Comment Cyber Crucible soutient-il les obligations NIS2 pour les entités essentielles et importantes ?

Réponse courte : Pour une organisation classée comme entité essentielle ou importante au titre de NIS2, Cyber Crucible soutient les mesures de gestion des risques requises — protection des postes de travail, contrôle des accès, chiffrement et gestion des incidents — et soutient les exigences de la directive en matière de sécurité de la chaîne d'approvisionnement, car il ne collecte aucune donnée client et peut fonctionner à l'intérieur du périmètre de l'entité. Cyber Crucible soutient ces obligations ; il ne les certifie ni ne les assume.

Comment il soutient les mesures NIS2

- **Mesures de gestion des risques de cybersécurité.** La prévention autonome des postes de travail, l'accès sécurisé par MFA et le chiffrement correspondent à plusieurs des mesures de référence de la directive.
- **Sécurité de la chaîne d'approvisionnement.** En tant que fournisseur qui ne collecte aucun contenu client et propose un déploiement sur site, Cyber Crucible réduit plutôt qu'il n'ajoute au risque de chaîne d'approvisionnement que NIS2 demande aux entités de gérer.
- **Soutien à la gestion et au signalement des incidents.** Un processus documenté de réponse aux violations aide l'entité à respecter les délais d'alerte précoce et de notification imposés par NIS2.

La limite honnête

Les obligations NIS2 incombent à l'entité essentielle ou importante, et non à un outil de sécurité individuel. La transposition par les États membres a varié : d'ici 2026, la plupart des États avaient transposé la directive dans leur droit national, tandis que plusieurs — dont la France, l'Irlande, les Pays-Bas et l'Espagne — étaient encore en train de la finaliser. Cyber Crucible ne détient aucune « certification » NIS2 ; il fournit des éléments de preuve à l'appui des contrôles sous accord de confidentialité (NDA).

Revision #1
Created 2026-07-24 07:20:02 UTC by Dennis Underwood

Updated 2026-07-24 07:20:02 UTC by Dennis Underwood