Hes·so
Master

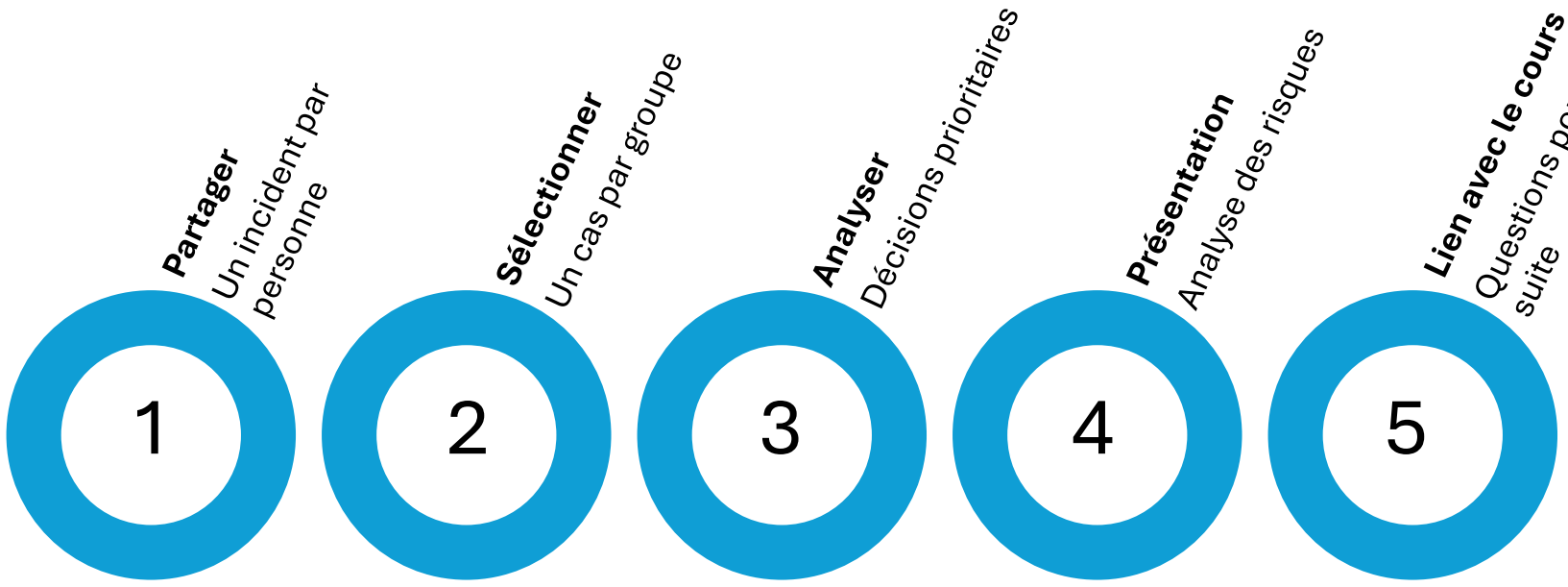
Management de la sécurité des systèmes d'information

MScBA orientation Management des SI

Ulysse Rosselet

Automne 2026

Passer d’un incident connu à une première décision managérale



Mini brainstorming

1 exemple par personne

- Chacun choisit un incident ou un événement lié à la sécurité de l'information
- A partir d'une situation vécue ou issue de l'actualité
  Vous pouvez anonymiser le cas et partager uniquement les choses que vous souhaitez raconter
- Expliquez rapidement l'incident au reste du groupe
  - Que s'est-il passé ?
  - Quelle information ou quel service était concerné ?
  - Qui ou quoi a subi les conséquences ?
  - Comment l'incident a-t-il été découvert ?

🕐 5-7 minutes

Exemples : phishing, document mal adressé, mot de passe partagé, panne, rançongiciel…

Choix du cas

Le meilleur cas n’est pas forcément le plus spectaculaire.

- **Compréhensible**
  Le groupe peut reconstituer les faits principaux.
- **Discutable**
  Plusieurs causes ou réponses semblent possibles.
- **Pertinent**
  Le cas soulève une question de management.

