

Formation-action : mise en situation cyberattaque (génie biomédical)

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.

PUBLIC VISÉ :

➤ Tout agent de la FPH travaillant aux services Biomédicaux

ORGANISÉ PAR :

➤ Déméter Santé

NOMBRE DE PARTICIPANTS :

➤ 8 à 16 participants

DURÉE :

➤ 1 jour

PRÉREQUIS :

➤ Aucun

CONTACT :

➤ contact@demeter-sante.fr
06-98-28-88-59

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 rebut des disques durs contenant des données de santé"

➤ "Etablir des protocoles d'action en cas de cyberattaque. "

MODALITÉS PÉDAGOGIQUES

➤ Expression guidée par questionnement.

➤ Travail en sous groupes

➤ Apports didactiques et conceptuels.

➤ Echanges

➤ Etude de cas, analyse de situations

➤ Démonstration, exercices

➤ Analyse, démarche réflexive autour du vécu et des situations de travail

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

- Des appareils connectés et donc vulnérables.
- Les bonnes pratiques pour la connexion d'équipement de santé.

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
- Mise en situation au travers d'un cas pratique
- Debriefing sur les résultats de la simulation et synthèse des différents 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 sécurisée

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 équipements réel.