# Jeudi 19 septembre 2024

J’ai commencé ma journée par finir la première formation de cybersécurité commencée la veille et ainsi que la 2ème. Cette formation était obligatoire et il a été demandé à Jérôme que je la couvre avant la semaine prochaine.  
  
J’ai aussi assisté au séminaire de mobilité responsable ainsi qu’au séminaire de risque interne et audit.  
  
Cet après-midi je compte continuer à analyser la documentation Microsoft au sujet de Copilot.  
  
Par ailleurs, après un peu de veille, j’ai appris le déploiement par Microsoft de Copilote Wave 2, un agent intégré à la suite 365 présentant de nouvelles interfaces intégrées et fonctionnalité pour des cas d’usages collaborateurs. Beaucoup de bien est dit de ce nouveau produit.

D’autres informations intéressantes ont été trouvées dans la documentation de Microsoft Copilote Studio concernant les défis relevé plus tôt dans la semaine. Cela concerne l’option d’IA générative qui peut-être utiliser en « secours » (donc non prioritaire face à la source d’information utilisée par le copilote, dans notre cas le sharepoint) pour essayer de répondre à l’utilisateurs si aucunes intentions (rubriques) n’auraient été déclenché par l’entrée envoyée par l’utilisateur.

De plus, un critère de modération de contenu (élevée, moyen ou bas) permet de « brider » les réponses fournies par l’option d’IA gen, impactant sa pertinence.

 Cela répond aux défis, ou plutôt à notre scepticisme concernant l’activation de cette option au sein du copilote, dans la crainte que l’IA fournirait des réponses hors sujets ou des hallucinations.

Ces informations sont donc rassurantes et nous pousse à croire que l’option d’IA gen est en réalité une option pertinente. Néanmoins, nous ne devons pas perdre de vue les risques qu’elle pourrait entraîner, et continuer à la monitorer.

J’ai fait part à Jérôme de cette découverte qui m’a fait part d’une remarque intéressante : la pertinence de l’option Gen AI, qui peut s’apparenter à la température du prompt engineering, doit être paramétrée de manière différente en fonctions des utilisations. Par exemple : La où l’ensemble des départements de Gecina nécessiteront des réponses à pertinence élevée, la communication pourrait utilisée le copilote pour faire de la génération d’image, auquel cas la pertinence devrait être plus basse pour permettre plus de flexibilité.

Mais cela soulève un nouveau défi : Si un utilisateur se fait passer pour un collaborateur qui travail dans un département dont le copilote autorise une pertinence plus basse (ex : communication et la génération d’image), est-ce que cet utilisateur serait en mesure de bypass le paramètre de pertinence pour une autre requête ?  
L’Entra ID est-elle suffisante pour sécuriser ce genre de cas d’usage (dans le sens où elle porterait en plus des droits d’accès aux information du Sharepoint, la hiérarchie de Gecina et l’appartenance de chaque utilisateur à son département de travail) ?

## Tester la portée des réponses génératives du copilote

Il est possible de teste les réponses génératives du copilote dans le volet de test du copilote. Il est à noter que les réponses génératives fonctionnent bien avec une grande variété de type de questions, et fonctionnent beaucoup moins bien lorsque la question porte sur les de ces 3 sujets :

* Questions personnelles
* Questions nécessitant un accès authentifié au contenu (à prendre en compte)
* Questions qui n’ont aucun contenu associé sur une URL spécifiée

## Formulation de questions