🕑 2 minutes

Analyse rapide: canevas A3

A · CE QUI AVAIT DE LA VALEUR

Information ou service
Personnes concernées
Confidentialité, intégrité ou disponibilité ?

B · CE QUI S'EST PASSÉ

Événement déclencheur
Faiblesse exploitée
Conséquences

C · POURQUOI LE SYSTÈME A CÉDÉ

Facteurs humains
Organisation du travail
Dispositifs techniques

D · COMMENT MAÎTRISER LE RISQUE

Prévenir, détecter, réagir
Choisir une mesure prioritaire
Justifier l'arbitrage

A · L’information qui avait de la valeur

Commencez par ce que l’organisation cherchait à protéger

C

CONFIDENTIALITÉ

Une personne non autorisée accède à l’information.

I

INTÉGRITÉ

L’information change ou devient difficile à croire.

D

DISPONIBILITÉ

L’information ou le service devient inaccessible.

QUESTION CLÉ

Pour qui l’impact compte-t-il le plus?

B + C · Déroulement de l’incident

1 DÉCLENCHEUR	2 FAIBLESSE	3 INCIDENT	4 CONSÉQUENCES
Quel événement lance la séquence ?	Qu’est-ce qui rend l’incident possible ?	Que se passe-t-il réellement ?	Quels effets pour l’organisation ?

Cherchez au moins un facteur dans chaque dimension

HUMAIN	ORGANISATION	TECHNIQUE
Erreur, pression, compréhension, contournement	Procédure, responsabilité, contrôle, ressources	Accès, configuration, sauvegarde, journalisation

D · Les réponses possibles

PRÉVENIR

Réduire la probabilité

DÉTECTER

Repérer l'incident rapidement

RÉAGIR

Limiter l'impact et rétablir

Votre décision

Quelle mesure mettriez-vous en place en premier ?

