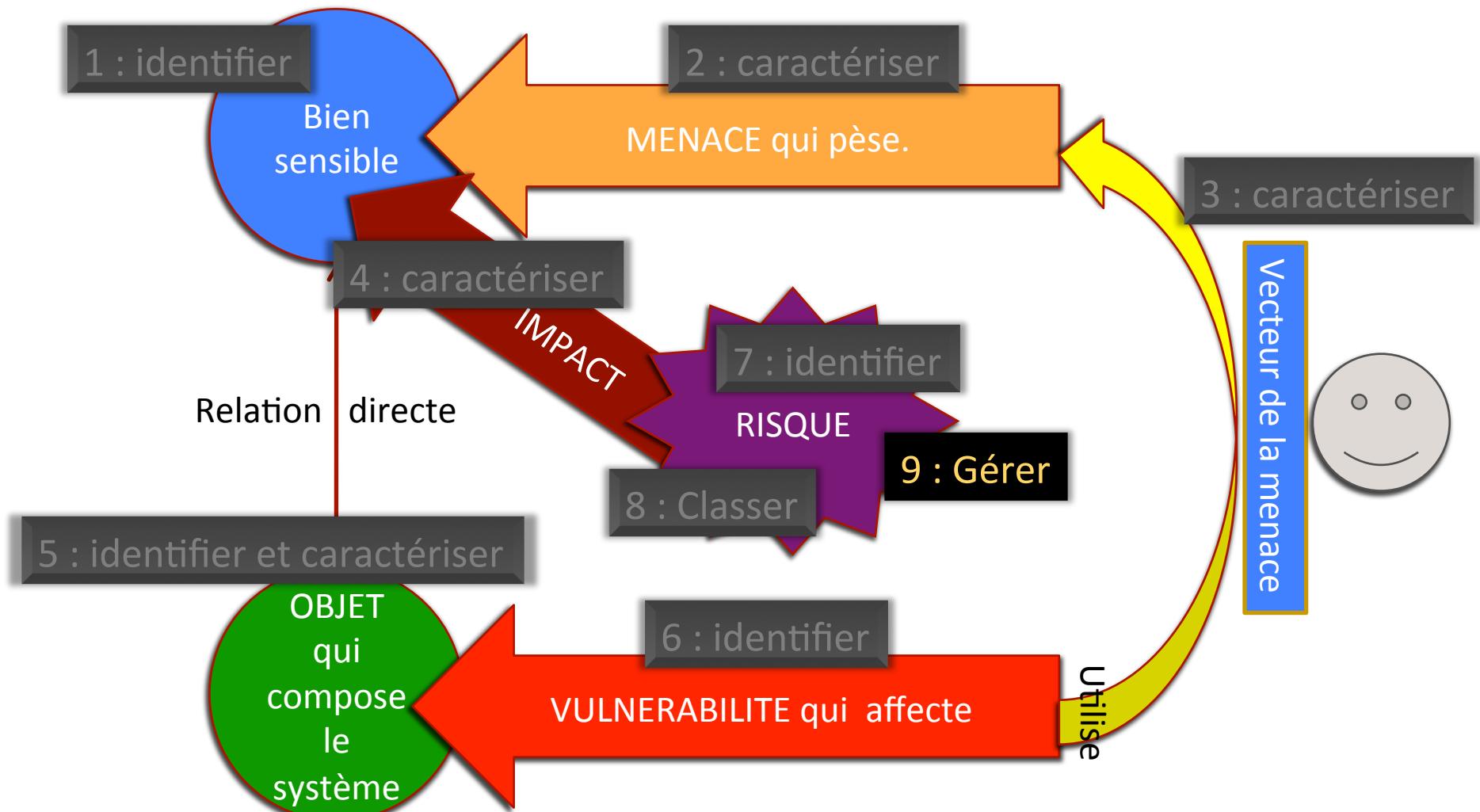
Etapes et tâches de l'analyse de risque.

- Vraisemblance :
 - Définir une échelle de vraisemblance en cohérence avec le cadre de l'étude (système existant ≠ système futur).
 - Directement déduite du scénario de menace.
 - Vulnérabilité :
 - 3 : majeures constatées sur le système
 - 2 : existes sur ces composants (CTOS).
 - 1: niveau de sécurité assuré
 - Scénario :
 - 3 : Connue et détaillée.
 - 2 : partiellement documenté.
 - 1 : conceptuel.

Expliquer pour chaque niveau

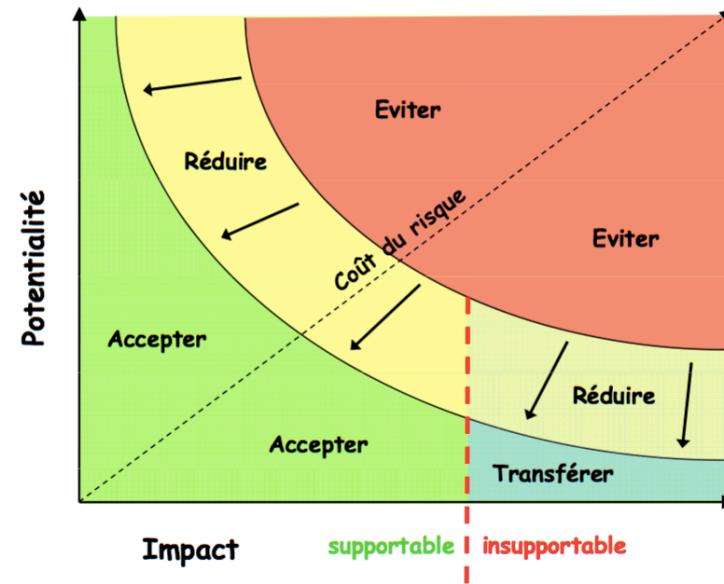
		Vulnérabilité		
		1	2	3
Scénario	3	2	3	4
	2	1	2	4
	1	0	1	2

Etapes et tâches de l'analyse de risque.



Etapes et tâches de l'analyse de risque.

- Objectif :
 - A partir des risques identifiés et classés il faut identifier les moyens de sécurité à mettre en place pour ramener le risque à un niveau acceptable.
 - → définir la stratégie de gestion de risque.
 - Négociation avec le détenteur du système cible de l'analyse en particulier sur le niveau d'effort qui sera consenti (RH, externalisation, finance...).



Etapes et tâches de l'analyse de risque.

Déterminer les mesures de sécurité

- Quelles mesures doivent être mise en place ?
- Servent-elles à la prévention, la protection, ou la récupération ?
- Sur quels biens supports reposent-elles ?

Analyser les risques résiduels

- Quelles sont les nouvelles valeurs de gravité et vraisemblance ?
- Quels sont les scénarios toujours possibles ?

- Stratégie de gestion des risques.
 - L'évaluation du risque constitue l'entrée de la gestion des risques.
 - Nécessite la mise en place de mesures de sécurité qui permettent de réduire, éviter, transférer et accepter le risque.
 - L'ensemble des mesures de sécurité et les risques résiduels acceptés constituent la politique de gestion des risques.
 - La politique de gestion des risques doit être adaptée :
 - Au niveau de sécurité constaté et attendu.
 - Quel est l'intérêt de préconiser une mesure de très bas niveau technique quand les fondamentaux de la sécurité ne sont pas en place → niveau de prise en compte adapté.
 - Aux enjeux de l'analyse de risque.
 - Dans le cadre d'une PME pour améliorer la sécurité globale d'un SI, un plan d'actions peut être suffisant.
 - Dans le cadre de la contractualisation pour la réalisation d'un service, d'une fonction, d'un produit de sécurité majeur, les mesures de sécurité devront être déclinées en exigences de sécurité.
 - La politique de sécurité est un cadre général qui doit être instancié et géré en mode projet.

Etapes et tâches de l'analyse de risque.

- Des mesures :
 - Organisationnelles.
 - Personnel, organisation, gestion, environnement.
 - Techniques.
 - Matériel, logiciel, réseau, support, environnement.
 - Qui ciblent :
 - La confidentialité.
 - L'intégrité.
 - La disponibilité.
 - Afin de traiter le risque.



Etapes et tâches de l'analyse de risque.

Objectif de sécurité

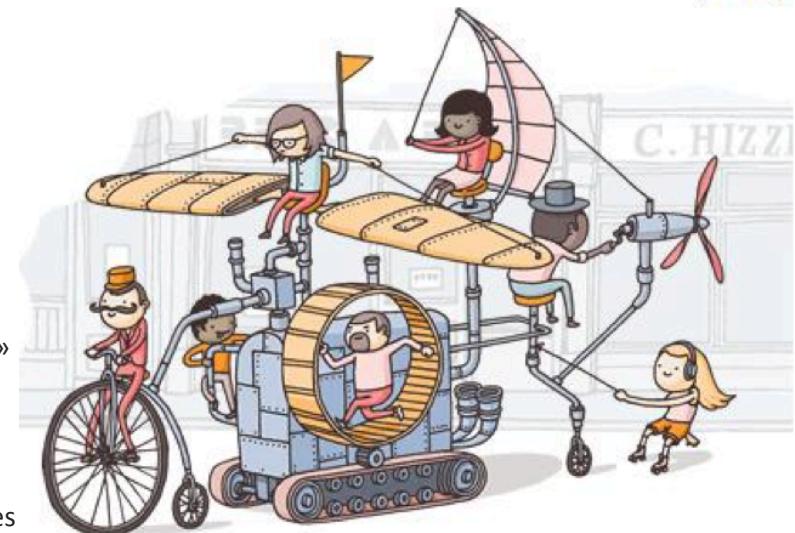
- Cadre la gestion de risque pour chaque risque.

Mesure de sécurité

- C'est le moyen de traiter un risque de sécurité de l'information ; la nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables.

Les exigences de sécurité

- Dans un cadre d'ingénierie classique, la conception et le développement requièrent la rédaction d'exigence.
- Définitions : « Ce qui est commandé par qqch, nécessité, obligation. »
« Ce qu'une personne exige, réclame à une autre. »
- Mathématiquement → Exigence = Fonction
- « La gestion des exigences consiste à gérer les exigences hiérarchisées d'un projet, à détecter les incohérences entre elles et à assurer leur traçabilité. »
- Ces exigences ont généralement comme origine, une analyse des risques. Le but est de diminuer l'arrivée ou la gravité d'événements dangereux.



Etapes et tâches de l'analyse de risque.

