

Technologies de l'information

Cours:

**Sécurité des systèmes
informatiques**

Séance # 2

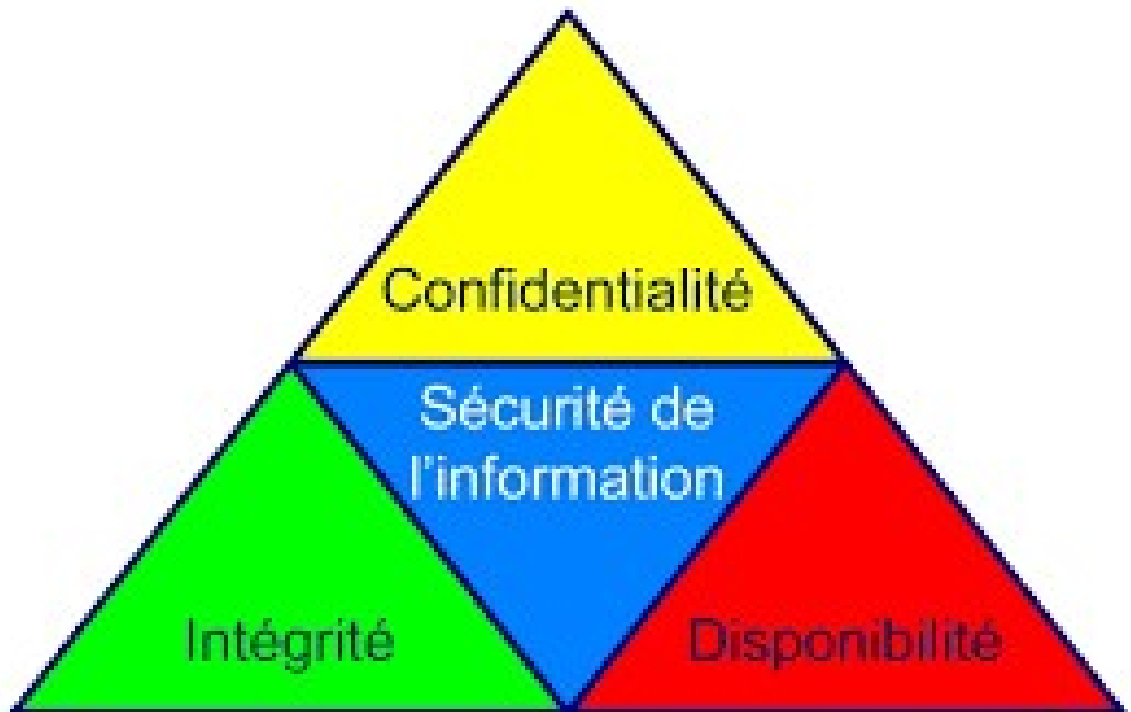
Préparé par: Blaise Arbouet



DESS

Sécurité de l'information

- Quoi protéger?
- Les **propriétés** de l'information notamment :
 - Sa disponibilité ;
 - Son intégrité ;
 - Sa confidentialité.



Sécurité de l'information

- Disponibilité :

- Rendre l'information accessible et utilisable sur demande par une entité autorisée lorsque nécessaire.

Disponibilité de
l'information

- Intégrité :

- Sauvegarder la cohérence, l'exactitude et l'exhaustivité de l'information.

Intégrité de l'information

- Confidentialité :

- S'assurer que l'information n'est pas mise à la disposition ou divulguée à des personnes, des entités ou des processus non autorisés.

Confidentialité de
l'information

Autres définitions

GESTION DE RISQUE: le processus qui permet d'identifier et d'évaluer les risques en vue d'élaborer un plan visant à minimiser et à maîtriser ces risques et leurs conséquences potentielles pour une entreprise.

ACTIF: Ce qui est important pour l'organisation

MENACE: Quelque chose qu'on doit craindre

VULNÉRABILITÉ: Une faille ou une faiblesse d'un actif

RISQUE: La vraisemblance qu'une menace exploite une vulnérabilité afin d'impacter un actif.

Enjeux de confidentialité

- Espionnage
- Fouille dans les poubelles
- Ecoute clandestine
- Ecoute telefonique
- Ingenierie sociale
- Etc...



