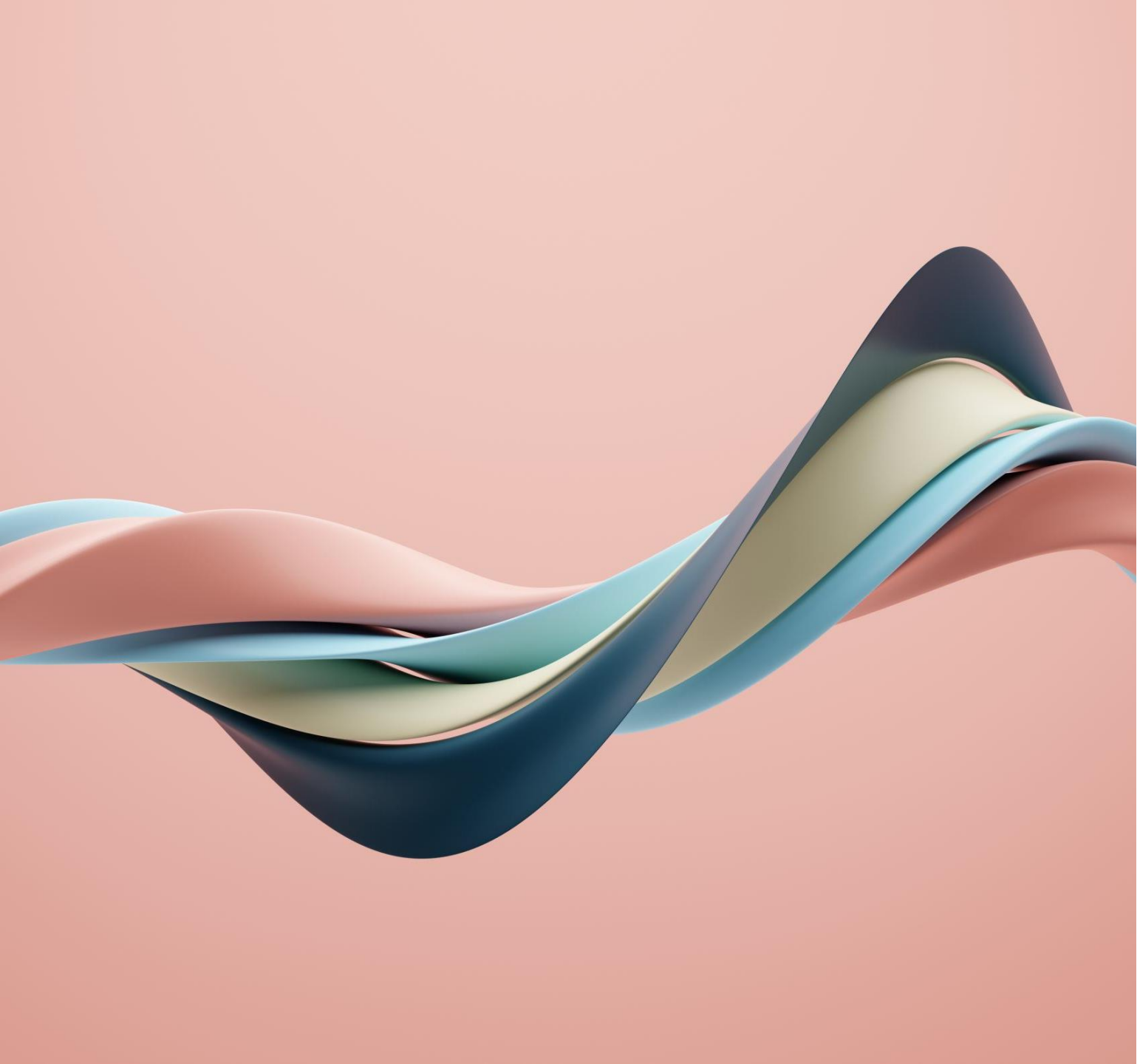

Sécurité et gouvernance de l’Intelligence Artificielle

OBJECTIFS DE LA FORMATION

- Comprendre les vulnérabilités des systèmes d'IA et les techniques pour les protéger.
- Comprendre les enjeux de sécurisation et de gouvernance des systèmes IA dans des environnements industriels et organisationnels, ainsi que les spécificités liées à la protection des modèles génératifs.
- Tirer parti des capacités de l'IA pour renforcer la défense des systèmes d'information.
- Explorer les différentes formes d'utilisation malveillante de l'IA, des contenus frauduleux aux attaques physiques sur systèmes connectés, et apprendre à détecter et contrer ces menaces.
- Développer un sens logique et intuitif de l'attaque et de la défense en IA.

PRÉSENTATIONS

- Votre rôle, votre expérience, votre background.
- Vos attentes de la formation.
- Ce qui vous semble pertinent.

PROGRAMME

01	**Sécurité de l'IA traditionnelle**	~35%
02	**Sécurité de l'IA élargie**	~30%
03	**IA pour la sécurité**	~20%
04	**Détournement malveillant ou offensif de l'IA**	~15%

PETIT AVANT-PROPOS

Les informations échangées et les activités pratiques proposées ont pour unique but la compréhension, la prévention et la détection des risques liés aux technologies d'IA.

Elles ne visent en aucun cas à fournir des idées, méthodes, outils ou recettes exploitables pour nuire, pénétrer, tromper ou compromettre des systèmes réels.

DÉPÔT GITHUB DE LA FORMATION

https://github.com/BEESPE/202512-BNP-secugouvia.git