Formation DPC

Comment prévenir, détecter et réagir à une cyberattaque au sein d'une structure de soins ?

Séquence de formation

Modalité : Séance de simulation

Durée : Trois heures

Objectif : A l'issue de cette formation, le professionnel sera capable de :

Identifier et corriger les vulnérabilités, notamment humaines, de son environnement numérique de travail, afin de prévenir les cyberattaques et réagir efficacement en cas d'incident de cybersécurité lors d'une situation d'urgence clinique.

Objectifs généraux et sous-objectifs spécifiques :

- Accompagner le professionnel de santé dans la compréhension des enjeux de la cybersécurité
  - ⇨ Définir et expliquer les fondamentaux ainsi que les enjeux de la cybersécurité
  - ⇨ Identifier les vulnérabilités, notamment humaines, susceptibles d'être exploitées par un cyberattaquant
  - ⇨ Connaitre les bonnes pratiques pour sécuriser son environnement numérique de travail et protéger les données personnelles conformément au RGPD

- Développer une posture professionnelle critique et responsable face aux outils numériques
  - ⇨ Exercer un esprit critique face aux outils et aux données numériques
  - ⇨ Faire preuve de calme et de lucidité face à une situation numérique ambiguë ou à risque

- ⇨ Réagir de manière adéquate, en mobilisant ses compétences professionnelles, face à des données faussées ou altérées

➢ Réagir de manière appropriée en cas d'incident de cybersécurité entraînant une perte de données
- ⇨ Rester informé et vigilant face aux cybermenaces
- ⇨ Mobiliser ses compétences pour assurer la continuité des soins en mode dégradé
- ⇨ Informer et alerter les bons interlocuteurs, et comprendre les étapes clés de la procédure

- **1. Introduction (10 minutes)**

○ **Animateur** : Présentation individuelle et tour de table pour connaitre les participants ainsi que leurs attentes. Ensuite, annonce claire des objectifs pédagogiques de la séance de simulation.

○ **Support** : Ruban pédagogique de la formation présentant de manière détaillée les objectifs d'apprentissage et le déroulement de la séance, structurée en trois scénarios.

- **2. Scénario 1 : Comprendre la cybersécurité et adopter les bonnes pratiques (45 minutes)**

○ **Objectifs** : Définir et expliquer les fondamentaux ainsi que les enjeux de la cybersécurité
Identifier les vulnérabilités humaines exploitables lors par un cyberattaquant
Connaitre les bonnes pratiques pour sécuriser son environnement numérique

○ **Déroulé** :

❖ Briefing – situation immersive de cybersécurité (10 minutes) :
- ▪ Présentation du cadre et des objectifs de la séance
- ▪ Explication du déroulé et des attendus du premier atelier
- ▪ Présentation de l'environnement et de ce que les apprenants vont y rencontrer
- ▪ Rappel des règles de confidentialité et du cadre bienveillant de la simulation

▪ Situation active (10 minutes) :

La mise en situation se déroulera avec **trois groupes de quatre apprenants**, chaque groupe installé dans **une salle de consultation** reconstituée de manière réaliste.

Les apprenants y retrouveront les éléments habituels d'un environnement de soins : un poste informatique mobile (Ergotron), des éléments d'identification professionnelle, ainsi que divers dispositifs numériques périphériques connectés, etc.

Leur rôle sera d'**observer** attentivement cet espace, avec une posture critique, afin d'**identifier** les éléments pouvant représenter une faille de sécurité ou être exploités par une personne malveillante : dispositifs mal sécurisés, informations sensibles exposées, etc.

Chaque groupe consignera ses observations et les éléments problématiques identifiés sur une feuille dédiée, pour préparer le temps de restitution collective.

- ❖ Débriefing – restitution collective (25 minutes)
  - Temps d'apprentissage et de réflexion autour du premier scénario
  - Phase réaction/descriptive : questions ouvertes pour engager la réflexion, avec un retour de chaque groupe sur leurs observations.
  - Phase d'analyse : identification et mise en lumière des éléments problématiques et des failles relevées. Compréhension des risques encourus et discussion sur ce qui aurait pu être évité.

  Cette phase conduit à l'exploration des bonnes pratiques de cybersécurité essentielles pour les professionnels.

  - Phase de synthèse : réflexion collective et synthèse du debrief : éléments à corriger, à éviter dans son propre travail : bonnes pratiques numériques c'est l'affaire de tous !