Credit: Sharvari Kale

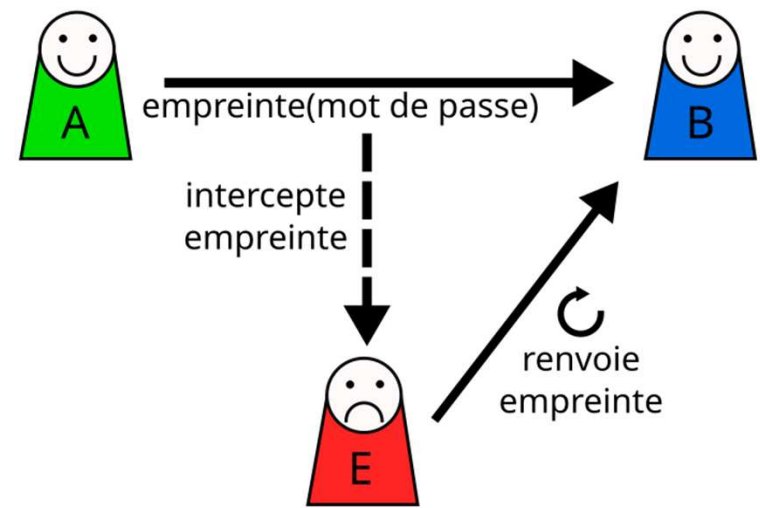
Cas concret: Violation de données chez LastPass

En 2022, LastPass, un gestionnaire de mots de passe populaire, a subi une importante violation de données. Des attaquants ont accédé aux données sensibles de ses clients, notamment à des coffres-forts de mots de passe chiffrés. Cette violation a exposé le risque d'accès non autorisé aux informations personnelles et confidentielles, soulignant l'importance de mesures de sécurité robustes pour protéger les données sensibles.



Enjeux d'intégrité

- Modification non autorisée
- Usurpation d'identité
- Attaque de l'homme du milieu (man-in-the-middle)
- Attaque par rejeu (replay attack)
- Etc..



Cas concret: Cyberattaque Planeta

En janvier 2024, le Centre russe d'hydrométéorologie spatiale, connu sous le nom de Planeta, a été attaqué par des pirates informatiques pro-ukrainiens identifiés comme la « BO Team ». Ils ont supprimé 2 pétaoctets de données critiques, impactant les secteurs militaires, de l'aviation civile et de l'agriculture. Cette attaque a perturbé les opérations de plus de 50 organismes publics, dont le ministère russe de la Défense, mettant en évidence les graves conséquences d'une atteinte à l'intégrité des données dans les infrastructures critiques. La suppression d'une telle quantité de données critiques a compromis la **fiabilité** et **l'exactitude** des informations dans de nombreux secteurs.



Enjeux de disponibilité

- Déni de service (DoS)
- Panne de courant
- Panne matérielle
- Panne de service
- Destruction



Cas concret: Panne Microsoft due à Crowdstrike

Le 19 juillet 2024, un problème avec le logiciel de sécurité des terminaux de CrowdStrike a provoqué des pannes système généralisées avec l'erreur

« DRIVER_OVERRAN_STACK_BUFFER », affectant les systèmes Windows. La panne a impacté des services majeurs, notamment des banques, des compagnies aériennes et des services Microsoft, les rendant indisponibles pendant une longue période.



wooclap

Quizz de pratique sur
le triangle CID



Génération de groupe

<https://www.classtools.net/random-group-generator/>



« Menace »

«Quelque chose que l'on doit craindre. Incident ou sinistre qui peut affecter les actifs. Évènement redouté.»*

Plusieurs **sources** de menaces :

- Source **humaine** agissant délibérément (attaque, fraude, sabotage, vol)
- Source humaine accidentelle (erreur, omission)
- Source **naturelle** (inondation, feu, panne d'électricité)
- Source **environnementale** (conflit social, pandémie)

Quid de la cybermenace?

Une **cybermenace** est une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient, ou à perturber le monde numérique en général.



