Description du type d'audit

L'activité réalisée était de type Test d'intrusion web.

Un test d'intrusion web a pour objectif de vérifier la perméabilité d'un site internet à des attaques venant de l'extérieur ou d'utilisateurs malveillants. Pour cela, tous les points d'accès publics sont testés afin de vérifier leur comportement face à des requêtes malveillantes. Le cloisonnement entre utilisateurs est aussi testé si nécessaire afin de vérifier la bonne ségrégation entre eux.

Il a été décomposé en plusieurs scénarios d'attaque :

- Boîte noire
- Boîte grise avec des comptes ayant les profils suivants "collaborateur", "manager" et "administrateur"

Périmètre

Le périmètre de l'audit couvrait l'application SIRH proposée par Eurécia déployée sur :

- https://pentest.eurecia.dev

Le test d'intrusion a eu lieu du 30/06/2025 au 11/07/2025 et son contre audit du 04/11/2025 au 07/11/2025.

La version auditée lors du contre audit était la version 11.154.0-SNAPSHOT.

Évaluation globale du niveau de sécurité

CYBLEX Consulting évalue le niveau globale de sécurité selon l'échelle ci-dessous :

> **FAIBLE** : L'audit a relevé des faiblesses critiques qui permettent à un acteur malveillant de prendre le contrôle de tout le périmètre ou d'équipements critiques, d'accéder à des informations sensibles ayant un fort impact métier ou de mettre à mal durablement la continuité du service.
>
> **MOYEN** : L'audit a relevé des faiblesses pouvant avoir un impact limité sur le fonctionnement de tout ou partie du périmètre audité. Un acteur malveillant peut accéder à certaines données non sensées être accessibles avec son niveau de privilèges. L'exposition trop importante de certains services augmente significativement la surface d'attaque et les risques associés.
>
> **SATISFAISANT** : L'audit a relevé des déviations par rapport aux bonnes pratiques de sécurité. Les vulnérabilités découvertes peuvent donner accès à des informations mais celles-ci ont un impact métier faible. L'accès aux services n'est pas mis en danger, ou alors de manière très limitée.
>
> **ÉLEVÉ** : L'audit n'a relevé aucune vulnérabilité exploitable. Les bonnes pratiques de sécurité sont mises en œuvre. S'il y a des déviations par rapport à celles-ci, elles sont mineures et sans impact immédiat.

Au vu de la corrections des vulnérabilités identifiées, CYBLEX Consulting évalue le niveau de sécurité général à :

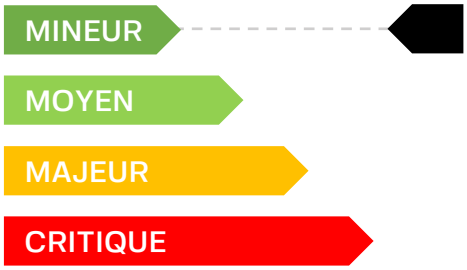
Niveau de sécurité estimé

Évaluation globale du niveau de risque

CYBLEX Consulting évalue le niveau globale du risque selon l'échelle ci-dessous :

> **MINEUR**: Le risque d'exploitation sur le système d'information est faible. Aucune action importante n'est à prévoir.
>
> **MOYEN :** Le risque d'exploitation sur le système d'information est modéré. L'audit a relevé des déviations par rapport aux bonnes pratiques de sécurité. Les vulnérabilités découvertes peuvent directement impacter les utilisateurs de l'application. Des actions préventives pour réduire les vulnérabilités et éviter une escalade sont à prévoir.
>
> **MAJEUR** : L'audit a relevé des faiblesses pouvant causer des dommages importants. Bien que ces problèmes n'entraînent pas de compromission immédiate du système, des impacts métiers importants peuvent avoir lieu. Des correctifs doit être planifier rapidement afin de planifier des correctifs.
>
> **CRITIQUE**: L'audit a relevé des faiblesses critiques pouvant entraîner des impacts majeures sur l'application ou une compromission totale du système. Des actions urgentes sont à prévoir afin de remédier aux problèmes identifiés.

Au vu de la corrections des vulnérabilités identifiées, CYBLEX Consulting évalue le niveau global du risque à :



Niveau global du risque

CYBLEX Consulting
Nom du responsable :
Christophe Vendran
Fonction du responsable :
Directeur Général
Signature :
Christophe VENDRAN Certifié par yousign