Risque	Évitemen	Réduction	Prise	Transfert
Risque lié à l'indisponibilité d'un devis au-delà de 72h		(X)	X	
Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	(X)	X	X	(X)
Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h		(X)	X	
Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	(X)	X	X	(X)
Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de visualisations au-delà de 72h		(X)	X	
Risque lié à l'altération de visualisations sans pouvoir la détecter		X	(X)	(X)
Risque lié à la compromission de visualisations, jugées comme publiques		(X)	X	
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h		(X)	X	
Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver		X	(X)	(X)
Risque lié à la compromission du contenu du site Internet public		(X)	X	

Etapes et tâches de l'analyse de risque.

- Quels sont les leviers pour la gestion du risque ?
 - Peut-on agir sur les conséquences (impact/gravité) d'un fait redouté ?
 - Cela dépend de la nature du risque.
 - On peut définir des mesures de sécurité qui permettent de prévenir le risque. On recherche à anticiper pour limiter l'impact.
 - Peut-on agir sur la menace ?
 - Non, sauf dans des cas particuliers.
 - Peut-on agir sur les vulnérabilités ?
 - C'est le cadre le plus évident. On est dans l'adaptatif et dans le correctif.
 - Trois axes :
 - Le curatif → on corrige, on améliore, dans le contexte opérationnel → on est dans le maintien en condition de sécurité.
 - Le préventif → on prévoit, on limite dans la conception, dans la réalisation → on est dans la construction de la sécurité.
 - Le prédictif → on anticipe au niveau politique → on est dans l'organisation de la sécurité.



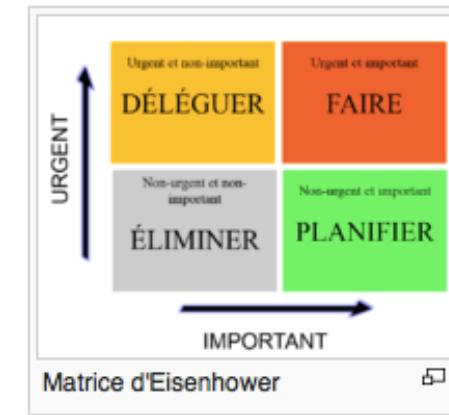
Etapes et tâches de l'analyse de risque.

- Agir sur la menace :
 - Hors scope.
- Agir sur les conséquences (diminuer l'impact/gravité) :
 - Au niveau de la prévention. Exemple : Séparer les biens les plus sensibles des éléments les moins sécurisés.
- Agir sur les scénarios (diminuer la vraisemblance):
 - Ne pas rentrer dans une course à la correction systématique en mode urgence.
 - Mettre en dimension les vulnérabilités :
 - Rechercher l'efficacité.
 - Rationnaliser.
 - Diversifier les solutions → notions de défense en profondeur.
 - Proposer des mesures qui pérennissent la diminution des risques (fuite en avant de la correction répétitive de vulnérabilité).



Etapes et tâches de l'analyse de risque.

- Prendre tous les scénarios de risques.
- Lister les points convergents de ces scénarios.
 - Etape du scénario
 - Exemple : l'élément hostile peut se connecter facilement au réseau de l'entreprise.
- Identifier la ou les vulnérabilités clés des points convergents.
- Lister les mesures qui traitent la vulnérabilité.
- Exemple de référentiel de mesures : thèmes ISO 27002 pour les aspects organisationnels.
- Rechercher au minimum 2 à 3 mesures différentes qui réduisent réduisent ou suppriment ces vulnérabilités « importantes » (au sens des scénarios de risques (la divulgation de crypto1 est-elle une vulnérabilité importante ?).
- Classer les mesures concurrentes en fonction :
 - De leur impact sur la vraisemblance/impact.
 - Validation / vecteur de sécurité.
 - De leur persistance.
 - Du coût et de la réalisabilité.
 - Utilisation de la matrice d'Eisenhower.
- Retenir la (les) mesures les plus performantes.
 - Proposition de scénarios alternatifs.
- Traiter les vulnérabilités qui ne convergent pas.



Efficacité

Mesure de sécurité	R1	R2	R3	R4	R5	R6	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques				X			LOG – MacOS X	7.1. Responsabilités relatives aux biens		X	
Désactivation des composants inutiles sur le serveur	X	X	X	X	X	X	LOG – Serveurs logiciels du réseau interne	10.1. Procédures et responsabilités liées à l'exploitation	X		
Mise à jour régulière de l'antivirus des serveurs et de sa base de signatures	X		X		X	X	LOG – Windows XP	10.4. Protection contre les codes malveillant et mobile		X	

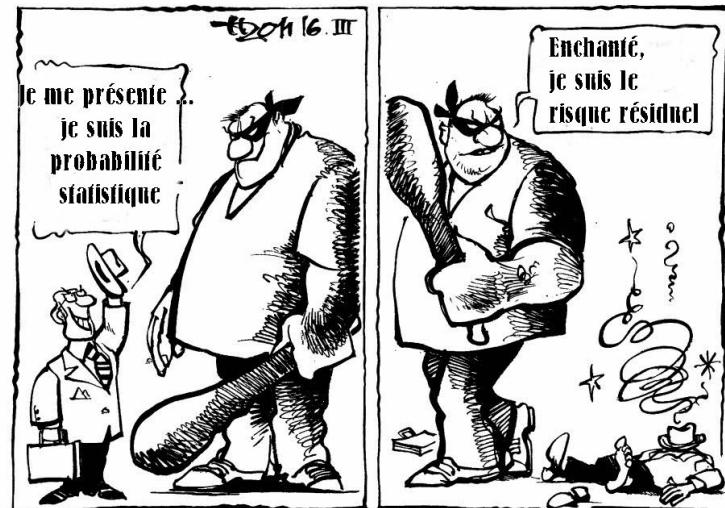
Couverture

Importance = f (coût/couverture, efficacité)

5. Politiques de sécurité de l'information
6. Organisation de la sécurité de l'information
7. Sécurité des ressources humaines
8. Gestion des actifs
9. Contrôle d'accès
10. Cryptographie
11. Sécurité physique et environnementale
12. Sécurité liée à l'exploitation
13. Sécurité des communications
14. Acquisition, développement et maintenance des systèmes d'information
15. Relations avec les fournisseurs
16. Gestion des incidents liés à la sécurité de l'information
17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
18. Conformité

Etapes et tâches de l'analyse de risque.

- Pour chaque scénario de risque évaluer le niveau de vraisemblance après application des mesures.
- Reformuler le scénario de risque.
- Mettre en évidence le risque résiduel.



Etapes et tâches de l'analyse de risque.

Risques résiduels	Gravité	Vraisemblance
<i>Risque lié à l'indisponibilité d'un devis au-delà de 72h</i>	2. Limitée	2. Significative
<i>Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h</i>	2. Limitée	2. Significative
<i>Risque lié à l'indisponibilité de visualisations au-delà de 72h</i>	2. Limitée	2. Significative
<i>Risque lié à la compromission de visualisations, jugées comme publiques</i>	1. Négligeable	4. Maximale
<i>Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h</i>	2. Limitée	2. Significative
<i>Risque lié à la compromission du contenu du site Internet public</i>	1. Négligeable	4. Maximale

Mettre en comparaison le risque initiale et le risque résiduel. Expliquer
La nature du risque résiduel.

Le risque résiduel sera « formellement » accepté
par l'entité détentrice du système.

Etapes et tâches de l'analyse de risque.

- Plan d'action :
 - Lister les rôles et affecter les responsabilités pour la mise en œuvre des mesures de sécurité.
 - Evaluer les moyens nécessaires (RH, finance...).
 - Définir à minima un jalon de début et un de fin. Pour les mesures complexes, définir des jalons intermédiaires.
 - Suivre l'avancement du plan d'action.
 - Communiquer vers les différents acteurs.



Plan général

- Introduction, présentation générale du cours.
- Objectifs de l'analyse de risque.
- Les différentes étapes et tâches de l'analyse de risque.
- **Les méthodes d'AR, focus sur EBIOS.**
- Mise en œuvre des outils et des savoir faire, projet.
- Restitution.
- Conclusion, fin du cours.



Les méthodes d'AR, focus sur EBIOS

- L'analyse du risque nécessite l'utilisation d'une méthode.
- Le choix de la méthode est très important :
 - Coût d'acquisition.
 - Type de processus.
 - Nature des risques couverts...
- Nécessite donc un focus sur les méthodes.



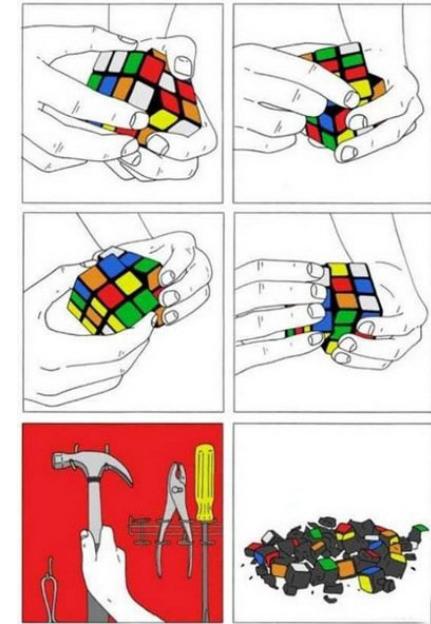
Les méthodes d'AR, focus sur EBIOS

- La réalisation d'une analyse de risque nécessite une l'emploi d'une méthode.
- Qu'est-ce qu'une méthode ?
 - Le mot **méthode** vient du grec ancien μέθοδος (methodos) qui signifie la poursuite ou la recherche d'une voie pour réaliser quelque chose. Le mot est formé à partir du préfixe μετά, μέθ- (meta, meth-) « après, qui suit » et de οδός (odos) « chemin, voie, moyen ».



Les méthodes d'AR, focus sur EBIOS

- Deux composantes majeures constituent une méthode :
 - Une démarche qui définit « le mode d'emploi » de la méthode.
 - Début, fin, périmètre, validation, cas particulier...
 - Des concepts d'appréhension ou une représentation du sujet cible du processus
 - Modèle, Abstraction...



Les méthodes d'AR, focus sur EBIOS

- Dans le cadre de l'analyse de risque l'ingénierie des méthodes est important pour :
 - Le choix d'une méthode parmi plusieurs.
 - La spécification d'une méthode.
 - La qualification d'une méthode.
 - Le choix d'un prestataire.
 - ...

