

CYBERSÉCURITÉ / DOCUMENT ÉLÈVE

LIVRET DE SÉQUENCE — Repérer, analyser et protéger

1CIEL · 1C_CYB_03 · 10 h · salle informatique / poste élève

Nom : _____ Groupe / binôme : _____

Poste : _____ Date : ____ / ____ / ____

Ta mission

Tu aides une petite organisation à réagir correctement face à des messages, comptes et données numériques à risque. Tous les exemples du livret sont fictifs.

Tu apprends à — distinguer un fait d'une hypothèse, repérer des indices de risque, choisir une vérification sûre et proposer une mesure proportionnée.

Tu dois montrer — une décision justifiée à partir d'indices précis et des recommandations applicables.

SÉCURITÉ

Ne clique jamais sur un lien d'exercice hors des documents fournis. Ne saisis aucune donnée personnelle dans un service tiers. Aucun scan, test offensif ou essai sur un système réel non autorisé.

SUR TA TABLE

ce livret, le dossier 03_DOSSIER_RESSOURCES_ELEVE_1C_CYB_03, un stylo et le fichier DEMO_SAUVEGARDE.txt ; aucun compte à créer. Les pièces A à E, les feuilles de réponse et les réessais sont dans le dossier de ressources.

REPÈRE DANS LE MESSAGE

Dans un message, repère d'abord : adresse réelle de l'expéditeur → domaine du lien → demande formulée → urgence → pièce jointe.

À repérer : les éléments observables avant toute interprétation.

COMMENCE ICI

Écris de mémoire deux réflexes que tu appliques avant d'ouvrir un lien reçu par message. Puis compare avec ton voisin sans modifier ta première réponse.

ACTIVITÉ 1 — Lire un message suspect avant d’agir — 2 h

Lis la pièce A complète dans le dossier de ressources : adresse réelle facturation@support-exemple.invalid ; objet « Action immédiate — facture bloquée » ; urgence 30 minutes ; bouton « Consulter ma facture » ; destination https://factures-support.invalid/connexion ; aucune pièce jointe. Le domaine habituel fourni pour comparaison est factures.exemple.invalid. Compare ensuite avec la pièce B et complète la feuille de réponse S1.

Lire le message avant de décider

PIÈCE A • message reconstitué, pas une capture de messagerie réelle

Message reçu

1 Service facturation

facturation@support-exemple.invalid

2 Action immédiate — facture bloquée

Votre règlement a échoué. Connectez-vous dans les 30 minutes pour éviter la suspension.

Consulter ma facture

3 Destination affichée au survol :

https://factures-support.invalid/connexion

Pièce jointe : aucune

1 Adresse réelle
≠ nom affiché

2 Demande
et délai

3 Destination
du bouton

À comparer au domaine habituel : factures.exemple.invalid

Regarde les repères 1 à 3 : recopie les faits avant de proposer une explication. Les adresses sont fictives ; ne les ouvre pas.

1. Sans cliquer, relève quatre éléments vérifiables : expéditeur réel, objet, niveau d’urgence, domaine du lien ou nom de pièce jointe.

2. Pour chaque élément, écris : FAIT OBSERVÉ → CE QUE J’EN DÉDUIS → CE QUE JE FAIS.

Réponse : _____

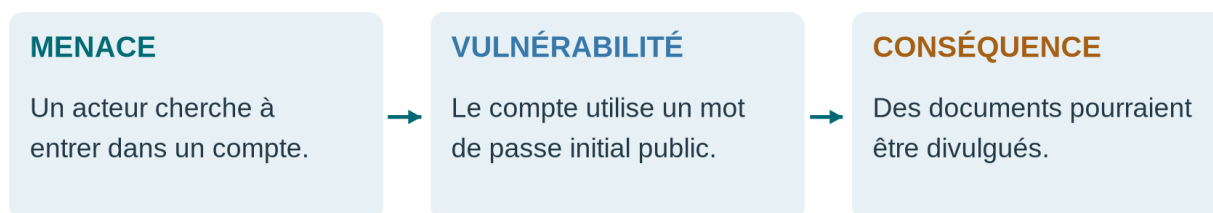
3. Avant la mise en commun, formule une hypothèse : qu’est-ce qui pourrait provoquer un dommage, quelle faiblesse serait exploitée et quelle conséquence pourrait en découler ?