ENISA Threat Landscape 2024







Exemples de menaces

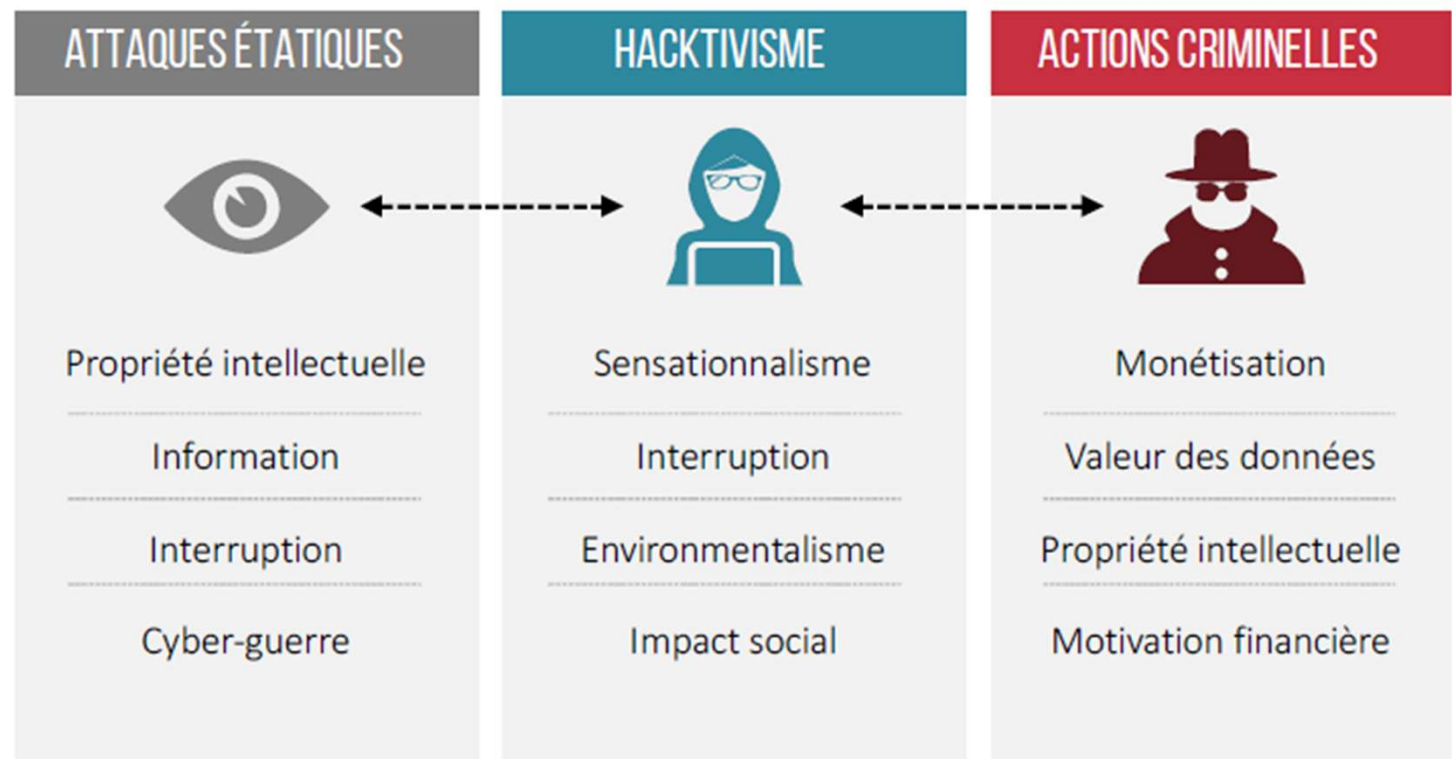
TYPE DE MENACES	EXEMPLES	
DOMMAGE PHYSIQUE	Pollution	Accident majeur
	Dégât des eaux	Incendie
CATASTROPHES NATURELLES	Phénomène climatique	Phénomène volcanique
	Phénomènes sismique	Phénomène météorologique
PERTE DE SERVICES ESSENTIELS	Panne d'électricité	Panne de la climatisation
	Panne du matériel de télécommunications	Perte d'alimentation en eau
PERTURBATION DUE À DES RAYONNEMENTS	Rayonnements électromagnétiques	Impulsions électromagnétiques
	Rayonnements thermiques	
COMPROMISSION D'INFORMATION	Divulgaration	Espionnage à distance
	Piégeage de logiciel	Géolocalisation
DÉFAILLANCES TECHNIQUES	Panne de matériel	Dysfonctionnement du matériel
	Saturation du système d'information	Dysfonctionnement du logiciel
ACTIONS NON AUTORISÉES	Corruption de données	Traitement illégal de données
	Reproduction frauduleuse de logiciel	Utilisation de contrefaçons
COMPROMISSION DES FONCTIONS	Erreur d'utilisation	Usurpation de droits
	Abus de droits	Reniement d'actions