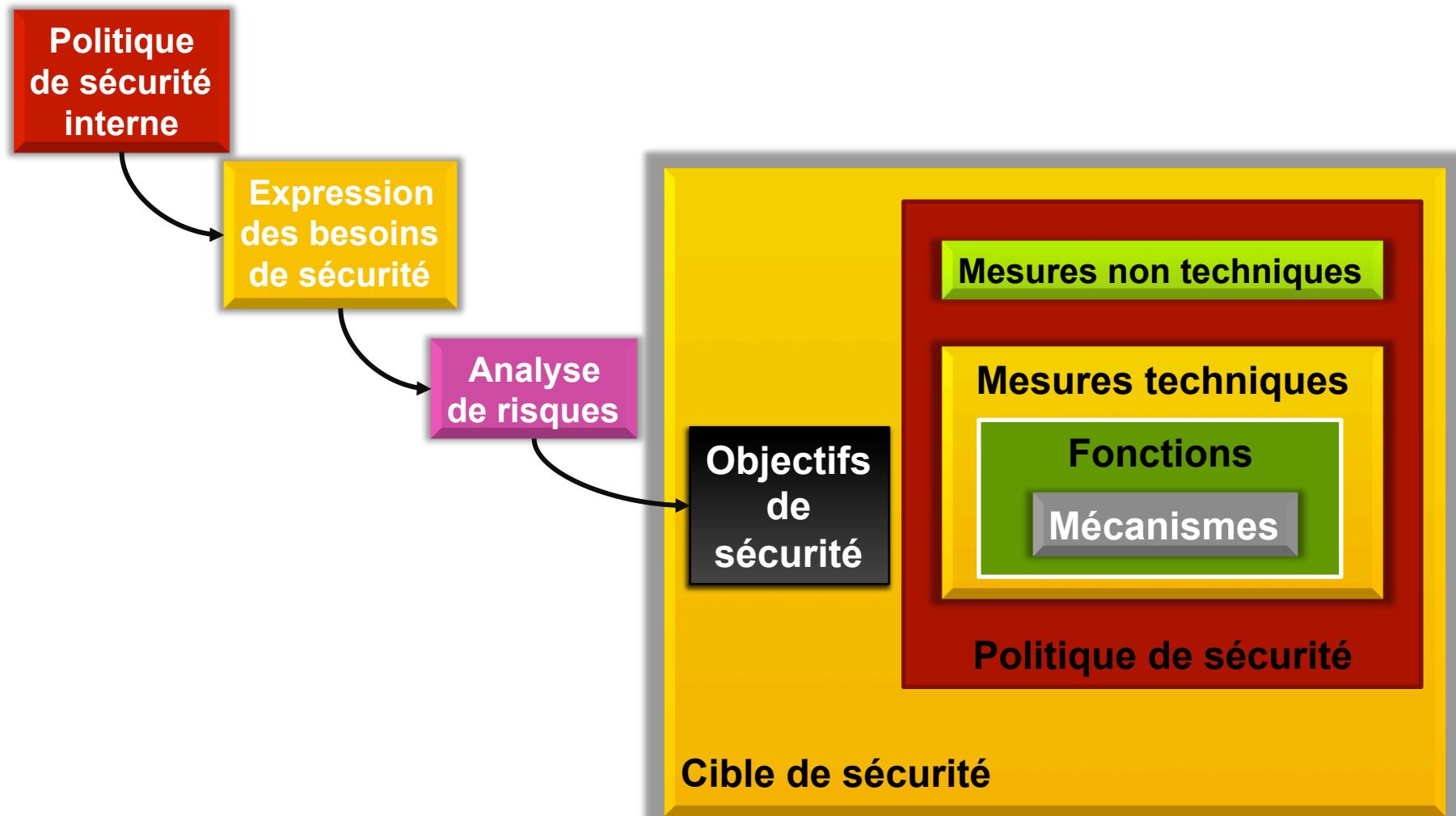


Les méthodes d'AR, focus sur EBIOS

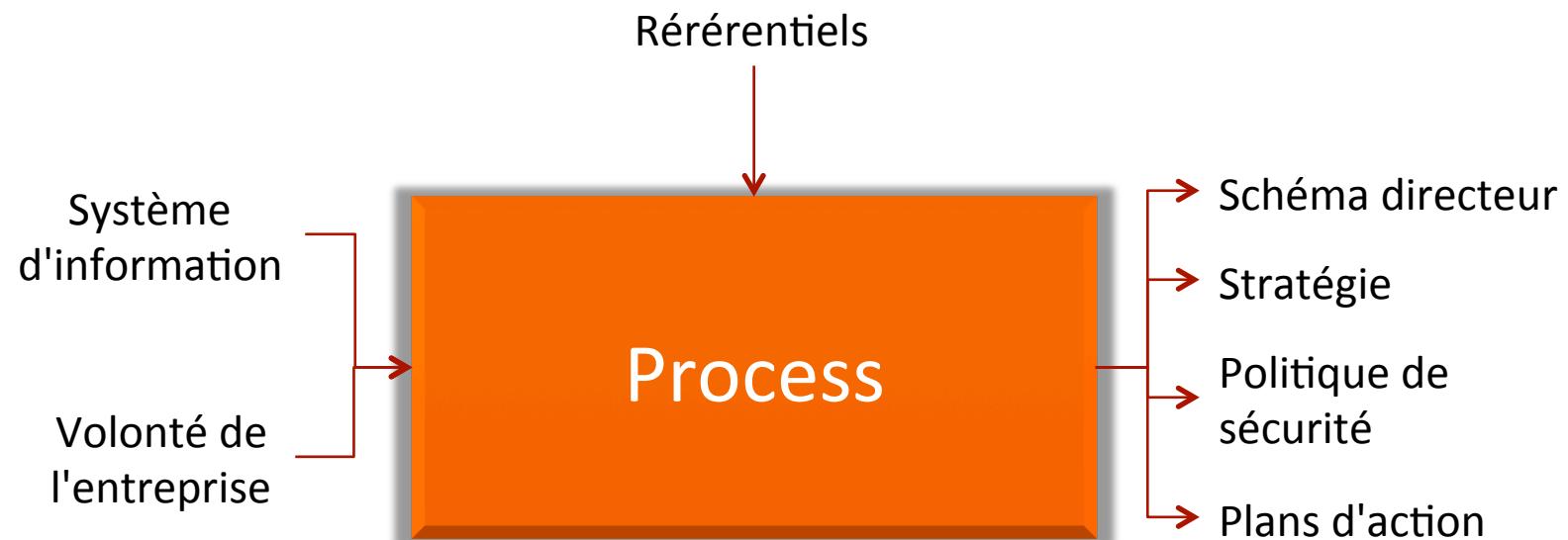
- **Pourquoi faire un FOCUS sur EBIOS ?**
 - Méthode "officielle" dans le domaine étatique.
 - Processus de maintien en condition actif.
 - Gratuité (à préciser !).
 - Outilage informatique (à préciser !).
 - Des stages de formation et de spécialisation.
 - Une expertise importante.
 - Méthode aboutie qui répond dans les grandes lignes aux exigences d'une méthode → référence.
 - Au programme les années précédentes.
 - ...
 - Compatible avec les normes ISO 13335 (GMITS), ISO 15408 (critères communs) et ISO 17799.



Les méthodes d'AR, focus sur EBIOS

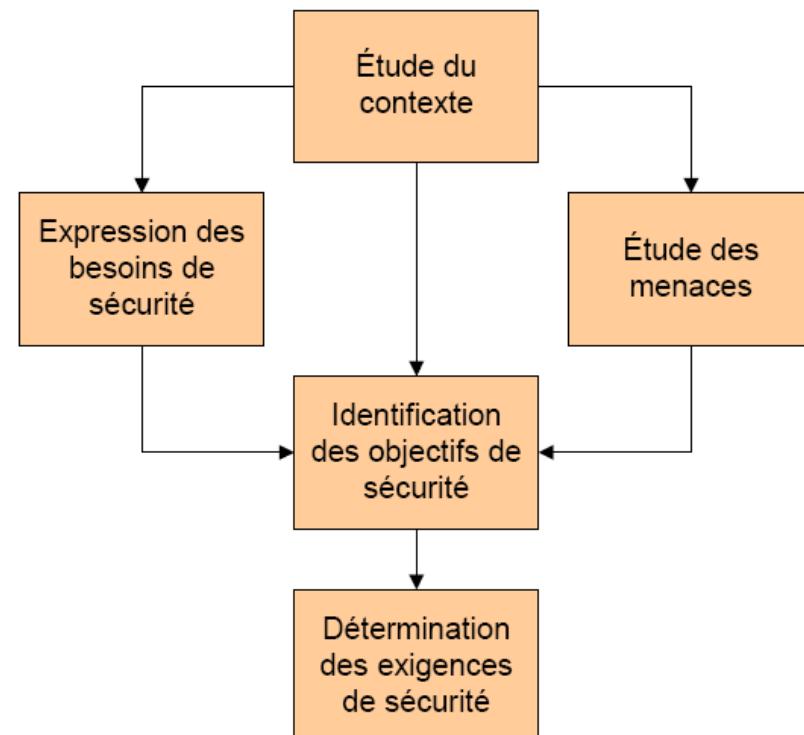


Les méthodes d'AR, focus sur EBIOS



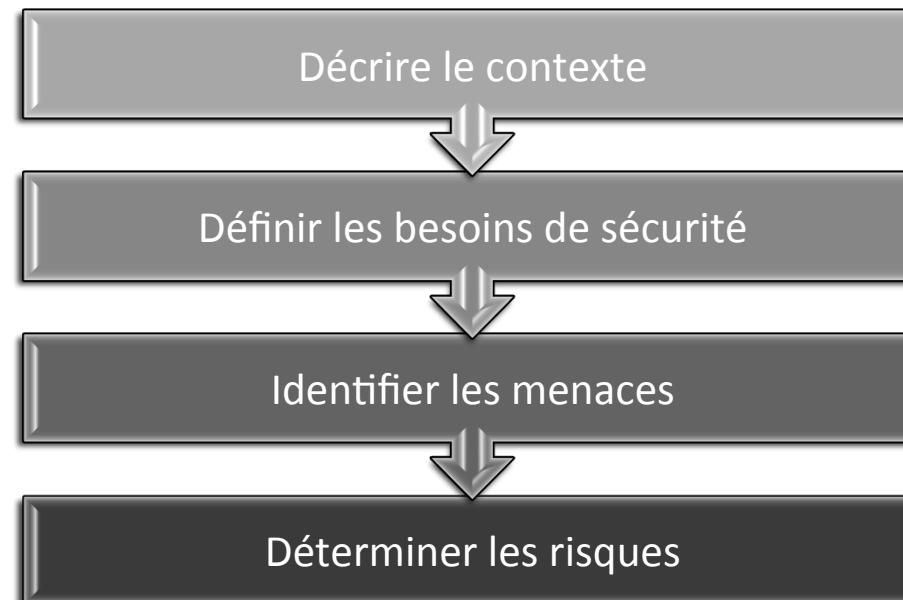
Les méthodes d'AR, focus sur EBIOS

- ↗ **Processus général :**
 - ↗ Etude du contexte
 - ↗ Expressions des besoins
 - ↗ Etude des menaces
 - ↗ Identification des besoins de sécurité
 - ↗ Détermination des exigences de sécurité



