



**POLYTECHNIQUE
MONTRÉAL**

UNIVERSITÉ
D'INGÉNIERIE

INF8085 : Cybersécurité

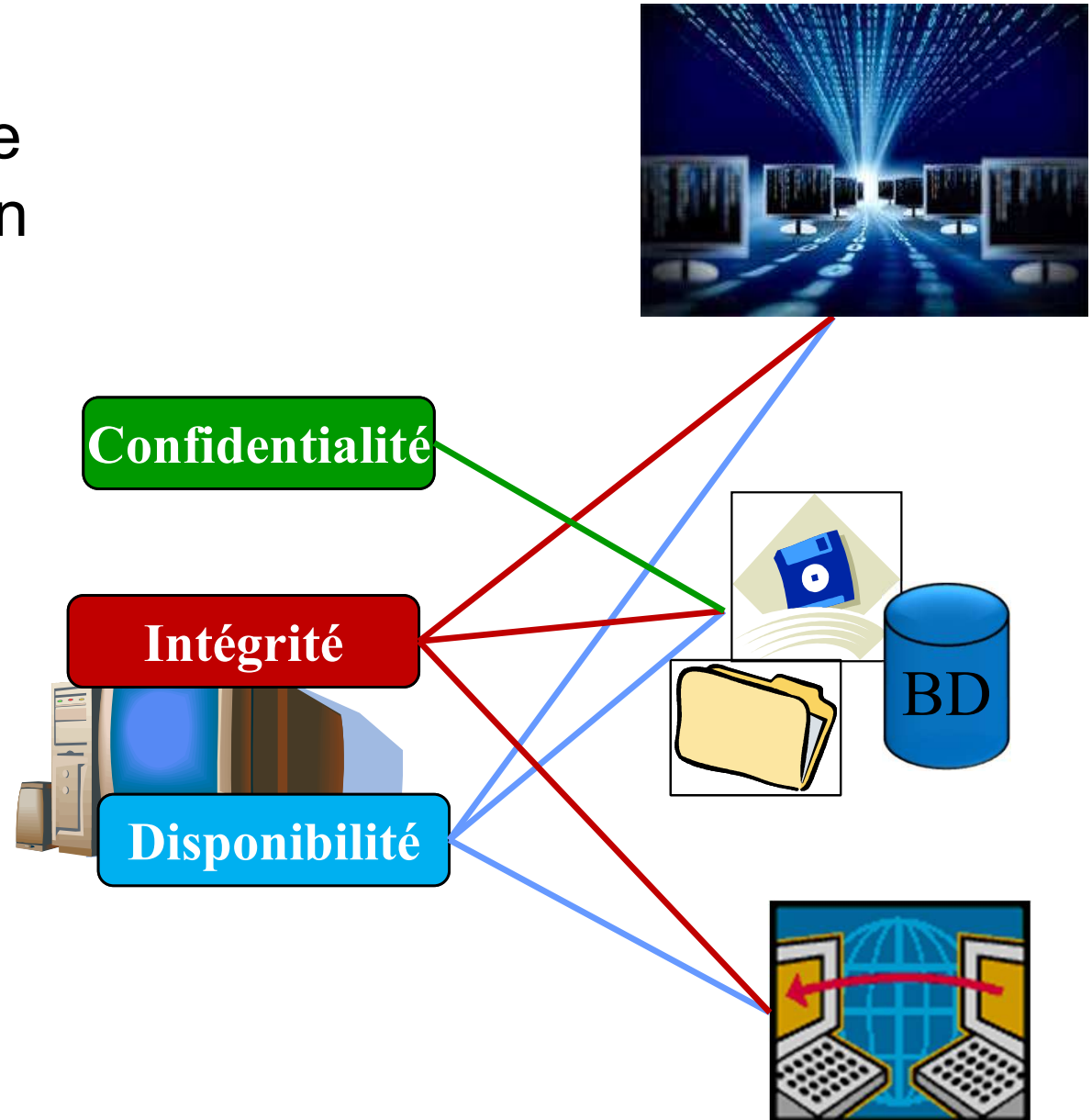
Introduction : Concepts de base et motivation

Frédéric Cuppens



Qu'est-ce que la sécurité informatique ?

