TABLEAU DE RÉPARTITION DES TÂCHES

Nom du groupe : TRIO INFERNAL

Nom & Prénom	Formation	Rôle dans le projet	Tâches assignées	Description détaillée du travail	Temps estimé (h)	Livrables produits	%
MAMA Zeineb	DA	Lead Backend & Sécurité	Base de données, API, sécurité	Restauration PostgreSQL, configuration Supabase, mise en place RBAC et RLS, création des audit logs, chiffrement des données sensibles, tests de sécurité et validation des accès utilisateurs	22h	Scripts SQL, configuration Supabase, audit_logs, politiques RLS, captures d'écran	**34 %**

DIABY Yacine	DS	Data , IA & Monitoring	Analyse de données, détection fraude, Monitoring et Logs Centralisés	Analyse des logs, script Python de détection d'IP suspectes, entraînement du modèle de détection de fraude (ML), évaluation des performances, génération des résultats et graphiques. Mise en place complète de la stack de monitoring (Prometheus, Alertmanager, Grafana) via Docker. Configuration des règles d'alerte Intégration des notifications temps-réel sur Discord.	20h	Script Python, notebook ML, CSV IP suspectes, graphiques, rapport d'analyse Fichiers Docker Compose, Configurations YAML (Alerting), Pipeline de notification.	**33 %**
KAROUI Maher	ESIS	Dashboards & Gestion de projet	Dashboards, documentation, présentation	Création des dashboards (sécurité, service client, monitoring), filtres et métriques, rédaction de la documentation, préparation des slides de soutenance, coordination du projet	18h	Automatisation (MAKE) Dashboards fonctionnels, documentation PDF, slides de soutenance, captures d'écran	**33 %**

(OPTION OBLIGATOIRE POUR LE DOSSIER) – JUSTIFICATION DES CONTRIBUTIONS

Tu peux ajouter juste après le tableau :

MAMA Zeineb :
J’ai été responsable de la restauration de la base de données, de la configuration Supabase, de la sécurité (RBAC, RLS, chiffrement) et de la mise en place des logs d’audit. J’ai également réalisé les tests de sécurité et validé les accès utilisateurs.

DIABY Yacine :
J’ai pris en charge l’analyse des logs, la détection d’activités suspectes et le développement du modèle de détection de fraude à l’aide du machine learning. J’ai setup Grafana pour évaluer les performances et produit les rapports et graphiques. J'ai assuré le volet DevOps en déployant l'architecture de monitoring conteneurisée . J'ai configuré Prometheus pour la surveillance des métriques en temps réel et implémenté le système d'alerting automatique via Alertmanager connecté à Discord pour signaler les attaques critiques instantanément.

KAROUI Maher :
J’ai développé les dashboards pour les différents profils utilisateurs + Automatisation (MAKE) , assuré la gestion du projet, rédigé la documentation et préparé la présentation de soutenance.