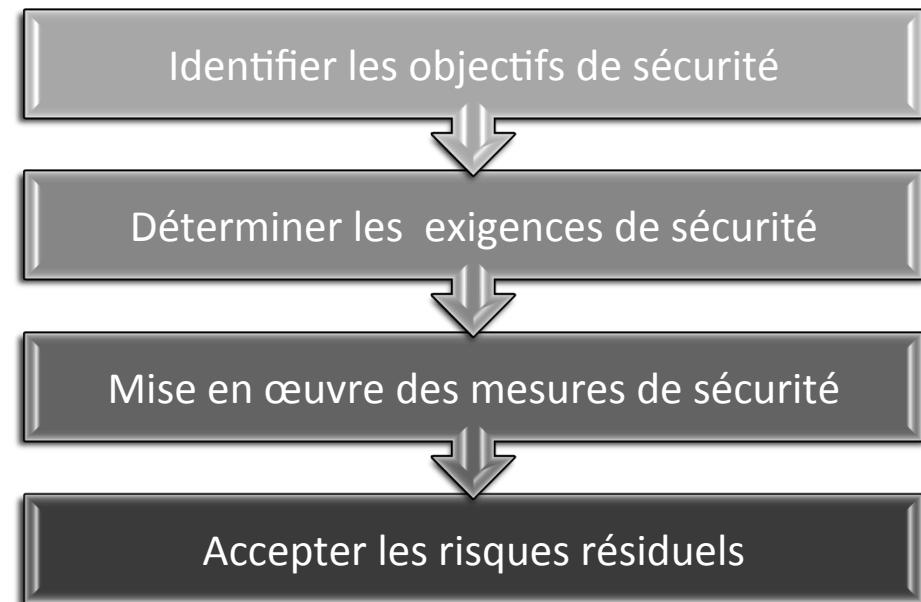
Les méthodes d'AR, focus sur EBIOS

- **Processus d'analyse :**
 - Composantes
 - Evaluation des risques

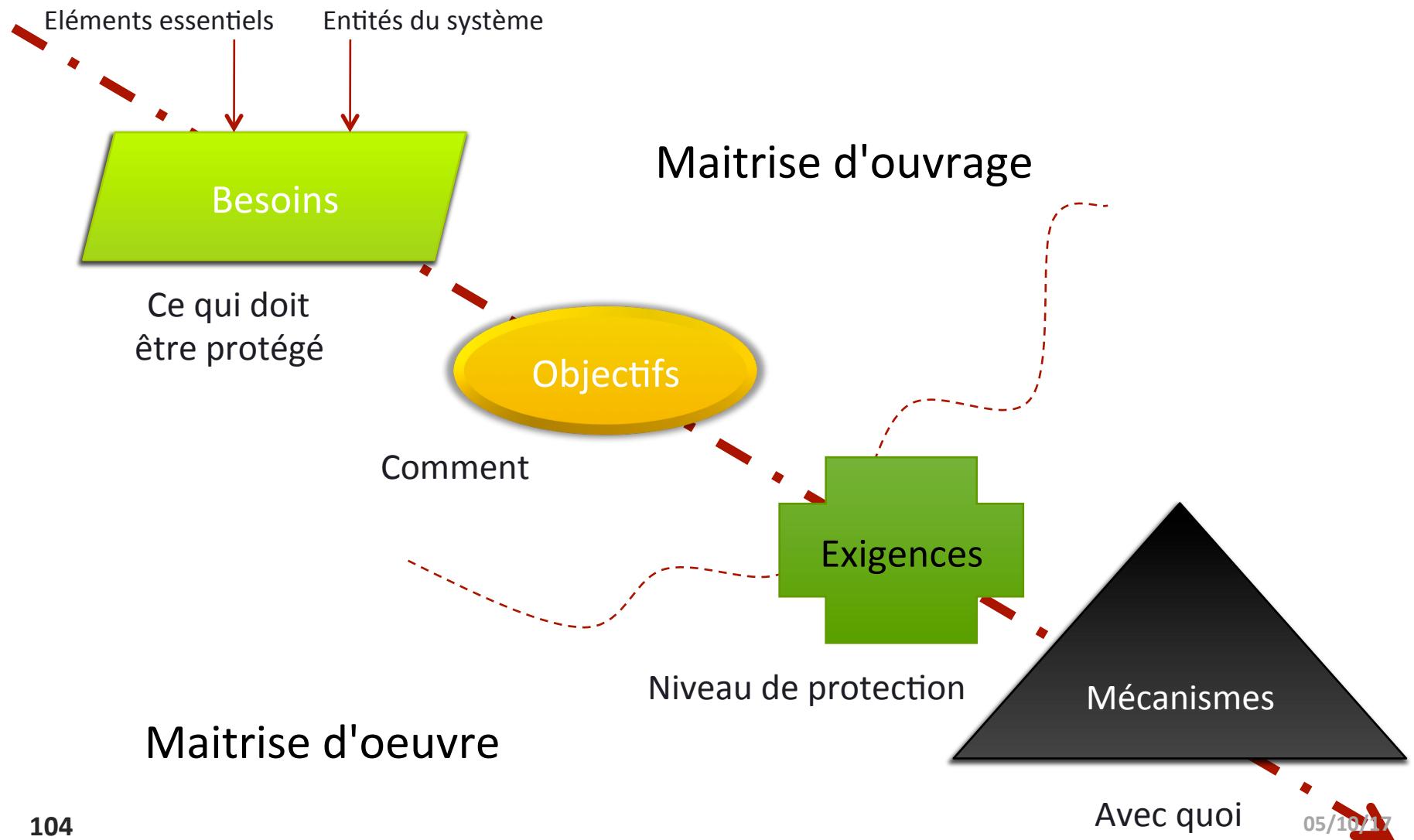


Les méthodes d'AR, focus sur EBIOS

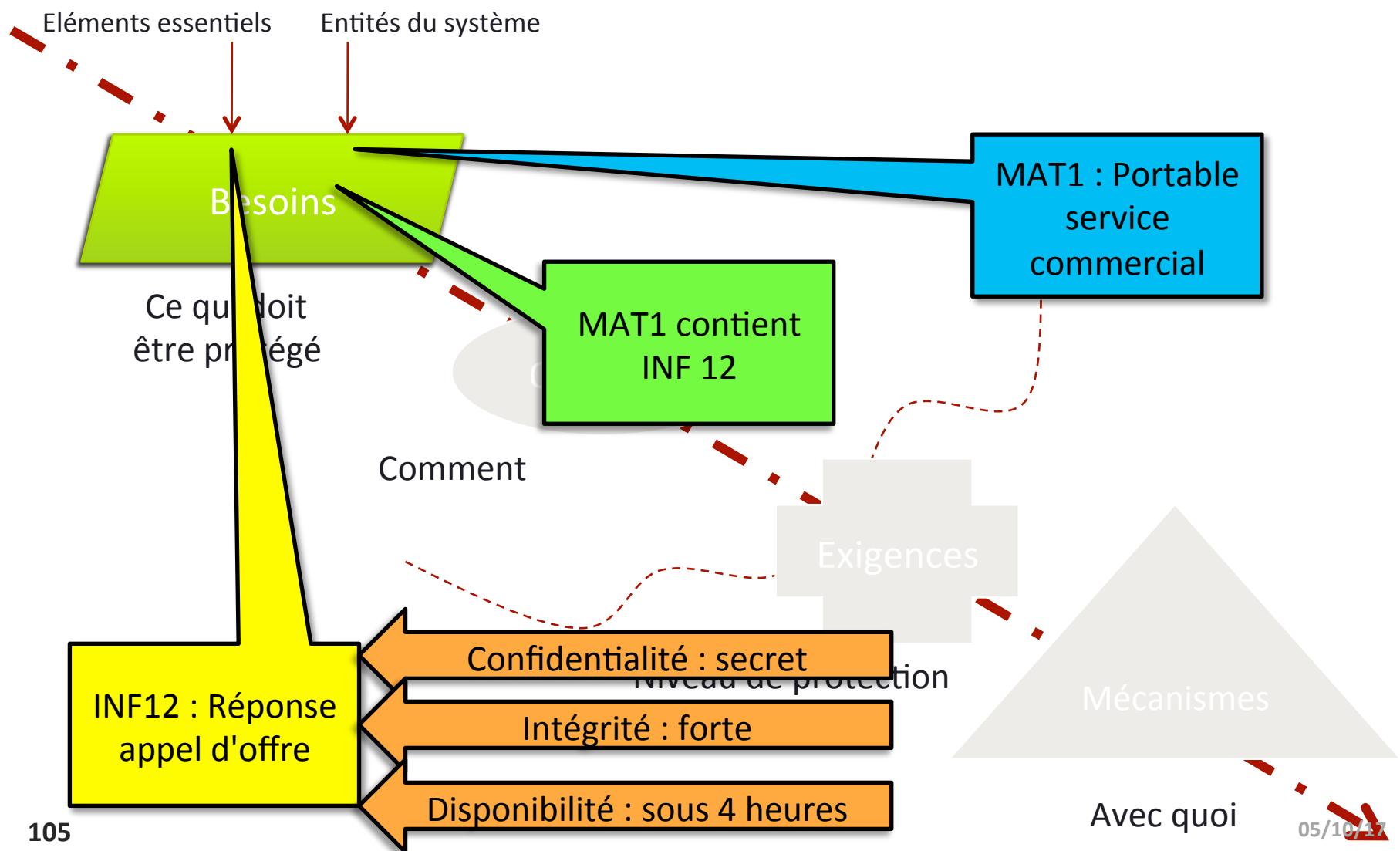
- ↗ Processus de sélection et mise en œuvre des mesures concernant le risque :
 - ↗ Refus
 - ↗ Optimisation
 - ↗ Transfert
 - ↗ Acceptation