Efficacité probable

Coût et difficulté

Acceptabilité pour les utilisateurs

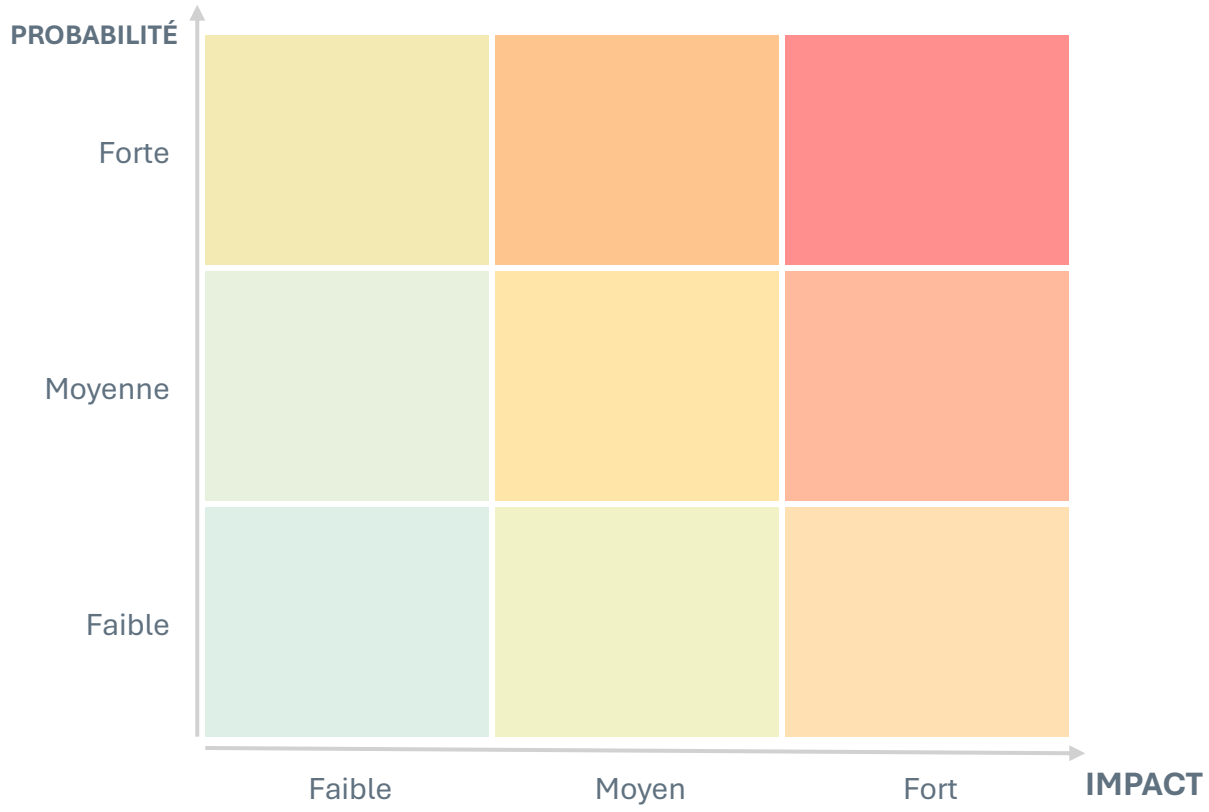
Restitution et carte des risques

https://docs.google.com/presentation/d/1noJpTCt-PnaggsPg5NUUbCeL_X4wVHq2-VLs4vps94/

90 secondes par groupe

- L'information à protéger
- L'incident en une phrase
- La faiblesse principale
- La conséquence la plus grave
- La mesure prioritaire retenue

Impact	Exemples de critères
Fort	- Perte financière > 1 mois de CA - Perte de clients stratégiques - Besoin de lancer une campagne de communication
Moyen	- Perte financière > 1 semaine de CA - Perte de clients non stratégiques - Besoin de négocier un arrangement à l'amiable
Faible	- Perte financière < 1 semaine de CA - Pas de perte de client - Aucun impact sur l'image de marque



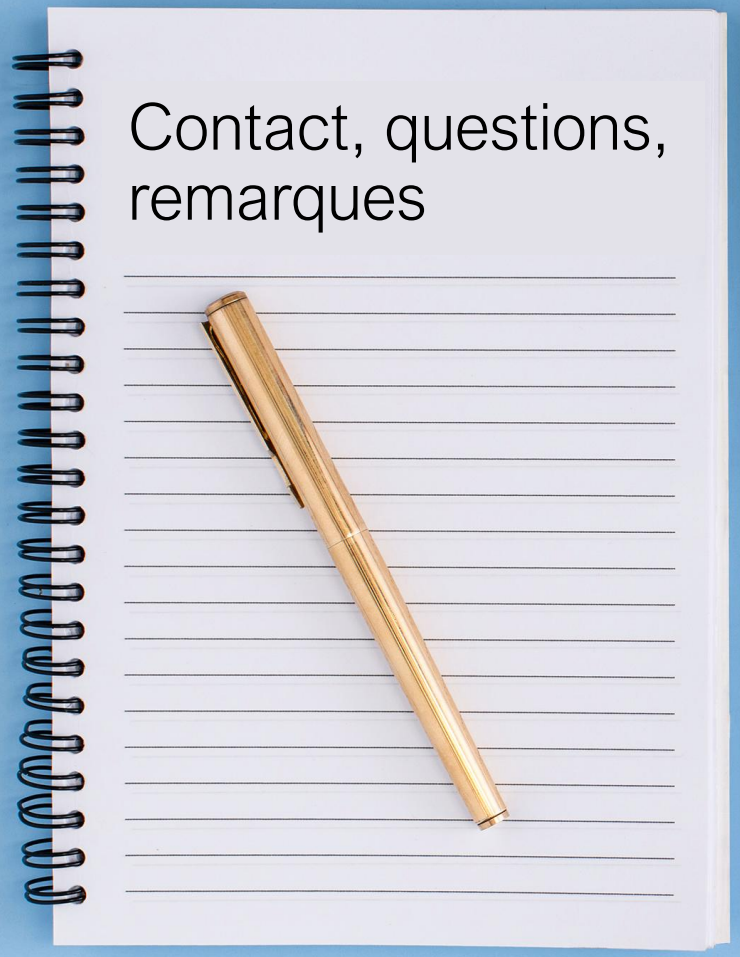
Placez votre incident. Expliquez vos hypothèses.

