

Des faits pour décider

Ressources et feuilles de réponse · activités 1 à 5 du livret

Ce dossier complète le livret de séquence. Ouvre uniquement les pages indiquées par ton professeur. Les messages, organisations et personnes utilisés dans les exercices sont inventés. Les adresses en .invalid sont des exemples : ne cherche pas à les ouvrir.

La méthode, sur un premier exemple

Fait : un message demande de communiquer un code de connexion reçu sur le téléphone.

Hypothèse : quelqu'un pourrait chercher à prendre le contrôle du compte.

Vérification sûre : contacter le support par le canal déjà connu, sans utiliser le numéro du message.

Décision : ne pas transmettre le code et prévenir le responsable interne.

Le fait décrit une information visible. L'hypothèse propose une explication : elle n'est pas encore prouvée. Une décision peut rester prudente même quand on ne connaît pas l'origine exacte du message.

Avant de commencer

Nom : _____ Groupe : _____ Date : _____

Donne un fait que tu pourrais observer dans un message, puis une hypothèse différente de ce fait.

Règle de travail

Analyse seul avant de comparer avec ton voisin. Ne transforme pas une supposition en certitude.

Quand une information manque, écris « non fourni ». Ne crée aucun compte et ne saisis aucun vrai mot de passe.

S1 • Deux messages à comparer

Pièces A et B • lire les données, pas seulement le titre

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**

Pièce A reconstituée : compare les repères 1 à 3 au contexte ci-dessous. Les adresses sont fictives ; ne les ouvre pas.

Contexte A : la facture n'a pas été demandée. Le prestataire habituel utilise **factures.exemple.invalid**. Le numéro connu du prestataire est dans le carnet de contacts de l'organisation, pas dans ce message.

PIÈCE B — MESSAGE REÇU

Nom affiché : Service facturation

Adresse réelle : facturation@factures.exemple.invalid

Objet : Facture demandée — dossier 42

Texte : La facture demandée hier est disponible dans votre espace habituel. Vous pouvez l'ouvrir depuis votre favori déjà enregistré. Aucun mot de passe n'est demandé par retour de mail.

Pièce jointe : aucune

Contexte B : le dossier 42 et la demande d'hier figurent dans le registre interne. Le responsable retrouve la même facture en ouvrant l'espace habituel depuis son favori.

Ton travail

Pour A, relève l'adresse réelle, le domaine de destination et la demande. Pour B, relève ce qui peut être recoupé par un autre canal. La bonne orthographe et HTTPS ne suffisent pas, à eux seuls, à prouver l'identité de l'expéditeur.

S1 • Analyser et vérifier

Feuille de réponse individuelle

Fait précis de la pièce A	Hypothèse possible	Vérification ou action sûre

Ma première décision pour A et ce qui la justifie :

Pourquoi B permet-il une conclusion mieux étayée ? Quelle limite reste présente ?

Réessai — une seule différence

PIÈCE C : l'adresse réelle et le domaine sont ceux d'un collègue connu, mais il demande un code de connexion temporaire et exige le secret. Il ne répond pas à ton appel sur son numéro déjà enregistré.

Un contact connu suffit-il pour envoyer le code ? Donne un fait, une hypothèse et une action sûre.

Après le retour du professeur : ma correction principale est...

S2 • Mettre les bons mots

Référence courte puis entraînement

Menace, faiblesse et conséquence : trois rôles différents

Exemple de compréhension • pas la correction des situations à classer

MENACE

Un acteur cherche à entrer dans un compte.



VULNÉRABILITÉ

Le compte utilise un mot de passe initial public.



CONSÉQUENCE

Des documents pourraient être divulgués.

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.

Repère les trois rôles dans cet exemple, puis classe les situations différentes du tableau et de l'exercice.

Mot	Sens utile pour la séquence
Menace	Ce qui peut porter atteinte au système ou aux données.
Vulnérabilité	Faiblesse qui peut être exploitée.
Conséquence	Effet possible : perte d'accès, divulgation, modification de données...
Risque	Possibilité qu'une menace exploite une faiblesse, avec des conséquences ; on considère leur gravité et leur vraisemblance.
Hameçonnage	Tentative de tromper une personne pour lui faire transmettre une information ou réaliser une action.
Rançongiciel	Logiciel malveillant qui peut bloquer l'accès aux données et exiger une rançon.

