Sujet d'évaluation - Cybersécurité / sciences

Exemple hors gestion, aligné sur la méta-trame en 4 Blocs (ACAI)

Discipline : cybersécurité et sciences du numérique

Niveau : Bac+5 ou formation continue · Travail individuel

Durée de travail : 2 h 30 · Livrable : dossier de 5 pages + oral de 5 minutes

Contexte

Un laboratoire de l'Université de Guyane signale une vague de courriels de hameçonnage (phishing) très

ciblés, en français et en portugais, usurpant l'adresse de la direction des systèmes d'information. Plusieurs

agents ont cliqué. Un poste sous Linux présente un comportement anormal. La direction vous confie une

réponse en 48 heures. Des extraits d'en-têtes de courriels et de journaux système vous sont fournis en séance.

Votre mission

Vous êtes analyste en cybersécurité junior. Vous traitez l'incident en 4 Blocs, en utilisant l'IA comme

outil professionnel sous contrôle, jamais comme source d'autorité.

Règle d'Or (chaque production assistée par IA)

Indiquez ce que l'IA a produit, ce que vous avez modifié, pourquoi. Sans traçabilité : 10/20 maximum.

Bloc 1 - Comprendre et vérifier (~40 min)

A partir des en-têtes et journaux fournis, demandez à une IA d'expliquer les indices de compromission, puis

vérifiez chaque affirmation. Classez : vérifiable / douteuse / hallucination, avec source (documentation

ANSSI, CVE officielles). Signalez l'information la plus dangereuse si elle était utilisée sans vérification

(par exemple une commande système inventée).

Bloc 2 - Produire avec RCCF (~40 min)

Rédigez un prompt RCCF pour générer un message d'alerte clair aux agents (que faire, ne pas faire). Comparez

deux outils, retravaillez à la main la version finale (ton, exactitude, absence de jargon). Traçabilité obligatoire.

Bloc 3 - Sécurité des données et éthique (~35 min)

Justifiez pourquoi l'analyse des journaux contenant des données personnelles ne doit pas être soumise à un

service d'IA tiers, et proposez une alternative souveraine (par exemple un modèle auto-hébergé type Ollama).

Argumentez le compromis sécurité / commodité.

Bloc 4 - Encadrer et recommander (~30 min)

Identifiez les risques (RGPD sur les données de journalisation, obligations de notification) et rédigez 5

recommandations d'hygiène numérique + une mini-charte d'usage de l'IA pour le laboratoire.

Grille sur 20

Critère	Barème
Bloc 1 - Vérification, détection d'hallucinations techniques	/4
Bloc 2 - Prompt RCCF et message retravaillé	/5
Bloc 3 - Sécurité des données et souveraineté	/4
Bloc 4 - Cadrage RGPD et recommandations	/3
Traçabilité (Règle d'Or)	/2
Oral : défense des choix techniques	/2
Total	/20

Oral (5 minutes)

Exposé des choix de réponse à l'incident, puis questions de relance (par exemple : pourquoi ne pas avoir

fait confiance à la commande proposée par l'IA ?).