Atelier S2 — Enquête sur une fraude assistée par IA

DOSSIER ÉTUDIANT • NOVACHIPS

Durée	Organisation	Positionnement
50 minutes	Groupes de 3 à 4	S2.4 — Atelier formatif, après S2.1 à S2.3

Votre mission

Vous intervenez comme cellule de sensibilisation et d'analyse des risques de Novachips, fabricant fictif de chips personnalisées. Une série de messages a suscité des doutes. Votre groupe doit étudier la messagerie de démonstration, documenter les indices et recommander une réponse adaptée. Vous ne devez pas chercher à compromettre la plateforme.

Accès aux environnements

- Site public : https://novachips.portail-cyber.akademiedudigital.com/site-accueil.html
- Intranet : https://novachips-intranet.portail-cyber.akademiedudigital.com/intranet-accueil.html
- Messagerie : https://novachips-intranet.portail-cyber.akademiedudigital.com/intranet-messagerie.html
- SOC fictif : https://novachips-soc.portail-cyber.akademiedudigital.com/plateforme-soc.html

Utilisez uniquement les comptes de démonstration et les données fictives proposées par les plateformes. Aucune sollicitation de tiers, aucun envoi réel, aucun téléchargement ou exécution d'une pièce jointe inconnue.

Déroulement — 50 minutes

Phase	Durée	Travail attendu
1 · Prise en main	5 min	Repérer les espaces de la messagerie et les fonctions utiles (recherche, détails, signalement).
2 · Enquête	15 min	Sélectionner deux messages suspects ou discutables ; relever les indices visibles.
3 · Analyse	15 min	Qualifier chaque tentative : cible, mécanisme de persuasion, risque, vérification.
4 · Réponse	10 min	Proposer les bons réflexes et, si approprié, utiliser le signalement au SOC dans la simulation.
5 · Restitution	5 min	Présenter un cas, une incertitude et trois mesures concrètes.

Grille d'enquête à compléter

Élément	Message A	Message B
Objet et expéditeur	_____	_____
Indices vérifiables (adresse, domaine, urgence, demande, pièce, contexte)	_____	_____
Hypothèse d'attaque et niveau de confiance	_____	_____
Conséquences possibles pour Novachips	_____	_____
Vérification hors canal / action de défense	_____	_____

Questions de réflexion

- Quelles techniques d'ingénierie sociale sont utilisées ? Distinguez les faits des suppositions.
- En quoi l'IA pourrait-elle rendre le contenu plus convaincant ? Peut-on prouver qu'un message a été produit par IA à partir de son style seul ?
- À qui signaler le message ? Quelle vérification indépendante demander avant un virement, une connexion ou un partage de données ?

Livrable attendu

Une fiche de groupe (une à deux pages) : deux analyses argumentées, une recommandation de signalement, trois mesures prioritaires et les incertitudes non résolues. La qualité des justifications compte davantage que le nombre de messages examinés.

Ressources de référence

ANSSI : https://cyber.gouv.fr/ • Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/ • Portail Cyber de l'Akadémie : https://portail-cyber.akademiedudigital.com/