Atelier S3 — Protéger les données dans un usage IA

DOSSIER ÉTUDIANT • NOVACHIPS

Durée	Organisation	Séquence
60 minutes	Groupes de 3 à 4	S3.3 — Mesures de protection (O2, O3, O4)

Situation professionnelle

Novachips personnalise des chips avec photos et messages. Dans le cadre d'un travail fictif de préparation d'une réponse à un client, un collaborateur souhaite soumettre à un assistant IA un extrait de dossier de commande. Votre mission est de rendre ce contenu utilisable dans un assistant sans exposer inutilement les informations sensibles. Vous n'avez pas à développer ni à installer un modèle.

Plateformes et documentation

- Site Novachips : https://novachips.portail-cyber.akademiedudigital.com/site-accueil.html
- Intranet Novachips : https://novachips-intranet.portail-cyber.akademiedudigital.com/intranet-accueil.html
- Portail Cyber : https://portail-cyber.akademiedudigital.com/
- CNIL — IA : https://www.cnil.fr/fr/intelligence-artificielle
- ANSSI : https://cyber.gouv.fr/

L'intranet sert à comprendre le contexte métier. Le document d'exercice ci-dessous est un exemple pédagogique construit pour cet atelier, et non une donnée réellement extraite de l'intranet. Aucun compte ou service IA externe n'est indispensable.

Pièce A — Extrait de dossier de commande fictif

Champ	Valeur fictive
Commande	NC-2026-0147
Client	Camille Durand
Contact	camille.durand@example.org
Téléphone	06 00 00 00 24
Livraison	12 rue des Inventeurs, 69000 Lyon
Produit	Lot de chips personnalisées, 250 sachets
Message à imprimer	« Félicitations pour ton diplôme ! »
Photo transmise	Portrait client : fichier portrait-camille.jpg
Observation interne	Réclamation précédente : délai ; geste commercial de 15 %
Demande au modèle	Rédiger un message poli confirmant la prise en charge et expliquant la préparation du lot

Déroulement — 60 minutes

Phase	Durée	Mission
1. Observer	10 min	Repérer les données personnelles, commerciales et potentiellement sensibles.
2. Classer	15 min	Classer chaque champ : nécessaire / à reformuler / à masquer ou exclure. Justifier.
3. Assainir	20 min	Produire une version minimale du contexte et un prompt rédigé sans information inutile.
4. Contrôler	10 min	Appliquer une grille de vérification : exposition, exactitude, divulgation, contrôle humain.
5. Restituer	5 min	Expliquer deux mesures prises et un risque résiduel.

Travail demandé

- Identifier au moins cinq champs et justifier leur classification selon le besoin du message.
- Écrire un prompt réutilisable ne contenant ni nom, ni adresse, ni contact, ni photo, ni information interne inutile.
- Proposer trois mesures complémentaires : choix de l'outil, règles d'accès/partage, validation humaine ou conservation.
- Comparer l'usage d'un assistant cloud et d'un assistant local : quels risques demeurent dans les deux cas ?

Production attendue

Une fiche de réponse complétée : classement des données, texte assaini, prompt minimal, contrôles appliqués et limites. Si un assistant IA est autorisé en séance, utiliser uniquement le texte assaini. Ne transmettre aucun document réel ni donnée personnelle à un outil tiers.

Repères documentaires

CNIL : https://www.cnil.fr/fr/intelligence-artificielle • OWASP GenAI : https://genai.owasp.org/ • ANSSI : https://cyber.gouv.fr/