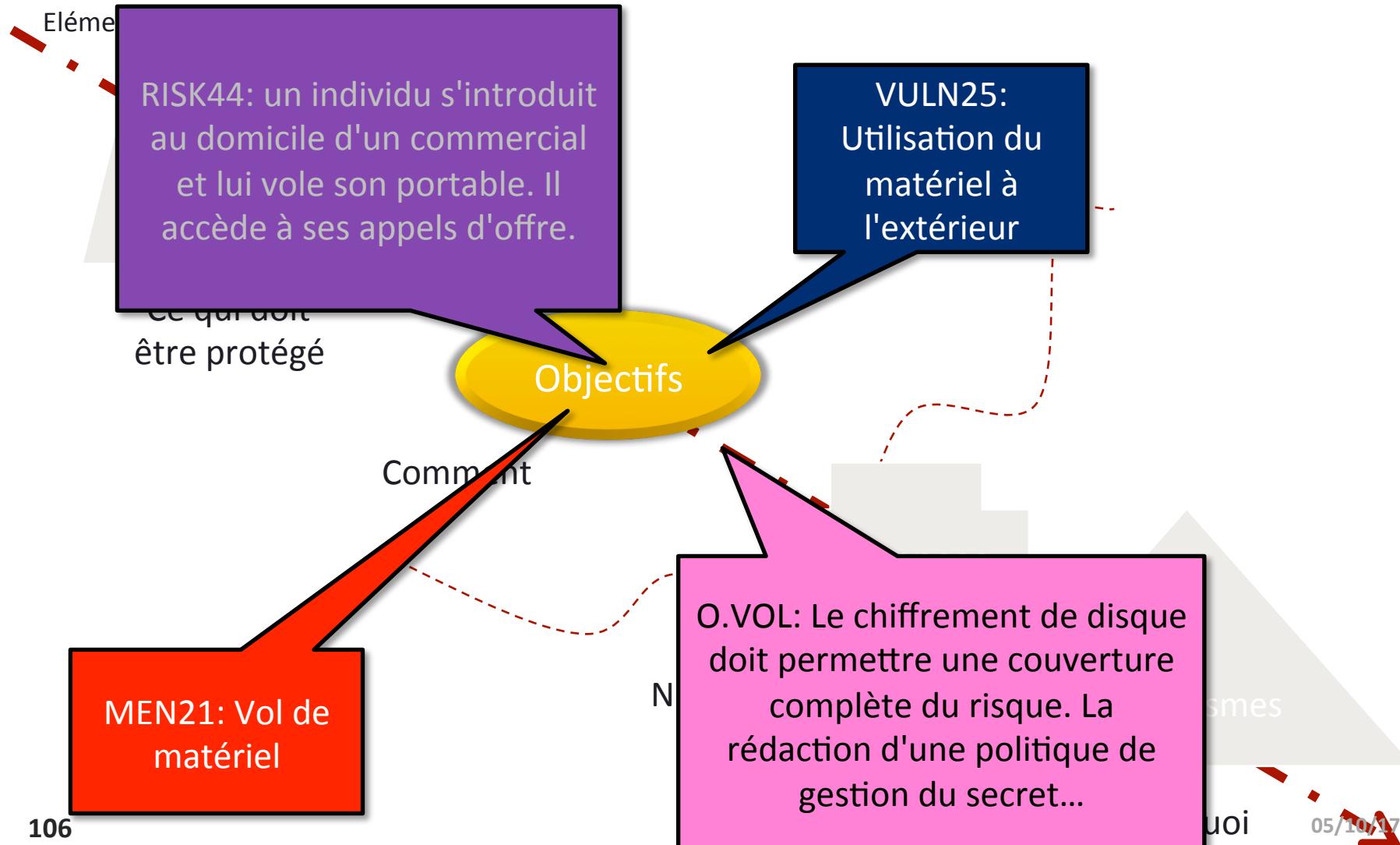
Les méthodes d'AR, focus sur EBIOS



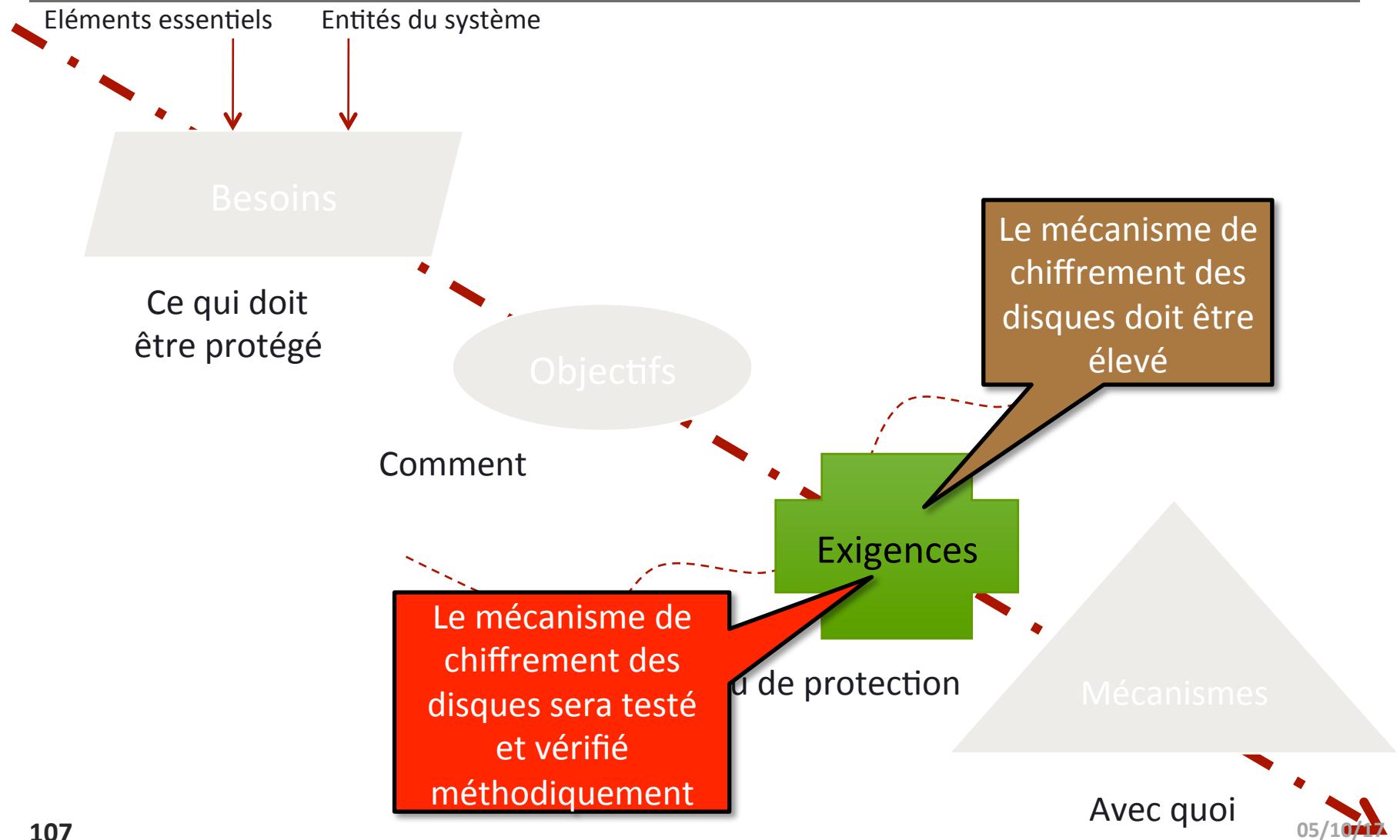
Les méthodes d'AR, focus sur EBIOS



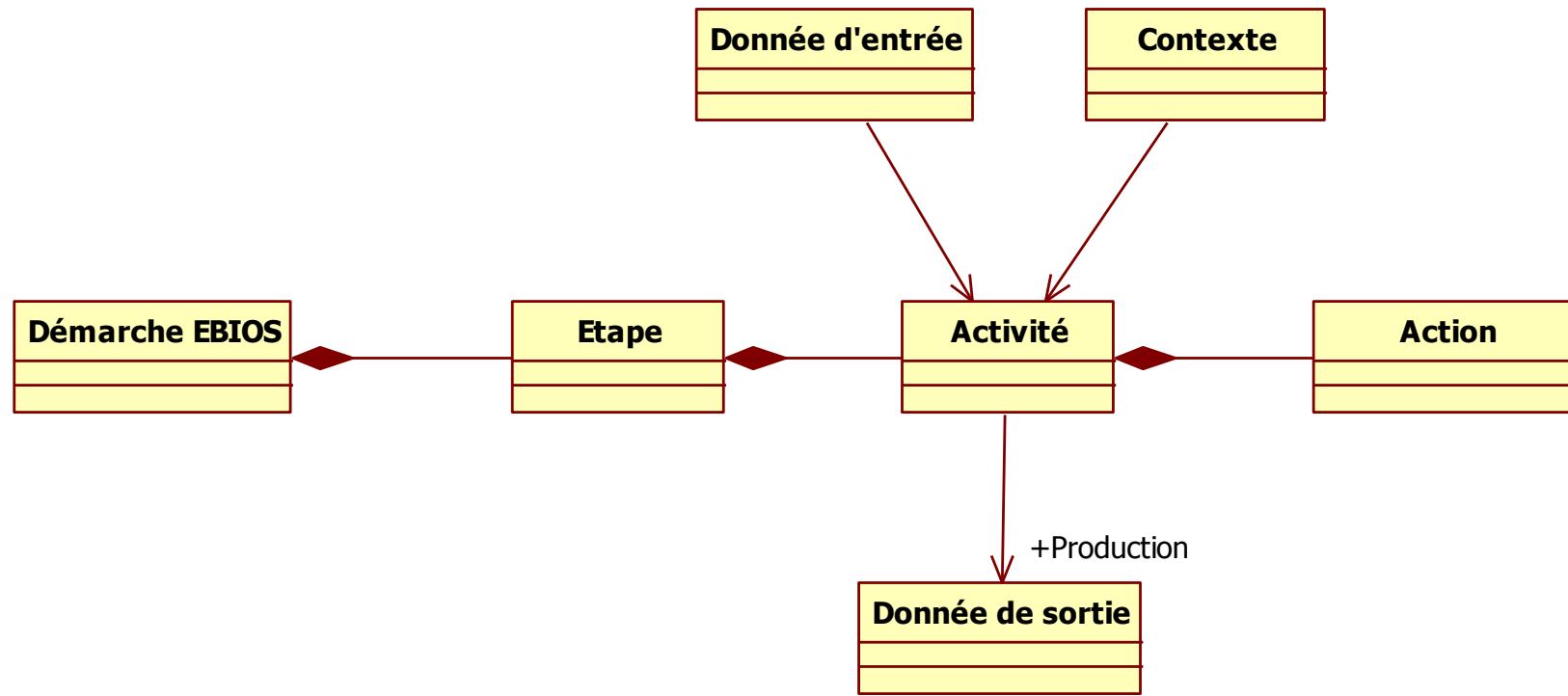
Les méthodes d'AR, focus sur EBIOS



Les méthodes d'AR, focus sur EBIOS

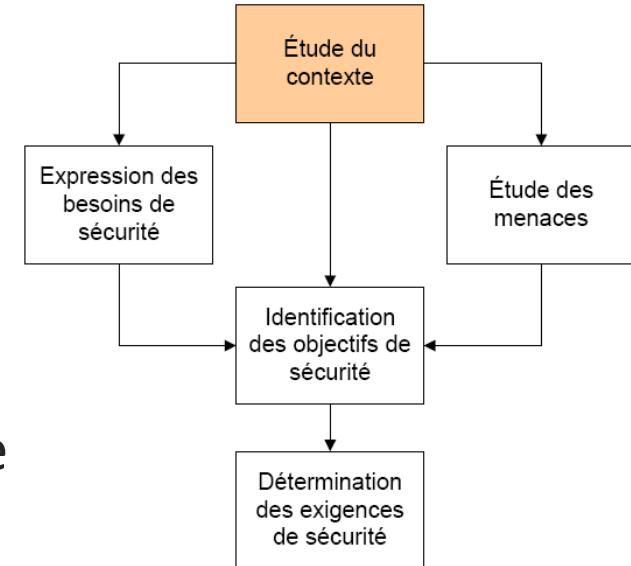


Les méthodes d'AR, focus sur EBIOS

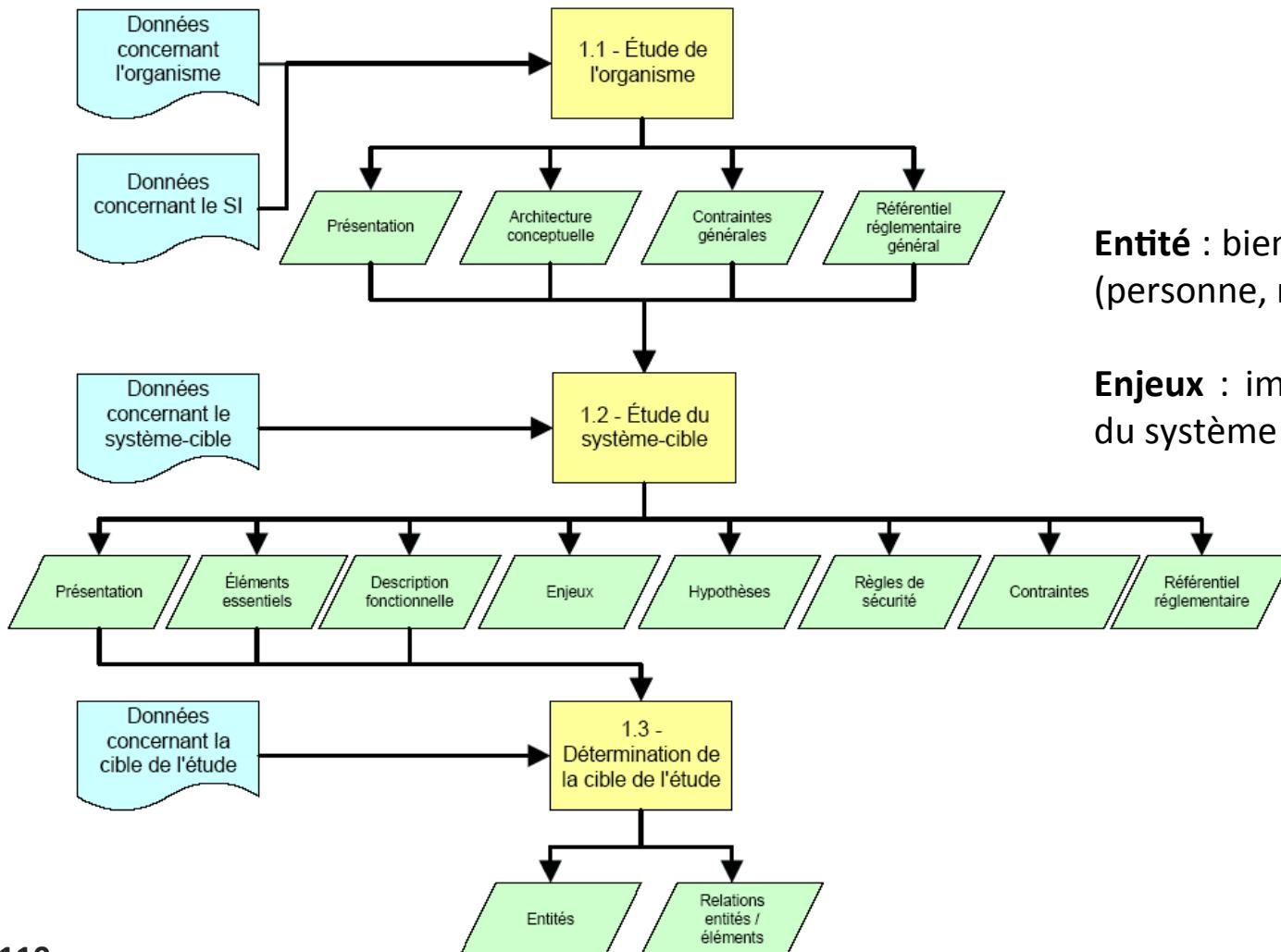


Les méthodes d'AR, focus sur EBIOS

- **Les différentes étapes de la méthode :**
 - E1 : Etude du contexte.
 - E2 : Expression des besoins de sécurité.
 - E3 : Etudes des menaces.
 - E4 : Identification des objectifs de sécurité.
 - E5 : Détermination des exigences de sécurité.

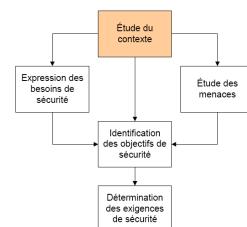


