Dossier de présentation · Novachips

Kit pédagogique IA & Cybersécurité | Contexte commun aux ateliers S1 à S5

01 L'entreprise et son activité

Novachips est une entreprise fictive spécialisée dans la personnalisation de chips : visages, photos, textes et logos imprimés directement sur les chips, avec personnalisation des sachets. Le site vitrine met en avant une fabrication à Lyon, quatre saveurs et une commande en ligne. Les éléments décrits ci-dessous sont issus des interfaces de simulation ; ils ne constituent pas une description d'une entreprise réelle.

02 Environnements numériques existants

Interface	Ce que l'on peut y découvrir	Usage dans le cursus
Site public	Offre, personnalisation, parcours de commande et communication commerciale	S1 : actifs exposés et types de données clients
Intranet / connexion	Écran d'accès collaborateurs et informations de connexion	S1 : identification des risques et des pratiques visibles
Intranet / accueil	Messagerie, NovaGPT, RH, comptabilité, administration, actualités internes	S1 à S3 : données, usages IA, sécurité organisationnelle
SOC	Alertes, signalements, journaux, flux, événements et incidents simulés	S4 : analyse défensive et investigation
Espace formateur	Environnement pédagogique, consignes et fonctions d'évaluation	Réservé à l'animation et à la correction

03 Carte fonctionnelle simplifiée

Clients et visiteurs → Site public / commandes personnalisées → Données commerciales et visuels transmis par les clients. Collaborateurs → Intranet → Messagerie, documents, services métiers et assistant NovaGPT. Équipe de supervision → SOC fictif → Alertes, signalements et événements.

Cette représentation est une carte fonctionnelle d'apprentissage : elle ne prétend pas décrire l'architecture réseau ou les véritables flux applicatifs des plateformes.

04 Axes de vigilance pédagogique

- Confidentialité des photos, messages, données de commande et dossiers internes.
- Contrôle des accès aux espaces collaborateurs et aux fonctions d'administration.
- Périmètre documentaire et autorisations de l'assistant NovaGPT.

- Usages non maîtrisés d’outils IA externes, transferts de données et partage.
- Traçabilité, signalement et analyse des événements de sécurité.

05 Parcours Novachips sur cinq séquences

Séquence	Mission progressive
S1	Explorer l’environnement et cartographier les actifs, données et premiers risques.
S2	Analyser une tentative de fraude ou de phishing fictif.
S3	Étudier et mettre en œuvre des mesures de protection de données et d’usages IA.
S4	Investiguer des événements à partir des interfaces SOC et intranet.
S5	Produire et défendre un diagnostic de sécurité priorisé.

06 Accès aux plateformes

Site public — https://novachips.portail-cyber.akademiedudigital.com/site-accueil.html

Connexion intranet — https://novachips-intranet.portail-cyber.akademiedudigital.com/intranet-connexion.html

Accueil intranet — https://novachips-intranet.portail-cyber.akademiedudigital.com/intranet-accueil.html

SOC fictif — https://novachips-soc.portail-cyber.akademiedudigital.com/plateforme-soc.html

Espace formateur — https://novachips-trainer.portail-cyber.akademiedudigital.com/accueil-formateur.html

Consignes de sécurité : n’utiliser que des identités et données fictives ; ne pas tenter d’accès hors périmètre ; ne jamais saisir de données personnelles réelles ; ne pas tester de phishing auprès de tiers. Les plateformes sont des supports de simulation, pas des cibles à attaquer.

Références

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