Cybersec & Safety Partners

CYBERSECURITE DES DISPOSITIFS MEDICAUX IEC 81001-5-1

Réalisable en présentiel ou à distance (FOAD)

Type	Référence	Durée	Tarif HT
INTER	1.01.04.0018	1 jour (7 h)	960 €
INTRA	2.01.04.0019	1 jour (7 h)	1980 €*

* forfait pour 6 pers max

DESCRIPTIF DE LA FORMATION

Cette formation est une introduction à la démarche de cybersécurité appliquée aux dispositifs médicaux, décrivant les processus du cycle de vie du dispositif médical et de son logiciel et les méthodologies utilisables pour répondre aux exigences règlementaires et normatives relatives à la gestion des risques de cybersécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de la formation, l'apprenant sera capable de :

- Situer la cybersécurité dans l'écosystème médical et appréhender les exigences règlementaires en la matière
- Conduire l'appréciation des risques de cybersécurité
- Mettre en œuvre les exigences de la norme IEC 81001-5-1
- Planifier le détail des actions à mener et des vérifications à effectuer pour chaque partie du cycle de vie du DM
- Sélectionner les outils requis pour mener des audits de code
- Planifier la réponse à un incident de cybersécurité

PROGRAMME

- **Introduction – rappel des concepts de base**
- **Contexte règlementaire et normatif de la cybersécurité des DM**
  Règlements UE et US, principes et démarche
  Panorama des normes applicables
- **Exigences de l'IEC 62304 et de l'IEC 60601-1**
- **Présentation de la norme IEC 81001-5-1**
  Processus et activités requis
- **Présentation des normes IEC 62443 & 60601-4-5**
  Définition des niveaux de sureté et des exigences fondamentales
  Détermination des capacités de sureté : IEC 62443-4-2
  Application aux SEMP : IEC 60601-4-5
- **Normes collatérales applicables aux DM connectés**
  IEC 80001-1 et rapports techniques associés
- **Gestion des risques de sureté**
  Appréciation des risques / ISO 14971
  Modélisation des menaces (*Threat Modeling*)
  Evaluation des vulnérabilités / standard CVSS
- **Processus de développement sécurisé**
  Standard de conception sécurisée (*Secure by design*)
  Utilisation de logiciels tierce-partie (SOUP, OTS)
- **Outils d'audit de cybersécurité des logiciels**
- **Réponse aux évènements de cybersécurité**
- **Questions et conclusion**

INFORMATIONS UTILES

Public concerné
Ce stage s'adresse aux chef de projet ou de produits, développeurs logiciels, architectes système, responsables cybersécurité, auditeurs internes, responsables des règlements et affaires médicales.

Prérequis
Principes généraux d'ingénierie système et logiciel ; la connaissance du système de gestion de l'assurance qualité (ISO 13845) et des principes de base de la gestion des risques est souhaitable.

Moyens pédagogiques, techniques et d'encadrement
Un support de cours numérique est remis à chaque apprenant. Le déroulé pédagogique de la session liste les méthodes retenues.

Modalités de suivi du stagiaire
Questionnaire d'entrée, quiz en cours de formation, questionnaire de sortie et questionnaire de satisfaction sont les outils de suivi mis en œuvre.

Conditions d'accès
Groupe constitué en fonction de la demande, au moins 4 semaines avant le début de la session.

Accueil situation de handicap
Notre offre de formation est accessible à tous. En cas de situation de handicap nécessitant un aménagement particulier, vous pouvez joindre notre **Correspondant Handicap** au :
Tél : 05 61 30 69 00 Email : formation@isit.fr

Plusieurs formats de formations possibles, veuillez nous contacter.