Les méthodes d'AR, focus sur EBIOS



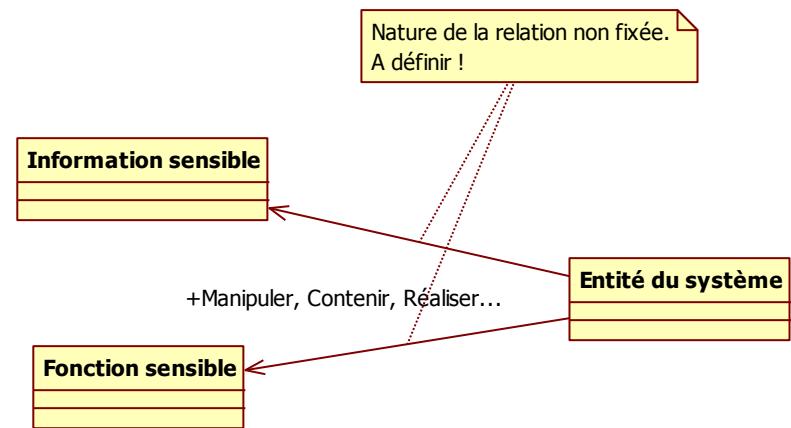
Entité : bien de différente nature (personne, matériel...)

Enjeux : importance stratégique du système dans l'entreprise



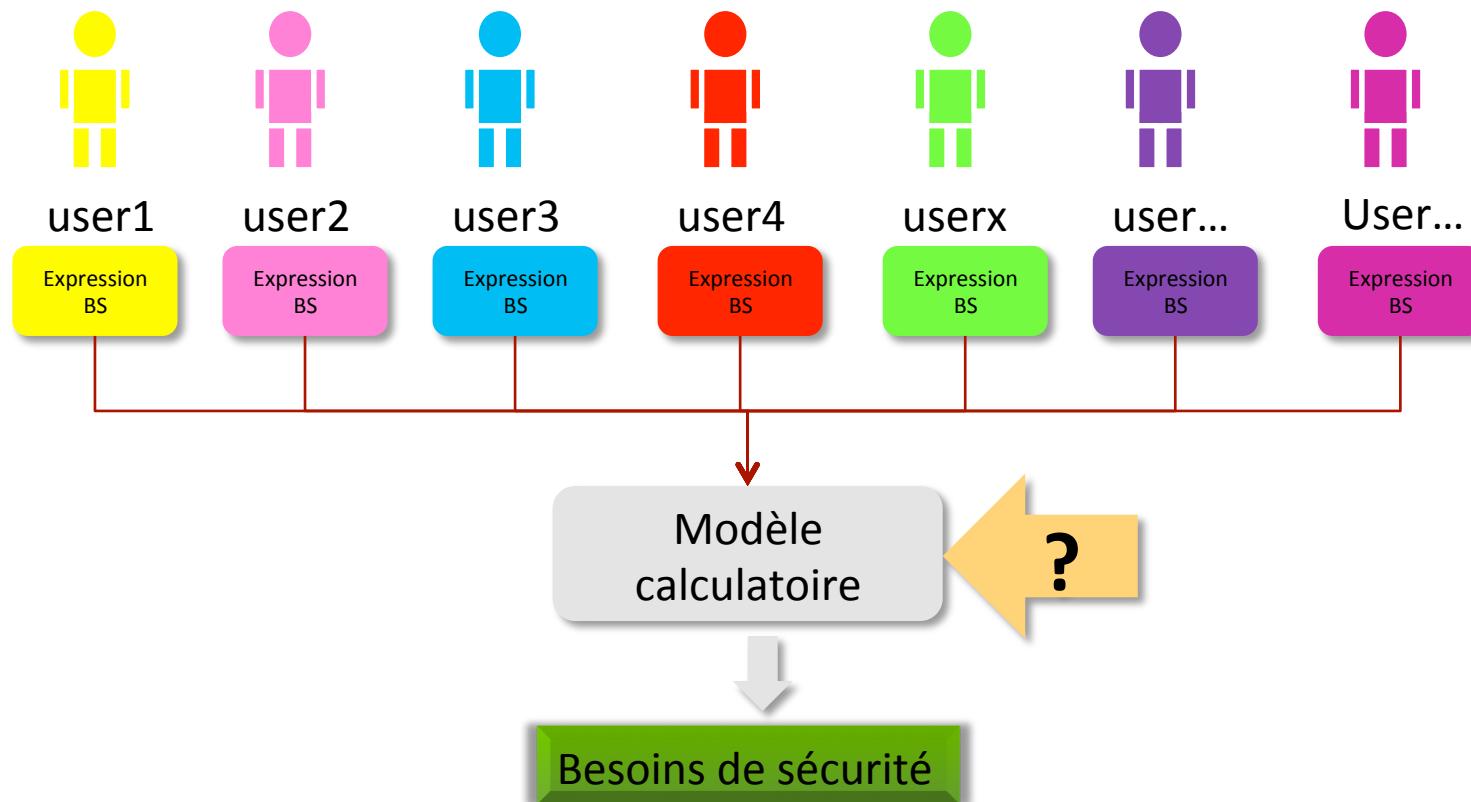
Les méthodes d'AR, focus sur EBIOS

- **Etape 1 : Retour d'expérience.**
 - Ne pas oublier de définir l'objectif précis de l'analyse.
 - Qu'est-ce qui doit être produit, pourquoi...
 - Formaliser l'objectif et les conditions → mandat de l'analyse.
 - E1 A1.2 → Etape lourde et cruciale.
 - Eléments intermédiaires à prendre en compte (ce qui est nécessaire à un attaquant pour atteindre son objectif) !
 - MODELE CALCULATOIRE ?!....
 - Attention aux relations «héritée » ! A supprimer...

