

Cours 2 — Rapport REX et escalade N3 (TCIEL)

Cours 2 — Rapport REX et escalade N3 (TCIEL)

Fiche de cours — co-construite à partir du TP2 Réponse Incident. Distribuer APRÈS le TP2.

1) Ce que tu as rédigé en TP2, formalisé

En TP2, tu as complété la dernière étape de la méthode N2 : clôturer le ticket GLPI et rédiger un rapport synthétique. Ce cours formalise la structure officielle d'un **rapport REX** (Return on Experience) et les règles de communication vers le N3 et la CNIL.

2) Structure du rapport REX N2

Un rapport REX complet comporte **6 sections obligatoires**. Sans les 6, le rapport n'est pas recevable par le N3 ou un auditeur externe.

RAPPORT D'INCIDENT N2	
1. EN-TÊTE	Référence ticket, date, technicien, client
2. RÉSUMÉ	3 lignes max : quoi, quand, impact
3. TIMELINE	Chronologie horodatée des événements
4. CAUSE RACINE	Vulnérabilité identifiée (technique)
5. ACTIONS	Containment + Remediation + vérifications
6. RECOMMANDATIONS	Mesures préventives pour éviter la prochaine occurrence

Section 1 — En-tête

Informations minimales obligatoires :

Référence ticket (ex. : GLPI #4782)

Date d'ouverture et date de clôture

Technicien N2 (nom + structure)

Client concerné (entreprise, localisation)

Criticité finale (P1/P2/P3/P4)

Section 2 — Résumé exécutif

3 lignes maximum. Ce résumé est lu par des personnes qui n'ont pas le temps de lire tout le rapport. Exemple OceanBio : « *Compromission du compte SSH admin du portail web d'OceanBio (Le Port) le 08/04/2026. Accès non autorisé à des données biologiques entre 03:12 et 04:45. Containment effectué le même jour — service sécurisé. Escalade N3 en cours pour évaluation RGPD.* »

Section 3 — Timeline

La timeline construite en phase d'analyse devient la pièce centrale du rapport. Elle doit être :
 Horodatée à la seconde (ou à la minute si les logs ne donnent pas plus)
 Organisée du plus ancien au plus récent
 Chaque entrée = source + événement + criticité

Section 4 — Cause racine

Règle : une seule cause racine (pas une liste). Les autres facteurs sont des causes contributives.
 Format attendu : « La cause racine est [description technique précise]. Cette configuration permettait [mécanisme de l'attaque]. »

Exemple : « La cause racine est l'activation de l'authentification SSH par mot de passe (PasswordAuthentication yes) sans limitation de tentatives sur le compte admin. Cette configuration permettait une attaque par brute force automatisée. »

Section 5 — Actions réalisées

Lister chronologiquement toutes les actions avec :
 L'horodatage de l'action
 La commande ou procédure appliquée
 Le résultat observé

Règle : ne pas lister des actions hypothétiques. Uniquement ce qui a été fait et vérifié.

Section 6 — Recommandations

Mesures préventives concrètes, applicables, priorisées. Format recommandé :

Priorité	Recommandation	Responsable	Délai
IMMÉDIAT	Déployer l'auth SSH par clé sur tous les serveurs	Admin sys OceanBio	J+2
COURT TERME	Installer fail2ban — blocage automatique après 5 échecs SSH	N2 SecuRun	J+7
MOYEN TERME	Audit complet de la configuration SSH sur les autres serveurs	N3 + OceanBio	M+1

3) Les règles de communication N2

Vers le N3

Le message d'escalade N3 doit permettre au N3 de **prendre une décision en moins de 30 secondes**. Il contient :

La criticité et le type d'incident (1 ligne)
 La timeline synthétique (3-4 événements clés)
 Les actions déjà menées (containment + remediation si fait)
 La raison de l'escalade (ce qui dépasse le périmètre N2)

Ce que tu attends du N3 (investigation complémentaire, validation RGPD, communication client)

À ne PAS faire : envoyer un message sans timeline, sans mentionner ce que tu as déjà fait, ou sans formuler clairement ce que tu attends du N3. Un N3 qui reçoit « j'ai un problème sur OceanBio, tu peux regarder ? » doit rappeler — c'est du temps perdu.

Vers la CNIL (obligation RGPD)

Si l'incident implique des **données personnelles** (données identifiant des personnes physiques) :

Délai légal : **72 heures** à partir de la détection (article 33 RGPD)

Qui notifie : le **responsable de traitement** (OceanBio, pas SecuRun) — mais SecuRun doit alerter OceanBio sans délai

Contenu minimal : nature de la violation, catégories de données concernées, nombre de personnes affectées (estimé), conséquences probables, mesures prises

Attention : si le délai de 72h est dépassé, l'entreprise peut être sanctionnée par la CNIL (jusqu'à 4% du CA annuel mondial ou 20M€). Ce n'est pas négociable.

Vers le client

Le client (OceanBio) doit être informé :

Que l'incident a eu lieu (sans détails techniques inutiles)

Que des mesures ont été prises

De ce qu'il doit faire de son côté (changer ses mots de passe, activer MFA, etc.)

Le message client se rédige **sans jargon technique** — il s'adresse à des non-techniciens.

4) Vocabulaire N2 complémentaire

Terme	Définition
REX	Return on Experience — rapport post-incident : chronologie, causes, actions, recommandations
Cause racine	La vulnérabilité ou défaillance technique qui a rendu l'incident possible
Cause contributive	Facteur aggravant, mais pas la cause principale (ex. : mot de passe faible + cause racine : SSH mal configuré)
Notification CNIL	Obligation légale RGPD de déclarer une violation de données personnelles dans les 72h
Responsable de traitement	Entité légalement responsable du traitement des données (ici : OceanBio)
Sous-traitant	Prestataire qui traite des données pour le compte du responsable (ici : SecuRun 974)
Fail2ban	Outil Linux qui bloque automatiquement les IPs après N tentatives de connexion échouées
Authentification par clé SSH	Méthode d'authentification SSH basée sur une paire clé privée/clé publique — plus sécurisée que le mot de passe

5) Checklist avant de clôturer un ticket N2

- ☐ Timeline complète et horodatée ?
- ☐ Cause racine identifiée (une seule, précise) ?
- ☐ Containment appliqué et vérifié ?
- ☐ Remediation appliquée et testée ?
- ☐ Données personnelles impliquées → CNIL notifiée ?
- ☐ Message d'escalade N3 envoyé si nécessaire ?
- ☐ Recommandations formulées ?
- ☐ Ticket GLPI à jour avec toutes les actions tracées ?

Si une case est décochée → le ticket n'est pas clôturable.

Cours 2 — TC_CYB_04_GESTION_INCIDENTS_N2 — TCIEL — Bac Pro CIEL — La Réunion