Classe puis justifie

Pour chaque situation, indique menace, vulnérabilité ou conséquence : un même mot de passe sur deux services ; une campagne de faux messages ; un fichier client divulgué ; un logiciel non mis à jour.

Qui fait quoi ?

Le responsable interne reçoit ton signalement et organise la réponse. L'ANSSI est une référence française pour la sécurité des systèmes d'information ; la CNIL pour la protection des données personnelles. Tu n'envoies pas automatiquement chaque message suspect à ces autorités.

Cas : le technicien hésite à conserver les dates de naissance de clients. Quel domaine de compétence est concerné ?

S3 • Choisir des mesures utiles

Données d'une petite organisation fictive

Constat	Contrainte connue
Un compte de messagerie est utilisé par quatre personnes.	Le service permet des comptes individuels et une MFA.
Les mises à jour du navigateur sont reportées depuis plusieurs semaines.	Une fenêtre de maintenance de 30 min est possible en fin de journée.
Les fichiers clients n'existent que sur un PC.	Un support de sauvegarde dédié et un responsable sont disponibles.
Tout le personnel dispose de droits administrateur sur le poste.	Seul le support installe les logiciels métier.

Une MFA combine des catégories différentes de facteurs : par exemple un mot de passe et une preuve de possession. Deux secrets mémorisés ne font pas deux facteurs différents. La MFA réduit certains risques, sans rendre le compte invulnérable.

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.

Deux catégories différentes sont associées. Cette illustration n'est pas un écran de connexion à utiliser.

Construis un plan, pas une liste de slogans

Faiblesse retenue	Mesure précise	Ordre / justification

Indique qui réalise la première action et comment tu vérifies son résultat :

S3 • Vérifier une sauvegarde

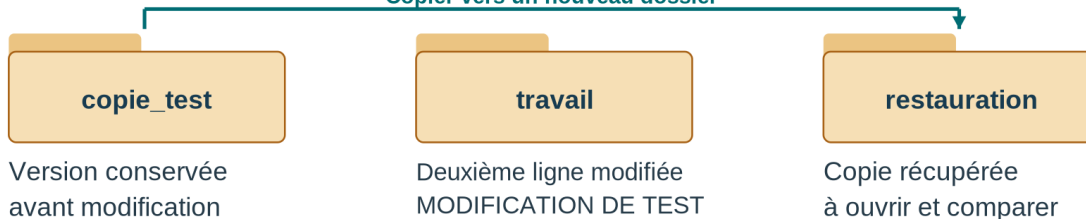
Manipulation locale sans compte et sans donnée réelle

Travaille uniquement dans un dossier d'exercice. Le fichier DEMO_SAUEGARDE.txt du pack contient trois lignes fictives. Aucune suppression de fichier personnel ou professionnel n'est autorisée.

Restaurer une copie sans écraser le travail

Manipulation de S3 • uniquement DEMO_SAUEGARDE.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.

Les flèches montrent la récupération de la copie_test vers restauration, sans écraser le fichier de travail.

1. Copie DEMO_SAUEGARDE.txt dans deux sous-dossiers : travail et copie_test.
2. Dans travail, remplace la deuxième ligne par « MODIFICATION DE TEST », puis enregistre.
3. Sans écraser aucun fichier, copie la version de copie_test dans un troisième dossier nommé restauration.
4. Ouvre la version restaurée et compare son contenu avec la version de travail.

Contrôle	Mon observation
Le fichier restauré s'ouvre-t-il ?	
La deuxième ligne est-elle l'ancienne ou la nouvelle ?	
Que prouve cette opération ?	
De quoi ces deux dossiers sur le même PC ne protègent-ils pas ?	

Cette activité entraîne la restauration. Deux dossiers sur le même disque ne constituent pas, à eux seuls, une stratégie de sauvegarde résistante à la panne, au vol ou au chiffrement de ce disque. Une synchronisation peut aussi propager une suppression.

Tu avances vite : teste une limite

Les fichiers se synchronisent automatiquement vers un autre dossier et une suppression est reproduite. Propose un contrôle pour vérifier si une ancienne version est récupérable. Ne supprime rien : explique le test.