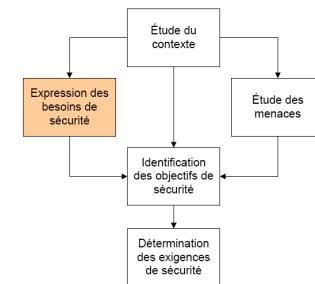
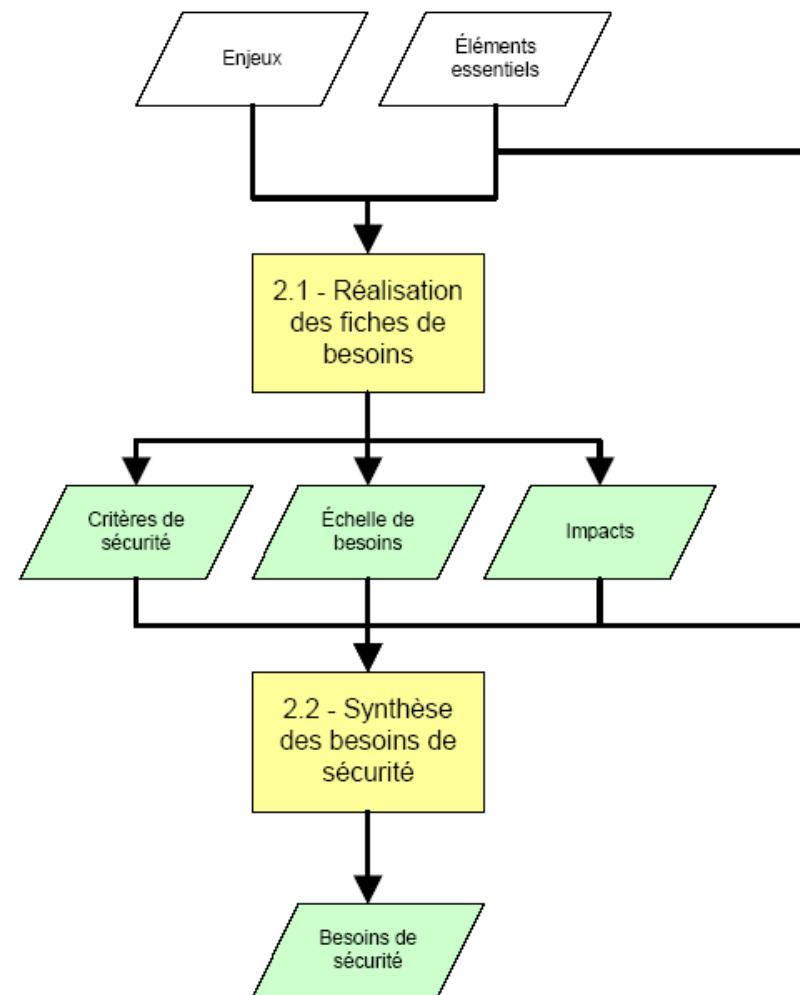


Les méthodes d'AR, focus sur EBIOS

- Modèle calculatoire ... ! ... ? Exemple



Les méthodes d'AR, focus sur EBIOS



ETAPE 2 : Expression du besoin de sécurité.

Besoin de sécurité : Expression de l'intention des MENACES ou des RISQUES et/ou satisfaire à des politiques de sécurité et à des hypothèses.

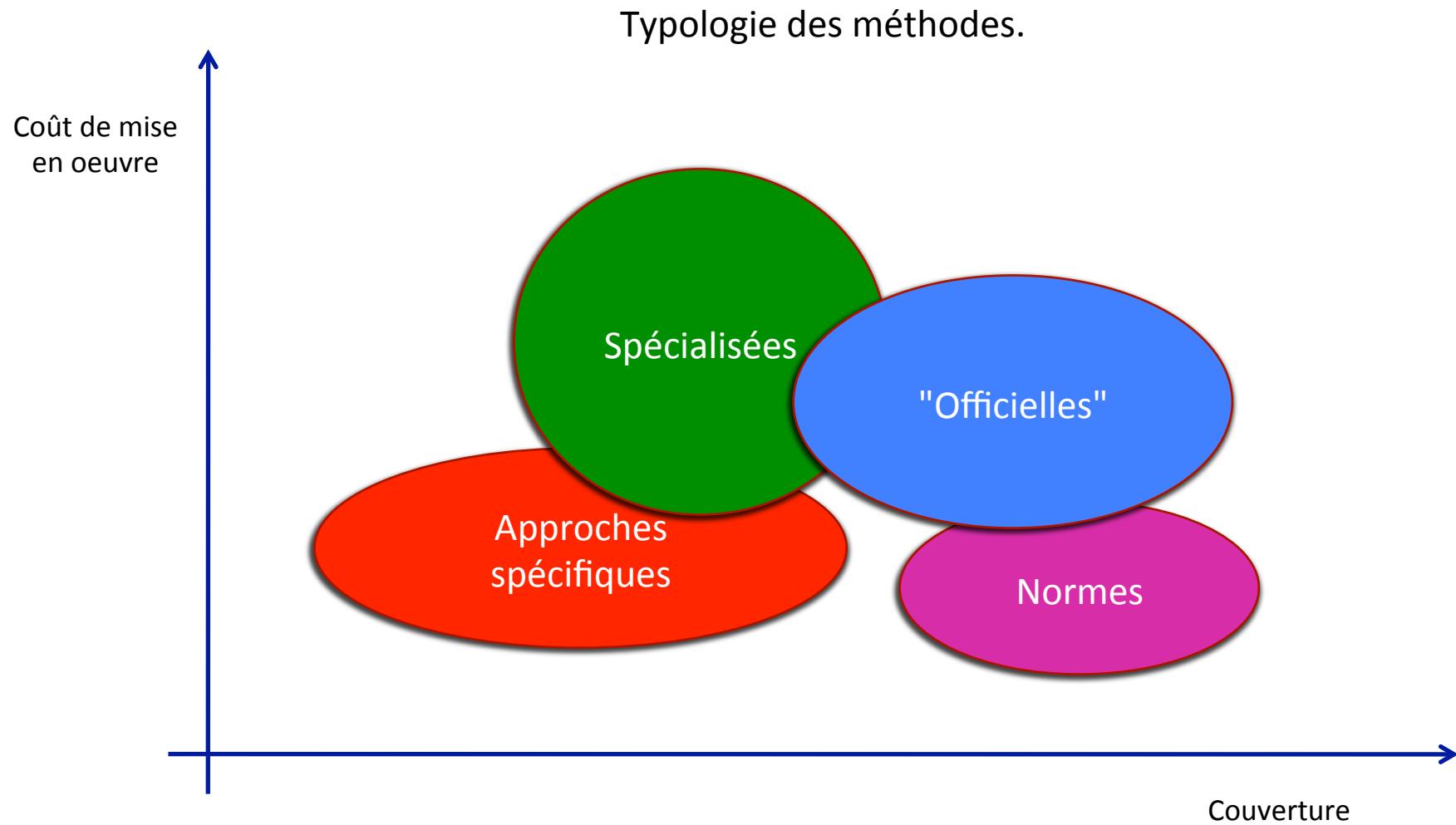
Les méthodes d'AR, focus sur EBIOS

- **Retour d'expérience :**
 - Modèle calculatoire pour la synthèse ?
 - Attention aux échelles qualitatives (très grave, pas grave...) !
 - Attention à l'intégrité !
 - Impact, même problème que pour les besoins de sécurité.



Vu sur Funimages.free.fr

Les méthodes d'AR, focus sur EBIOS



Les méthodes d'AR, focus sur EBIOS

↗ Approches spécifiques

↗ Détails :

- ↗ Sous ensemble du processus générique (exemple : analyse de vulnérabilité).

↗ Avantage :

- ↗ Mise en œuvre simple.
- ↗ Coût réduit.
- ↗ Rapidité de mise en œuvre.

↗ Inconvénients :

- ↗ Incomplète.
- ↗ Peu robuste.
- ↗ Pérénité, suivi.



Les méthodes d'AR, focus sur EBIOS

↗ Spécialisée

↗ Détails :

- ↗ Analyse de certains types de risques.

↗ Avantage :

- ↗ Mise en œuvre simple.
- ↗ Coût réduit.
- ↗ Rapidité de mise en œuvre.

↗ Inconvénients :

- ↗ Partielle.
- ↗ Mise en oeuvre.
- ↗ .

Les méthodes d'AR, focus sur EBIOS

↗ Norme

↗ Détails :

- ↗ Analyse des risques suivant un processus formalisé et un référentiel imposé.

↗ Avantage :

- ↗ Facilité d'application.
- ↗ Référentiel.
- ↗ Choix facilité.
- ↗ Reconnaissance "internationale".

↗ Inconvénients :

- ↗ Application rigide.
- ↗ Lourdeur de réalisation et d'évolution.
- ↗ Sans souplesse.
- ↗ Confiance à priori.

Les méthodes d'AR, focus sur EBIOS

↗ "Officielle"

↗ Détails :

- ↗ Processus d'analyse très cadre pour des systèmes d'information "à forte valeur ajoutée".

↗ Avantage :

- ↗ Coût de développement supporté par des organisations importantes.
- ↗ Forte expertise.
- ↗ Périmètre des référentiels.
- ↗ Hauteur de vue.