- La sécurité informatique consiste en la protection
 - systèmes,
 - données et
 - services
- Contre les menaces
 - délibérées
 - malveillantes
- Portant atteinte
 - confidentialité
 - intégrité
 - disponibilité





Sûreté de fonctionnement vs. Sécurité informatique

- En anglais : deux termes pour « sécurité »
 - *Safety*
 - *Security*
 - *Safety* \neq *Security*
- En français : un seul terme « sécurité »
 - Traduction de « *safety* » : Sûreté de fonctionnement (SDF)
 - Traduction de « *security* » : Sécurité informatique
 - Ou aussi « Sécurité des Systèmes d'Information » (SSI)



Sûreté de fonctionnement vs. Sécurité informatique

- Différence entre la SdF et la SSI
 - La SdF traite des fautes accidentelles (défaillances)
 - La SSI traite des fautes intentionnelles ou malveillantes (attaques)
- Mais il y a des liens entre SdF et SSI
 - Notamment une attaque (malveillante) peut causer une défaillance
 - En sens inverse, un attaquant peut profiter de (exploiter) une défaillance accidentelle pour réaliser une attaque
- Traduction de « Malveillant »
 - Malveillant = Malicious
 - Malicious ≠ Malicieux



Sécurité

Disponibilité

Intégrité

Confidentialité

Propriétés de sécurité



Rappel de génie logiciel

Propriétés de safety et de liveness

- Propriété de *liveness*
 - Propriété de vivacité en français
 - Quelque chose de « bon » va arriver
 - Exemple : Ce vaccin est efficace contre la Mpox (Variole simienne)
- Propriété de *safety*
 - Propriété de sûreté en français
 - Quelque chose de « mauvais » ne va pas arriver
 - Exemple : Ce vaccin n'a pas d'effet secondaire



- Disponibilité
 - Capacité d'un système informatique d'assurer ses fonctions sans interruption, retards ou dégradation, au moment où la demande en est faite
 - Propriété de liveness
- Capacité à rencontrer
 - les besoins et les spécifications
 - les contraintes de temps, de performance et de qualité
- Applicable aux systèmes / données / services



- Disponibilité en temps fini
 - Propriété de disponibilité « faible »
 - Garantie que le système / la donnée / le service sera accessible une fois que la demande en est faite
 - Mais sans donner de garantie sur la durée que cela va prendre
 - Exemple : Le serveur web est disponible 7j/7 et 24h/24



- Disponibilité en temps borné (ou contraint)
 - Propriété de disponibilité « forte »
 - Garantie que le système / la donnée / le service sera accessible au bout d'une durée maximale spécifiée à l'avance
 - Exemple 1 : le dossier médical sera accessible au bout d'une durée maximale de 5s
 - Exemple 2 : le service de paiement en ligne sera accessible au bout d'une durée maximale de 10s
 - Pertinent notamment dans les systèmes temps-réel



- Intégrité
 - Propriété de *safety*
 - Il ne faut pas que quelque chose de « mauvais » arrive aux systèmes, données et / ou services
 - Nombreux sens possibles !



- Intégrité (des données)
 - Propriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation
- Intégrité (d'un système ou d'un service)
 1. Capacité du système ou du service à préserver l'intégrité des données qu'il gère
 2. Protection du système ou du service contre les dysfonctionnements, les agressions et les attaques



- Intégrité des données (au sens *safety*)
 - Exactitude
 - Précision
 - Cohérence
- Intégrité des données (au sens *security*)
 - Pas de modification non autorisée des données
 - Modification autorisée seulement
- Lien entre ces deux définitions



Propriétés de sécurité

- Confidentialité
 - S'applique aux données
 - Assure que l'information n'est accessible qu'à ceux-celles dont l'accès est autorisé
 - Propriété de *safety*
- Qui peut « voir » quoi ?
 - Fait référence à la notion de « Secret »
- Plusieurs dimensions
 - Intérêts publics
 - Exemple : secret militaire
 - Intérêts privés
 - Exemple : secret industriel et commercial
 - Vie privée
 - Privacy en Anglais
 - Protection des « données à caractère personnel »



- Une quatrième propriété de sécurité est aussi souvent utilisée : Auditabilité
 - Il s'agit de disposer de l'information nécessaire et suffisante pour attribuer (généralement a posteriori) la responsabilité d'un fait à une personne
- Plusieurs autres noms possibles
 - Traçabilité, Imputabilité, Preuve
- Le terme « Auditabilité » fait référence au besoin « d'auditer » les activités du système informatique
 - Disponibilité des journaux
 - Journaux doivent être intègres pour avoir valeur de preuve