Source: ISO 27005, Annexe C

Agents de menaces

PIRATE INFORMATIQUE	ESCROC INFORMATIQUE	ESPIONNAGE INDUSTRIEL	INITIÉS
			
Isolé	Isolé	Renseignement	Employés peu qualifiés,
Groupe	Groupe	Entreprises	mécontents,
APT	Mafia organisée	Gouvernements étrangers	malveillants,
		Intérêts d'autres gouvernements	négligents,
			malhonnêtes
			Ex-employés

Motivations & moyens des menaces intentionnelles



« Vulnérabilité »

«Vulnérabilité : Faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux menaces qui le guettent. »*

Exemples :

Information transmise en clair sur Internet

Réseau privé sans coupe-feu

Système d'exploitation non mis à jour

Compte utilisateur générique

Ports non-utilisés sont ouverts

*Source: ISO/IEC 27005:2011

Types de vulnérabilités

Vulnérabilité logicielle

Vulnérabilité réseau

Vulnérabilités de configuration
et de processus

Menaces internes

Vulnérabilité physique

Vulnérabilité par débordement
de tampon



Exemples de vulnérabilités

TYPE D'ACTIFS SUPPORT	EXEMPLES DE VULNÉRABILITÉ	
MATÉRIEL	Absence de programme de remplacement périodique	
	Sensibilité aux variations de tension	Stockage non protégé
LOGICIEL	Tests de logiciel absents ou insuffisants	Absence de documentation
	Absences de traces d'audit	Absence de copies de sauvegarde
RÉSEAU	Voies de communication non protégées	Transfert de mots de passe en clair
	Mauvais câblage	Gestion réseau inadaptée (résilience routage)
PERSONNEL	Formation insuffisante à la sécurité	Absence de personnel
	Procédures de recrutement inadaptées	Absence de mécanisme de surveillance
SITE	Réseau électrique instable	Absence de protection physique du bâtiment
	Emplacement située dans une zone sujette aux inondations	Utilisation inadaptée ou négligente du contrôle d'accès physique au bâtiment
ORGANISME	Absence d'audits réguliers (supervision)	Absence de plans de continuité
	Absence de contrôle des actifs situés hors des locaux	Absence de revues de direction régulières

Source de vulnérabilités

Processus et procédures

Activités récurrentes de gestion

Environnement physique

Personnel

Configuration du système d'information

Matériels, logiciels et infra de communication

« Actif »

«Tout élément représentant de la valeur pour l'organisme»*

Exemples :

Liste de clients

Brevets et propriété intellectuelle

Processus de développement

Application, base de données

Réseau, système d'opération

Portables

*Source: ISO/IEC 27001:2005

Identification et classification des actifs

Identification des actifs

- Actif : Tout élément représentant de la valeur pour l'organisme
- Identification devrait être facilitée selon la méthode d'analyse choisie
 - Différentes catégories d'actifs
 - Reflète les objectifs d'affaires

Méthode d'identification des actifs informationnels

1. Identifier les processus d'affaires
2. Identifier les regroupements d'information utilisés dans chaque processus d'affaires
3. Identifier les systèmes et applications qui supportent les processus d'affaires et le traitement des informations
4. Identifier les propriétaires des informations

Exemple d'inventaire des actifs informationnels

Processus d'affaires	Regroupement d'informations	Systèmes	Propriétaire de l'actif
1 Produire les factures aux clients	Compte clients Bon de commandes Factures émises aux clients	Pro-finances Pro-finances Pro-finances	Directeur des ventes Directeur des ventes Directrice des finances
2 Payer les fournisseurs	Factures des fournisseurs Ententes fournisseurs Relevé de comptes Paiements électroniques	Oracle appro GED Contrats Oracle appro Application IF	Directeur de l'approvisionnement Directeur Affaires juridiques Directrice des finances Directrice des finances
3 Maintenir le grand-livre	Écritures comptables États des résultats	Système GL Système GL	Directrice des finances Directrice des finances