S4 • Garder ce qui est nécessaire

Fiche d'intervention fictive — panne d'impression

Mission : recontacter le client pour confirmer que l'impression fonctionne. Le rendez-vous a déjà eu lieu.

Fiche reçue : client A ; e-mail client-a@exemple.invalid ; téléphone ; date de naissance ; mot de passe de session ; adresse IP de l'imprimante ; résultat du test d'impression ; commentaire sur la vie privée du client.

Une donnée personnelle concerne une personne identifiée ou identifiable. Une adresse IP peut en être une selon son contexte. « Minimiser » signifie ne conserver que les données nécessaires à l'objectif annoncé, pas tout supprimer indistinctement.

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.

Les données sensibles sont une catégorie particulière des données personnelles. « Secret d'accès » désigne une autre notion.

Champ	Garder / retirer / préciser	Pourquoi ?
Moyen de recontact		
Date de naissance		
Mot de passe de session		
Adresse IP / résultat du test		
Commentaire privé		

Réécris une note d'intervention adaptée

Trois ou quatre lignes suffisent. Aucune donnée réelle, aucun secret.

Qui doit décider de la durée de conservation et des personnes autorisées à lire cette fiche ?

S5 • Un nouveau cas, sans modèle

Pièces D et E • analyse individuelle

PIÈCE D — PARTAGE INATTENDU

De : colleague@organisation.invalid

Objet : Document à approuver

Texte : Valide ce partage avant 16 h.

Destination visible : <https://partages-verification.invalid/ouvrir>

Contexte : aucun partage attendu. Le service habituel est documents.organisation.invalid. Le numéro du collègue figure dans l'annuaire interne. Aucune autre vérification n'a été faite.

PIÈCE E — MISE À JOUR

Une bannière dans une page web affirme : « Navigateur obsolète — télécharger correctif.exe ».

Le technicien n'a pas encore ouvert le menu de mise à jour du navigateur. Aucune vérification du fichier proposé n'a été réalisée.

Traite D et E séparément. La proximité dans le temps ne prouve pas une cause commune. Ne télécharge et n'ouvre rien.

Pièce	Fait observé	Vérification sûre	Décision
D			
E			

Rédige ton signalement au responsable : situation, faits, actions déjà réalisées et demande utile.

Je ne peux pas conclure que...

S5 • Réessayer et retenir

Contrôle après feedback — pas de note automatique

VARIANTE : appelé sur le numéro de l'annuaire, le collègue confirme qu'il n'a envoyé aucun document. Le service de mise à jour ouvert depuis le menu du navigateur indique qu'une mise à jour officielle est disponible.

Quelle information nouvelle change ta décision pour le partage ? Quelle procédure utilises-tu pour la mise à jour ?

Rappel sans support, à reprendre au cours suivant

Explique la différence entre fait et hypothèse. Donne une limite de la MFA et une limite de la synchronisation. Cite une donnée inutile dans la fiche d'intervention étudiée.

Préparer l'observation du professeur

Reprends la page « Montrer, expliquer et retenir » du livret. Prépare ton besoin, tes ressources et ta décision justifiée ; le professeur renseigne le tableau après t'avoir observé.

Origine des ressources

Messages, scénarios et exercices : créations pédagogiques pour ce pack, et non incidents réels. Les principes de sécurité s'appuient sur les références ci-dessous, consultées le 15/09/2026. Leur consultation en ligne n'est pas nécessaire pour faire les exercices.

CNIL — authentifier les utilisateurs : <https://www.cnil.fr/fr/securite-authentifier-les-utilisateurs>

CNIL — minimisation : <https://www.cnil.fr/fr/definition/minimisation>

Cybermalveillance.gouv.fr — reconnaître un mail de phishing :

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage>

Visuels : compositions pédagogiques originales ; messages et interfaces reconstitués. Ce ne sont ni des captures réelles ni des preuves d'essai.

CNIL — données sensibles : <https://www.cnil.fr/fr/definition/donnee-sensible>

ANSSI — gravité et vraisemblance : <https://aide.monservicesecurise.cyber.gouv.fr/fr/article/le-module-risques-comment-ca-fonctionne-ja82li/>