Generative AI & Cybersecurity

Apprentissage:

- peut limiter l'apprentissage
  - faut savoir l'utiliser correctement

Risques pour l'entreprise si tu mets des données confidentielles dans une IA qui les récupère

Des gens qui oublient des infos confidentielles dans les infos données (clé API oubliée au début)

Donne un accès plus facile au hacking de site fait par des personne peu informées

Ethical issues

tentatives de faire des demandes d'actions illégales (par exemple voler une voiture)

- marche plus si tu enrobes la demande (par exemple avec contexte de jeu vidéo)

deepfake peut bypass la biométrie

- Varie en fonction des données que tu expose sur internet.

dépendance aux IAs peut être dangereux

Intro IAM

- Élément conssitutifs d'une IAM = Identifiant + attributs
- Type de compte = Equipe + Privilège + Individuel + service
- Modèle le plus répendu des habilitations =