Propriétaire vs fiduciaire des actifs informationnels

Propriétaire est responsable de :

- L'identification et la classification des actifs informationnels
- Définition et révision des droits d'accès aux actifs informationnels

Fiduciaire (*custodian*) est responsable de :

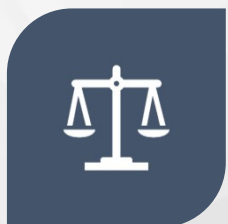
- Maintenir les mesures de sécurité appropriées conformément aux exigences et objectifs établis

L'imputabilité devrait demeurer au propriétaire des actifs informationnels

Classification des actifs

- **Objectif:** Déterminer la valeur de l'actif pour l'organisation afin d'établir des mesures de protection proportionnellement adéquates
- **Critères de classification : D-I-C**
 1. Sensibilité de l'information
 2. Criticité ou importance de l'information: Impact de l'indisponibilité ou de la perte d'intégrité de l'actif informationnel sur l'organisation

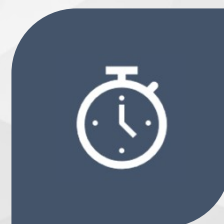
Autres critères à considérer



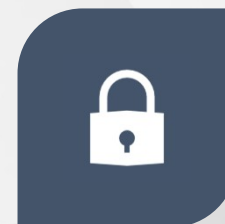
EXIGENCES LÉGALES
ET RÉGLEMENTAIRES



VALEUR DE L'ACTIF



DURÉE DE VIE UTILE



IMPLICATIONS POUR
LA SÉCURITÉ

Niveaux de confidentialité

Les 2 schémas les plus communs

Secteur privé ou commercial	Militaire
N/A	Top Secret
Secret	Secret
Confidentiel	Confidentiel
Interne ou sensible	Sensible
Public	Non classifié

Niveaux de confidentialité - Schéma du secteur privé

Niveaux	Définitions	Exemples
Public	Information dont la divulgation publique a été autorisée par son propriétaire et qui n'est pas susceptible de causer un préjudice à l'organisation	Services et coordonnées de l'entreprise
Privé ou sensible	Information dont la divulgation sans autorisation préalable à l'extérieur de l'organisation pourrait causer un préjudice à l'organisation, sans avoir cependant d'impact sur ses activités .	Bottin des employés, procédures administratives
Confidentiel	Actif dont la divulgation sans autorisation préalable est susceptible de causer un préjudice significatif à l'organisation ou à ses clients.	Renseignements personnes sur les clients, coût de revient des produits
Secret	Actif dont la divulgation sans autorisation préalable est susceptible de causer un préjudice d'une très grande gravité à l'organisation.	Projet d'acquisition d'une entreprise, brevet en développement

Niveaux d'intégrité - Exemple

Niveaux	Définitions	Exemples
Faible	Information pour laquelle l'organisation peut tolérer certains écarts (restant cependant acceptables) d'autant plus que les impacts qui y sont associés ont beaucoup moins d'importance.	Liste des cours suivis par les employés, compétences recherchées par poste
Modéré	Information qui se doit d'être exacte et dont l'inexactitude peut entraîner des conséquences significatives sur l'organisation.	Feuilles de temps du personnel, statistiques sur les ventes
Élevé	Information qui se doit d'être exacte en tout temps et dont l'inexactitude peut entraîner des conséquences grave pour l'organisation ou ses clients.	Transactions financières Information médicale

Niveaux de disponibilité - Exemple

Niveaux	Définitions	Exemples
Faible	Information dont l'impact de non-disponibilité est minime. On considère qu'une interruption pouvant aller jusqu'à une semaine demeure acceptable.	Rapports de gestion
Modéré	Information dont la non-disponibilité apporte des impacts moins importants sur les opérations de l'organisation. On considère qu'une interruption maximale de deux à trois jours reste acceptable.	Information requise pour la production d'états de compte
Élevé	Information pour laquelle on doit assurer la disponibilité presque en tout temps. On considère qu'une interruption maximale de 24 heures est acceptable.	Information sur les comptes clients

Classification des actifs – seuils d'impact

Niveau 1 (Faible)	Impact non-significatif : incidences plutôt négligeables, limitées à un secteur de l'entreprise.
Niveau 2 (Moyen)	Impact limité : incidences notables, limitées à un secteur de l'entreprise.
Niveau 3 (Élevé)	Impact grave : Incidences importantes pour l'entreprise ou la clientèle, ne menaçant pas la survie ou l'intégrité de l'entreprise dans son ensemble ou la vie ou la santé de personnes.
Niveau 4 (Très élevé)	Impact extrêmement grave : Incidences très graves menaçant la survie ou l'intégrité de l'entreprise dans son ensemble ou ayant des conséquences très graves pour la clientèle.