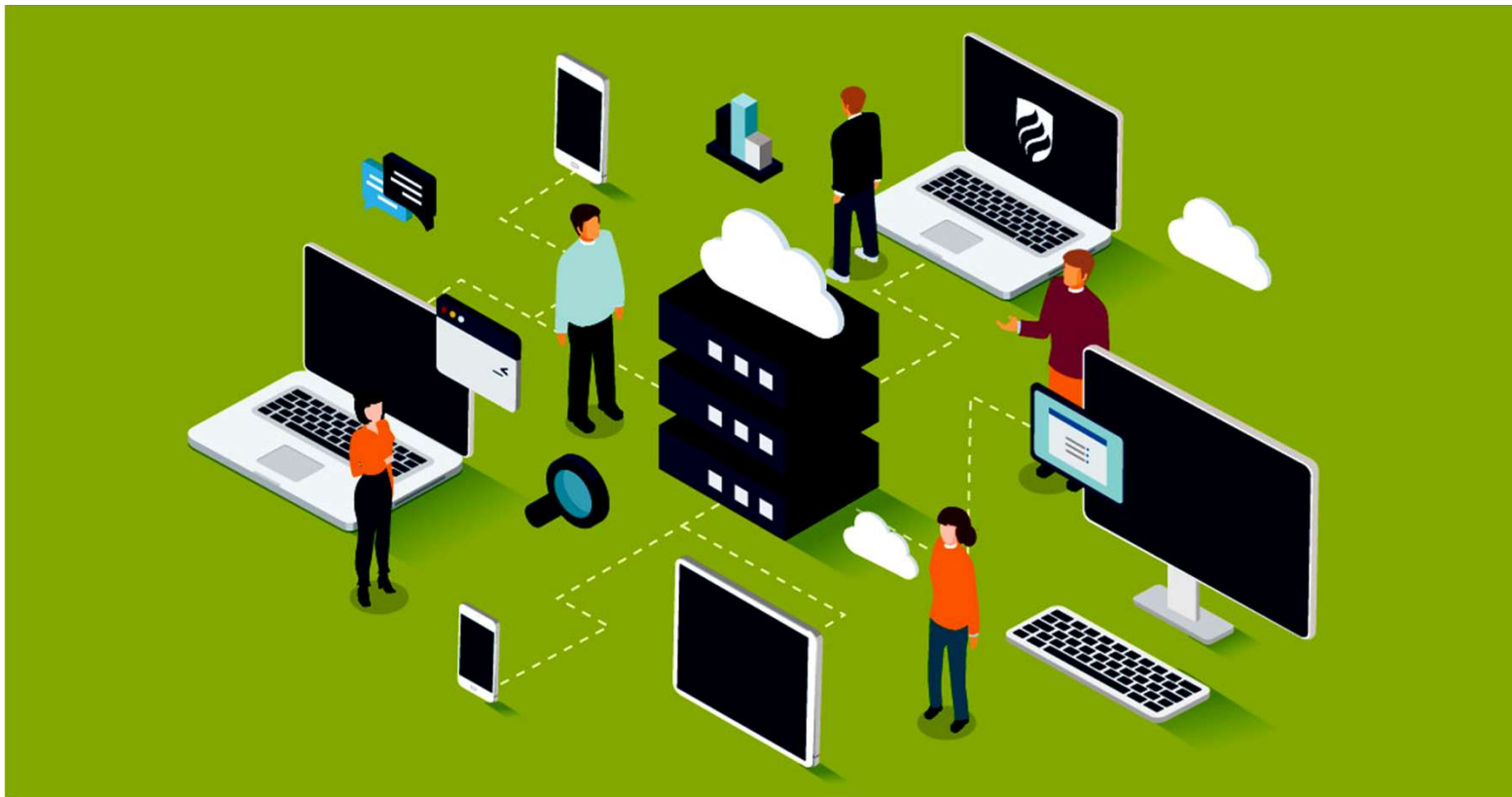


- Cyber sécurité : qu'est-ce qui change par rapport à la sécurité informatique ?
 - Changement de périmètre
 - Changement de paradigme



