NORD-PAS DE CALAIS
Axe : n/c

Cybersécurité : mise en situation d'une cyberattaque (génie biomédical)- Déméter Santé

Contexte

L’écosystème du secteur de la santé évolue considérablement avec le développement de nouveaux outils numériques, leur lot d’avantages et de risques numériques. Ces risques numériques ne sont plus aujourd’hui à prendre à la légère, s’il y a 10 ans une panne informatique pouvait engendrer des désagréments passagers, elle peut aujourd'hui mettre à l’arrêt des services complets et impacter la continuité des soins. Les services Biomédicaux gèrent une grande quantité de données confidentielles ainsi que des équipements et des services indispensables à la continuité des soins. A ce titre la protection des données, la réactivité et la reprise sur incident sont des critères qui doivent sans cesse être challengés et améliorés. La réalité d’une cyberattaque impose des évolutions dans les pratiques.

Objectifs

- **Comprendre** à quoi sert la SSI dans un établissement de santé"
- **Comprendre** les interactions entre le service biomédical et le service sécurité informatique"
- **Connaître** le risque de piratage des appareils médicaux"
- **Communiquer** efficacement avec le SSI"
- **Savoir être** vigilant lors de la maintenance des appareils médicaux
- **Définir** un protocole de mise au rebus des disques durs contenant des données de santé"
- **Etablir** des protocoles d’action en cas de cyberattaque.

Renseignements complémentaires

Financement

Fonds mutualisés ANFH (dans la limite des fonds disponibles)

Dates

Voir calendrier en annexe

Validité du marché

2026

Programme

Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service :

- Quelle est aujourd'hui l'état de la menace cyber ?
- Les principes de base de la SSI
- L'intégration des personnels biomédicaux dans la SSI

Comprendre les interactions entre le service biomédical et le service sécurité informatique :

- Vulnérabilité des appareils connectés
- Les bonnes pratiques pour la connexion

Connaître le risque de piratage des appareils médicaux

- Les attaques sur les appareils médicaux
- Savoir évaluer les risques pour un appareil ou une situation donnée

Communiquer efficacement avec le SSI :

- Communiquer avec la SSI pour maintenir la sécurité
- Quelle communication en période de crise
- Communiquer sur les évolutions des matériels et les remontées utilisateurs
- Bien communiquer la méthode CNV
- Debriefing sur les résultats de la simulation et synthèse des différent éléments

Savoir être vigilant lors de la maintenance des appareils médicaux :

- Les étapes de la maintenance
- Effacer et mettre au rebut un disque dur de manière sécurisé

Etablir des protocoles d'action en cas de cyberattaque

- Quels environnements techniques pour quel type de menaces
- Co-Construction d'un protocole d'action contre les menaces vues ci-dessus
- Mise en commun des plans d'actions et réflexion autour de leur construction et fonctionnement
- Mise en application d'un plan d'action sur équipement réel, si disponibilité, accord et validation de l'équipe SSI de l'établissement. Sinon mise en situation sur un scénario fournis par le formateur
- Debriefing sur le plan d'action avec la SSI et le formateur si simulation sur équipement réel

Public
Tout agent de la FPH travaillant aux services Biomédicaux

Exercice
2024

Code de formation
AFR 5.06

Nature
AFR

Organisé par
Déméter Santé

Durée
7 heures