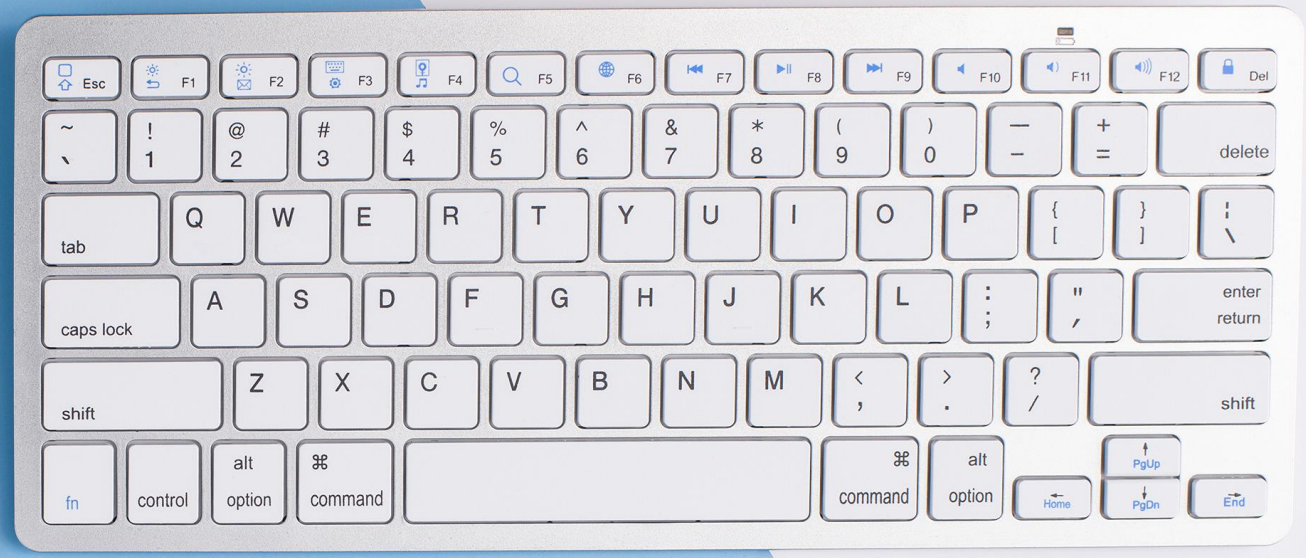
Ce que nous reprendrons la semaine prochaine

INFORMATION À PROTÉGER	—	**Actif informationnel**
C · I · D	—	**Objectifs de sécurité**
DÉCLENCHEUR + FAIBLESSE	—	**Menace et vulnérabilité**
PROBABILITÉ + IMPACT	—	**Évaluation du risque**
MESURES ET ARBITRAGE	—	**Traitement et gouvernance**

Objectifs du cours

- Comprendre les enjeux stratégiques, organisationnels, humains et techniques de la sécurité des systèmes d'information, ainsi que les principes permettant d'intégrer la sécurité dans leur gouvernance, leur conception et leur fonctionnement.
- Analyser les risques de sécurité organisationnels, techniques et humains, leurs impacts et les mesures de maîtrise applicables, y compris face aux technologies émergentes.
- Comprendre les enjeux juridiques et réglementaires liés à la sécurité de l'information et à la protection des données.
- Élaborer une politique de sécurité de l'information alignée sur les objectifs stratégiques de l'entreprise, intégrant la conformité, la gestion des risques et la continuité des activités.
- Concevoir une démarche structurée de management de la sécurité de l'information, fondée sur les normes et bonnes pratiques internationales.
- Appréhender la cybercriminalité ainsi que les principaux moyens de prévention, de lutte et d'enquête.





Ulysse Rosselet
Responsable d'orientation

Espace de l'Europe 21
CH-2000 Neuchâtel

ulysse.rosselet@he-arc.ch