Politique de sécurité : Parfait ! Avec un déploiement Jitsi pour des juristes et avocats, tu tombes pile dans le mille niveau sécurité et confidentialité. C'est exactement le type de cas d'usage qui justifie NILS1+2 et un RGPD strict.

Points clés pour ton mémoire :

Audit sécurité :

- Chiffrement bout-en-bout des communications
- Sécurisation des serveurs (pas de logs persistants)
- Isolation réseau et pare-feu
- Authentification renforcée

RGPD spécifique :

- Données sensibles (secret professionnel avocat-client)
- Durée de conservation des logs
- Droit à l'effacement
- Localisation des données (important pour les avocats)

NILS1+2 :

- Traçabilité des accès
- Intégrité des communications
- Disponibilité du service
- Gestion des identités

C'est un cas d'usage en or pour ton mémoire ! Tu as une vraie problématique métier avec des enjeux de confidentialité maximum. Les juristes sont ultra-sensibles à ces questions.

Tu as déjà identifié les principales vulnérabilités sur ton déploiement actuel ? Et comment tu comptes documenter la conformité RGPD ?

Ah parfait ! C'est beaucoup plus intéressant comme approche. Tu peux construire des scénarios de risques réalistes et proposer des solutions concrètes, sans être limité par les contraintes de l'entreprise.

Pour un déploiement Jitsi juristes/avocats, tu peux scénariser des trucs croustillants :

- **Risques RGPD** : fuites de données sensibles, logs persistants, serveurs hors UE
- **Risques sécurité** : interception communications, accès non autorisés, attaques DDoS
- **Risques métier** : perte de confidentialité avocat-client, indisponibilité pendant plaidoirie

Et pour chaque risque, tu peux proposer des solutions techniques concrètes que tu as implémentées ou testées.

C'est plus riche qu'un simple rapport de stage ! Tu peux montrer ta capacité d'analyse, ta compréhension des enjeux métier, et tes compétences techniques.

Tu as déjà identifié les principaux scénarios de risques que tu veux traiter ? Et tu comptes t'appuyer sur des référentiels spécifiques (ANSSI, ISO 27001...) ?

Excellente démarche ! Tu apportes une vraie valeur ajoutée en intégrant ANSSI, ISO27001, NIS-2 et RGPD alors que le modèle de base ne les couvrait pas.

C'est exactement ce qu'on attend d'un mémoire prospectif - pas juste suivre un template, mais identifier les manques et proposer des améliorations concrètes.

Pour un déploiement Jitsi dans le secteur juridique, ces référentiels sont effectivement cruciaux :

- **ANSSI** : guide sécurisation visioconférence
- **ISO27001** : SMSI et analyse de risques
- **NIS-2** : directive sur la sécurité des réseaux (applicable aux cabinets importants)
- **RGPD** : protection données personnelles et secret professionnel

Tu vas structurer comment l'intégration de ces référentiels dans ton analyse ? Un chapitre dédié à chaque norme ou plutôt intégrer les exigences dans chaque partie (audit, déploiement, monitoring) ?

C'est le genre d'approche qui montre que tu ne fais pas juste du copier-coller mais que tu réfléchis aux vrais enjeux du secteur.