

Exercices Cours 1 — Méthode N2 (TCIEL)

Exercices Cours 1 — Méthode N2 (TCIEL)

Durée : 25 min | Document élève — Pas de correction dans ce document

Exercice 1 — QCM rapide (5 min)

Coche la bonne réponse.

Q1. Dans la méthode N2, quelle est l'étape qui vient AVANT toute action de containment ?

- A. Rédiger le rapport REX
- B. Construire la timeline d'incident
- C. Désactiver le compte compromis
- D. Contacter le N3

Q2. Tu bloques l'IP suspecte dans le pare-feu. Tu es à quelle étape ?

- A. Analyse
- B. Remediation
- C. Containment
- D. Clôture

Q3. Un incident implique des données personnelles d'employés. Tu dois obligatoirement :

- A. Traiter l'incident seul sans en parler
- B. Notifier la CNIL dans les 72h et escalader au N3
- C. Clôturer le ticket en priorité
- D. Désactiver tous les comptes utilisateurs

Q4. L'incident OceanBio du TP1 était de criticité :

- A. P4 — Faible (anomalie suspecte)
- B. P3 — Moyenne (tentatives non réussies)
- C. P2 — Haute (compte compromis)
- D. P1 — Critique (compromission en cours, données accessibles)

Exercice 2 — Classer dans les bonnes étapes (5 min)

Pour chaque action, indique à quelle étape de la méthode N2 elle appartient (Détection / Analyse / Containment / Remediation / Clôture).

Action	Étape
Désactiver le compte admin avec usermod -L admin	
Lire le ticket GLPI transmis par le N1	
Appliquer un patch de sécurité sur le service web	
Extraire les IOC dans auth.log avec grep	
Rédiger le rapport d'incident avec chronologie et recommandations	
Bloquer l'IP 192.168.45.128 dans le pare-feu	
Tester que le service fonctionne après la correction	
Construire la timeline des événements	

Exercice 3 — Cas court : qualifier l'incident (10 min)

Lis le scénario et réponds aux questions.

Scénario : Un technicien N1 ouvre un ticket : « Depuis hier soir, des alertes de connexion s'affichent sur le serveur de fichiers de la clinique DentaSun 974 (Saint-Denis). 50 tentatives de connexion échouées sur le compte admin_serveur. Aucune connexion réussie détectée. Le service de fichiers est toujours fonctionnel. »

Q1. Quelle est la criticité de cet incident selon la matrice ? (P1/P2/P3/P4) Justifie.

Réponse : _____

Justification : _____

Q2. Quelle est la première chose à faire en tant que N2 avant de toucher quoi que ce soit ?

Réponse : _____

Q3. Rédige une hypothèse de cause en une phrase (format : « L'hypothèse est que... »).

Réponse : _____

Q4. Cite 2 actions de containment que tu effectuerais si les tentatives continuent.

Action 1 : _____

Action 2 : _____

Exercice 4 — Rédiger une phrase d'escalade (5 min)

Rédige en 2-3 phrases le message que tu envoies au N3 pour escalader l'incident OceanBio du TP1.

Objet : _____

Corps du message :

Exercices Cours 1 — TC_CYB_04 — TCIEL — Bac Pro CIEL