- **3. Scénario 2 : Développer une posture professionnelle et réagir de manière coordonnée et efficace face aux incertitudes des données numériques (1 heure)**

- **Objectifs** : Exercer un esprit critique face aux outils et aux données numériques
  Faire preuve de calme, lucidité face à une situation numérique ambiguë ou à risque
  Réagir de manière professionnelle, face à des données faussées ou altérées

- **Déroulé** :

  - ❖ Briefing – situation immersive de cyberattaque, données altérées (15 minutes) :
    - Présentation du cadre et des objectifs pédagogiques du scénario
    - Explication claire du scénario, des rôles de chacun et de la durée prévue.
    - Explication du contexte de la situation simulée, ainsi que les attendus vis-à-vis des apprenants
    - Présentation de l'environnement, de la situation, du matériel mis à disposition (notamment le mannequin de simulation), ainsi que des possibilités d'action durant les scénarios
    - Rappel des règles de confidentialité et du cadre bienveillant et sans jugement propre à la simulation, essentiel dans un contexte potentiellement plus stressant que le scénario précédent

    - Situation active (15 minutes) :

  La mise en situation se déroulera en **deux groupes**, un premier groupe sera en action **au bloc opératoire**, intervenant auprès d'un patient simulé (mannequin de haute technicité). Le second groupe **observera** la séance de simulation à distance, grâce à une projection en salle de débriefing.

  Ils seront immergés au sein d'une unité de soins intensifs en cardiologie, équipée de dispositifs de surveillance connectés. Une patiente, présentant un infarctus du

myocarde et sous monitoring, déclenche soudainement **plusieurs alertes** sur différents paramètres vitaux.

Les apprenants devront **évaluer la situation** et **réagir de manière appropriée** face à ces données qui semblent incohérentes et qui affluent.

Le groupe observateur, quant à lui, prendra des notes et analysera les comportements et pratiques numériques du premier groupe, en vue d'une restitution collective.

- ❖ Échange collectif – debriefing (30 minutes)
  - Retour et partage des ressentis liés à cette situation d'urgence (phase descriptive, analyse et synthèse), ainsi que des questions ou points soulevés par les participants.
  - Bref brief du scénario 3 : même patient, suite de la simulation, avec un focus sur les prochaines difficultés sur lesquelles être vigilant.

- **4. Scénario 3 : Adopter une réponse adaptée face à un incident de cybersécurité causant une perte de données (1 heure)**

- **Objectifs** : Rester informé et vigilant face aux cybermenaces
  Mobiliser ses compétences pour assurer la continuité des soins en mode dégradé
  Alerter les bons interlocuteurs, et comprendre les étapes clés de la procédure

- **Déroulé** :
  - ❖ Briefing (15 minutes)
    - Présentation du cadre et des objectifs pédagogiques du scénario
    - Explication claire du scénario, des rôles de chacun et de la durée prévue.
    - Rappel du contexte : rappel de la situation ayant précédé la prise en charge simulée
    - Rappel de l'environnement, des règles à suivre et du matériel disponible

    - Situation active (15 minutes) :

La mise en situation se déroulera à nouveau en deux groupes, avec inversion des rôles : le groupe observateur du scénario 2 deviendra participant actif, et inversement.

Cette troisième et dernière simulation se déroule toujours au bloc opératoire, avec le même mannequin et dans le même contexte.

Cette fois-ci, les données numériques seront totalement absentes : tous les dispositifs seront éteints ou coupés, aucune information digitale ne sera disponible.

Les apprenants devront donc s'appuyer uniquement sur leurs compétences cliniques, prendre les bonnes décisions et adopter les réflexes adéquats.

Le groupe observateur, quant à lui, prendra des notes et analysera les comportements et du premier groupe, en vue d'une restitution collective.

- ❖ Debriefing – restitution collective (30 minutes)
  - Temps d'apprentissage et de réflexion autour du troisième scénario, offrant l'opportunité de revenir sur les deux derniers scénarios, plus stressants.
  - **Phase descriptive :** questions ouvertes pour engager la réflexion, avec un retour de chaque groupe sur leurs observations, mais aussi sur leur ressenti : stress éprouvé, difficultés rencontrées, interrogations soulevées.
  - **Phase d'analyse :** identification et mise en lumière des éléments problématiques, des bonnes pratiques mises en œuvre, ainsi que des axes d'amélioration. Compréhension des risques liés à la compromission, puis à la perte totale des données, et de leurs impacts sur la pratique soignante. Discussion autour de la confiance à accorder à sa pratique clinique versus aux outils numériques.
  - **Phase de synthèse :** réflexion collective et conclusion du débriefing : quelles actions concrètes adopter ? À qui faire confiance ? Comment optimiser la collaboration en équipe ? Quelles données considérer comme fiables, et lesquelles nécessitent une vigilance accrue ? Qui alerter en cas d'incident,

- **6. <u>Conclusion</u> (5 à 10 minutes)**

- **Retour sur les points clés** abordés lors de la formation (définition, scénarios, enjeux, réflexivité)
- **Questionnaire en fin de formation** afin d'évaluer le format, les notions transmises, l'intérêt suscité et la satisfaction par rapport aux attentes.