4. Qui pourrait t’aider à vérifier ou traiter la situation ? Choisis un interlocuteur et justifie ton choix.

ACTIVITÉ 2 — Mettre les bons mots sur le bon problème — 1 h

Menace, faiblesse et conséquence : trois rôles différents

Exemple de compréhension • pas la correction des situations à classer



RISQUE = un scénario possible, pas le dommage seul

On considère ce qui pourrait se produire, sa vraisemblance et sa gravité.

Repère le rôle de chaque élément avant de choisir une protection.

Regarde les trois rôles dans cet exemple. Le risque décrit un scénario possible ; il ne se réduit pas à la conséquence.

Complète avec un exemple :

- Menace = ce qui peut provoquer un dommage. Exemple : _____

- Vulnérabilité = faiblesse exploitable. Exemple : _____

- Risque = possibilité qu'une menace exploite une faiblesse et ait des conséquences. On considère leur gravité et leur vraisemblance.

Repère à retenir : ANSSI → sécurité des systèmes / recommandations ; CNIL → données personnelles / RGPD.

Mini-test : un mot de passe réutilisé est-il une menace, une vulnérabilité ou une conséquence ?

Explique : _____

ACTIVITÉ 3 — Réduire le risque sur un poste de travail — 3 h

Situation : une petite organisation utilise des comptes partagés, repousse les mises à jour et conserve une seule copie des fichiers sur un PC.

Deux facteurs : deux catégories différentes

Repère de compréhension • aucune connexion ni donnée réelle à saisir



Deux mots de passe restent deux secrets de la même catégorie.
Une demande de validation inattendue ne doit pas être approuvée.

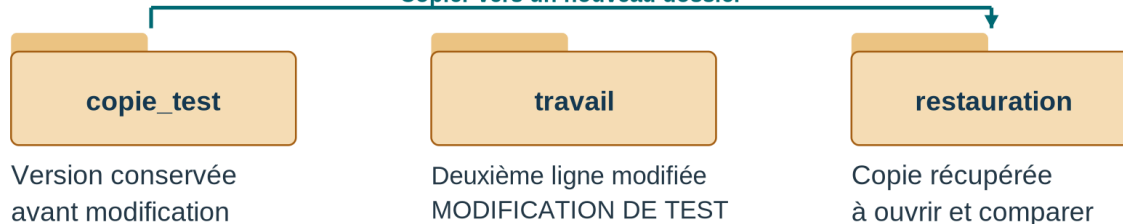
Regarde les deux catégories : la MFA associe par exemple un secret connu et un appareil possédé. Choisis ensuite des mesures qui répondent au cas.

1. Identifie trois faiblesses concrètes.
2. Propose une mesure pour chacune : MFA quand disponible, comptes nominatifs, mises à jour, sauvegardes distinctes, verrouillage, droits minimaux.
3. Priorise P1 / P2 / P3. Pour ta priorité 1, écris une justification en une phrase.
4. Vérifie ta proposition : la mesure réduit-elle bien la faiblesse repérée ?

Restaurer une copie sans écraser le travail

Manipulation de S3 • uniquement DEMO_SAUVEGARDE.txt dans le dossier d'exercice

Copier vers un nouveau dossier



Réussir une restauration ≠ résister à la perte du disque

Ici, les trois dossiers sont sur le même PC : c'est un exercice de restauration.
Une vraie sauvegarde demande une protection adaptée et des essais de récupération.

Regarde le sens de la copie : la version conservée va dans restauration, sans écraser celle de travail.

Complète le tableau S3 du dossier de ressources puis réalise l'exercice de restauration avec DEMO_SAUVEGARDE.txt, uniquement dans les dossiers d'exercice. Deux copies sur un même disque ne protègent pas de la panne de ce disque.

ACTIVITÉ 4 — Données personnelles : garder seulement ce qui est utile — 1 h

Données personnelles et secrets : ne pas confondre

Repère de S4 • catégories particulières au sens du RGPD, d'après la CNIL

DONNÉES PERSONNELLES

Elles concernent une personne identifiable.
Exemples : nom, contact, photo identifiable.

Dont les données dites « sensibles »

Exemples : santé, opinions politiques.
C'est une catégorie particulière, pas un groupe séparé.

SECRETS D'ACCÈS

Mot de passe, code
de connexion temporaire...
Ils doivent être protégés.