Périmètre de la sécurité informatique

- Technologie de l'information
 - IT en Anglais : Information Technology





Digitalisation de notre monde

Digitalisation de l'économie

Digitalisation de l'industrie

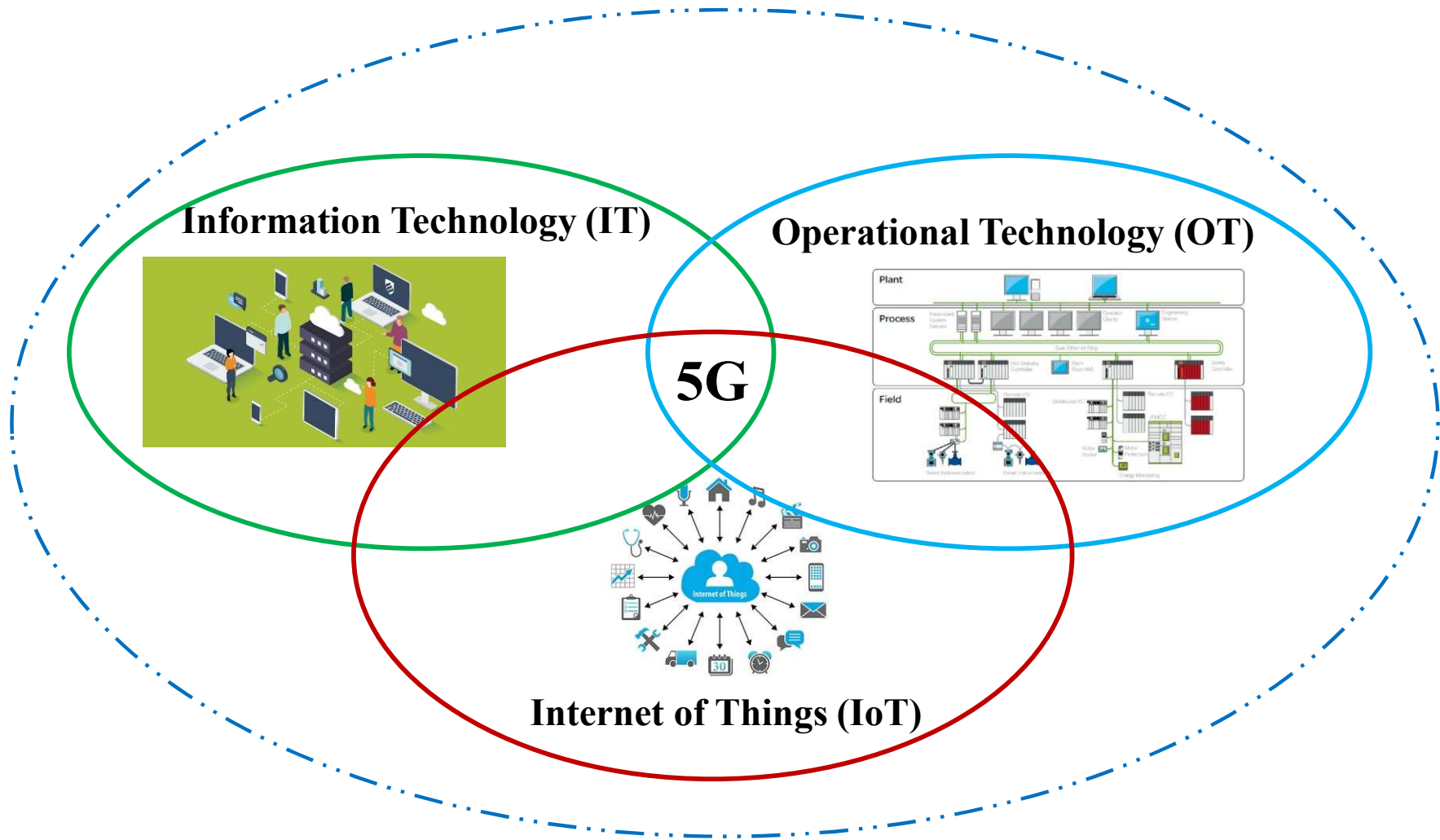
Digitalisation de la société



Changement de périmètre

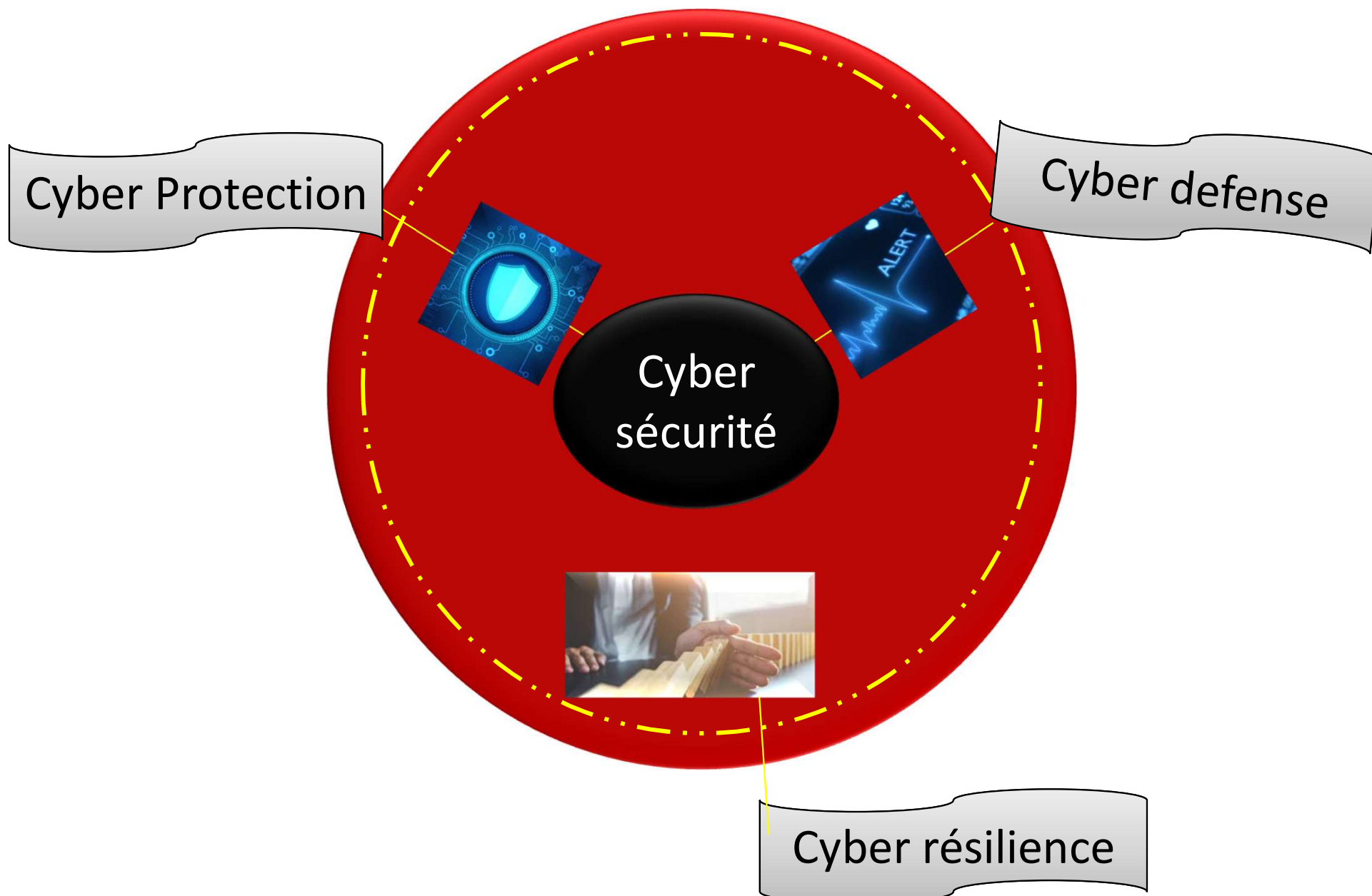


Périmètre de la cybersécurité





Paradigmes de la cybersécurité





Paradigmes de la cybersécurité

- Cyber protection : définition et limites
- Définition
 - Moyens techniques, physiques et organisationnels pour protéger le système contre les cyberattaques
 - Exemples : chiffrement, contrôle d'accès, filtrage réseau, contrôle de flux, tatouage, anonymisation, ...
- Limites
 - Impossible d'assurer une protection à 100%
 - Faute de conception, d'implantation, d'utilisation
 - Evolutions techniques et technologiques
 - L'erreur humaine





- Cyber défense : définition et limites
- Définition
 - Mesures techniques ou organisationnelles permettant la surveillance, l'appréciation de la sécurité et la réaction face aux cyberattaques
 - Exemples : IDS, SIEM, SOC
- Limites
 - Impossible d'assurer une détection à 100%
 - Attaques « zero day »
 - Techniques d'évasion
 - Attaques furtives



- Cyber résilience
- Définition
 - Capacité d'un système à résister à des cyberattaques qui réussissent

La question n'est pas :

Mon système va-t-il être attaqué ?

Mais,

Quand mon système va-t-il être attaqué ?



Paradigmes de la cybersécurité

- Cyber résilience : d'autres propriétés
- Absorbabilité
 - Capacité du système à absorber les conséquences d'une attaque sans souffrir d'une défaillance complète
- Adaptabilité
 - Capacité du système d'ajuster son comportement en fonction des changements de l'environnement ou de sous-ensembles du système lui-même
- Recouvrabilité
 - Capacité du système de revenir dans un état normal



- Cyber résilience : quelques exemples de solutions
 - Diversification fonctionnelle
 - Défense en profondeur
 - Défense dynamique et adaptative



**POLYTECHNIQUE
MONTREAL**

UNIVERSITÉ
D'INGÉNIERIE

Questions ?