

Évaluation — Gestion d'un incident N2 (TCIEL)

Évaluation — Gestion d'un incident N2 (TCIEL)

Durée : 2h | Sans VM — Documents de cours autorisés

Compétences évaluées :

C01 / C04 : analyse de la situation, prise en compte du besoin et communication de l'incident

C10 : exploitation des traces réseau et des logs

Informations élève : Nom _____ Prénom _____ Date
_____/_____/2026 Classe TCIEL

Consignes :

Lis l'intégralité du sujet avant de commencer. Les extraits de logs sont fournis en annexe (pages 3 et 4). Tu peux utiliser ta fiche de cours et tes notes de TP. Tu ne peux pas utiliser Internet ni communiquer avec tes camarades. Chaque réponse doit être justifiée sauf mention contraire.

Contexte professionnel

CyberPéi Solutions est un prestataire en cybersécurité basé à Saint-Denis (La Réunion, 12 techniciens). L'entreprise assure la sécurité informatique de **RunFroid 974**, une société de logistique frigorifique (Le Port, 67 salariés) qui gère la chaîne du froid pour des clients de la grande distribution réunionnaise.

RunFroid 974 exploite un **portail de suivi des livraisons** accessible en interne et depuis quelques postes autorisés à distance. Ce portail stocke les plannings de livraison, les coordonnées GPS des chauffeurs, les listes clients et les relevés de température des camions réfrigérés.

Ce matin, le responsable informatique de RunFroid 974 a constaté des anomalies dans les logs et a ouvert un ticket GLPI chez CyberPéi Solutions : « *Accès inhabituels sur le portail de suivi depuis hier soir. Des fichiers ont peut-être été téléchargés. Je ne sais pas depuis où ni par qui.* »

En tant que **technicien N2 chez CyberPéi Solutions**, tu prends en charge le ticket.

Extraits de logs fournis

(Voir annexe — pages 3 et 4)

Les fichiers fournis sont :

access.log — journal du portail web RunFroid (port 8080)

auth.log — journal d'authentification du portail

firewall.log — journal du pare-feu périmétrique

Questions

Partie A — Réception et qualification de l'incident

A1. En lisant le ticket GLPI, quelles sont les 3 premières informations que tu cherches à clarifier avant de consulter les logs ?

1. _____

2. _____
3. _____

A2. Après analyse des logs (annexe), qualifie l'incident selon la matrice de criticité P1-P4. Justifie ta réponse en citant au moins 2 éléments concrets tirés des logs.

Criticité : _____

Justification :

Partie B — Analyse des logs et construction de la timeline

B1. À partir des extraits de logs (annexe), identifie les 3 IOC (Indicators of Compromise) les plus significatifs. Pour chaque IOC, précise dans quel fichier log tu l'as trouvé.

IOC	Source (fichier log)

B2. Construis la timeline de l'incident. Tu dois avoir **au minimum 5 événements**, horodatés, avec source et criticité.

Date/Heure	Source	Événement	Criticité
			● Critique / ● Suspect / ● Normal

Partie C — Containment et remediation

C1. Propose 2 actions de containment immédiates à appliquer sur le système de RunFroid 974. Pour chaque action, précise la commande ou procédure et ce qu'elle permet d'obtenir.

Action 1 :

Commande/procédure : _____

Ce qu'elle permet : _____

Action 2 :

Commande/procédure : _____

Ce qu'elle permet : _____

C2. Identifie la cause racine de l'incident (une seule, précise). Justifie.

Cause racine : _____

Justification : _____

C3. Propose 2 actions de remédiation adaptées à cette cause racine. Chaque action doit corriger la cause, pas seulement limiter les effets.

Action 1 :

Action 2 :

Partie D — Communication et clôture

D1. Rédige le **résumé exécutif** du rapport REX de cet incident (3 lignes maximum). Ton résumé doit permettre à un directeur non-technicien de comprendre ce qui s'est passé, sans jargon.

D2. Analyse le point RGPD :

Des données personnelles ont-elles potentiellement été exposées lors de cet incident ? (Oui/Non)

Réponse : _____

Justifie en citant le type de données concernées :

Si oui : quelle action légale dois-tu déclencher, dans quel délai, et qui en est responsable ?

Action : _____

Délai : _____

Responsable : _____

ANNEXE — Extraits de logs

(Données fictives — à des fins pédagogiques uniquement)

Extrait 1 — auth.log (portail RunFroid 974)

2026-04-09 21:43:12 portal[2841]: Login attempt for user admin from 41.202.219.47

2026-04-09 21:43:12 portal[2841]: Login successful for user admin from 41.202.219.47

2026-04-09 21:43:15 portal[2841]: Session opened for user admin (session_id: a9f2c831)

2026-04-09 22:15:44 portal[2841]: Session closed for user admin (session_id: a9f2c831)

2026-04-10 07:02:11 portal[2841]: Login attempt for user admin from 192.168.1.10

2026-04-10 07:02:11 portal[2841]: Login successful for user admin from 192.168.1.10

Extrait 2 — access.log (portail web RunFroid, port 8080)

41.202.219.47 - admin [09/Apr/2026:21:43:15 +0400] "GET /dashboard HTTP/1.1" 200 4521
41.202.219.47 - admin [09/Apr/2026:21:44:02 +0400] "GET /clients/list HTTP/1.1" 200 28934
41.202.219.47 - admin [09/Apr/2026:21:44:18 +0400] "GET /clients/export?format=csv HTTP/1.1" 200 152348
41.202.219.47 - admin [09/Apr/2026:21:45:03 +0400] "GET /planning/livraisons HTTP/1.1" 200 9871
41.202.219.47 - admin [09/Apr/2026:21:45:31 +0400] "GET /planning/export?format=csv HTTP/1.1" 200 87421
41.202.219.47 - admin [09/Apr/2026:21:46:12 +0400] "GET /chauffeurs/positions HTTP/1.1" 200 3344
41.202.219.47 - admin [09/Apr/2026:21:47:00 +0400] "GET /admin/config HTTP/1.1" 403 512
41.202.219.47 - admin [09/Apr/2026:22:15:44 +0400] "GET /logout HTTP/1.1" 200 128
192.168.1.10 - admin [10/Apr/2026:07:02:15 +0400] "GET /dashboard HTTP/1.1" 200 4521

Extrait 3 — firewall.log (pare-feu périmétrique RunFroid)

2026-04-09 21:40:03 DENY TCP 41.202.219.47:54821 -> 192.168.10.5:22 SYN
2026-04-09 21:41:55 DENY TCP 41.202.219.47:54823 -> 192.168.10.5:3389 SYN
2026-04-09 21:43:08 ACCEPT TCP 41.202.219.47:54831 -> 192.168.10.5:8080 SYN
2026-04-09 22:15:47 DROP TCP 41.202.219.47:54999 -> 192.168.10.5:8080 FIN
2026-04-09 22:16:02 DENY TCP 41.202.219.47:55001 -> 192.168.10.5:22 SYN

Évaluation TC_CYB_04 — TCIEL — Bac Pro CIEL — La Réunion