« Secret » ne signifie pas
automatiquement « sensible »
au sens de l'article 9 du RGPD.

Pour chaque champ : de quoi a-t-on besoin pour réaliser cette intervention ?

Le contexte compte : une donnée inutile pour une mission peut être nécessaire pour une autre.

Regarde le cadre emboîté : les données sensibles font partie des données personnelles. Un secret d'accès est une autre notion.

Lis la fiche d'intervention fictive complète de l'activité S4 dans le dossier de ressources. Utilise uniquement les champs réellement fournis dans ce cas.

1. Entoure les données personnelles ou potentiellement personnelles selon le contexte.
2. Barre toute donnée qu'un technicien ne devrait pas conserver en clair dans cette fiche.
3. Explique le principe de minimisation avec tes mots : _____
4. Qui est l'acteur institutionnel français de référence pour la protection des données ?

ACTIVITÉ 5 — Transfert : décider et expliquer — 3 h

Lis les pièces D et E du dossier de ressources : partage inattendu vers partages-verification.invalid au lieu de documents.organisation.invalid, et bannière web proposant correctif.exe. Traite les deux faits séparément : leur proximité ne prouve pas une cause commune.

Un doute ? Vérifier sans utiliser le lien reçu

Méthode de S5 • elle ne prouve pas, à elle seule, qu'un message est authentique

1 OBSERVER

Adresse réelle, destination, demande et contexte.



2 VÉRIFIER

Ouvrir le service habituel ou utiliser un contact connu.



3 DÉCIDER

Dire ce qui est établi, ce qui reste incertain.

Tant que le doute reste : pas de clic, de secret transmis ni de fichier ouvert.

Signale au responsable selon la procédure interne.

Un nom familier, HTTPS ou une bonne orthographe ne garantissent pas l'authenticité.

Regarde les trois étapes. Applique la méthode séparément à D et à E, sans affirmer que leur cause est la même.

1. Sépare les faits des hypothèses.
2. Donne les vérifications sûres à faire sans ouvrir le lien. Indique le besoin à traiter, le matériel, les logiciels ou documents utiles et la personne à contacter.
3. Décide : ouvrir / demander confirmation par un autre canal / signaler / supprimer. Justifie.
4. Rédige six recommandations maximum, classées de la plus urgente à la moins urgente.
5. Termine par : « Je ne peux pas conclure que... » puis indique la limite de ton analyse.

TU AS FINI QUAND : tes décisions citent des faits observables, aucune donnée personnelle n'a été saisie sur un service tiers, et chaque recommandation répond à un risque ou une faiblesse identifiée.

OBSERVATION / TRACE ET REPRISE

Montrer, expliquer et retenir

APPEL PROFESSEUR — OBSERVATION

Avant l'appel : ☐ j'ai cité au moins un fait précis ☐ ma mesure répond au problème identifié

Montre : ton analyse de l'activité 5, le besoin identifié, les ressources utiles et l'ordre de tes recommandations.

Explique : pourquoi ta première action réduit le risque sans créer un nouveau danger.

Élèves interrogés : chacun explique à son tour sa décision et répond à une question du professeur.

Validation professeur — le professeur coche après t'avoir observé. Une case vide signifie « non observé ». Pendant l'attente, vérifie que chaque recommandation cite un fait précis.

Critère observé / Ce que je montre	Pas encore	En cours	Avec aide	Autonome
C04 — Le besoin est identifié ainsi que les ressources matérielles, logicielles et humaines Je montre : le besoin à traiter, les outils utiles et la personne à contacter.				
C01 — L'argumentation développée lors de la présentation et de l'échange est de qualité Je montre : une décision justifiée par un fait, puis je réponds à une question.				

Après le retour du professeur, corrige puis réessaie.

À retenir

1) Fait avant hypothèse. 2) Menace ≠ vulnérabilité ≠ conséquence. 3) Vérifier sans cliquer. 4) MFA, mises à jour, sauvegardes et comptes nominatifs réduisent des risques fréquents. 5) ANSSI : sécurité des systèmes ; CNIL : données personnelles. 6) On ne collecte que les données nécessaires.

Sans regarder la fiche : cite un indice observable et la vérification sûre associée.

Ta réponse corrigée :

POUR TERMINER

Conserve le livret corrigé. Au prochain cours, le rappel se fera sans fiche à partir d'un nouveau message fictif.