

Cours 1 — Méthode N2 : 5 étapes, matrice de criticité, escalade (TCIEL)

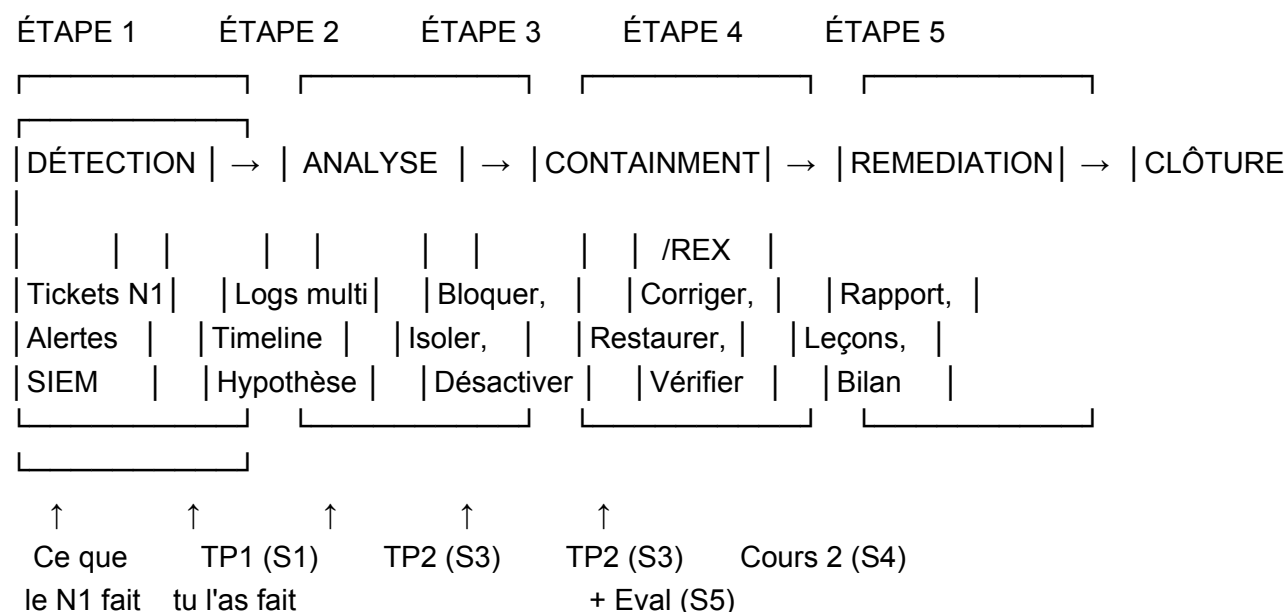
Cours 1 — Méthode N2 : 5 étapes, matrice de criticité, escalade (TCIEL)

Fiche de cours — co-construite à partir du TP1 Analyse Logs. Distribuer APRÈS le TP1.

1) Ce que tu as manipulé en TP1, formalisé

En TP1, tu as analysé 4 sources de logs pour reconstituer un incident sur le portail d'OceanBio. Sans le savoir, tu as appliqué les **3 premières étapes de la méthode N2**. Ce cours les formalise.

2) La méthode N2 en 5 étapes (ANSSI/NIST)



Étape 1 — Détection

Sources d'alerte possibles : ticket GLPI transmis par le N1, alerte SIEM/antivirus, signalement utilisateur, monitoring Zabbix/Nagios.

Ce que fait le N2 à cette étape : lire le ticket N1, qualifier l'incident (est-ce vraiment du N2 ?), ouvrir son propre ticket de suivi.

Étape 2 — Analyse

C'est ce que tu as fait en TP1. On appelle ça la **phase d'investigation** :

Identifier les sources de logs disponibles

Extraire les événements suspects (grep, journalctl, Event Viewer)

Croiser les sources par IP et par horodatage

Construire la **timeline d'incident**

Formuler une **hypothèse de cause** (ex : brute force SSH suivi d'une compromission du compte admin)

Règle d'or : on n'agit PAS avant d'avoir la timeline. Agir sans comprendre = risquer d'effacer des preuves ou d'aggraver l'incident.

Étape 3 — Containment

Objectif : **empêcher la propagation** de l'incident sans encore le corriger.

Actions typiques de containment :

Désactiver le compte compromis (usermod -L admin)

Bloquer l'IP suspecte dans le pare-feu (iptables -A INPUT -s 192.168.45.128 -j DROP)

Isoler la VM ou le service concerné du reste du réseau

Changer les mots de passe sur tous les comptes avec droits similaires

Important : le containment est temporaire. Il protège le système pendant qu'on prépare la remediation. **Ne jamais supprimer de preuves** pendant le containment (logs, captures).

Étape 4 — Remediation

Objectif : **corriger la cause** et remettre le système dans un état sain.

Actions typiques :

Appliquer le correctif (patch, mise à jour, reconfiguration)

Restaurer depuis une sauvegarde propre si le système est trop compromis

Renforcer la configuration (désactiver SSH root, activer l'authentification par clé, MFA)

Tester que le service fonctionne correctement après correction

Vérification obligatoire après remediation : tester que l'attaquant ne peut plus se connecter, que le service fonctionne pour les utilisateurs légitimes, que les logs montrent un état normal.

Étape 5 — Clôture / REX

Objectif : **documenter, fermer le ticket et apprendre**.

Rédiger le **rapport d'incident N2** (REX — Return on Experience)

Mettre à jour le ticket GLPI (N1→N2, actions, clôture)

Formuler les **recommandations de prévention** (pourquoi est-ce arrivé ? Comment éviter la prochaine fois ?)

Transmettre au N3 si l'incident dépasse le périmètre N2 (données personnelles compromises → obligation RGPD)

3) Matrice de criticité (P1 à P4)

Priorité	Criticité	Exemples	Délai d'intervention
P1	Critique	Compromission en cours, service down, exfiltration de données	< 1 heure
P2	Haute	Compte compromis, malware détecté, service dégradé	< 4 heures
P3	Moyenne	Tentatives d'intrusion répétées (pas encore réussies), vulnérabilité détectée	< 24 heures
P4	Faible	Anomalie suspecte, alerte isolée non confirmée	< 72 heures

L'incident OceanBio du TP1 = **P1** dès 02:47 (compromission réussie en cours).

4) Arbre de décision : escalader en N3 ?

Incident reçu en N2



As-tu les droits et compétences pour le traiter ? —Non—→ Escalade N3



Oui



L'incident implique-t-il des données personnelles ? —Oui—→ Notifier CNIL (72h)



Non



L'incident est-il résolu et documenté ? —Non—→ Escalade N3 si >4h P1



Oui



Clôturer le ticket, rédiger le REX

5) Vocabulaire N2

Terme	Définition
IOC	Indicator of Compromise — signe concret d'une compromission (IP suspecte, horaire anormal, commande inhabituelles)
Containment	Actions visant à stopper la propagation de l'incident sans encore le corriger
Remediation	Actions visant à corriger la cause et remettre le système dans un état sain
REX	Return on Experience — rapport d'incident post-mortem : chronologie, causes, actions, recommandations
Timeline	Chronologie horodatée des événements, pièce centrale de l'analyse N2
GLPI	Logiciel de ticketing (Gestion Libre de Parc Informatique) — outil de suivi des incidents
Escalade	Transmission de l'incident à un niveau supérieur (N3) quand le N2 ne peut pas le résoudre

Cours 1 — TC_CYB_04_GESTION_INCIDENTS_N2 — TCIEL — Bac Pro CIEL — La Réunion