Exemples d'attributs d'impact

- Incapacité de l'organisation à remplir sa mission
- Perte de l'image ou dommage à la réputation
- Perte de confiance de la clientèle
- Perturbation des activités de l'organisme
- Infraction aux lois ou aux règlements
- Impossibilité de remplir ses obligations contractuelles
- Atteinte à la vie privée
- Pertes financières
- Augmentation des coûts
- Atteinte à la sécurité du personnel, des clients...
- Dommages matériels

Arbre ou matrice de décision

TYPE D'IMPACT	DISPONIBILITÉ	INTÉGRITÉ	CONFIDENTIALITÉ
Incapacité de l'organisation à remplir sa mission	1 (Bas)	2 (Moyen)	3 (élevé)
Perte de l'image ou dommage à la réputation	3 (élevé)	1 (Bas)	2 (Moyen)
Perte de confiance de la clientèle	1 (Bas)	2 (Moyen)	4 (Très Élevé)
Perturbation des activités de l'organisme	3 (élevé)	2 (Moyen)	3 (élevé)
Infraction aux lois ou aux règlements	1 (Bas)	3 (élevé)	2 (Moyen)
Synthèse de classification (valeur la plus haute)	3 (élevé)	3 (élevé)	4 (Très Élevé)

Exercice # 1

Pour chacun des actifs informationnels suivant, identifiez le **niveau de confidentialité** approprié (public, privé, confidentiel, secret):

1. Numéro d'assurance sociale
2. Date d'anniversaire
3. Mission de l'entreprise
4. Application de recherche d'emploi disponible sur le site Web de l'organisation
5. Formule pour produire un vaccin
6. Information médicale
7. Plan d'acquisition d'une entreprise
8. Application traitant les transactions bancaires

Les méthodes d'analyse de risque

Questions?

En avez-vous?



Références

<https://learn.microsoft.com/en-us/purview/data-map-classification-apply-manual>

<https://www.youtube.com/watch?v=v8LqmzBUaOo>: Data classification

<https://www.terranosecurity.com/fr/blogue/classification-de-l-information-ou-des-actifs-informationnels>

<https://www.pearsonitcertification.com/articles/article.aspx?p=3167978&seqNum=2>

https://www.splunk.com/en_us/blog/learn/vulnerability-types.html

<https://www.bdtask.com/blog/types-of-cyber-threats-in-cyber-security>

<https://iti.ca/uploads/2024/05/ITI-livre-blanc-Les-6-faibles-de-securite-informatique-les-plus-communes-1.pdf>

<https://fastercapital.com/topics/types-of-vulnerabilities-and-their-impact.html>

Exercice # 2

- Compagnie ABC met en place un site web transactionnel pour commander des jeux électroniques
- Serveur transactionnel a un système d'exploitation qui n'a pas été mis à jour depuis 2 ans et des failles sont connues et ont été exploitées à quelques reprises dans l'industrie
- Les clients ouvrent un compte en s'inscrivant en ligne et un code d'utilisateur et mot de passe par défaut leur est transmis par courriel. Le même mot de passe est assigné à tous les clients.
- Paiement par carte de crédit. Il n'y a pas de chiffrement de la communication ni du numéro de carte de crédit une fois stocké sur le serveur transactionnel.
- Les employés de la compagnie sont sensibilisés à la sécurité et ont signé un engagement de non-divulcation.
- Tous les employés ont accès à tous les systèmes.
- Les transactions sont journalisées mais les journaux ne sont revus qu'une fois par année

Exercice # 2 (suite)

- En utilisant la grille de seuils d'impact fourni en classe, attribuer une valeur aux composantes du DIC pour chaque actif désigné en remplissant la matrice de classification (au moins 3 enregistrements).