📅 Emploi du temps prévisionnel (20 heures)

Phase 1 : Mise en place et Analyse de processus (4h)

L'objectif est de maîtriser les outils de base et de créer les premiers rapports[2].

- **Adrien :** Création des scénarios de test (boucle infinie, fuite mémoire, blocage I/O). (Correspond au point **2.1.1** [3])
- **Oscar :** Développement du script Ruby de rapport d'analyse incluant PID, nom, état, consommation et fichiers ouverts. (Correspond au point **2.1.3** [4])
- **Gabriel :** Documentation de la méthodologie de diagnostic et interprétation des états de processus (R, S, D, Z, T). (Correspond au point **2.1.2** [5])

Phase 2 : Diagnostic Réseau & Outils Avancés (5h)

Parallélisation des tâches réseau et des outils de performance système[6666].

- **Gabriel :** Simulation des problèmes réseau : service inaccessible, latence, DNS défaillant, pare-feu bloquant. (Correspond au point **2.2.1** & **2.2.2**)
- **Adrien :** Développement du script d'audit réseau automatisé pour identifier les services exposés et connexions suspectes. (Correspond au point **2.2.3** [8])
- **Oscar :** Exploration des outils avancés (iotop, sar, vmstat) et création du tableau de bord de diagnostic (format texte ou HTML). (Correspond aux points **2.4.1 & 2.4.2** [9])

Phase 3 : Investigation Forensique (5h)

Analyse méthodique des logs et investigation après incident simulé[10].

- **Gabriel & Oscar :** Mise en place de deux scénarios d'incident (ex: intrusion, saturation disque) et rédaction des rapports d'investigation. (Correspond aux points **2.3.1 & 2.3.4**

[11111111])

- **Adrien :** Développement du script d'analyse automatique de logs pour détecter des patterns suspects. (Correspond au point **2.3.4** [12])
- **Collectif :** Reconstitution de la chronologie de l'incident : quoi, quand, qui, comment. (Correspond au point **2.3.3** [13])

Phase 4 : Orchestration, Docker et Finalisation (4h)

Intégration technique et préparation des livrables finaux[14141414].

- **Adrien :** Création du Dockerfile intégrant tous les outils et rédaction de la documentation d'utilisation. (Correspond aux points **2.5.2 & 2.5.3** [15])
- **Oscar :** Développement du script Ruby "maître" orchestrant tous les scripts d'analyse développés. (Correspond au point **2.5.1** [16])
- **Gabriel :** Finalisation du dépôt Git et rédaction du guide de référence des commandes étudiées. (Correspond au point **3.1** [17171717])

Phase 5 : Préparation à la soutenance (2h)

Simulation et vérification des compétences acquises[18].

- **Collectif :** Entraînement au diagnostic en direct sur un problème préparé par l'enseignant. (Correspond au point **3.2** [19])
- **Collectif :** Revue finale de la capacité à expliquer et interpréter les sorties des commandes. (Correspond au point **3.2** [20])

Résumé de la charge de travail par personne

Nom	Focus Technique	Focus Rédactionnel
Adrien	Scénarios (2.1.1), Audit réseau (2.2.3), Analyse logs (2.3.4), Docker (2.5.2)	Documentation Docker (2.5.3)
Oscar	Script Processus (2.1.3), Dashboard (2.4.1), Orchestrateur (2.5.1)	Rapports d'incidents (2.3.4)
Gabriel	Problèmes réseau (2.2.1), Incidents (2.3.1)	Méthodologie (2.1.2), Guide (3.1)