↗ Inconvénients :

- ↗ Aucune prise sur le processus de développement.
- ↗ "Outil" d'expert.
- ↗ Confiance à priori trop importante.
- ↗ Spécialisation difficile.

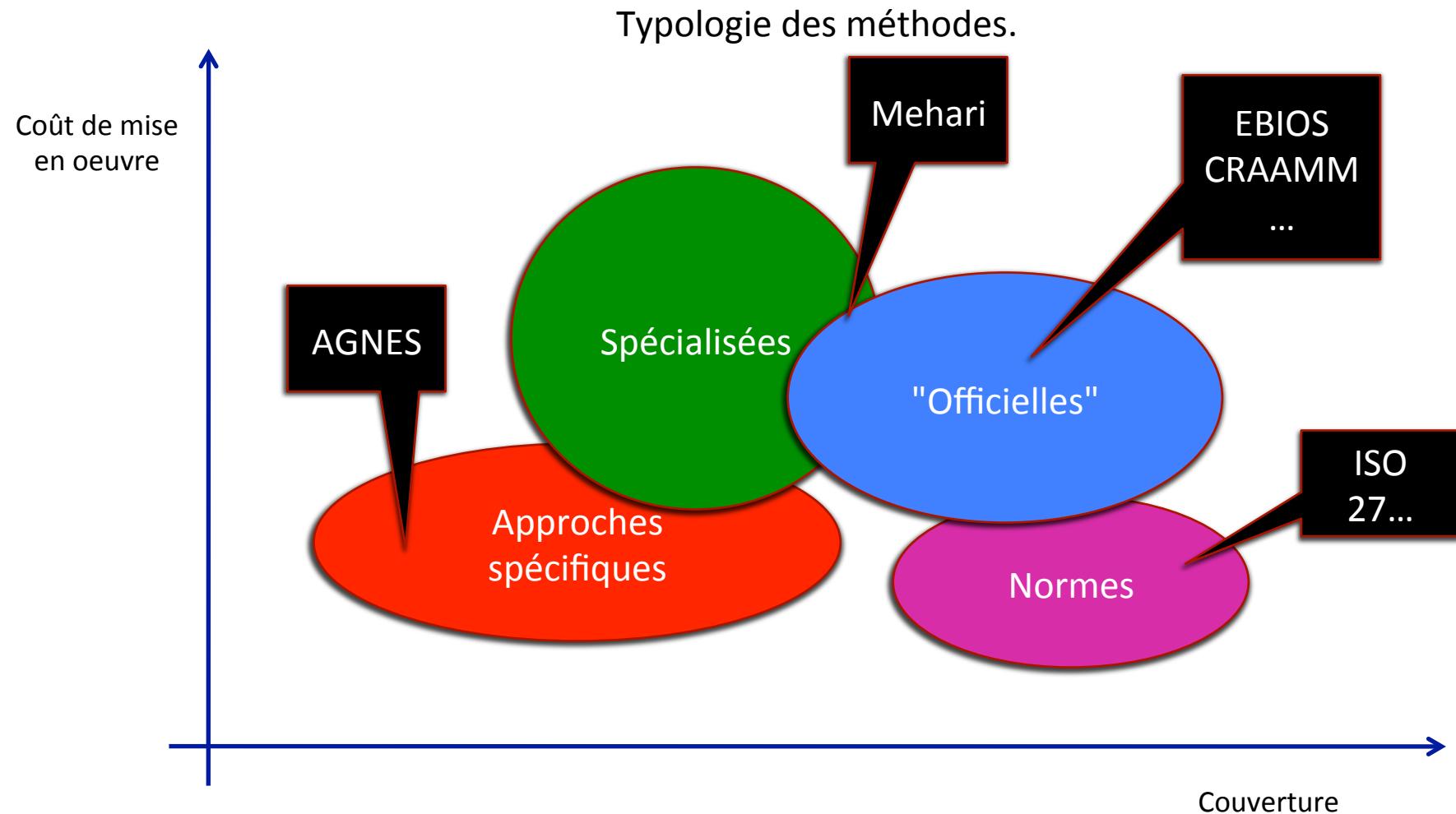
Les méthodes d'AR, focus sur EBIOS



⁽¹⁾ Origine Cogisys, Euriware.

Méthode	Auteur	Détail
EBIOS	ANSSI (SGDNS)	
Melissa	DGA	MC terminé
MARION	CLUSIF	Remplacée par Mehari
Mehari	CLUSIF	
Octave	Université Carnegie Mellon	
ITBPM	BSI (équivalent DCSSI en Allemagne)	
CRAMM	Siemens (MOU) UK (MOA)	
BS 7799	--	
ISO 17799	--	
ISO	--	
TRA-1 EMR	Gouvernement canadien	
AGNES	AREVA	
SCORE	Ageris Consulting	
CALLIO	Callio technologie	

Les méthodes d'AR, focus sur EBIOS



Les méthodes d'AR, focus sur EBIOS

- **Retour d'expérience.**
- **Réflexion autour de la sous traitance de l'analyse de risque :**
- Charge interne / capacité à mettre en oeuvre
- Portée des résultats (interne – externe).
- Objectivité / subjectivité PDV interne / externe
- Critères de choix de la sous traitance (ex : sous traitance autres services)
- Sensibilité des informations concernées (vulnérabilités, K société...)
- Responsabilités / résultats



Les méthodes d'AR, focus sur EBIOS

Retour d'expérience

- Référentiel
 - Vulnérabilité de bas niveau.
 - Menace macroscopique.
 - Paradoxe du référentiel



Les méthodes d'AR, focus sur EBIOS

Retour d'expérience

- **Problèmes constatés lors de la conduite d'une analyse de risque.**
- Refus de participation.
- Orientation du PDV par commanditaire.
- Découverte *in situ* de preuves d'attaque (exemple organisationnel et exemple technique).
- Découverte de données / obligation déclaration autorité police ou judiciaire.
- Pugilat à la présentation des résultats (2).
- Mise en cause de l'équipe d'audit :
 - Capacité – compétence.
 - Incidents techniques.
 - PDV évolutifs...



Les méthodes d'AR, focus sur EBIOS

- ↗ Retour d'expérience.
- ↗ Les limites de l'analyse de risque.
- ↗ <http://magazine.qualys.fr/conformite-organisation/gestion-risque-limites/>
- ↗ <http://magazine.qualys.fr/conformite-organisation/analyse-risque-defauts/>

Les limites de la gestion du risque

👤 Jerome Salz le 31 mars 2011 - 11:51, dans la rubrique Conformité & Bonnes pratiques

💬 2 commentaires, rejoignez la discussion !

🏷️ ebios · gestion des risques · iso 27005 · petit-déjeuner securityvibes · risk management



a gestion du risque est-elle vraiment une science exacte ? C'est la question posée à l'occasion de notre dernier petit-déjeuner SecurityVibes en date. Selon Gilles Afchain, responsable de la sécurité de l'information chez Areva, gérer le risque c'est surtout connaître les limites de l'exercice. Selon lui, chaque variable de la formule de calcul du risque (probabilité et gravité) se base sur des valeurs souvent avancées arbitrairement. « *L'occurrence et l'impact sont estimées à dire d'experts* », précise Gilles Afchain. Et

Plan

- Introduction, présentation générale du cours.
- Objectifs de l'analyse de risque.
- Les différentes étapes et tâches de l'analyse de risque.
- Les méthodes d'AR, focus sur EBIOS.
- **Mise en œuvre des outils et des savoir faire, projet.**
- Restitution.
- Conclusion, fin du cours.



Bureau d'étude

- Sujet COMEXIS

Bureau d'étude

- par groupes.
- Travaux libres avec séances de regroupement.
- Point de situation informel par groupe.
- Réorientation si nécessaire.
- Contact avec EB par messagerie :
eric.bornette@laposte.net

Bureau d'étude

↗ 2 DO

Plan

- Introduction, présentation générale du cours.
- Objectifs de l'analyse de risque.
- Les différentes étapes et tâches de l'analyse de risque.
- Les méthodes d'AR, focus sur EBIOS.
- Mise en œuvre des outils et des savoir faire, projet.
- **Restitution.**
- Conclusion, fin du cours.

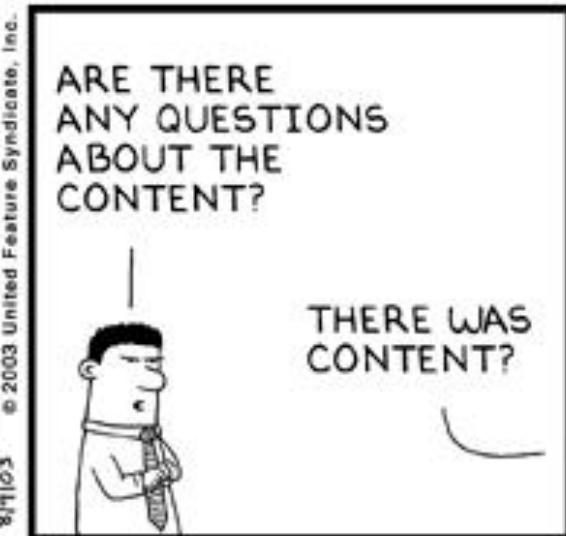
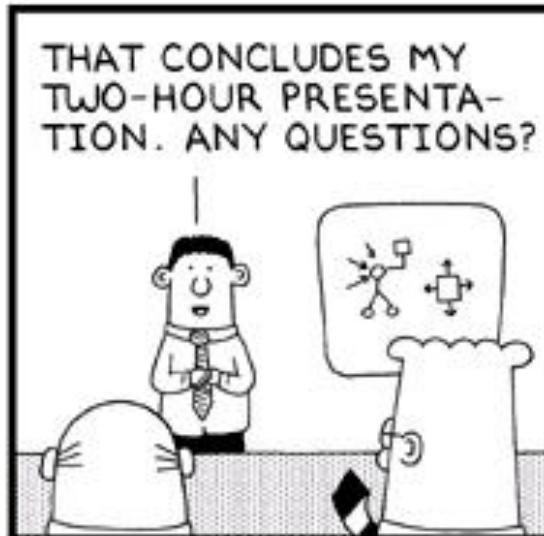


Plan

- Introduction, présentation générale du cours.
- Objectifs de l'analyse de risque.
- Les différentes étapes et tâches de l'analyse de risque.
- Les méthodes d'AR, focus sur EBIOS.
- Mise en œuvre des outils et des savoir faire, projet.
- Restitution.
- Conclusion, fin du cours.



Conclusion



© 2003 United Feature Syndicate, Inc.