INTRA

INTER

CYBERSÉCURITÉ POUR LES DISPOSITIFS MÉDICAUX : CONTEXTE NORMATIF, FOCUS SUR LA NORME IEC 81001-5-1

OBJECTIFS

Comprendre les principales règlementations et normes applicables à la cybersécurité des dispositifs Médicaux.
Mesurer l'impact des directives et comprendre les activités les plus importantes à mettre en place dans votre organisation.
Acquérir une compréhension détaillée de la norme 81001-5-1 et son articulation avec la norme IEC 62304.

MOYENS PÉDAGOGIQUES

Projection du cours, support de cours papier et clés USB
Chaque point de la formation sera illustré par des exemples concrets afin que les participants puisse s'approprier le sujet.

MÉTHODES UTILISÉES

La progression pédagogique du participant est évaluée tout au long de la formation au moyen de QCM.

PUBLIC

> RSSI, responsable qualité ou réglementaires, dirigeant de société développant des dispositifs médicaux. Ingénieurs et techniciens d'études

PRIX HT
1 300 € par personne

DATES
13 mai 2026

DURÉE
1 jour (7 heures)

LIEU
LCIE

INTERVENANT
Expert en cybersécurité des dispositifs médicaux

PRÉ-REQUIS
Connaissance du cycle de développement d'un dispositif médical
Compréhension des principaux termes utilisés en cybersécurité

PARCOURS DE FORMATION

> Panorama des réglementations et normes applicables :

- Guidances FDA sur la cybersécurité
- Guidance MDR sur la cybersécurité (MDCG)
- Normes applicables : UL 2900-2-1, AAMI TIR 57, IEC 81001-5-1

> Les Piliers de la cybersécurité pour les dispositifs médicaux

- L'analyse de risque cybersécurité : modèle des menaces, méthode STRIDE, la cotation des risques avec les CVSS, les contremesures (contrôles de sécurité), les documents attendus, lien avec l'analyse de risque de sécurité
- Les tests de pénétration : scan de vulnérabilités, tests de fuzzing, test de pénétration structuré, analyse du Code source & binaire, rapport de test de pénétration, correction et lien avec l'analyse de risque

> Focus sur la norme 81001-5-1

- Intégration dans le process de développement et lien avec l'IEC 62304
- Exigences générales
- Description du produit d'un point de vue cybersécurité
- Exigences pour les phases de spécification, design et implantation
- Suivi et traçabilité des problèmes de cybersécurité
- Les différents tests de cybersécurité à effectuer
- Gestion de vulnérabilité et mise à jour logicielles
- Gestion des incidents
- Documentation cybersécurité pour les utilisateurs